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

Confidentiality

Availability

Integrity
## Information Security Controls

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrative</strong></td>
<td>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</td>
</tr>
</tbody>
</table>
Security Governance Lifecycle

- Risk Assessment
- Measurement and Assurance
- Security Strategy
- Security Management
- Security Policy
- Security Architecture

Governance, Risk, and Compliance

InfoDefense™
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

**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Status: Please enter &quot;yes&quot; if fully compliant with the requirement</th>
<th>Recommendation</th>
<th>Estimated Date of Completion</th>
<th>Remediation Owner</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1</td>
<td>A formal process for approving and testing all network connections and changes to the firewall and router configurations</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.2</td>
<td>Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.3</td>
<td>Current diagram that shows all cardholder data flows across systems and networks</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.4</td>
<td>Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.5</td>
<td>Description of groups, roles, and responsibilities for management of network components</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.6</td>
<td>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</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.7</td>
<td>Requirement to review firewall and router rule sets at least every six months</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notes:
- An “internal network” is any network that is internal 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.

1.2.2: Secure and synchronize router configuration files.

1.2.3: Install perimeter firewalls between any wireless network and the cardholder data environment, and configure those firewalls to deny, control (if such traffic is necessary for business purposes), or permit only authorized traffic from between the wireless environment into and the cardholder data environment.

1.3: Prohibit direct public access between the Internet and any system component in the cardholder data environment.
## NIST Cyber Security Framework

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

**Executive Level**
- **Focus:** Organizational Risk
- **Actions:** Risk Decision and Priorities

**Business/Process Level**
- **Focus:** Critical Infrastructure Risk Management
- **Actions:** Selects Profile, Allocates Budget

**Implementation/Operations Level**
- **Focus:** Securing Critical Infrastructure
- **Actions:** Implements Profile

**Implementation Progress**
- Changes in Assets, Vulnerability and Threat

**Mission Priority and Risk Appetite and Budget**

**Changes in Current and Future Risk**

**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

<table>
<thead>
<tr>
<th>Service</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Records</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Benefits Administration</td>
<td>M</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>Recruiting</td>
<td>H</td>
<td>H</td>
<td>L</td>
</tr>
</tbody>
</table>
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

- Policy
  - Standard
    - Procedure
      - Supporting Document
    - Procedure
      - Supporting Document
  - Standard
    - Procedure
      - Supporting Document
    - Procedure
      - Supporting Document
    - Procedure
      - Supporting Document

InfoDefence™
Overview
Description
This policy contains high-level information protection mandates as set forth by executive management in response to enterprise risk and regulatory compliance requirements. As with all corporate IT policies, supporting 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 protection.

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

Applicability
There are two audiences for policies: general users and users that perform IT functions. This policy is directed at users that perform IT functions.

Sanctions for Non-compliance
This policy is compulsory. Failure to comply may result in reprimand and/or employment termination.

Policy Statements
Policy
Information will be protected in a way that reduces IT risk and complies with applicable regulations.

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.

© ISACA
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