

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

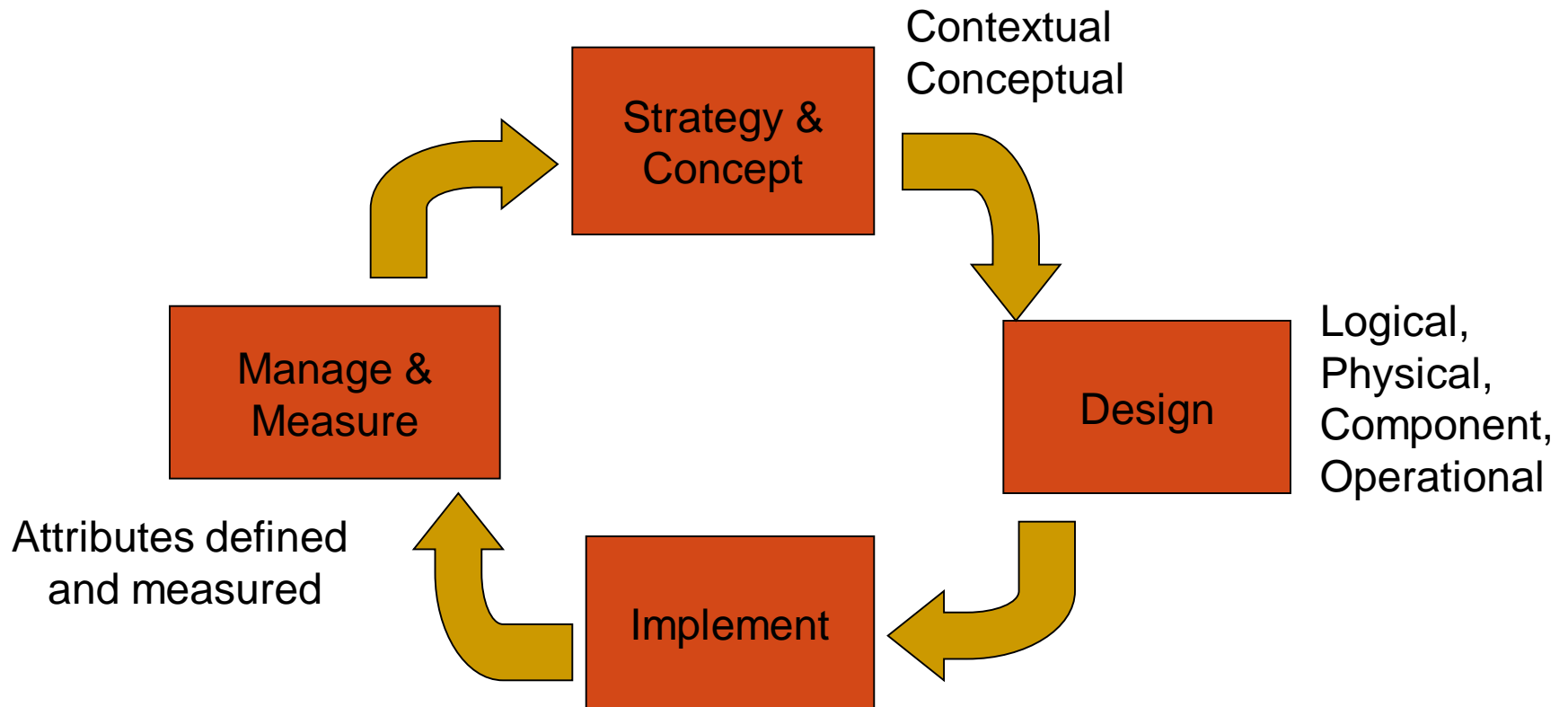


SECURITY FRAMEWORK

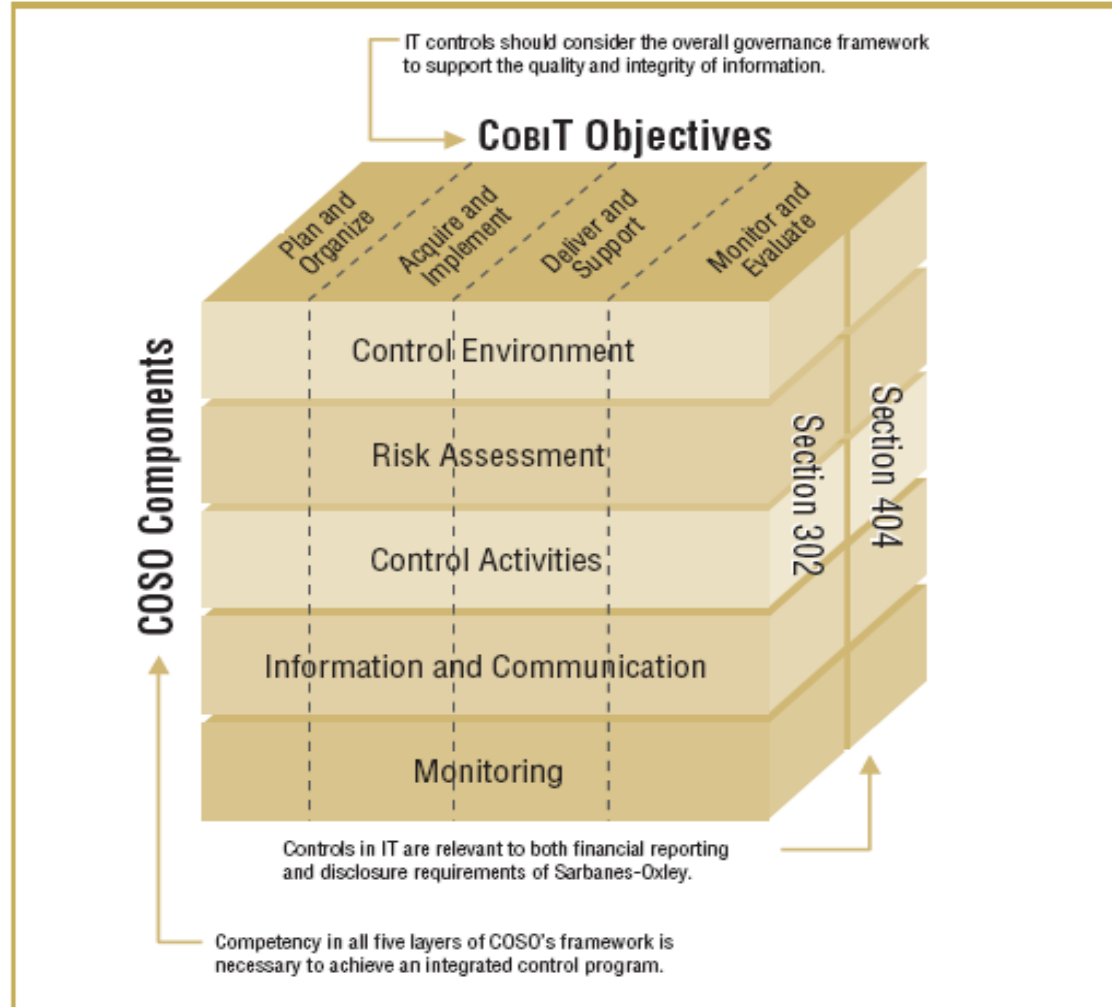
Framework: COBIT, CMM



SABSA LIFECYCLE

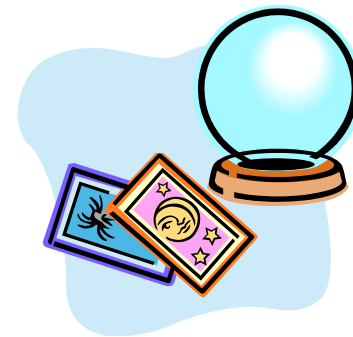


COBIT ADDRESSES SARBANES-OXLEY: CORPORATIONS



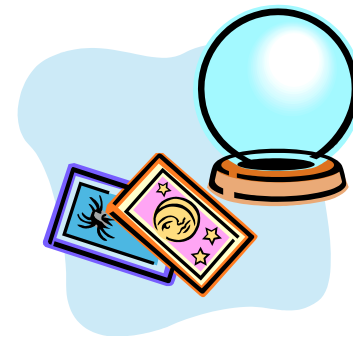
COBIT 5: EVALUATE, DIRECT AND MONITOR (EDM)

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



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



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



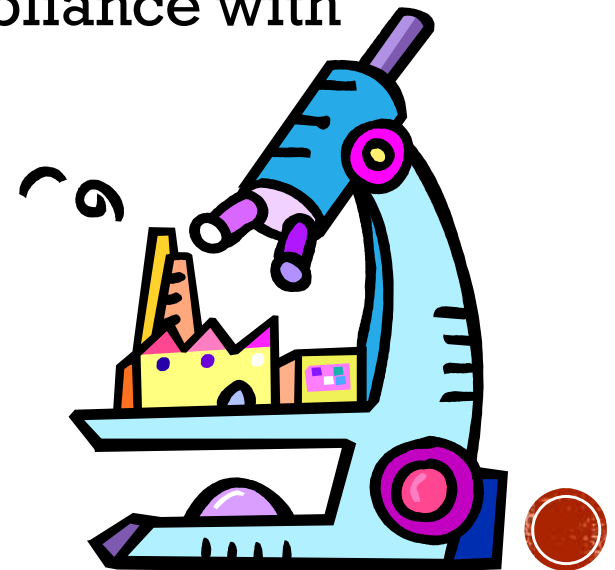
COBIT 5: DELIVER, SERVICE AND SUPPORT

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



COBIT 5: MONITOR, EVALUATE AND ASSESS

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

Abbrev.	Description	Achievement Level
N	Not Achieved	0-15%
P	Partially Achieved	15-50%
L	Largely Achieved	50-85%
F	Fully Achieved	85-100%



COBIT 5

CAPABILITY MATURITY MODEL

Level 5 Optimizing Process Continual improvement works to achieve current/future business goals
Level 4 Predictable Process Operating effectiveness operates with measured limits
Level 3 Established Process The process is fully documented, implemented, and achieves outcomes
Level 2 Managed Process Processes are managed via scheduling, monitoring, and config. mgmt.
Level 1 Performed Process Control processes are functional; process purpose is achieved
Level 0 Incomplete Process Control processes are not implemented in a workable way

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?

Where we are

Where we want to be

COBIT Levels

Lvl
0

Lvl
1

Lvl
2

Lvl
3

Lvl
4

Lvl
5

Incomplete

Performed

Managed

Established

Predictable

Optimizing



CAPABILITY 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:

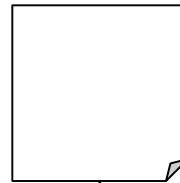
Predictable Process

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

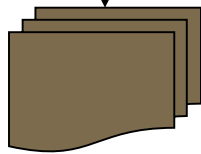


POLICY DOCUMENTATION

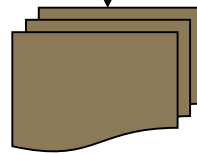
Policy: Direction for Control
Philosophy of organization
Created by Senior Mgmt
Reviewed periodically



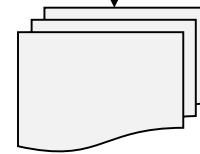
Employees must understand intent
Auditors test for compliance



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



LEVEL 4 — QUANTITATIVELY CONTROLLED

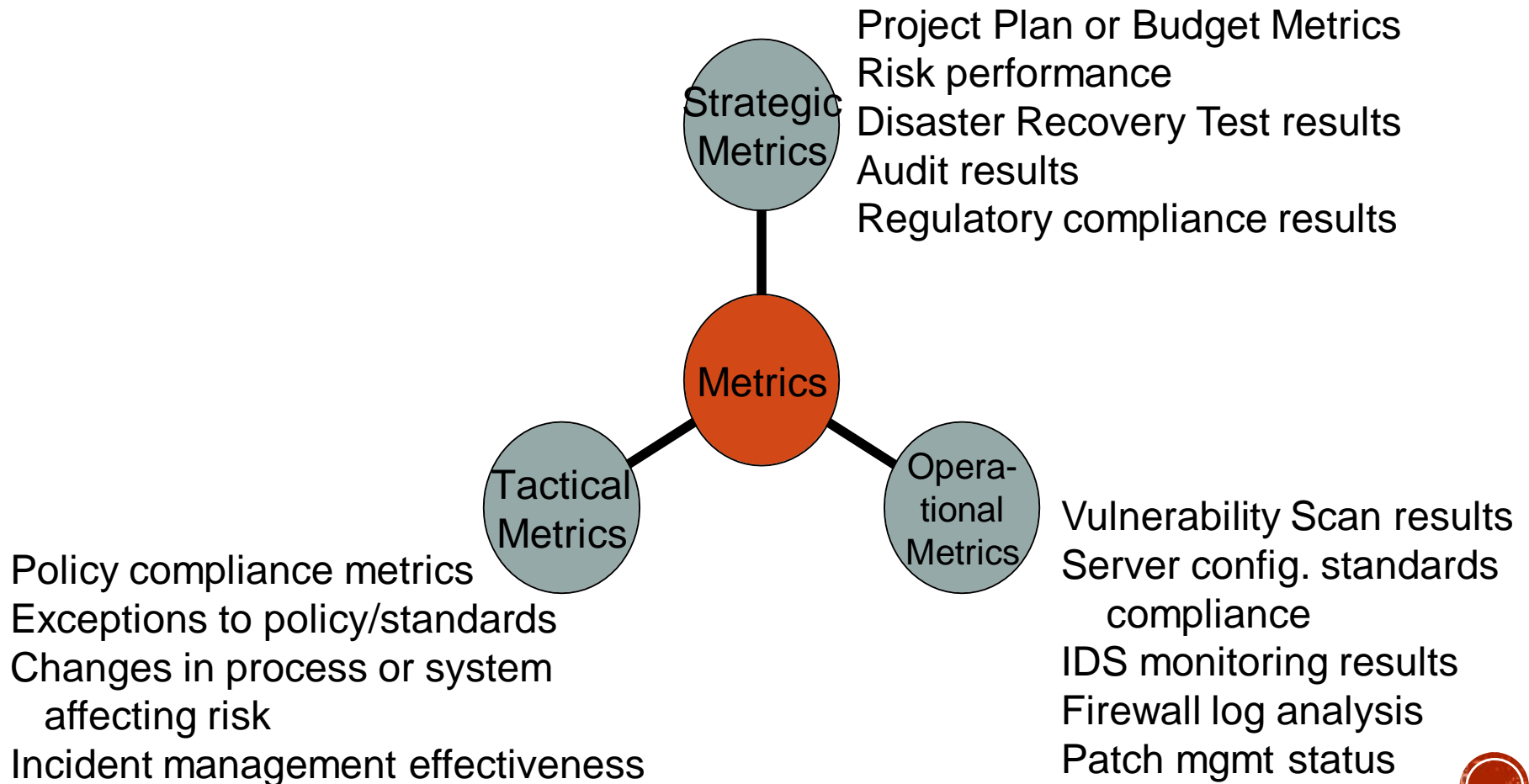
- Measurable goals for security quality exist
- Measures are tied to the business goals of the organization

Common Features include:

- Establish Measurable Quality Goals
- Objectively Manage Performance (SLA)



MONITORING FUNCTION: METRICS



MONITORING FUNCTION: METRICS

Risk:

The aggregate ALE
% of risk eliminated, mitigated,
transferred
of open risks due to inaction

Cost Effectiveness:

What is:
Cost of workstation security per user
Cost of email spam and virus
protection per mailbox

Operational Performance

Time to detect and contain incidents
% packages installed without problem
% of systems audited in last quarter

Organizational Awareness:

% of employees passing quiz, after
training vs. 3 months later
% of employees taking training

Technical Security Architecture

of malware identified and neutralized
Types of compromises, by severity &
attack type
Attack attempts repelled by control
devices
Volume of messages, KB processed
by communications control devices

Security Process Monitoring:

Last date and type of BCP, DRP, IRP
testing
Last date asset inventories were
reviewed & updated
Frequency of executive mgmt review
activities compared to planned



WORKBOOK: METRICS

METRICS SELECTED

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

Lunatic gunman
 FERPA Violation

Major Risks:

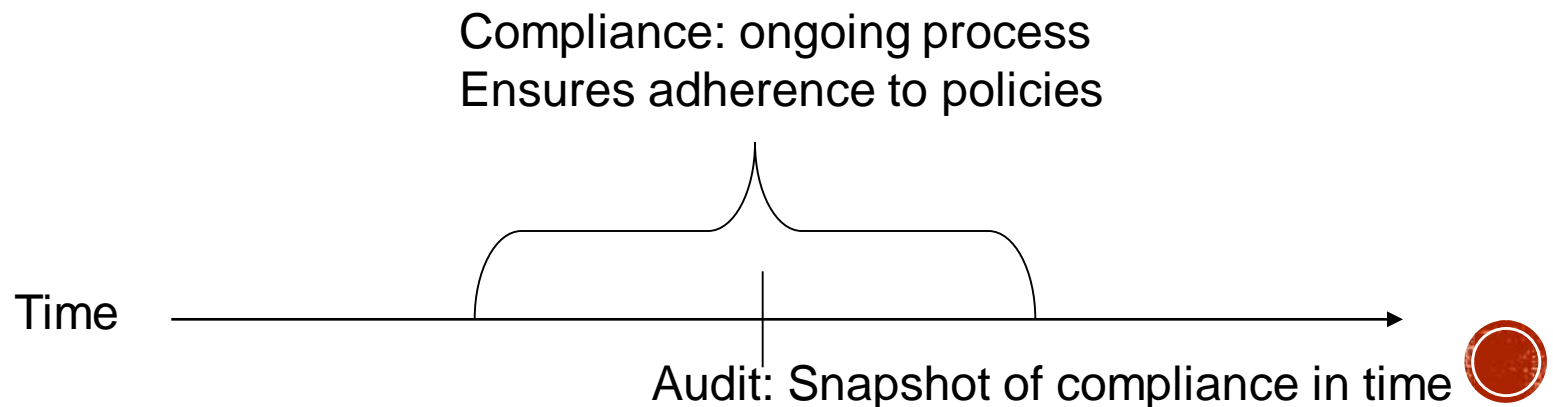
Cracking Attempt
 Web Availability

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

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



QUESTION

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



QUESTION

“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



QUESTION

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



QUESTION

“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



QUESTION

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



INFORMATION SECURITY GOVERNANCE



Governance

Policy

Risk



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

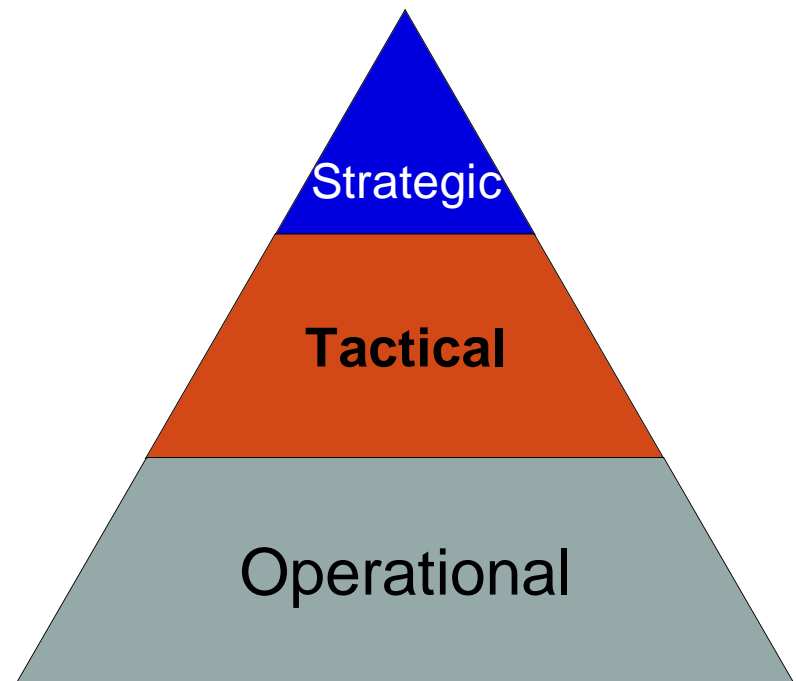


STRATEGIC PLANNING PROCESS

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

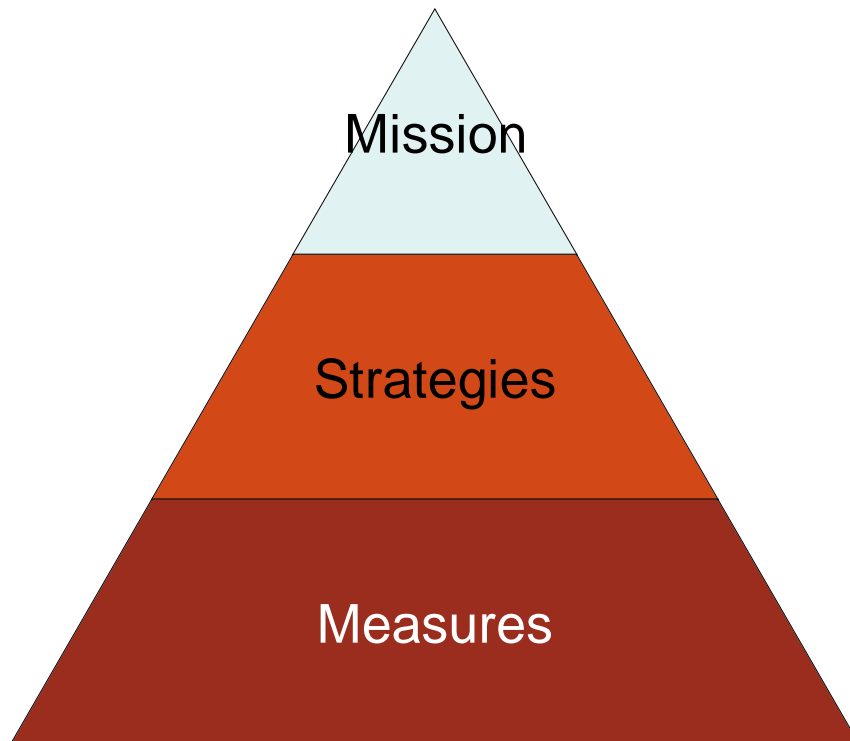
Tactical: During next 12 months:

- 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

Financial Goals

How should we appear to stockholder?

Vision:

Metrics:

Performance:

Internal Business Process

What business processes should we excel at?

Vision:

Metrics:

Performance:

Customer Goals

How should we appear to our customer?

Vision:

Metrics:

Performance:

Learning and Growth Goals

How will we improve internally?

Vision:

Metrics:

Performance:

CASE STUDY: IT GOVERNANCE

STRATEGIC PLAN – TACTICAL PLAN

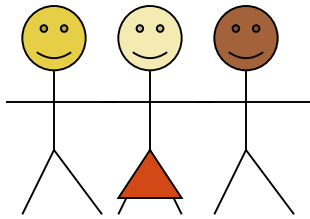
Strategic Plan Objective	Time frame
Incorporate the business	5 yrs
Pass a professional audit	4 yrs

Tactical Plan: Objective	Time frame
Perform strategic-level security, includes:	1 yr
Perform risk analysis	6 mos.
Perform BIA	1 yr
Define policies	1 yr

CASE STUDY: IT GOVERNANCE OPERATIONAL PLANNING

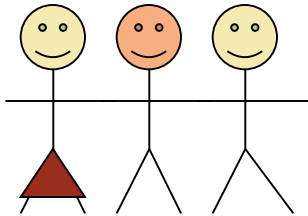
Operational Plan Objectives	Timeframe/ Responsibility
Hire an internal auditor and security professional	March 1 VP Finance
Establish security team of business, IT, personnel	Feb 1: VP Finance & Chief Info. Officer (CIO)
Team initiates risk analysis and prepares initial report	April 1 CIO & Security Team

SECURITY ORGANIZATION



Board of Directors

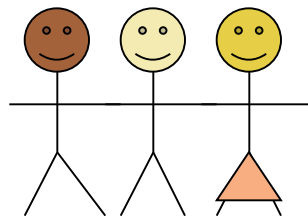
Review Risk assessment & Business Impact Analysis
Define penalties for non-compliance of policies



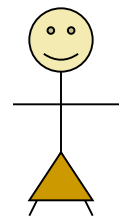
Executive Mgmt

Defines security objectives and
institutes security organization

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



**Security
Steering
Committee**

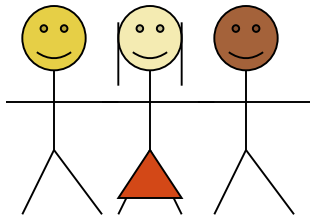


**Chief Info
Security
Officer (CISO)**

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



IT GOVERNANCE COMMITTEES



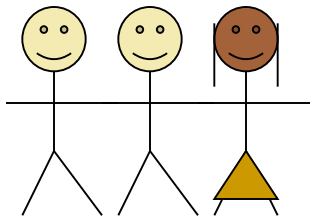
Board members
& specialists

IT Strategic Committee

Focuses on Direction and Strategy

Advises board on IT strategy and alignment

Optimization of IT costs and risk



Business executives
(IT users), CIO, key
advisors (IT, legal, audit,
finance)

IT Steering Committee

Focuses on Implementation

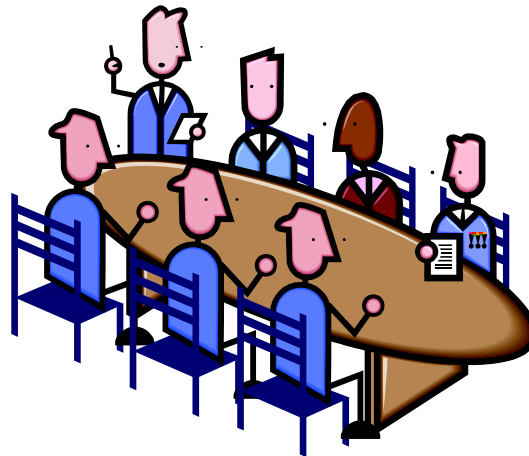
Monitors current projects

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



QUESTION

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



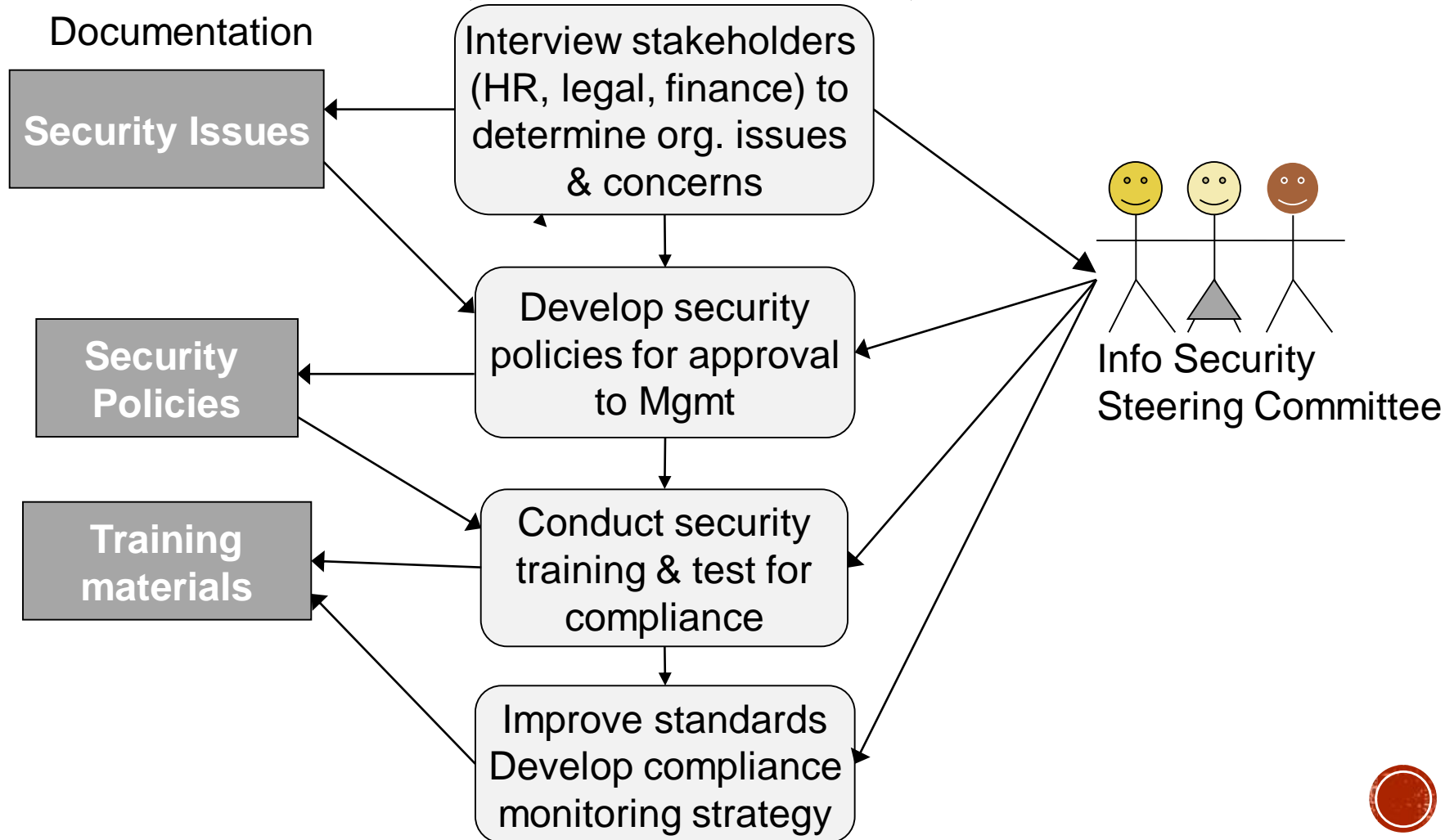
QUESTION

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

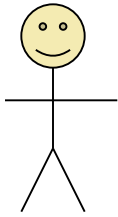


ROAD MAP FOR SECURITY (NEW PROGRAM)

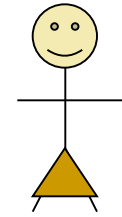


SECURITY RELATIONSHIPS





SECURITY POSITIONS



Security Architect

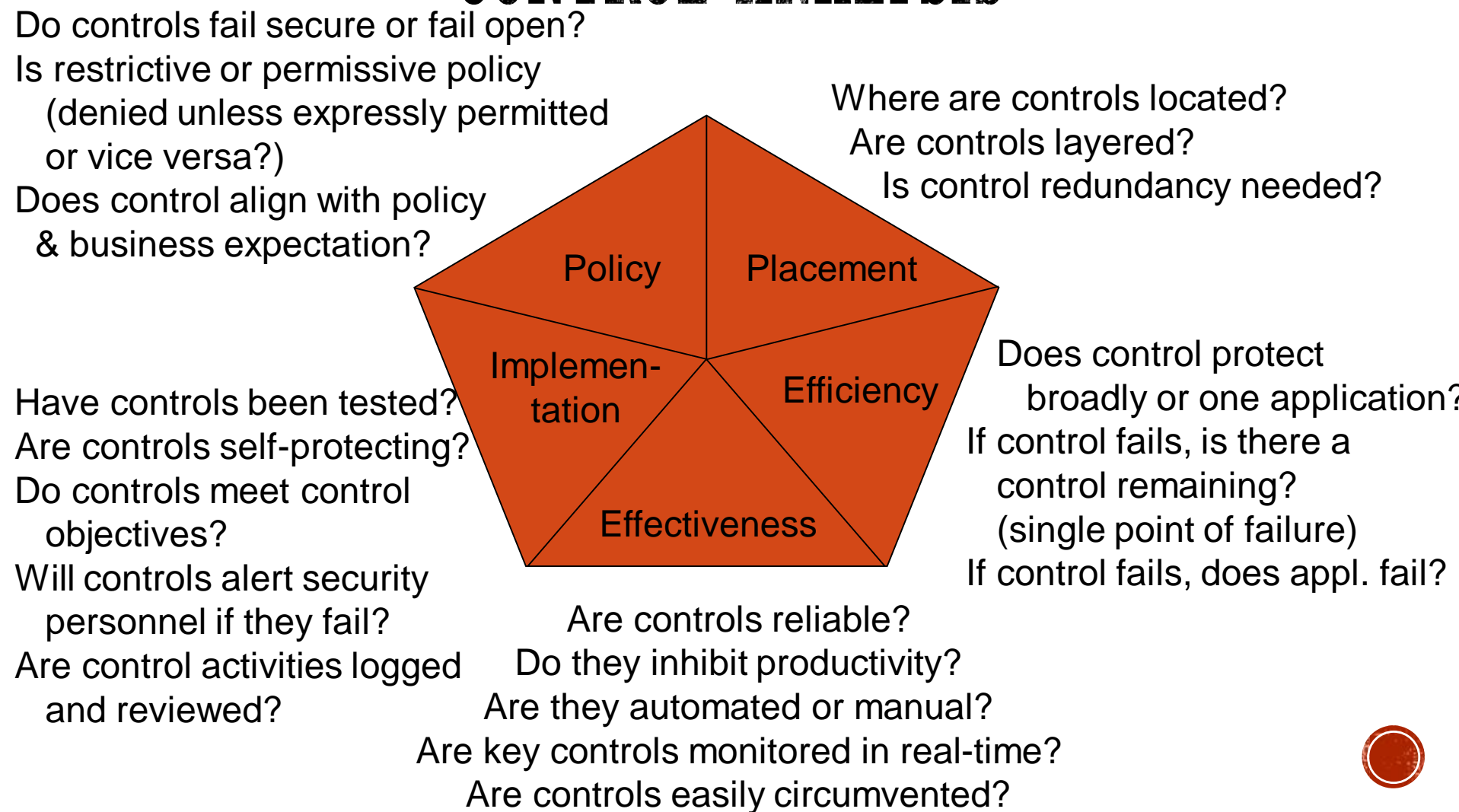
- Design secure network topologies, access control, security policies & standards.
- Evaluate security technologies
- Work with compliance, risk mgmt, audit

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



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?



QUESTION

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



QUESTION

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



QUESTION

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



QUESTION

The role most likely to test a control is the:

1. Security Administrator
2. Security Architect
3. Quality Control Analyst
4. Security Steering Committee



QUESTION

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



QUESTION

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



QUESTION

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

