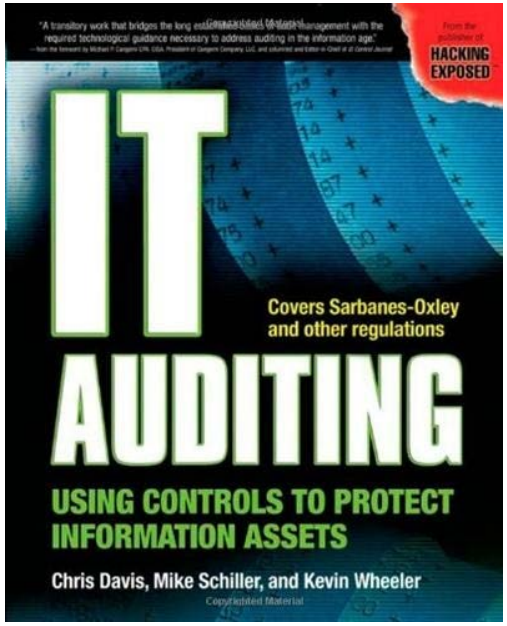
InfoDefense™
Strategic Information Security

# Auditing the Information Security Function

Kevin Wheeler, CISSP, CISA

# A Little About Me

- Over 17 Years of Information Security Experience
- Founder of InfoDefense
- Frequent Speaker at Conferences and Industry Events
- Author of *IT Auditing: Using Controls to Protect Information Assets*

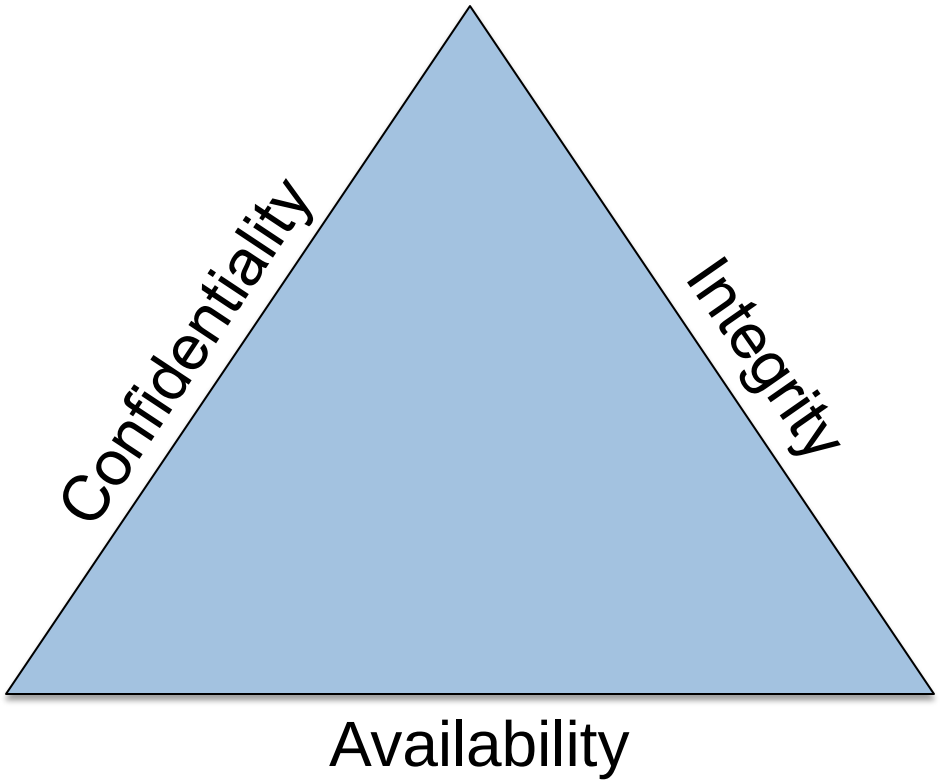


# Agenda

1. Information Security Level-set
2. Information Security Frameworks
3. Auditing Information Security Technical Controls
4. Auditing Information Security Governance
5. Information Security Maturity

# Information Security Level-Set

# Information Security Triad



# Information Security Controls

| | |
|---|---|
| **Technical** | Access Control Systems, Multi-Factor Authentication, Firewalls, Encryption Systems, Uninterruptible Power Supplies, Intrusion Detection Systems, Malware Protection Software, Redundant Systems or System Components, Back-up Systems, Audit and Logging Systems, System Hardening |
| **Physical** | Security Guard, Card-key Physical Access Control Systems, Alarm Systems, Safes, Fire Suppression Systems, HVAC Systems, Fences, Lighting, Security Cameras |
| **Administrative** | Acceptable Use Policy, Business Continuity Plan, Password Policy, Incident Response Plan, System Baseline Configurations, Remote Access Policy, File Recovery Procedures, Information Classification, Security Awareness Training, Audits and Assessments, Non-disclosure Agreements |

# Security Governance Lifecycle

# Information Security Frameworks

# Information Security Frameworks

- ISO 27001
- COBIT 5.0
- NIST 800-53
- NIST Cyber Security Framework
- PCI DSS

# PCI DSS 3.0

| PCI DSS Requirements Version 3.0 | Milestone | Status: *Please enter "yes" if fully compliant with the requirement* | If compliance status is "no", please complete the following | | | |
|---|---|---|---|---|---|---|
| | | | Recommendation | Estimated Date of Completion | Remediation Owner | Comments |
| ***Requirement 1: Install and maintain a firewall configuration to protect cardholder data*** | | | | | | |
| **1.1** Establish and implement firewall and router configuration standards that include the following: | | | | | | |
| **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations | 6 | | | | | |
| **1.1.2** Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks | 1 | | | | | |
| **1.1.3** Current diagram that shows all cardholder data flows across systems and networks. | 1 | | | | | |
| **1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the Internal network zone | 2 | | | | | |
| **1.1.5** Description of groups, roles, and responsibilities for management of network components. | 6 | | | | | |
| **1.1.6** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation for security features implemented for those protocols considered to be insecure.<br>Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2 | 2 | | | | | |
| **1.1.7** Requirement to review firewall and router rule sets at least every six months. | 6 | | | | | |
| **1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.<br><br>**Note**: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. | | | | | | |
| **1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. | 2 | | | | | |
| **1.2.2** Secure and synchronize router configuration files. | 2 | | | | | |
| **1.2.3** Install perimeter firewalls between any all wireless networks and the cardholder data environment, and configure these firewalls to deny or, control (if such traffic is necessary for business purposes), permit only authorized any traffic from between the wireless environment into and the cardholder data environment. | 2 | | | | | |
| **1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment. | | | | | | |
| **1.3.1** Implement a DMZ to limit inbound traffic to only system components that | | | | | | |

# NIST Cyber Security Framework

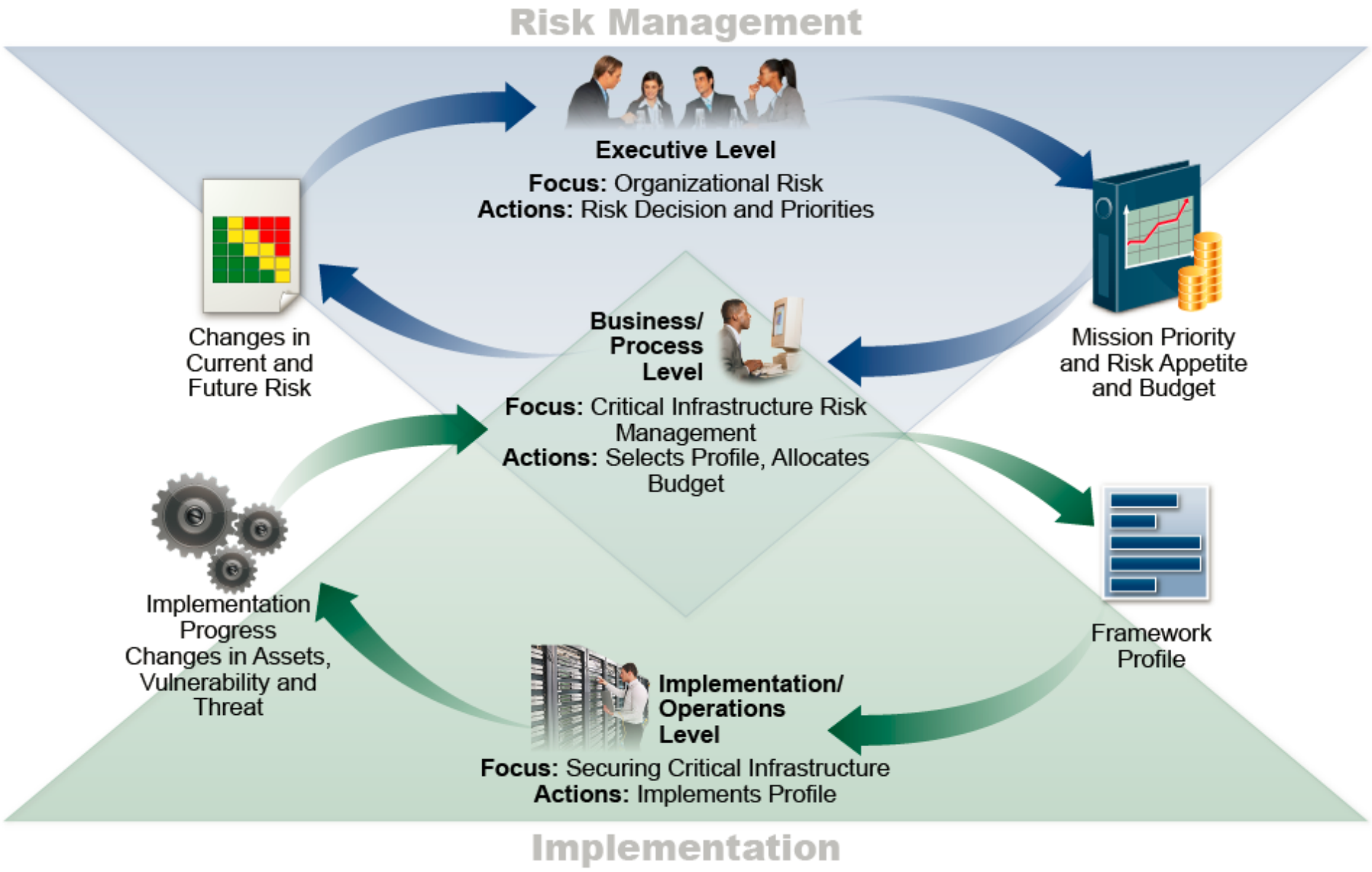
| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

# Auditing Information Security

# Information Security Program Elements

1. IT Governance, Risk and Compliance Management
   - Risk Management
   - Polices, Standards and Procedures
   - Security Architecture
2. Identity and Access Management
3. Network Security
4. System Security
5. Application Security
6. Threat and Vulnerability Management
7. Business Continuity and Disaster Recovery
8. Data Center Security

# Auditing Risk Management




**Source:** NIST Cyber Security Framework

# Risk Analysis and Management

1. Identify Information Assets
2. Quantify and Qualify Risks
3. Assess Vulnerabilities
4. Remediate Control Gaps
5. Managing Ongoing Risk

# Information Criticality Matrix

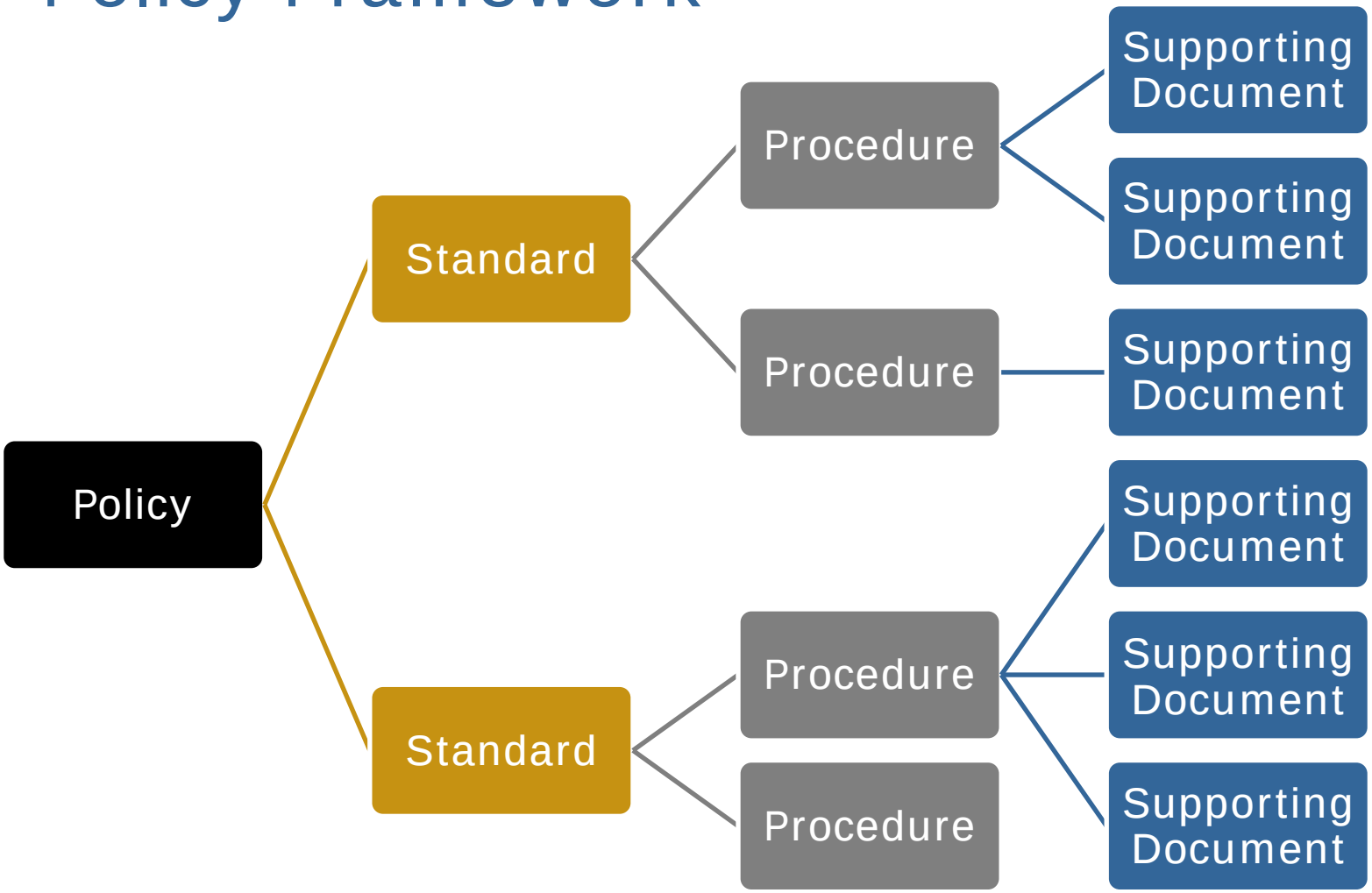
| | | | |
|---|---|---|---|
| Employee Records | H | H | M |
| Benefits Administration | M | L | M |
| Recruiting | H | H | L |

# Risk Management Audit Tips

1. Business vs. Technology Focused
2. Top Down Approach (Business Function → Process → Application)
3. Use Tools to Identify the Location of Critical Information
4. Measure Confidentiality, Integrity and Availability Risk
5. Express Risk in Business Terms

# Auditing Policies, Standards and Procedures

# IT Policy Framework



# Policies and Procedures

[Company L

| Policy Title: | Information Protection Policy | | | | |
|---|---|---|---|---|---|
| Policy Number: | ITP-01 | Version: | 0.1 | Effective Date: | mm/d |

Approved By: *(Authorized Signer Name)*

Date Approved

## Overview

### Description

This policy contains high-level information protection mandates as set forth by executive manageme
response to enterprise risk and regulatory compliance requirements. As with all corporate IT policie
standards outline the technical security requirements and procedures outline the methods used to
maintain security controls. The following policy statements are not meant to specify the methods of

### Purpose

The Information Protection Policy was set forth to protect [Company Name] from unauthorized info
disclosure and other information security risks. Many of the policy statements below have been de
response to regulatory requirements.

### Applicability

There are two audiences for policies: general users and users that perform IT functions. This policy i
users that perform IT functions.

### Sanctions for Non-compliance

This policy is compulsory. Failure to comply may result in reprimand and/or employment terminatio

## Policy Statements

### Policy

***Information will be protected in a way that reduces IT risk and complies with applicable re***

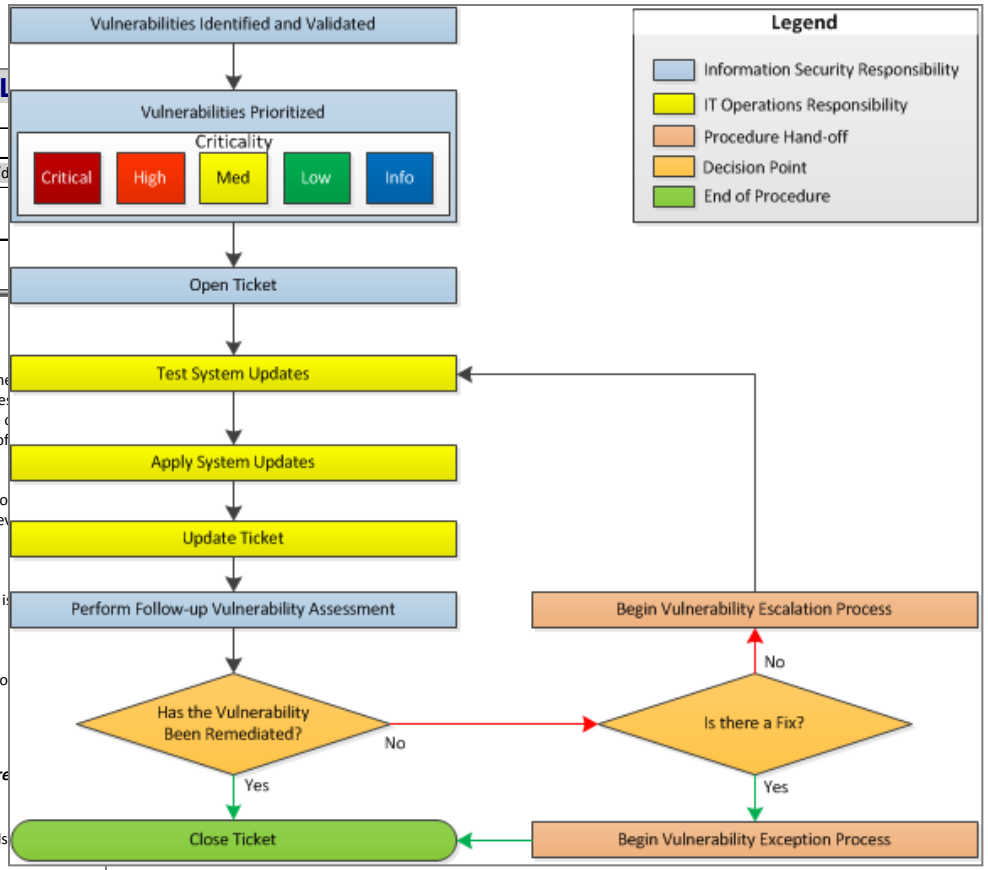
### Clarifying Policy Statements

**1)** System access must be strictly controlled. See the Access Control Standard for additional details

**2)** Sensitive information residing on enterprise systems must be protected by appropriate security controls according to its level of sensitivity. See the Systems Security Policy and Sensitive Information Protection Standard for additional information.

**3)** Private cryptographic keys must be stored and managed in a secure manner. See the Encryption Standard for more information.

**4)** New employees, contract employees and business partners that will have access to sensitive information must undergo a background check.

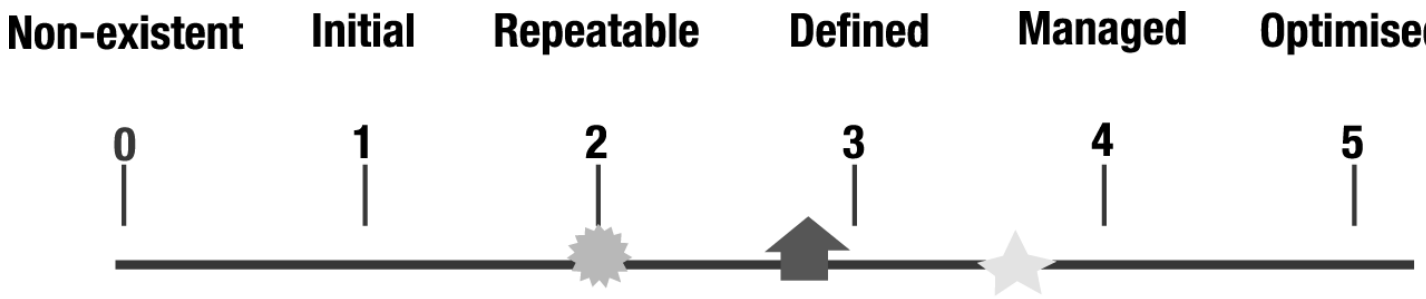


# Security Policy Audit Tips

1. Use a Standard or Framework to Ensure Proper Coverage
2. Ensure Readability and Applicability
3. Ensure that Statements are in the Proper Document Type
4. Look for References to Internal Standards
   - General
   - Technical Configuration
5. Look for Procedures that Map to Standards → Policies

# Information Security Maturity

# Security Maturity Measurement




**LEGEND FOR SYMBOLS USED**

- Enterprise current status
- Industry average
- Enterprise target

**LEGEND FOR RANKINGS USED**

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

# How Do Most Organizations Rate?

## CMM Level 2

People

- Some technical personnel trained in security
- Immature security organization (if any)
- Most employees unaware of corporate security policies

Process

- Basic processes such as change control, backup/restore, etc.
- Little or no process automation
- Immature risk and security strategy

Tools

- Firewall, Anti-virus, Spam protection and other basic security tools
- Sometimes advanced point solutions such a network IDS or multi-factor authentication
- Little or no integration of security tools
- No real-time visibility into security

# What is the Target Maturity Level?

## CMM Level 3+

People

- Subject matter experts within the security organization, other IT functions well-trained in security
- Security organization is an integral part of the business
- Employees understand and embrace security policies and information handling best practices

Process

- IT processes are well defined
- Labor intensive processes such as password resets are automated
- IT risk is actively managed using a well defined security strategy

Tools

- Security technologies are optimized and fully integrated
- Advanced security technologies are employed according to the security strategy (plan)
- Security personnel have real-time visibility into organizational security at all times enabling rapid response to incidents
- Systems are highly standardized and managed efficiently

# Security From Inhibitor to Enabler

**Security** (Yesterday)

- Lock down systems
- Keep the bad things out
- Protect only infrastructure
- Disparate and disconnected

**Security** (Today)

Protect Information and Interactions

Prioritized, Risk Based Approach

Standardize, Audit and Automate Processes

# Communicating Audit Findings

1. Express Findings in Business Terms
2. Communicate the Strengths as well as Deficiencies
3. Use Industry Standards to Back up Findings
4. Obtain Agreement from Audit Subjects

# Thank You!

Kevin Wheeler, CISSP, CISA
(972) 992-3100 Ext 101
kevin.wheeler@infodefense.com