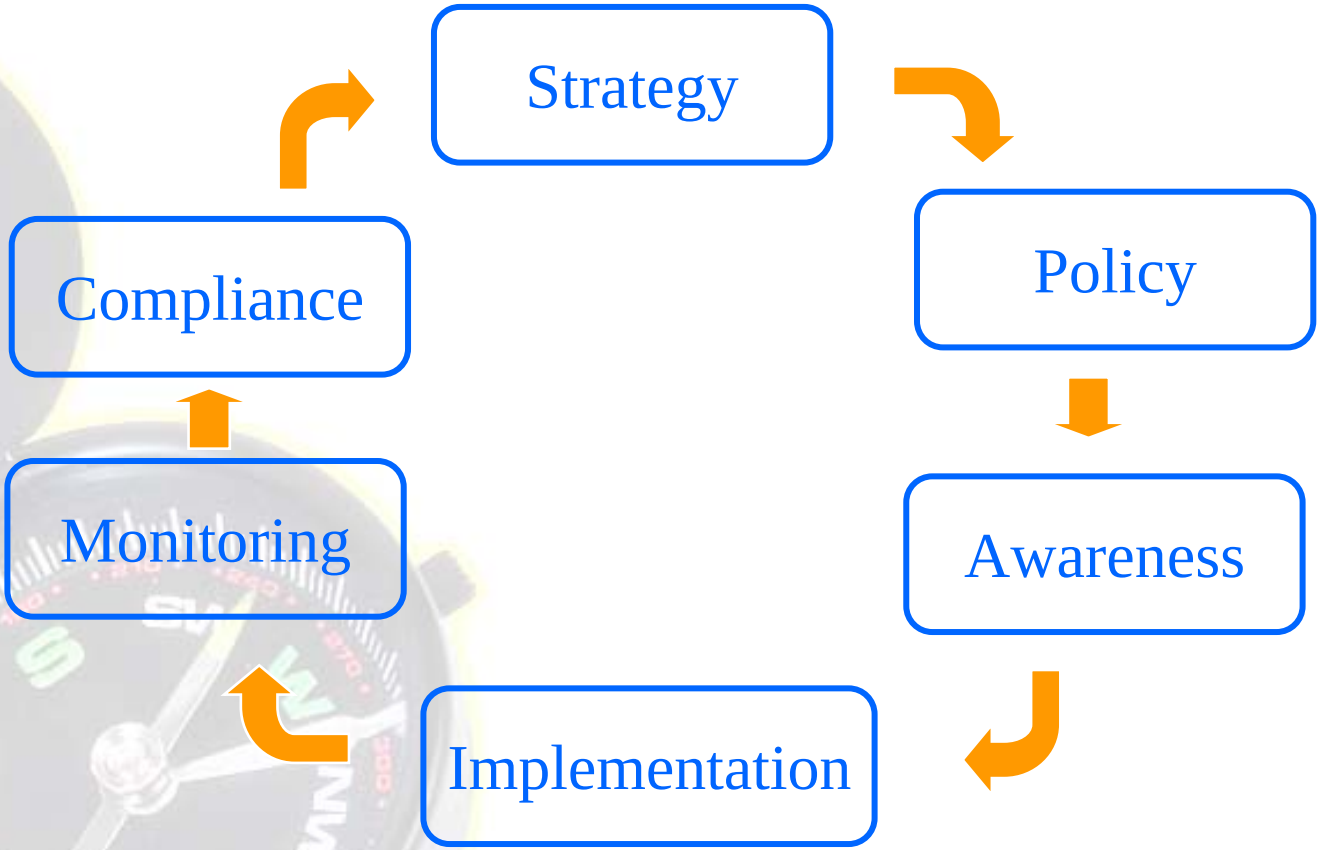

INFORMATION
SECURITY
MANAGEMENT
CONFERENCE
Stepping Through the Info Security Program
Jennifer Bayuk, CISA, CISM
TO GOVERNANCE
ISACA
Serving IT Governance Professionals

Infosec Program

How to:

- compose an InfoSec Program
- cement a relationship between InfoSec program and IT Governance
- design roles and responsibilities to ensure accountability
- identify and allocate resources to achieve InfoSec program objectives
- tell if an InfoSec program is achieving objectives

Security Program Composition



Infosec Program Definition

- Process by which an organization effects security
  - In response to a management concern about information systems
    - With respect to computers as assets, operational integrity, data confidentiality, assets controlled by software, or any combination of the above
- Default process owner is the highest ranking IT manager delegated the responsibility for addressing security concerns with respect to technology

CISM InfoSec Manager Tasks

Content Area 1 –Information Security Governance
Develop an information security strategy aligned with business goals and objectives.
Align information security strategy with corporate governance.
Develop business cases justifying investment in information security.
Identify current and potential legal and regulatory requirements affecting information security.
Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.
Obtain senior management commitment to information security.
Define roles and responsibilities for information security throughout the organization.
Establish internal and external reporting and communication channels that support information security.
Content Area 2 – Information Risk Management
Establish a process for information asset classification and ownership.
Implement a systematic and structured information risk assessment process.
Ensure that business impact assessments are conducted periodically.
Ensure that threat and vulnerability evaluations are performed on an ongoing basis.
Identify and periodically evaluate information security controls and countermeasures to mitigate risk to acceptable levels
Integrate risk, threat and vulnerability identification and management into lifecycle processes (e.g., development, procurement, and employment lifecycles)
Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.
Content Area 3 – Information Security Program Development
Develop and maintain plans to implement the information security strategy.
Specify the activities to be performed within the information security program.
Ensure alignment between the information security program and other assurance functions (e.g., physical, HR, quality, IT).
Identify internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
Ensure the development of information security architectures (e.g., people, processes, technology).
Establish, communicate, and maintain information security policies that support the security strategy.
Design and develop a program for information security awareness, training, and education.
Ensure the development, communication, and maintenance of standards, procedures, and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement)
Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).
Establish metrics to evaluate the effectiveness of the information security program.
Content Area 4 – Information Security Program Management
Manage internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.
Ensure that the information security controls agreed to in contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties) are performed
Monitor, measure, test, and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
Ensure that information security is an integral part of the systems development process.
Ensure that information security is maintained throughout the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement)
Ensure that noncompliance issues and other variances are resolved in a timely manner.
Provide information security awareness, training and education to stakeholders (e.g., business process owners, users, information technology).
Provide information security advice and guidance (e.g., risk analysis, control selection) to the organization.
Content Area 5 – Incident Management and Response
Develop and implement processes for detecting, identifying, analyzing, and responding to information security incidents.
Establish escalation and communication processes and lines of authority.
Develop plans to respond to and document information security incidents.
Establish the capability to investigate information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing)
Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers)
Integrate information security incident response plans with the organization's Disaster Recovery (DR) and Business Continuity Plan (BCP).
Organize, train, and equip teams to respond to information security incidents.
Periodically test and refine information security incident response plans.
Manage the response to information security incidents.
Conduct reviews to identify causes of information security incidents, develop corrective actions, and reassess risk.

Program developed as part of these tasks must cover process by which all these other tasks are accomplished.

Information Security Governance

***Certified Information Security Manager Governance Tasks are*:**

1 Develop an information security strategy aligned with business goals and objectives.
2 Align information security strategy with corporate governance.
3 Develop business cases justifying investment in information security.
4 Identify current and potential legal and regulatory requirements affecting information security.
5 Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.
6 Obtain senior management commitment to information security.
7 Define roles and responsibilities for information security throughout the organization.
8 Establish internal and external reporting and communication channels that support information security.

Information Security Risk Management

Certified Information Security Manager Risk Management Tasks are:

1. Establish a process for information asset classification and *ownership*.
2. Implement a systematic and structured information risk assessment process.
3. Ensure that business impact assessments are conducted periodically.
4. Ensure that threat and vulnerability evaluations are performed on an ongoing basis.
5. Identify and periodically evaluate information security controls and countermeasures to mitigate risk to acceptable levels
6. Integrate risk, threat and vulnerability identification and management into lifecycle processes (e.g., development, procurement, and employment lifecycles)
7. Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.

Information Security Program Management

***Certified Information Security Manager Program Management Tasks are*:**

1 Manage internal and external resources required to execute the information security program.
2 Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.
3 Ensure that the information security controls agreed to in contracts are performed
4 Monitor, measure, test, and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
5 Ensure that information security is an integral part of the systems development process.
6 Ensure that information security is maintained throughout the organization's processes and life cycle activities
7 Ensure that noncompliance issues and other variances are resolved in a timely manner.
8 Provide information security awareness, training and education to stakeholders.
9 Provide information security advice and guidance to the organization.

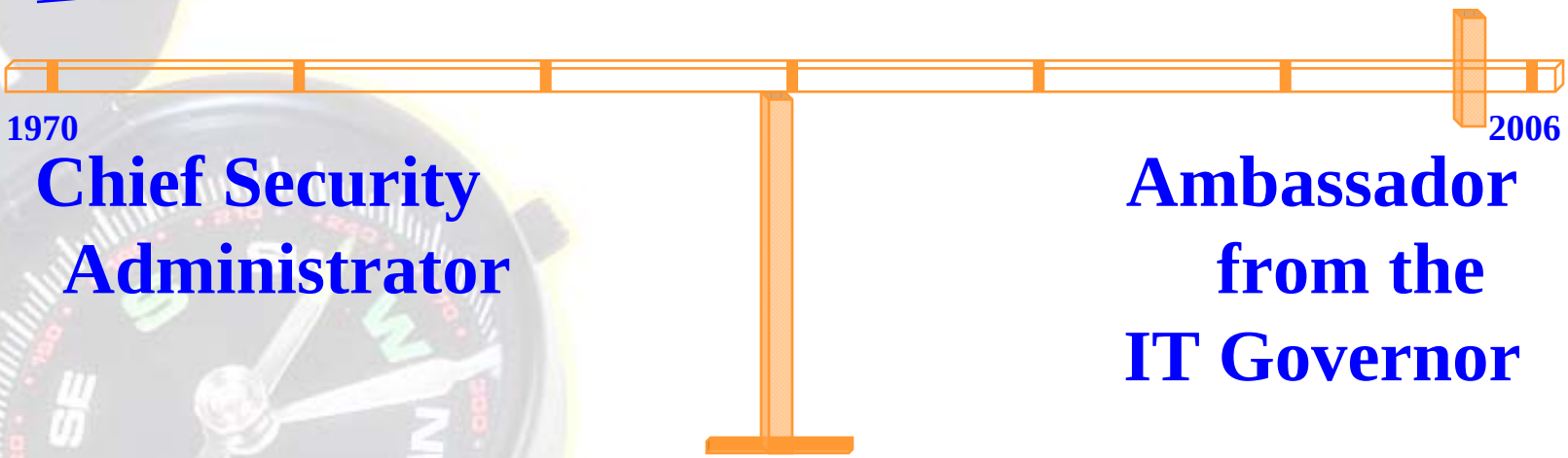
Incident Management and Response

Certified Information Security Manager Incident Management and Response Tasks are:

1. Develop and implement processes for detecting, identifying, analyzing, and responding to information security incidents.
2. Establish escalation and communication processes and lines of authority.
3. Develop plans to respond to and document information security incidents.
4. Establish the capability to investigate information security incidents.
5. Develop a process to communicate with internal parties and external organizations.
6. Integrate information security incident response plans with the organization's Disaster Recovery (DR) and Business Continuity Plan (BCP).
7. Organize, train, and equip teams to respond to information security incidents.
8. Periodically test and refine information security incident response plans.
9. Manage the response to information security incidents.
10. Conduct reviews to identify causes of information security incidents, develop corrective actions, and reassess risk.

Information Security & IT Governance

Infosec program evolution



1970

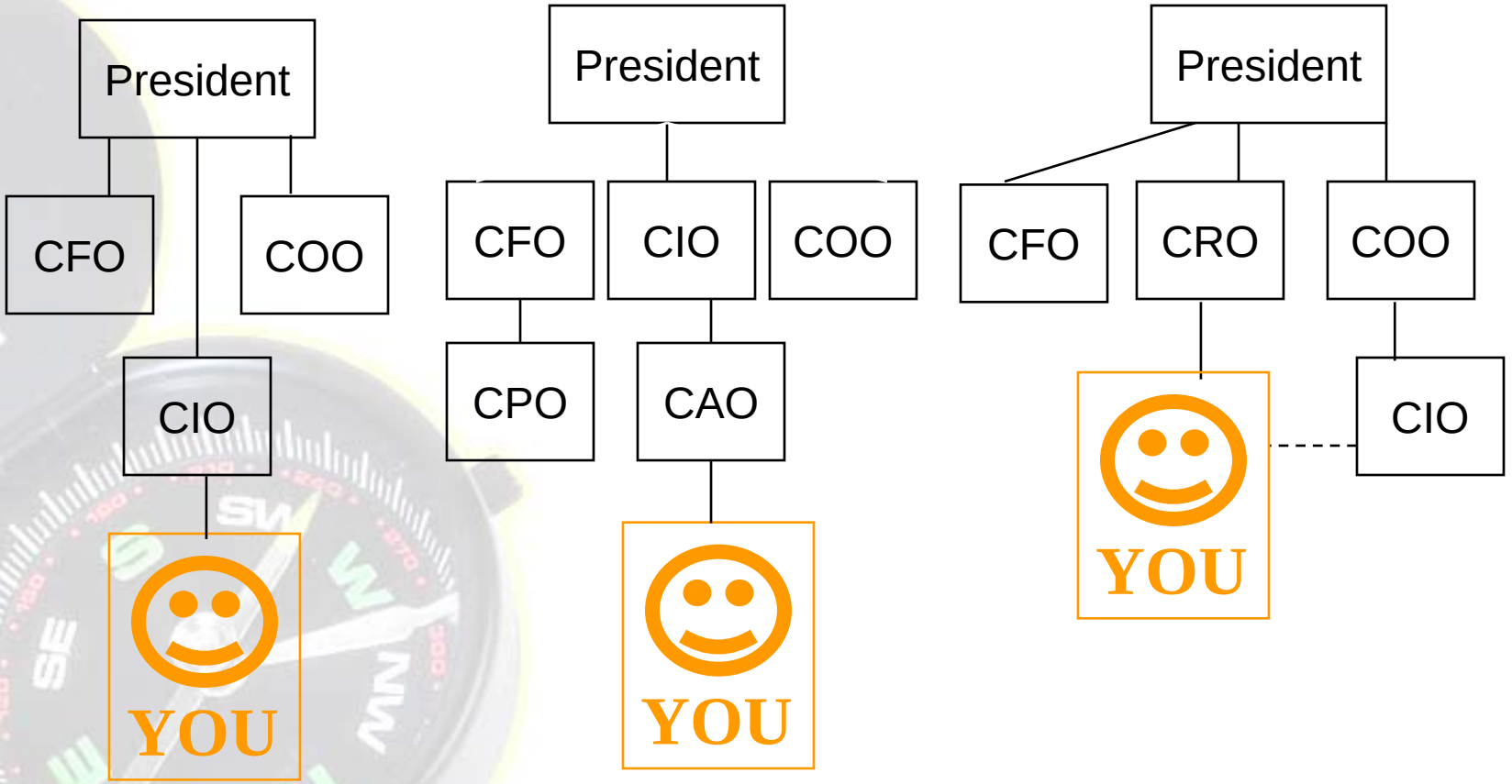
Chief Security Administrator

2006

Ambassador from the IT Governor

Ambassadors need a home base

What does your org chart look like?



Whose support do you need to make organization-wide policy?

Information Security & IT Governance

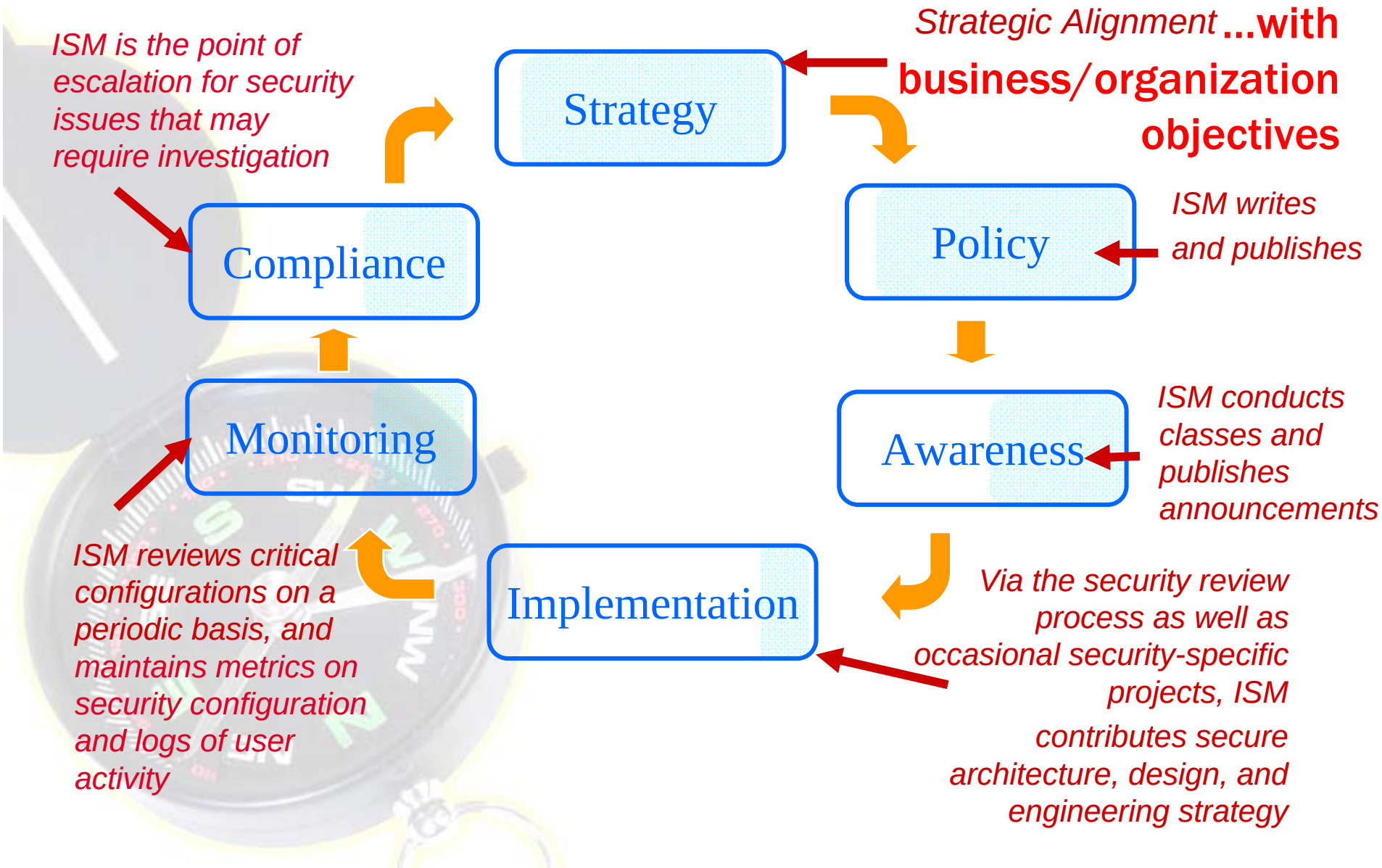
There are five basic outcomes of effective security governance:

- **Strategic alignment**
- **Risk management**
- **Value delivery**
- **Resource management**
- **Performance measurement**

What does management want from the security program? What constitutes success?
This can only be done in conjunction with whoever commissioned the program.

CISM Program Development Task 1: Develop & maintain plans to implement the InfoSec strategy.

Security Management Program Overview



Risk Management

…is business driven and comprises:

- **Credit Risk**
- **Market Risk**
- **Operational Risk**
  - **Information technology**
    - ***Information Security***

Information Security Risk Assessment

All business functions have vulnerabilities, however…

Vulnerabilities != Exploits

Threats != Exploits

Vulnerabilities + Threats != Exploits

Vulnerabilities + Threats *allow* Exploits

Exploits != Damage

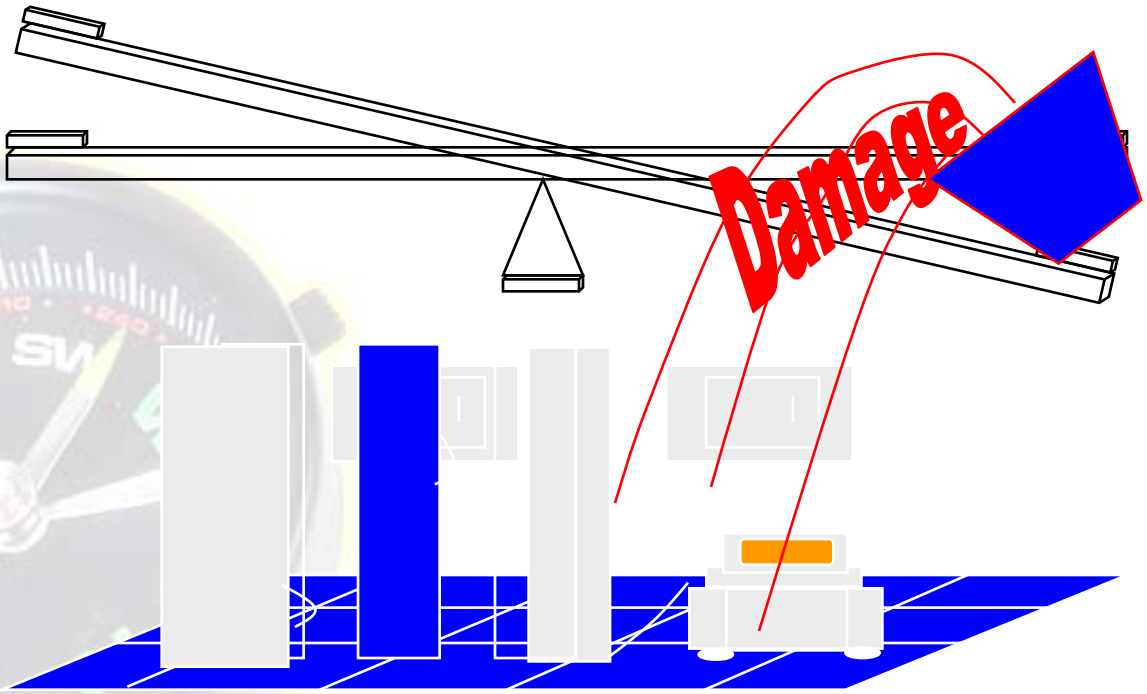
Exploits + Service/Data/Financial Loss = Damage

Controls *minimize probability of* Exploits

Evaluation of expectation of damage must be continuous.

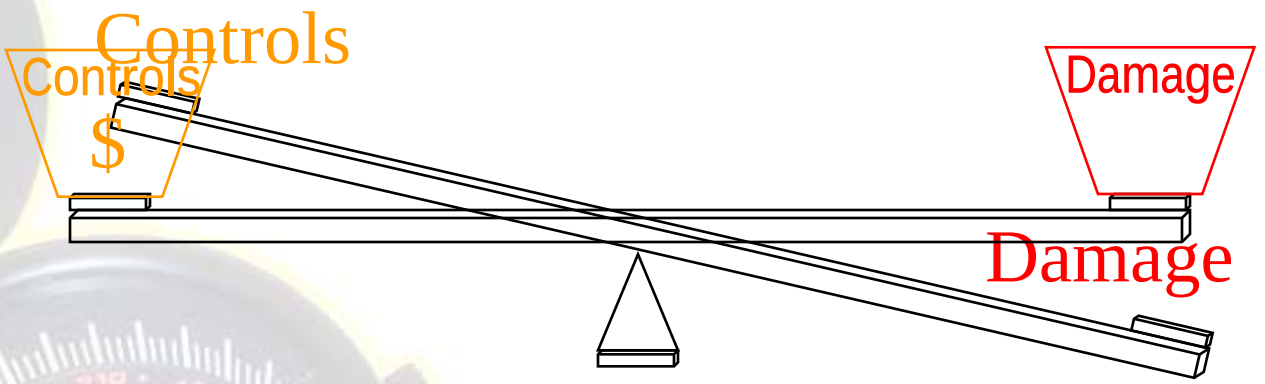
Controls must be proportionate to damage expectation.

Risk/Reward Tradeoff



IT Environment

Value Delivery



IT Environment

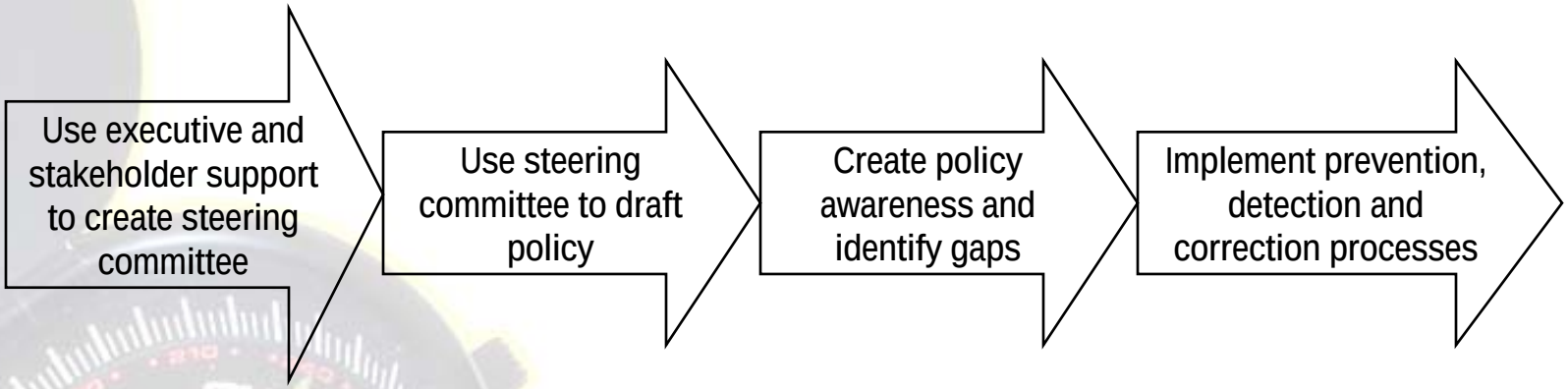
Information Security Strategy

Task 2: Specify the activities to be performed within the InfoSec program.

Process	**Organizational workflow designed to achieve management goals for information protection.**
Metrics	**Measurable artifacts that demonstrate management goals for information protection are met.**

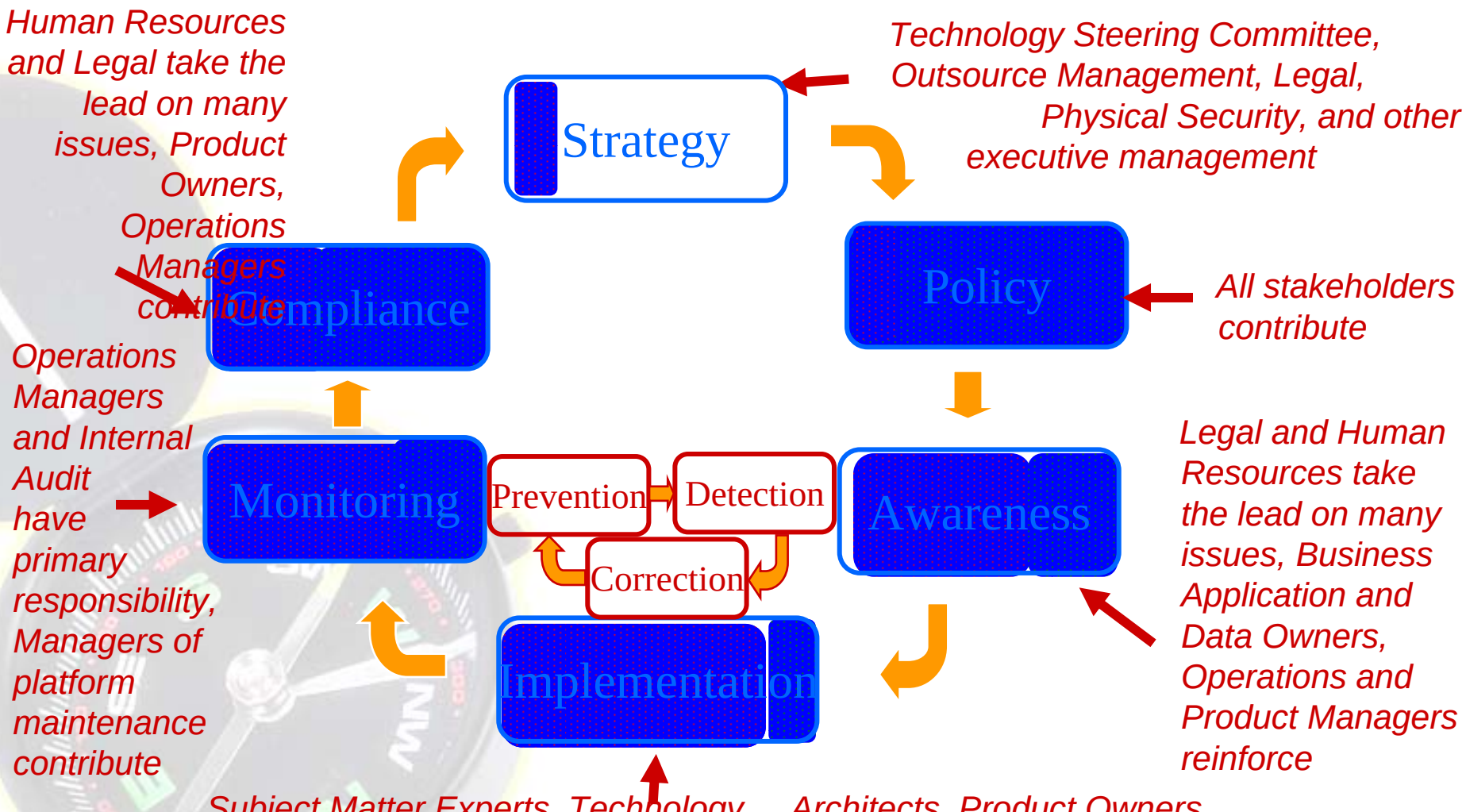
Both must be transparent enough to allow executive/business management to understand where & how support is required to maintain Information Security Objectives.

InfoSec Program Stages



STAGE 1 **STAGE 2** **STAGE 3** **STAGE 4**

Security Management Program Contributors



Human Resources and Legal take the lead on many issues, Product Owners, Operations Managers contribute

Technology Steering Committee, Outsource Management, Legal, Physical Security, and other executive management

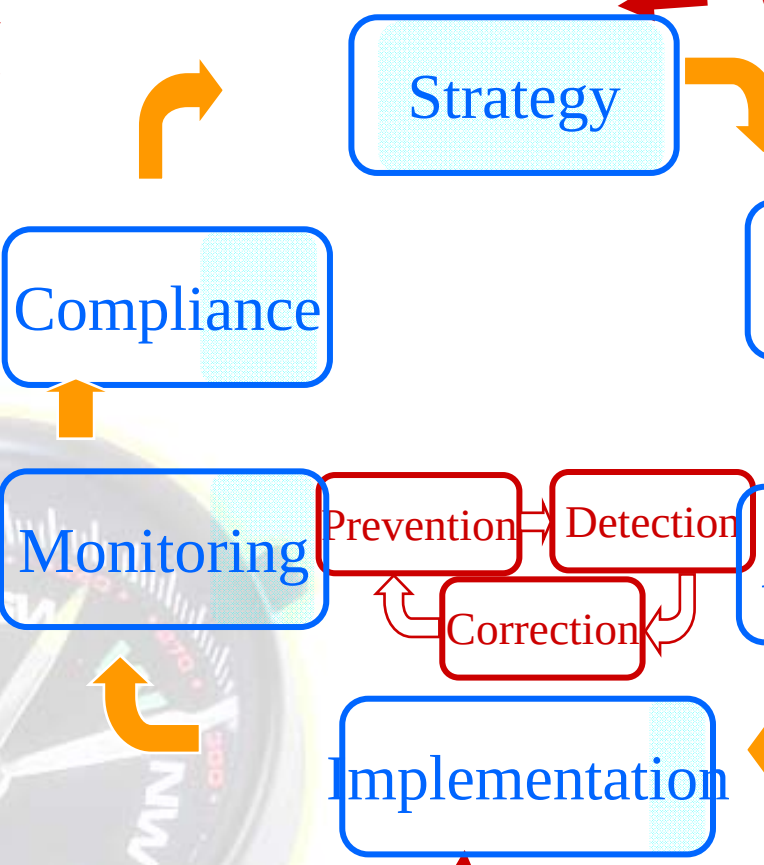
All stakeholders contribute

Operations Managers and Internal Audit have primary responsibility, Managers of platform maintenance contribute

Legal and Human Resources take the lead on many issues, Business Application and Data Owners, Operations and Product Managers reinforce

Subject Matter Experts, Technology Architects, Product Owners, Managers of Platform Maintenance, Systems Administrators, Operations Managers, Executive Assistants

Security Management Program Contributors



Human Resources and Legal take the lead on many issues, Product Owners, Operations Managers contribute

Technology Steering Committee, Outsource Management, Legal, Physical Security, and other executive management

All stakeholders contribute

Operations Managers and Internal Audit have primary responsibility, Managers of platform maintenance contribute

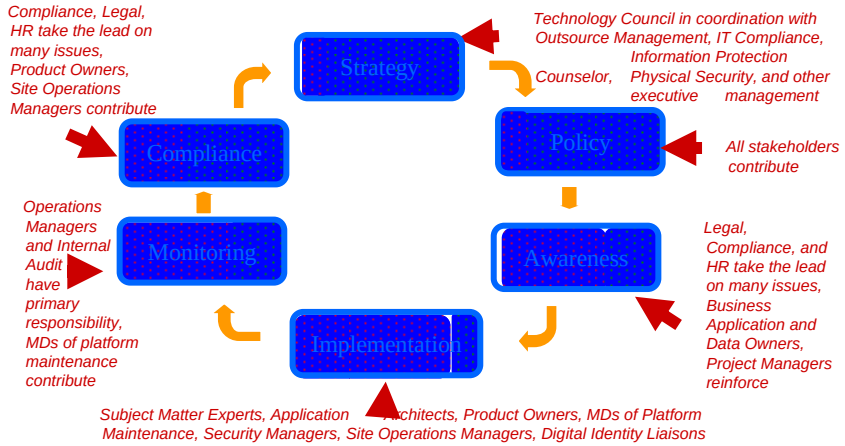
Legal and Human Resources take the lead on many issues, Business Application and Data Owners, Operations and Product Managers reinforce

Subject Matter Experts, Technology Architects, Product Owners, Managers of Platform Maintenance, Systems Administrators, Operations Managers, Executive Assistants

InfoSec Resources

Task 3: Ensure alignment between the InfoSec program & other assurance functions.

- Executive Management Steering Committee
- Chief Risk Officer
- Chief Privacy Officer
- Information Security Manager
- Director of IT Operations
- IT Site Operations Manager
- IT Implementation Management
- IT Subject Matter Experts
- Application Architects
- IT Project Managers
- IT Product Owners
- Security Administrators
- Business Application Owner
- Business Data Owner
- Procurement Manager
- Compliance Manager
- Physical Security Organization



InfoSec Roles and Responsibilities

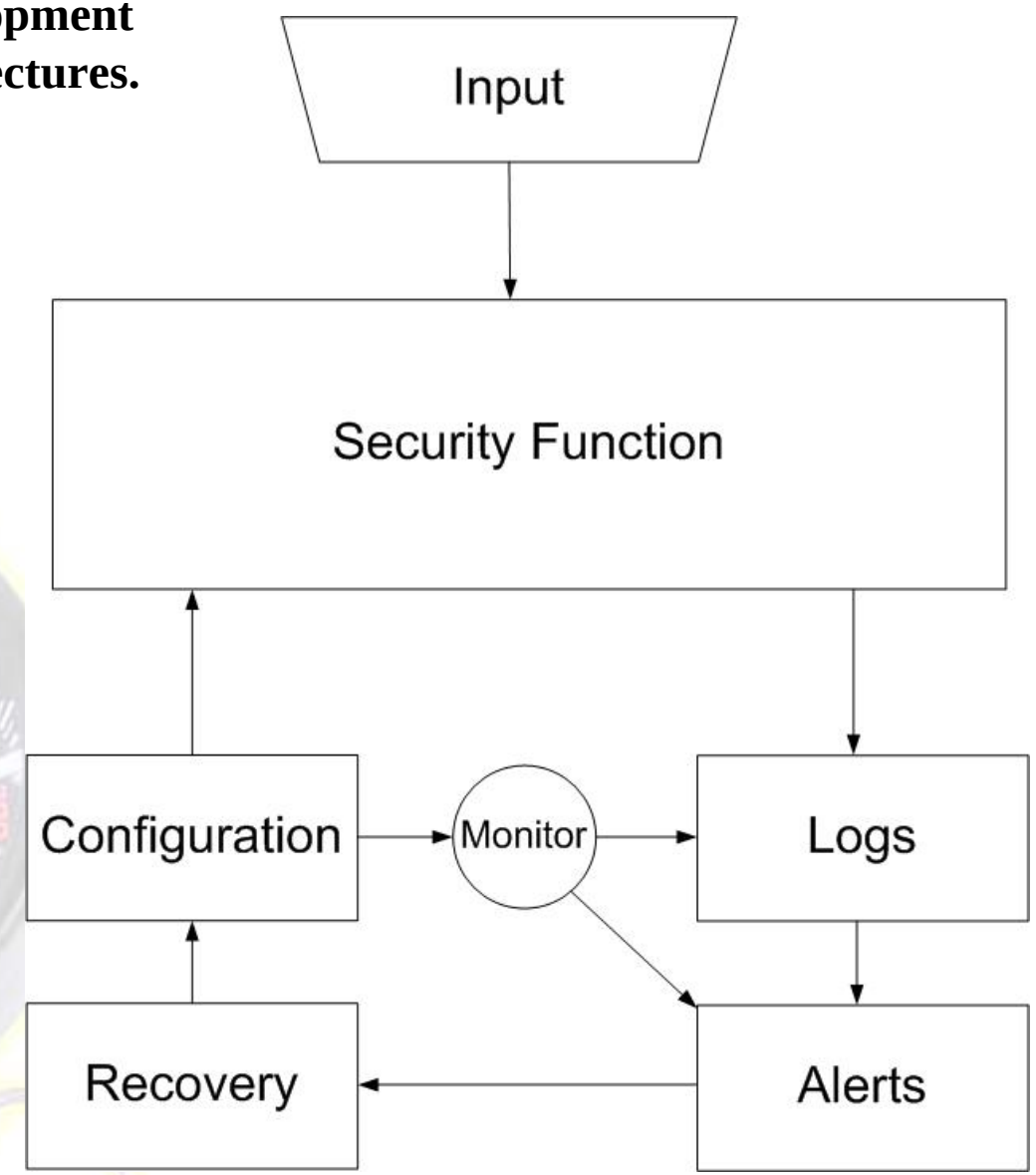
Task 4: Identify internal & external resources required to execute the InfoSec program

Where a person performs this role:	An associated InfoSec process responsibility is:	A sample key performance indicator is:
Manages the lifecycle of IT **applications** and platforms	Security Review Participation	Security-policy-compliant systems configuration
	Security Requirements Capture	Business requirements for confidentiality, integrity, and availability are documented
	Application Security Design	Technical implementation plans for meeting business process security requirements
	Change Control	Secure archive, retrieval, and compilation of organization-maintained source code and product customizations
	Security Upgrade Management	Testing and application of security software fixes
Procures IT services	Security Requirements Capture	Formal requirements for security in all Requests for Product Information and Proposals
	Contract Requirements	Business requirements for confidentiality, integrity, and availability in information service provider and technology maintenance contracts

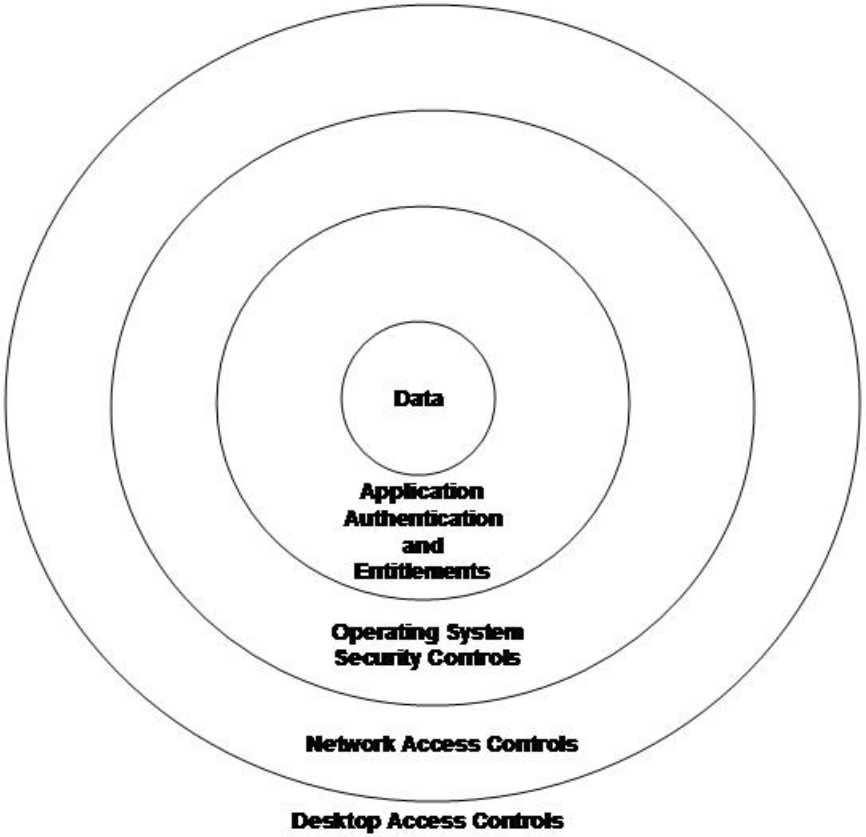
Given "realms" of business operation, resource identification involves not only specifying areas of responsibilities, but also making use of existing business and operational process.

Segue into Architecture

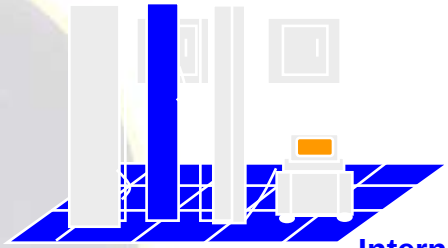
Task 5: Ensure the development of InfoSec architectures.



Security Controls Design



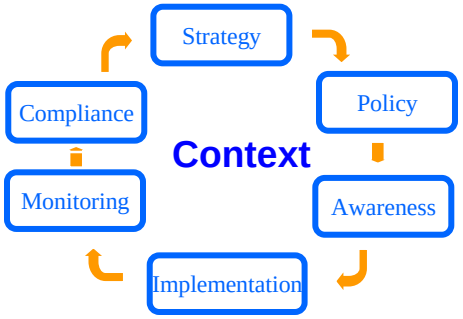
Efficiency and Effectiveness Outlook



Internal Alerts

Inventory

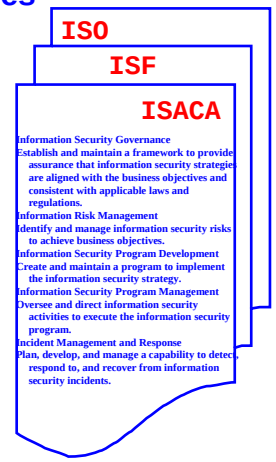
Synthesis



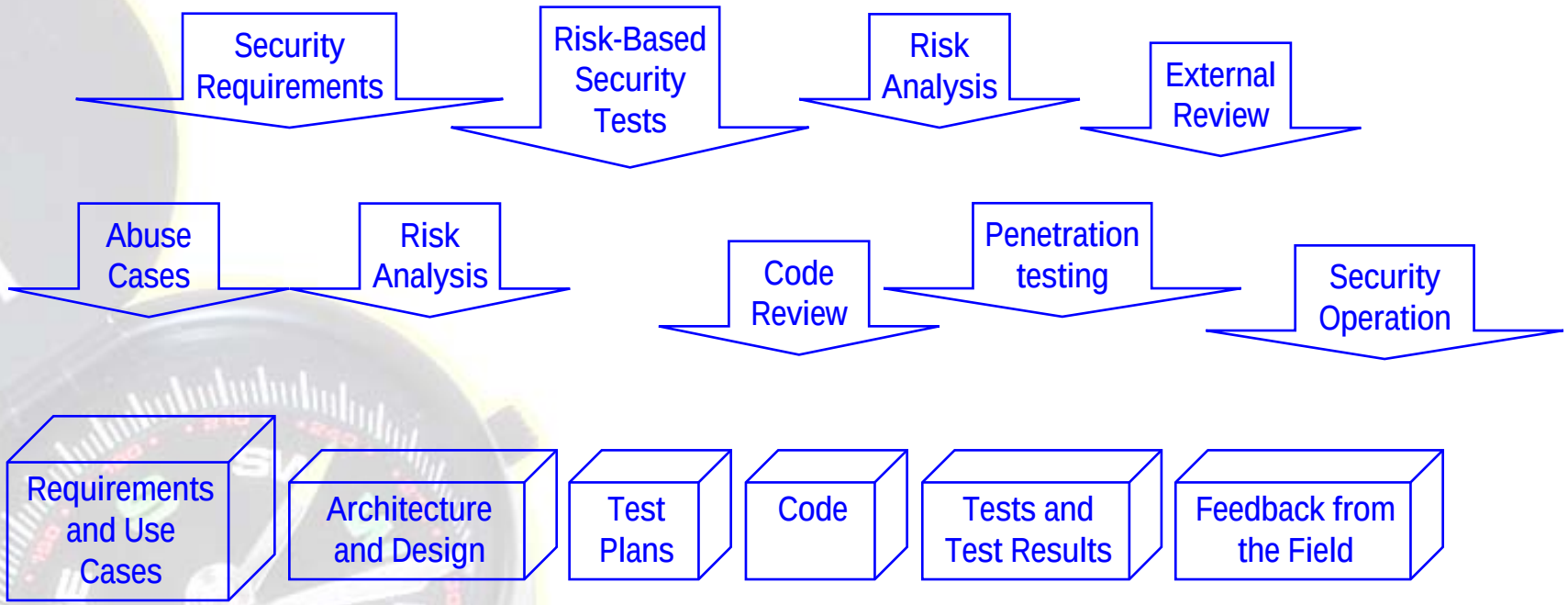
External Alerts

```
From: Alert Service - Vulnerabilities
Subject: VULNERABILITY ALERT!!!
Date:    5/10/2006 1:20 PM
Summary: A buffer overflow has been
      discovered in the XYZ software that
      can be exploited to gain
      administrative access.
Impact: Denial of service; possible code
      execution
Severity: 2 (Medium)
Corrective Action: Administrators are
      advised to upgrade to the latest
      version of XYZ, Version 12.3,
      available at: http://www.xyz.com (
      http://www.xyz.com )
END ALERT
```

Best Practices

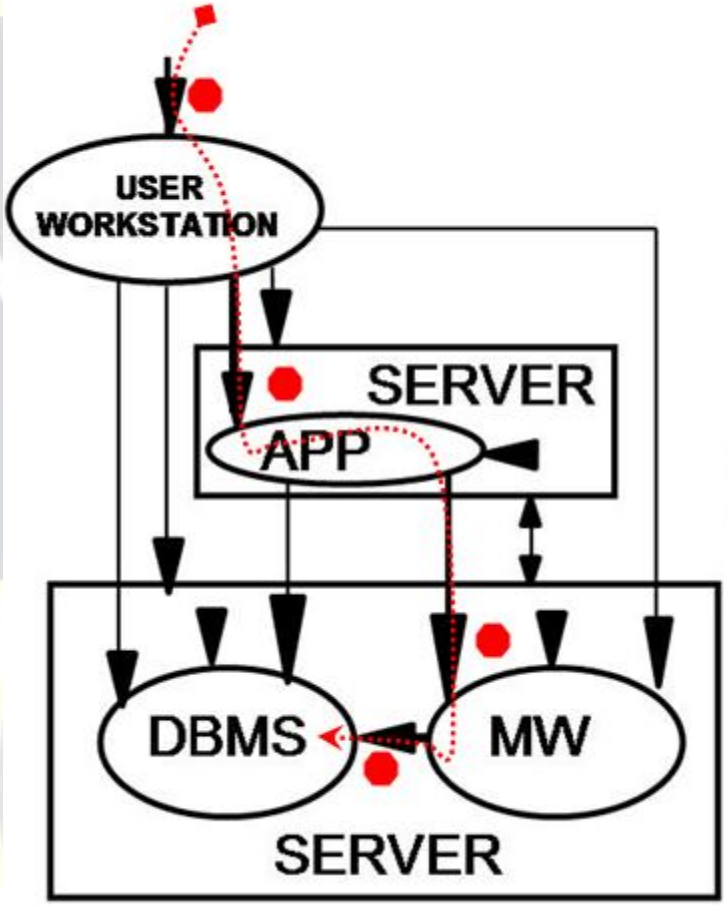


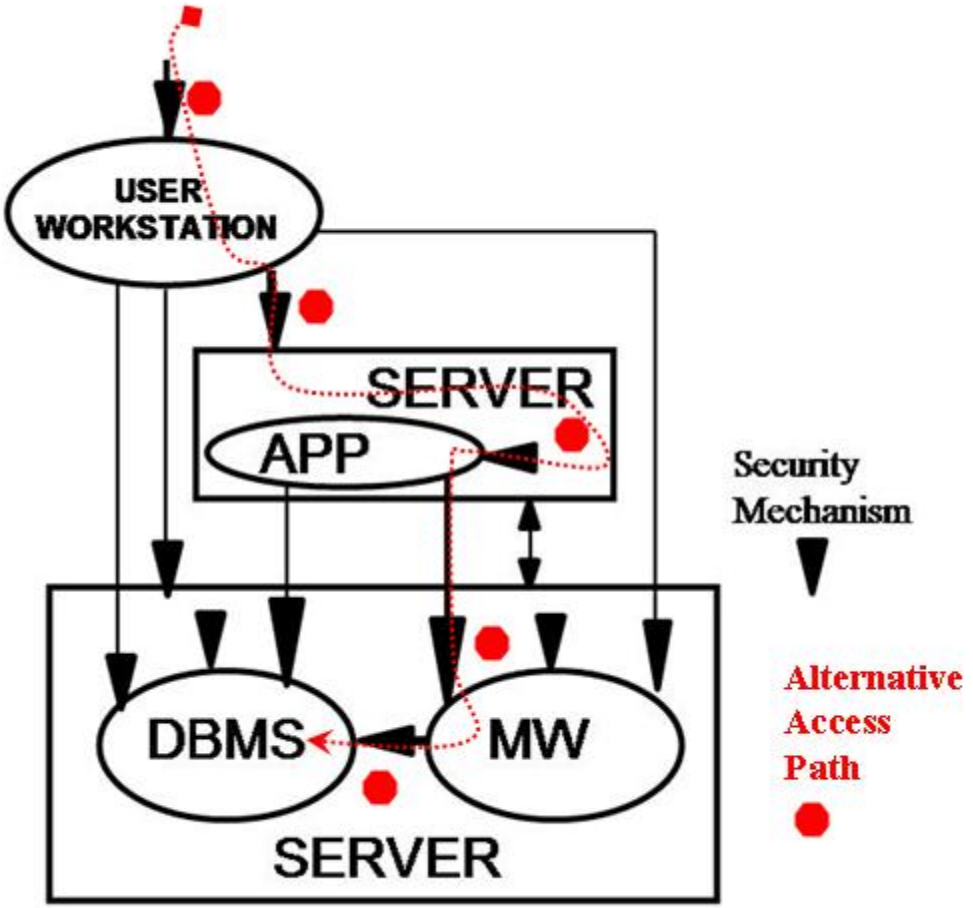
Best Practices Comparison



Source: Software Security

Detailed Control Design/Assessments





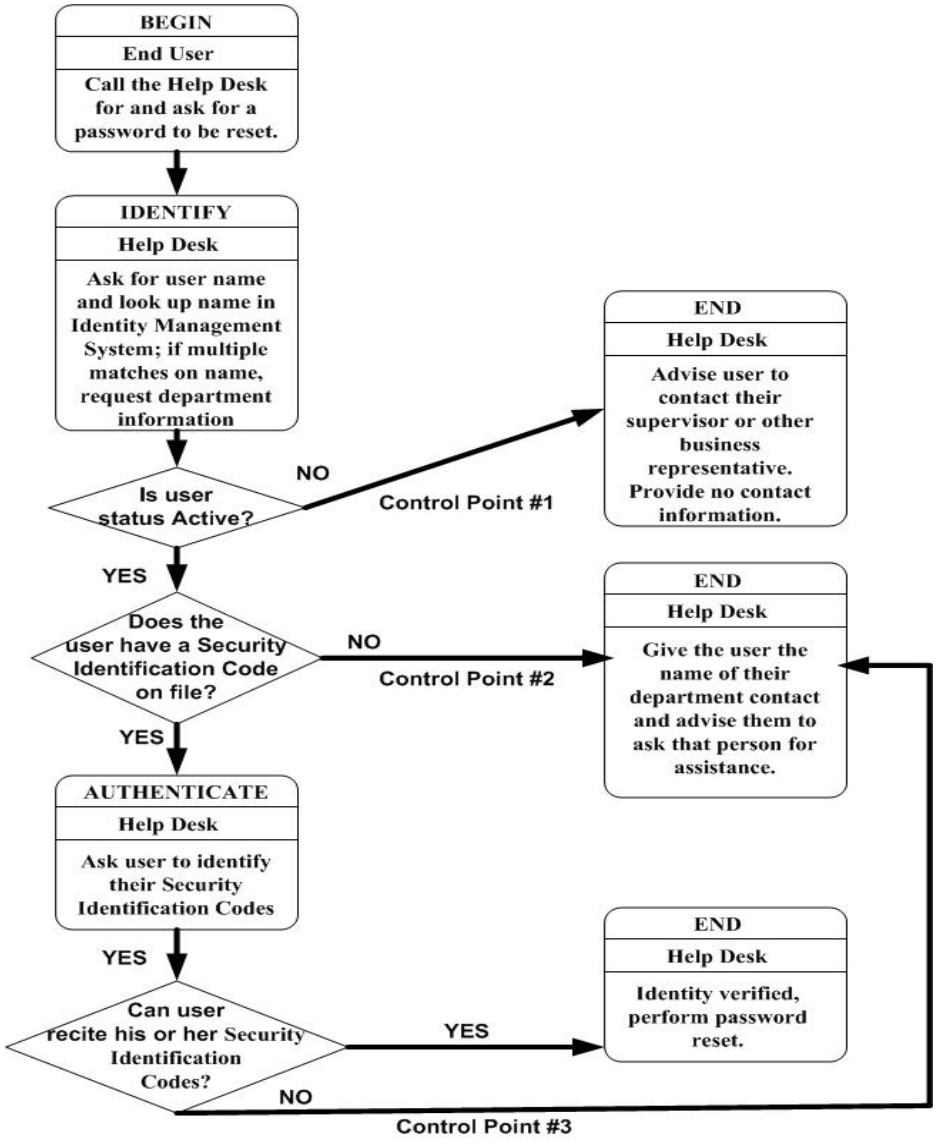
Security Awareness

Task 6: Establish, communicate, & maintain InfoSec policies that support the InfoSec strategy.

- Basic - applies to all, even if there is just one, e.g. Google Appliance, Stratus
- Architectural - warranted where data exposure warrants redundant controls
  - Database Management Systems
  - Network
  - Telecommunications etc etc etc
- Operating System Platform - warranted where multiple instances warrant consistency
  - UNIX
  - Microsoft
  - z/OS etc etc etc
- Situational - applies to process more than technology
  - Internet and Third Party
  - Personal Computing
  - Security Service Level Agreement
  - Vendor Access etc etc etc
- Application - applies to business applications whether developed in house or externally

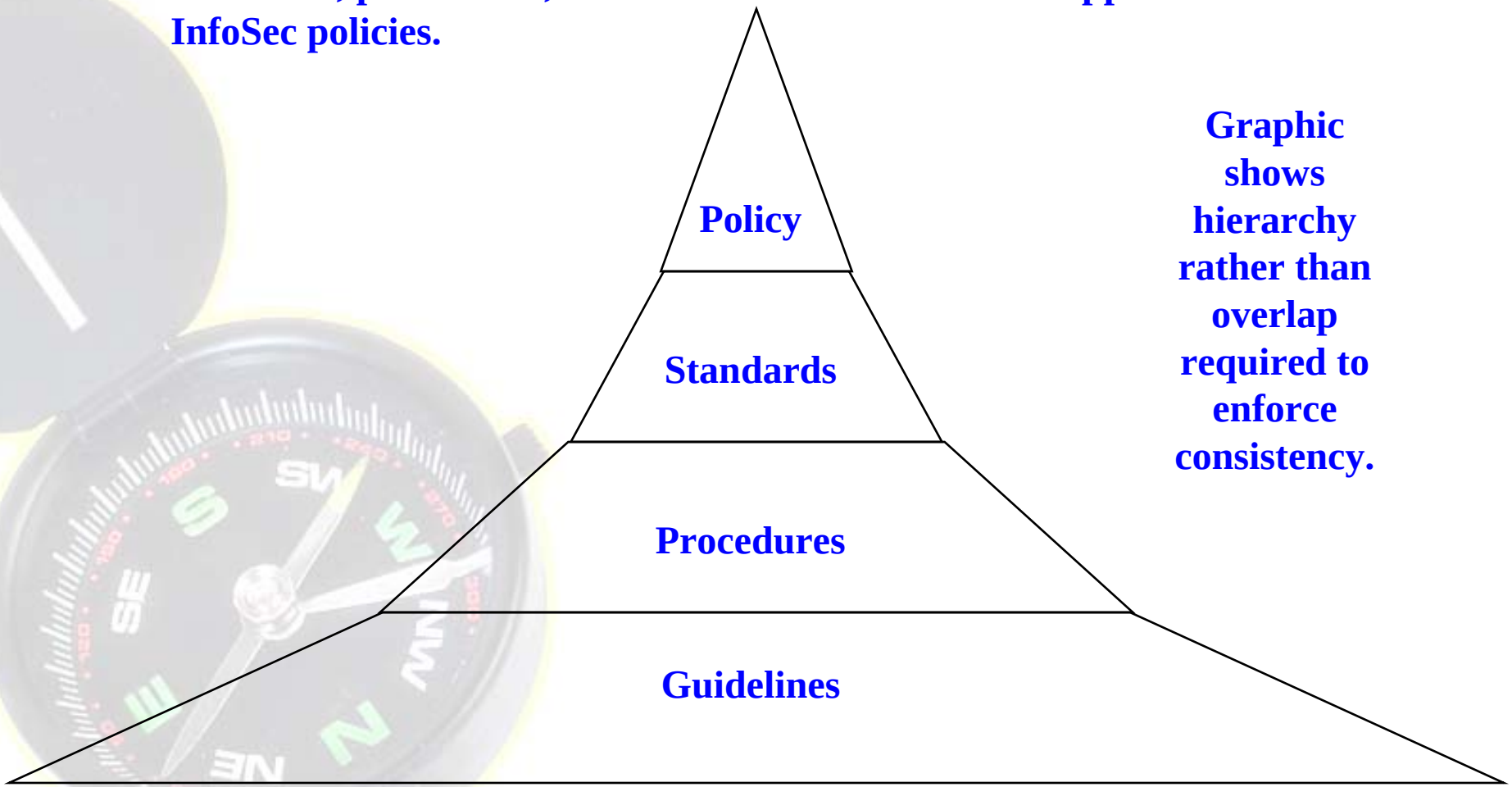
Security Training

Task 7: Design and develop a program for InfoSec awareness, training, & education.



Layers of support

Task 8: Ensure the development, communication, & maintenance of standards, procedures, & other documentation that support InfoSec policies.



Graphic shows hierarchy rather than overlap required to enforce consistency.

Security Controls Implementation

Task 9: Integrate InfoSec requirements into the organization's processes & life cycle activities.

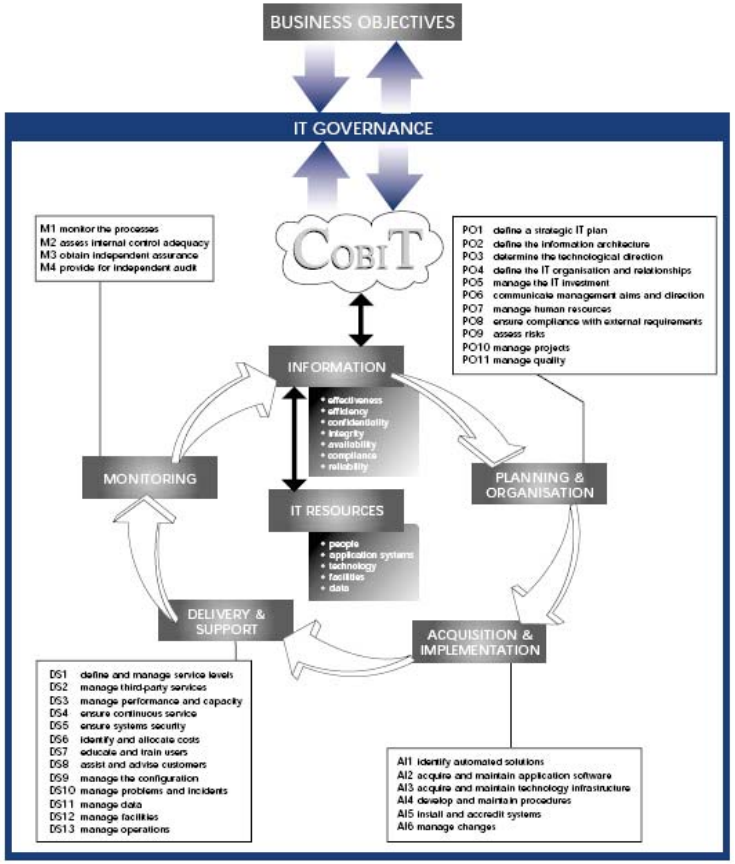
Plan-Do-Check-Correct *– The COBIT version*

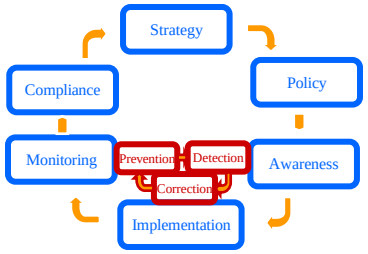
Plan-Secure-Confirm-Remediate *– A popular Software Vulnerability guide version*

Prepare-Detect-Respond-Improve *– Carnegie Mellon's CERT version*

Observe-Orient-Decide-Act *– A US Military version*

Restrict-Run-Recover *– A Big 4 consultant's version*





Security Service-level Agreements

Task 10: Develop a process to integrate InfoSec controls into contracts.

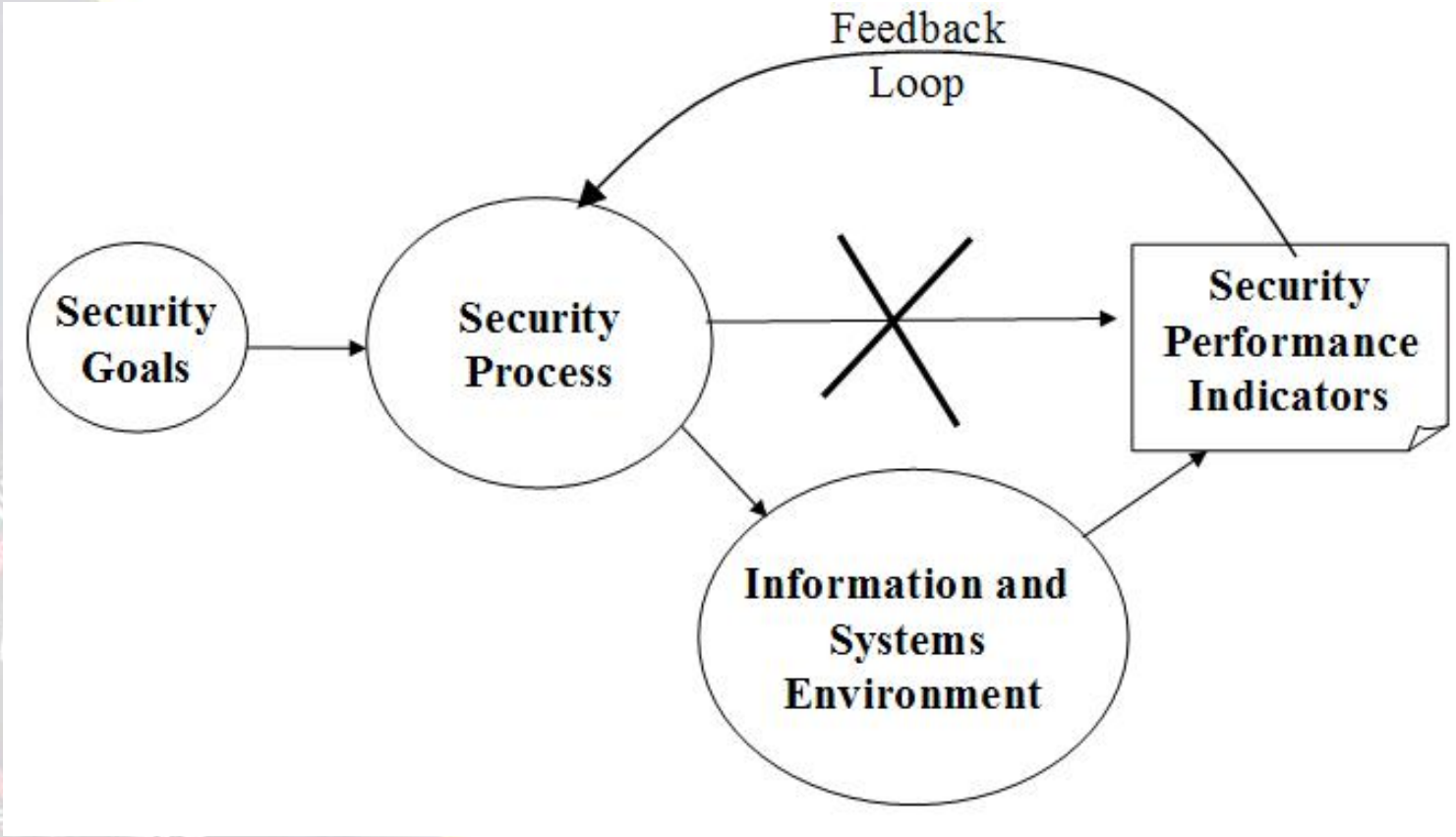
Minimum Security Requirements for XXX

Definition: Potential Access Device – Any device within the service provider network that facilitates the transport, storage, or processing of <My Organization's> data and any device within the service provider network that may be used to access such a device, either directly or via a network connection.

1. Service Provider will provide physical security to Potential Access Devices. Only those Service Provider or Service Provider subcontractor employees whose job functions require physical access to Potential Access Devices should be granted such access.
2. The default settings on all network equipment, operating systems, and applications that are Potential Access Devices shall be to deny all access.
3. The Service Provider shall use industry-standard anti-virus and anti-spyware techniques to protect potential access devices from tampering and hacking attempts.
4. Wherever the Service Provider allows access to the application from a network that hosts systems not administered by the Service Provider (e.g., the Internet, a private line customer, etc), the Service Provider shall implement a firewall to help prevent unauthorized access to the Software or the administered systems, which firewall will consist of state of the art hardware and software designed and properly configured to control or limit access to Potential Access Devices.

Security Metrics

Task 11: Establish metrics to evaluate the effectiveness of the InfoSec program.

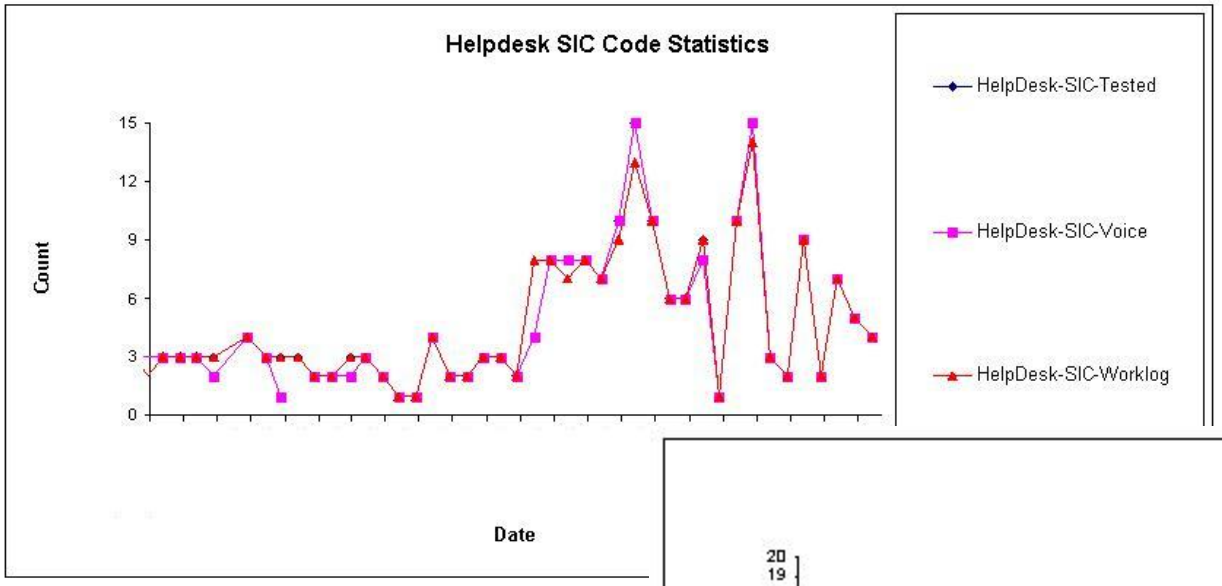


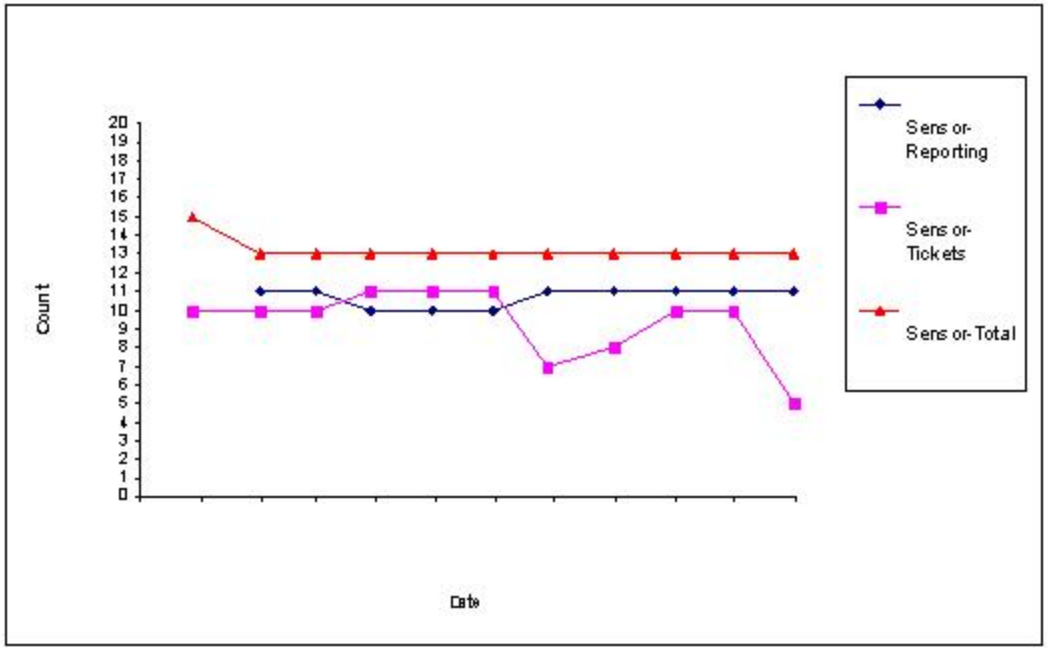
Performance Measurement

Cement the relationship between the InfoSec Program and IT Governance with meaningful report, such as:

Risk Management:	Stability and auditability of prevention measures. Incident Response and Recovery Preparedness.
Value Delivery:	Earned value analysis on projects plus overall trend analysis on the ISM portfolio, complete with updated projections based on variance analysis.
Resource Management:	Staffing, technology and organizational dependency data used in analysis of facilitation and/or impact to the security program.
Performance measurement:	Metrics that verify that control activities are achieving desired results. For example, an automated monitoring of security configuration and feedback on user anomaly reports

Security Metric Examples





Discussion

INFORMATION SECURITY MANAGEMENT CONFERENCE

ISACA
Serving IT Governance Professionals