SECURITY MANAGEMENT
ACKNOWLEDGMENTS

Material is sourced from:

- CISM® Review Manual 2012, ©2011, ISACA. All rights reserved. Used by permission.
- CISA® Review Manual 2011, ©2010, ISACA. All rights reserved. Used by permission.
- COBIT® 5: Enabling Processes. ©2012, ISACA. All rights reserved.
- COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT. ©2012, ISACA. All rights reserved.

Author: Susan J Lincke, PhD
Univ. of Wisconsin-Parkside

Reviewers/Contributors: Todd Burri, Kahili Cheng

Funded by National Science Foundation (NSF) Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and/or source(s) and do not necessarily reflect the views of the National Science Foundation.
OBJECTIVES

The student should be able to:

- Define quality terms: quality assurance, quality control
- Describe security organization members: CISO, CIO, CSO, Board of Directors, Executive Management, Security Architect, Security Administrator
- Define security baseline, gap analysis, metrics, compliance, policy, standard, guideline, procedure
- Describe COBIT, CMM, Levels 1-5
- Develop security metrics
SECURITY FRAMEWORK

Framework: COBIT, CMM
SABSA LIFECYCLE

Strategy & Concept

Manage & Measure
Attributes defined and measured

Implement

Design
Logical, Physical, Component, Operational

Contextual
Conceptual
COBIT ADDRESSES SARBANES-OXLEY: CORPORATIONS

IT controls should consider the overall governance framework to support the quality and integrity of information.

COSO Components

Control Environment
Risk Assessment
Control Activities
Information and Communication
Monitoring

Controls in IT are relevant to both financial reporting and disclosure requirements of Sarbanes-Oxley.

Competency in all five layers of COSO’s framework is necessary to achieve an integrated control program.

http://www.isaca.org/
COBIT 5:
EVALUATE, DIRECT AND MONITOR (EDM)

1. Ensure governance framework setting and maintenance
2. Ensure benefits delivery
3. Ensure risk optimization
4. Ensure resource optimization
5. Ensure stakeholder transparency

Source: COBIT® 5 2012 ISACA, All rights reserved.
COBIT 5:
ALIGN, PLAN AND ORGANIZE

1. Manage the IT management framework
2. Manage strategy
3. Manage enterprise architecture
4. Manage innovation
5. Manage portfolio
6. Manage budget and costs
7. Manage human resources
8. Manage relationships
9. Manage service agreements
10. Manage suppliers
11. Manage quality
12. Manage risk
13. Manage security

Source: COBIT® 5 2012 ISACA, All rights reserved.
COBIT 5: BUILD, ACQUIRE AND IMPLEMENT

1. Manage programs and projects
2. Manage requirements definition
3. Manage solutions identification and build
4. Manage availability and capacity
5. Manage organizational change enablement
6. Manage changes
7. Manage change acceptance and transitioning
8. Manage knowledge
9. Manage assets
10. Manage configuration

Source: COBIT® 5 2012 ISACA, All rights reserved.
COBIT 5:
DELIVER, SERVICE AND SUPPORT

1. Manage operations
2. Manage service requests and incidents
3. Manage problems
4. Manage continuity
5. Manage security services
6. Manage business process controls

Source: COBIT® 5 2012 ISACA, All rights reserved.
1. Monitor, evaluate and assess performance and conformance
2. Monitor, evaluate and assess the system of internal control
3. Monitor, evaluate and assess compliance with external requirements
KEY PROCESS: DELIVER, SERVICE AND SUPPORT
INCLUDES PROCESS: MANAGE SECURITY SERVICES

Which Includes Management Practices:
1. Protect against malware
2. Manage network and connectivity security
3. Manage endpoint security
4. Manage user identity and logical access
5. Manage physical access to IT assets
6. Manage sensitive documents and output devices
7. Monitor the infrastructure for security-related events

Which each include Activities...
Grading Each Process to Attain Level 1

<table>
<thead>
<tr>
<th>Abbrev.</th>
<th>Description</th>
<th>Achievement Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Not Achieved</td>
<td>0-15%</td>
</tr>
<tr>
<td>P</td>
<td>Partially Achieved</td>
<td>15-50%</td>
</tr>
<tr>
<td>L</td>
<td>Largely Achieved</td>
<td>50-85%</td>
</tr>
<tr>
<td>F</td>
<td>Fully Achieved</td>
<td>85-100%</td>
</tr>
<tr>
<td>Level 0 Incomplete Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control processes are not implemented in a workable way</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 1 Performed Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control processes are functional; process purpose is achieved</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 2 Managed Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes are managed via scheduling, monitoring, and config. mgmt.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 3 Established Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>The process is fully documented, implemented, and achieves outcomes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 4 Predictable Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating effectiveness operates with measured limits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 5 Optimizing Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continual improvement works to achieve current/future business goals</td>
</tr>
</tbody>
</table>

Source: COBIT® 5 2012 ISACA, All rights reserved.
SECURITY STANDARDS

These standards can be used to develop or advance a security program (if one is not in place):

- ISO/IEC 27001
- ISACA COBIT

**Gap Analysis:** What do we need to do to achieve our goal?

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lvl 0</td>
<td>Incomplete</td>
</tr>
<tr>
<td>Lvl 1</td>
<td>Performed</td>
</tr>
<tr>
<td>Lvl 2</td>
<td>Managed</td>
</tr>
<tr>
<td>Lvl 3</td>
<td>Established</td>
</tr>
<tr>
<td>Lvl 4</td>
<td>Predictable</td>
</tr>
<tr>
<td>Lvl 5</td>
<td>Optimizing</td>
</tr>
</tbody>
</table>

Where we are → Where we want to be → COBIT Levels
CABABILITY MATURITY MODEL

Level 1: Performed Process

- Security functions are accomplished but not documented
- Individuals have knowledge to perform their jobs

Level 2: Managed Process

- Projects are scheduled and monitored
- Work products are expected
- Documents and events are tracked via configuration management
CAPABILITY MATURITY MODEL

Level 3: Established Process

- Standardized IT/security processes are documented across organization
- Personnel are trained to ensure knowledge and skills
- Assurance (audits) track performance
- Measures are defined based upon the defined process

Level 4: Predictable Process

- Metrics are used to monitor performance
- The organization performs at a predictable level, which is known and managed
**Policy Documentation**

**Policy**: Direction for Control  
Philosophy of organization  
Created by Senior Mgmt  
Reviewed periodically

- Employees must understand intent  
- Auditors test for compliance

**Procedures**:  
Detailed steps to implement a policy.  
Written by process owners

**Standards**:  
An image of what is acceptable

**Guidelines**:  
Recommendations and acceptable alternatives
**EXAMPLE POLICIES**

- **Risks** shall be managed utilizing appropriate controls and countermeasure to achieve acceptable levels at acceptable costs.

- **Monitoring and metrics** shall be implemented, managed, and maintained to provide ongoing assurance that all security policies are enforced and control objectives are met.

- **Incident response** capabilities are implemented and managed sufficient to ensure that incidents do not materially affect the ability of the organization to continue operations.

- **Business continuity and disaster recovery plans** shall be developed, maintained and tested in a manner that ensures the ability of the organization to continue operations under all conditions.
POLICIES, PROCEDURES, STANDARDS

- **Policy Objective**: Describes ‘what’ needs to be accomplished
- **Policy Control**: Technique to meet objectives
  - **Procedure**: Outlines ‘how’ the Policy will be accomplished
  - **Standard**: Specific rule, metric or boundary that implements policy

- Example 1:
  - **Policy**: Computer systems are not exposed to illegal, inappropriate, or dangerous software
  - **Policy Control Standard**: Allowed software is defined to include ...
  - **Policy Control Procedure**: A description of how to load a computer with required software.

- Example 2:
  - **Policy**: Access to confidential information is controlled
  - **Policy Control Standard**: Confidential information SHALL never be emailed without being encrypted
  - **Policy Guideline**: Confidential info SHOULD not be written to a memory stick

Discussion: Are these effective controls by themselves?
QUALITY DEFINITIONS

**Quality Assurance**: Ensures that staff are following defined quality processes: e.g., following standards in design, coding, testing, configuration management

**Quality Control**: Conducts tests to validate that software is free from defects and meets user expectations
Measurable goals for security quality exist

Measures are tied to the business goals of the organization

Common Features include:

- Establish Measurable Quality Goals
- Objectively Manage Performance (SLA)
MONITORING FUNCTION: METRICS

Strategic Metrics
- Project Plan or Budget Metrics
- Risk performance
- Disaster Recovery Test results
- Audit results
- Regulatory compliance results

Tactical Metrics
- Policy compliance metrics
- Exceptions to policy/standards
- Changes in process or system affecting risk
- Incident management effectiveness

Operational Metrics
- Vulnerability Scan results
- Server config. standards compliance
- IDS monitoring results
- Firewall log analysis
- Patch mgmt status
## MONITORING FUNCTION: METRICS

<table>
<thead>
<tr>
<th>Risk:</th>
<th>Cost Effectiveness:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The aggregate ALE</td>
<td>What is:</td>
</tr>
<tr>
<td>% of risk eliminated, mitigated, transferred</td>
<td>Cost of workstation security per user</td>
</tr>
<tr>
<td># of open risks due to inaction</td>
<td>Cost of email spam and virus protection per mailbox</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Operational Performance</strong></th>
<th><strong>Organizational Awareness:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to detect and contain incidents</td>
<td>% of employees passing quiz, after training vs. 3 months later</td>
</tr>
<tr>
<td>% packages installed without problem</td>
<td>% of employees taking training</td>
</tr>
<tr>
<td>% of systems audited in last quarter</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Technical Security Architecture</strong></th>
<th><strong>Security Process Monitoring:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td># of malware identified and neutralized</td>
<td>Last date and type of BCP, DRP, IRP testing</td>
</tr>
<tr>
<td>Types of compromises, by severity &amp; attack type</td>
<td>Last date asset inventories were reviewed &amp; updated</td>
</tr>
<tr>
<td>Attack attempts repelled by control devices</td>
<td>Frequency of executive mgmt review activities compared to planned</td>
</tr>
<tr>
<td>Volume of messages, KB processed by communications control devices</td>
<td></td>
</tr>
</tbody>
</table>


# Workbook: Metrics

## Metrics Selected

What are the most important areas to monitor in your organization?

**Lunatic gunman**

**FERPA Violation**

## Major Risks:

- Cracking Attempt
- Web Availability

<table>
<thead>
<tr>
<th>Category</th>
<th>Metric</th>
<th>Calculation &amp; Collection Method</th>
<th>Period of Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategic</strong></td>
<td>Cost of security/terminal</td>
<td>Information Tech. Group</td>
<td>1 year</td>
</tr>
<tr>
<td></td>
<td>Cost of incidents</td>
<td>Incident Response totals</td>
<td>6 months</td>
</tr>
<tr>
<td><strong>Tactical</strong></td>
<td>% employees passing FERPA quiz</td>
<td>Annual email requesting testing</td>
<td>1 year</td>
</tr>
<tr>
<td></td>
<td>% employees completing FERPA training</td>
<td>Two annual trainings with sign-in. Performance review</td>
<td>1 year</td>
</tr>
<tr>
<td></td>
<td># Hours Web unavailable</td>
<td>Incident Response form</td>
<td>6 months</td>
</tr>
<tr>
<td><strong>Operational</strong></td>
<td># brute force attacks</td>
<td>Incident Response form</td>
<td>1 month</td>
</tr>
<tr>
<td></td>
<td># malware infections</td>
<td>Incident Response form</td>
<td>1 month</td>
</tr>
</tbody>
</table>
**COMPLIANCE FUNCTION**

**Compliance**: Ensures compliance with organizational policies

- E.g.: Listen to selected help desk calls to verify proper authorization occurs when resetting passwords

- Best if compliance tests are automated
LEVEL 5 — OPTIMIZING PROCESS

- Continuous improvement arise from measures and security event knowledge
- Current and future business goals are addressed
- Automated measures help in attainment
The difference between where an organization performs and where they intend to perform is known as:

1. Gap analysis
2. Quality Control
3. Performance Measurement
4. Benchmarking
“Passwords shall be at least 14 characters long, and require a combination of at least 3 of lower case, upper case, numeric, or symbols characters”. This is an example of a:

1. Standard
2. Policy
3. Procedure
4. Guideline
The PRIMARY focus of COBIT or CMM Level 4 is

1. Security Documentation
2. Metrics
3. Risk
4. Business Continuity
QUESTION

Product testing is most closely associated with which department:

1. Audit
2. Quality Assurance
3. Quality Control
4. Compliance
“Employees should never open email attachments, except if the attachment is expected and for business use”. This is an example of a:

1. Policy
2. Procedure
3. Guideline
4. Standard
The MOST important metrics when measuring compliance include:

1. Metrics most easily automated
2. Metrics related to intrusion detection
3. Those recommended by best practices
4. Metrics measuring conformance to policy
CORPORATE GOVERNANCE

**Corporate Governance:** Leadership by corporate directors in creating and presenting value for all stakeholders

**IT Governance:** Ensure the alignment of IT with enterprise objectives

- Responsibility of the board of directors and executive mgmt
Strategic Planning Process

**Strategic**: Long-term (3-5 year) direction considers organizational goals, regulation (and for IT: technical advances)

**Tactical**: 1-year plan moves organization to strategic goal

**Operational**: Detailed or technical plans
STRATEGIC PLANNING

Strategy:
- Achieve COBIT Level 4

Tactical: During next 12 months:
- Each business unit must identify current applications in use
- 25% of all stored data must be reviewed to identify critical resources
- Business units must achieve regulatory compliance
- A comprehensive risk assessment must be performed for each business unit
- All users must undergo general security training
- Standards must exist for all policies
STANDARD IT BALANCED SCORECARD

Establish a mechanism for reporting IT strategic aims and progress to the board

**Mission** = Direction E.g.:
- Serve business efficiently and effectively

**Strategies** = Objectives E.g.:
- Quality thru Availability
- Process Maturity

**Measures** = Statistics E.g.:
- Customer satisfaction
- Operational efficiency
## It Balanced Scorecard

<table>
<thead>
<tr>
<th>Financial Goals</th>
<th>Internal Business Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>How should we appear to stockholder?</td>
<td>What business processes should we excel at?</td>
</tr>
<tr>
<td>Vision:</td>
<td>Vision:</td>
</tr>
<tr>
<td>Metrics:</td>
<td>Metrics:</td>
</tr>
<tr>
<td>Performance:</td>
<td>Performance:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customer Goals</th>
<th>Learning and Growth Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>How should we appear to our customer?</td>
<td>How will we improve internally?</td>
</tr>
<tr>
<td>Vision:</td>
<td>Vision:</td>
</tr>
<tr>
<td>Metrics:</td>
<td>Metrics:</td>
</tr>
<tr>
<td>Performance:</td>
<td>Performance:</td>
</tr>
</tbody>
</table>
## Case Study: IT Governance

### Strategic Plan – Tactical Plan

<table>
<thead>
<tr>
<th>Strategic Plan Objective</th>
<th>Time frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorporate the business</td>
<td>5 yrs</td>
</tr>
<tr>
<td>Pass a professional audit</td>
<td>4 yrs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tactical Plan: Objective</th>
<th>Time frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform strategic-level security, includes:</td>
<td>1 yr</td>
</tr>
<tr>
<td>Perform risk analysis</td>
<td>6 mos.</td>
</tr>
<tr>
<td>Perform BIA</td>
<td>1 yr</td>
</tr>
<tr>
<td>Define policies</td>
<td>1 yr</td>
</tr>
</tbody>
</table>
## Operational Plan

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Timeframe/ Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hire an internal auditor and security professional</td>
<td>March 1 VP Finance</td>
</tr>
<tr>
<td>Establish security team of business, IT, personnel</td>
<td>Feb 1: VP Finance &amp; Chief Info. Officer (CIO)</td>
</tr>
<tr>
<td>Team initiates risk analysis and prepares initial report</td>
<td>April 1 CIO &amp; Security Team</td>
</tr>
</tbody>
</table>
SECURITY ORGANIZATION

Board of Directors

Review Risk assessment & Business Impact Analysis
Define penalties for non-compliance of policies

Executive Mgmt

Defines security objectives and institutes security organization

Senior representatives of business functions ensures alignment of security program with business objectives

Other positions:
Chief Risk Officer (CRO)
Chief Compliance Officer (CCO)

Security Steering Committee

Chief Info Security Officer (CISO)
**IT Governance Committees**

**IT Strategic Committee**
- Focuses on Direction and Strategy
- Advises board on IT strategy and alignment
- Optimization of IT costs and risk

**IT Steering Committee**
- Focuses on Implementation
- Monitors current projects
- Decides IT spending
IT STRATEGY COMMITTEE
MAIN CONCERNS

- Alignment of IT with Business
- Contribution of IT to the Business
- Exposure & containment of IT Risk
- Optimization of IT costs
- Achievement of strategic IT objectives
IT STEERING COMMITTEE
MAIN CONCERNS

- Make decision of IT being centralized vs. decentralized, and assignment of responsibility
- Makes recommendations for strategic plans
- Approves IT architecture
- Reviews and approves IT plans, budgets, priorities & milestones
- Monitors major project plans and delivery performance
EXECUTIVE MGMT INFO SECURITY CONCERNS

- Reduce civil and legal liability related to privacy
- Provide policy and standards leadership
- Control risk to acceptable levels
- Optimize limited security resources
- Base decisions on accurate information
- Allocate responsibility for safeguarding information
- Increase trust and improve reputation outside organization
The MOST important function of the IT department is:

1. Cost effective implementation of IS functions
2. Alignment with business objectives
3. 24/7 Availability
4. Process improvement
QUESTION

“Implement virtual private network in the next year” is a goal at the level:

1. Strategic
2. Operational
3. Tactical
4. Mission
QUESTION

Documentation that would not be viewed by the IT Strategy Committee would be:

1. IT Project Plans
2. Risk Analysis & Business Impact Analysis
3. IT Balanced Scorecard
4. IT Policies
Interview stakeholders (HR, legal, finance) to determine org. issues & concerns

Develop security policies for approval to Mgmt

Conduct security training & test for compliance

Improve standards

Documentation

Security Issues

Security Policies

Training materials

Info Security Steering Committee

Development of security policies

Steering Committee
SECURITY RELATIONSHIPS

- Security Strategy, Risk, & Alignment
- Hiring, training, roles & responsibility, Incident handling
- Security requirements sign-off, Acceptance test, Access authorization
- Security monitoring, Incident resp., Site inventory, Crisis management

CISO

- Exec. Mgmt
- Human Res.
- Business Mgmt
- Legal Dept.
- IT Operations
- Purchasing
- Quality Control
- S/W Dev.

Security requirements
Access control

Security requirements
in RFP
Contract requirements

Security requirements
and review
Change control
Security upgrade/test
SECURITY POSITIONS

Security Architect

- Design secure network topologies, access control, security policies & standards.
- Evaluate security technologies
- Work with compliance, risk mgmt, audit

Security Administrator

- Allocate access to data under data owner
- Prepare security awareness program
- Test security architecture
- Monitor security violations and take corrective action
- Review and evaluate security policy
SECURITY ARCHITECT: CONTROL ANALYSIS

Do controls fail secure or fail open?
Is restrictive or permissive policy
(denied unless expressly permitted or vice versa?)
Does control align with policy & business expectation?

Where are controls located?
Are controls layered?
Is control redundancy needed?

Policy
Placement

Have controls been tested?
Are controls self-protecting?
Do controls meet control objectives?
Will controls alert security personnel if they fail?
Are control activities logged and reviewed?

Does control protect broadly or one application?
If control fails, is there a control remaining?
If control fails, does appl. fail?

Implementation
Efficiency

Are controls reliable?
Do they inhibit productivity?
Are they automated or manual?
Are key controls monitored in real-time?
Are controls easily circumvented?

Effectiveness
EXAMPLE POLICY DOCUMENTS

Data Classification: Defines data security categories, ownership and accountability

Acceptable Usage Policy: Describes permissible usage of IT equipment/resources

End-User Computing Policy: Defines usage and parameters of desktop tools

Access Control Policies: Defines how access permission is defined and allocated

After policy documents are created, they must be officially reviewed, updated, disseminated, and tested for compliance
SECURITY ADMINISTRATOR: SECURITY OPERATIONS

- Identity Mgmt & Access control
- System patching & configuration mgmt
- Change control & release mgmt
- Security metrics collection & reporting
- Control technology maintenance
- Incident response, investigation, and resolution
IS AUDITOR & IT GOVERNANCE

- Is IS function aligned with organization’s mission, vision, values, objectives and strategies?
- Does IS achieve performance objectives established by the business?
- Does IS comply with legal, fiduciary, environmental, privacy, security, and quality requirements?
- Are IS risks managed efficiently and effectively?
- Are IS controls effective and efficient?
Who can contribute the MOST to determining the priorities and risk impacts to the organization’s information resources?

1. Chief Risk Officer
2. Business Process Owners
3. Security Manager
4. Auditor
A document that describes how access permission is defined and allocated is the:

1. Data Classification
2. Acceptable Usage Policy
3. End-User Computing Policy
4. Access Control Policies
The role of the Information Security Manager in relation to the security strategy is:

1. Primary author with business input
2. Communicator to other departments
3. Reviewer
4. Approves the strategy
The role most likely to test a control is the:

1. Security Administrator
2. Security Architect
3. Quality Control Analyst
4. Security Steering Committee
The Role responsible for defining security objectives and instituting a security organization is the:

1. Chief Security Officer
2. Executive Management
3. Board of Directors
4. Chief Information Security Officer
When implementing a control, the PRIMARY guide to implementation adheres to:

1. Organizational Policy
2. Security frameworks such as COBIT, NIST, ISO/IEC
3. Prevention, Detection, Correction
4. A layered defense
The persons on the Security Steering Committee who can contribute the BEST information relating to insuring Information Security success is:

1. Chief Information Security Officer
2. Business process owners
3. Executive Management
4. Chief Information Officer