

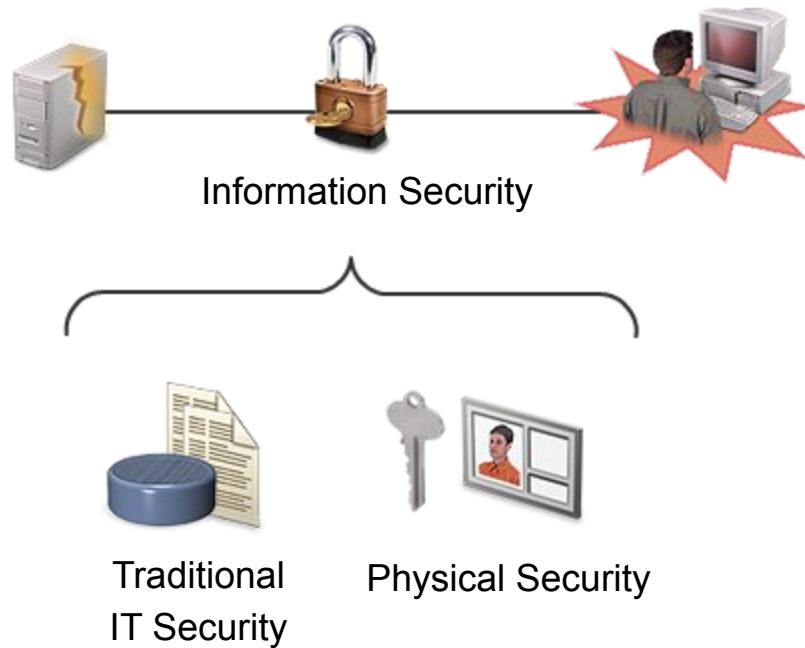
Course Outline

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Implementation
- Information Security Program Management
- Incident Management and Response

Information Security Governance

- Develop an Information Security Strategy
- Align Information Security Strategy with Corporate Governance
- Identify Legal and Regulatory Requirements
- Justify Investment in Information Security
- Identify Drivers Affecting the Organization
- Obtain Senior Management Commitment to Information Security
- Define Roles and Responsibilities for Information Security
- Establish Reporting and Communication Channels

Information Security



Business Goals, Objectives, and Functions



**Business
Goals**

Statements of the intent of the business



**Business
Objectives**

Specific targets or outcomes that the organization wants to achieve



**Business
Functions**

Activities that an organization performs to support an established business goal or objective

Business Goals and Information Security

To facilitate information security and business goals:

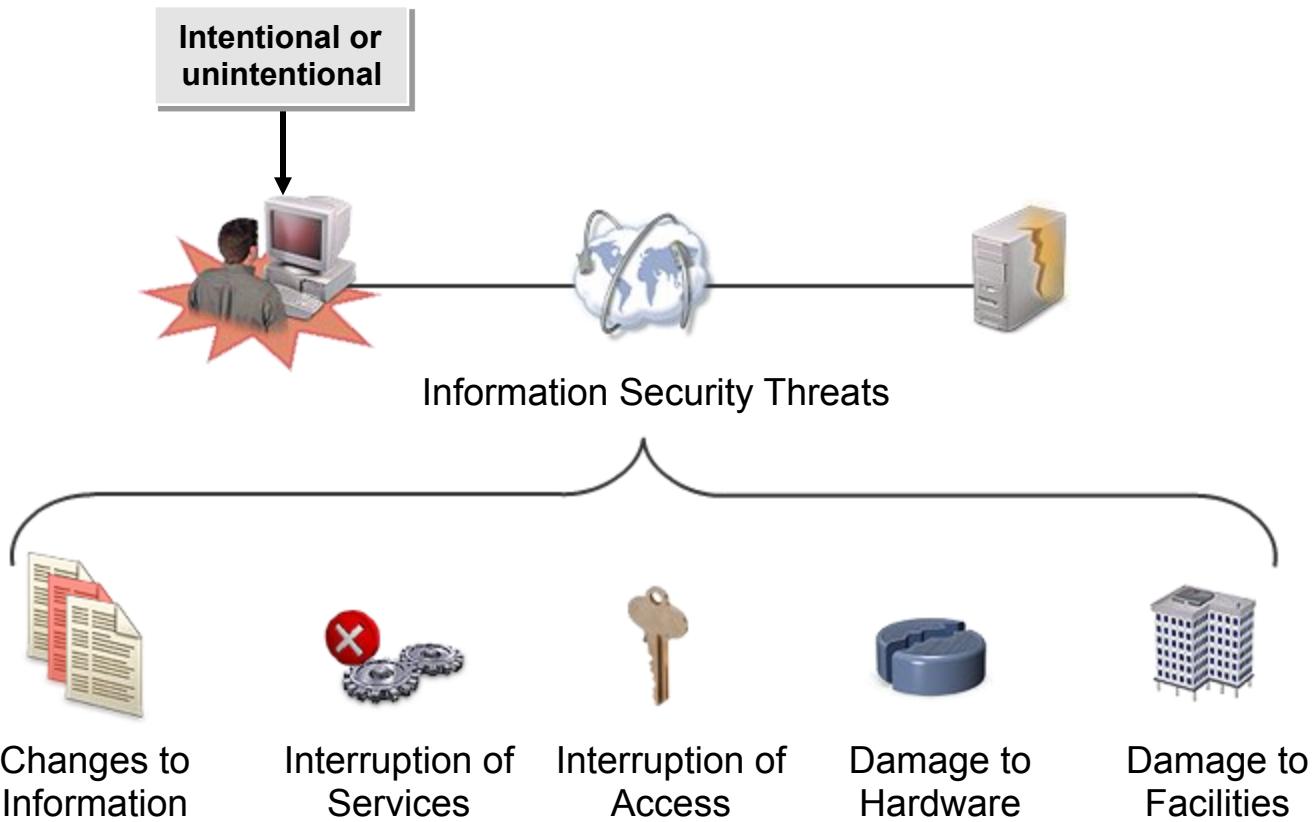
- ❑ Organizational management must support the information security infrastructure.
- ❑ Stakeholders must communicate to ensure goals:
 - Are coordinated.
 - Do not conflict.
 - Are advantageous to each other.
- ❑ The goals must be aligned to achieve executive buy-in and participation from the entire organization.



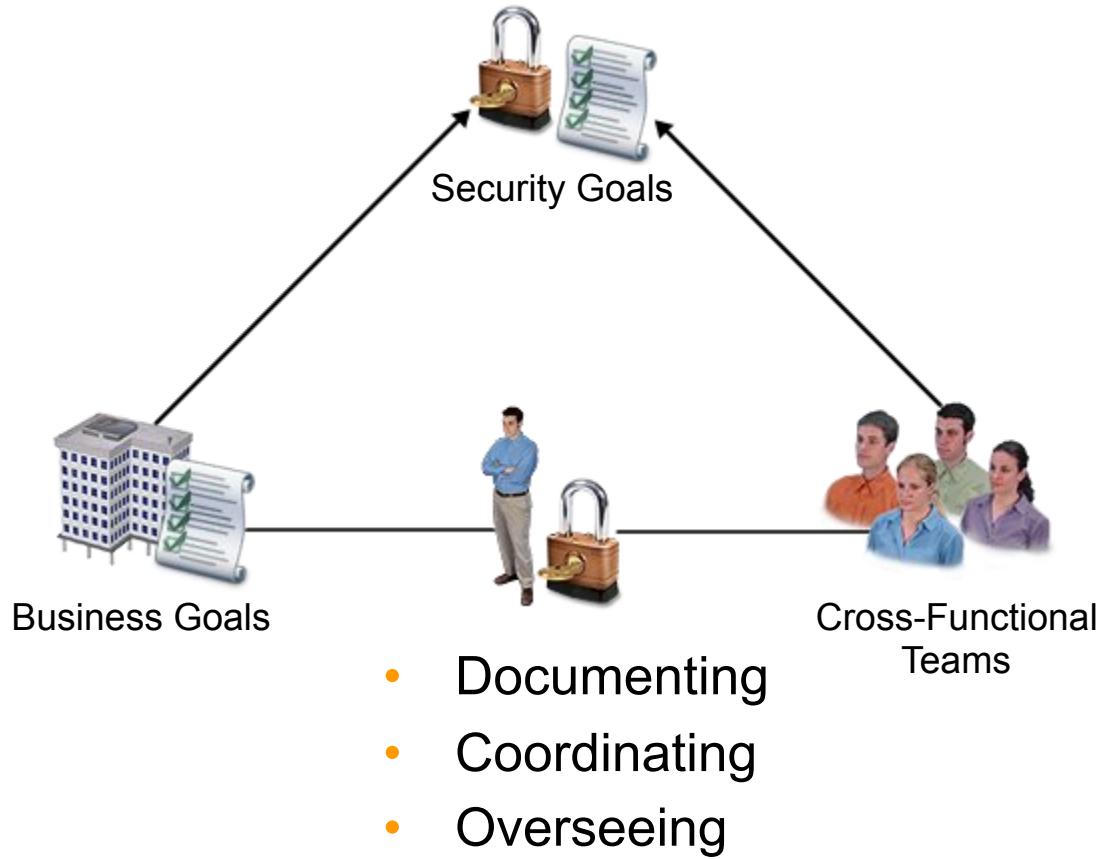
Information Security

Business Goals

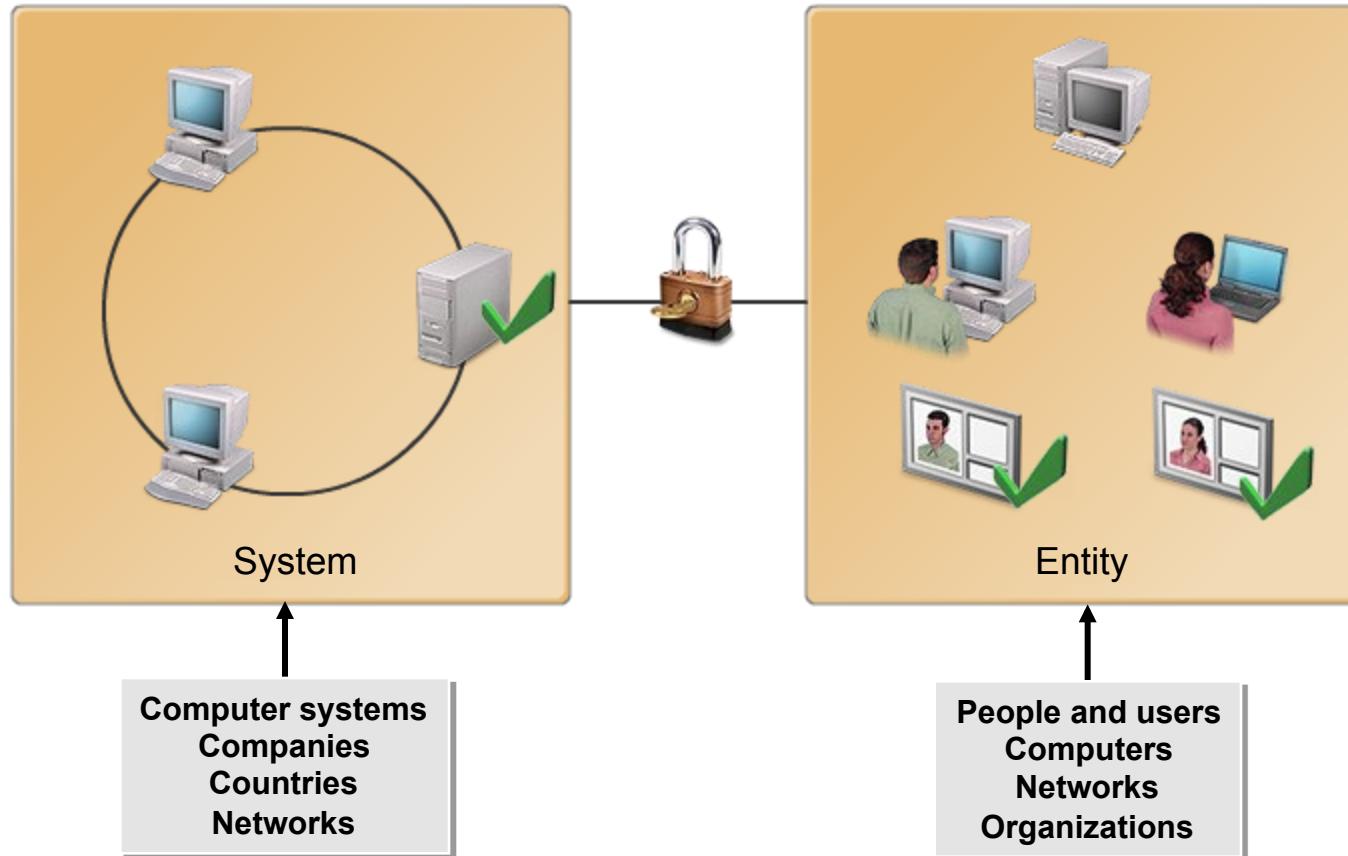
Information Security Threats



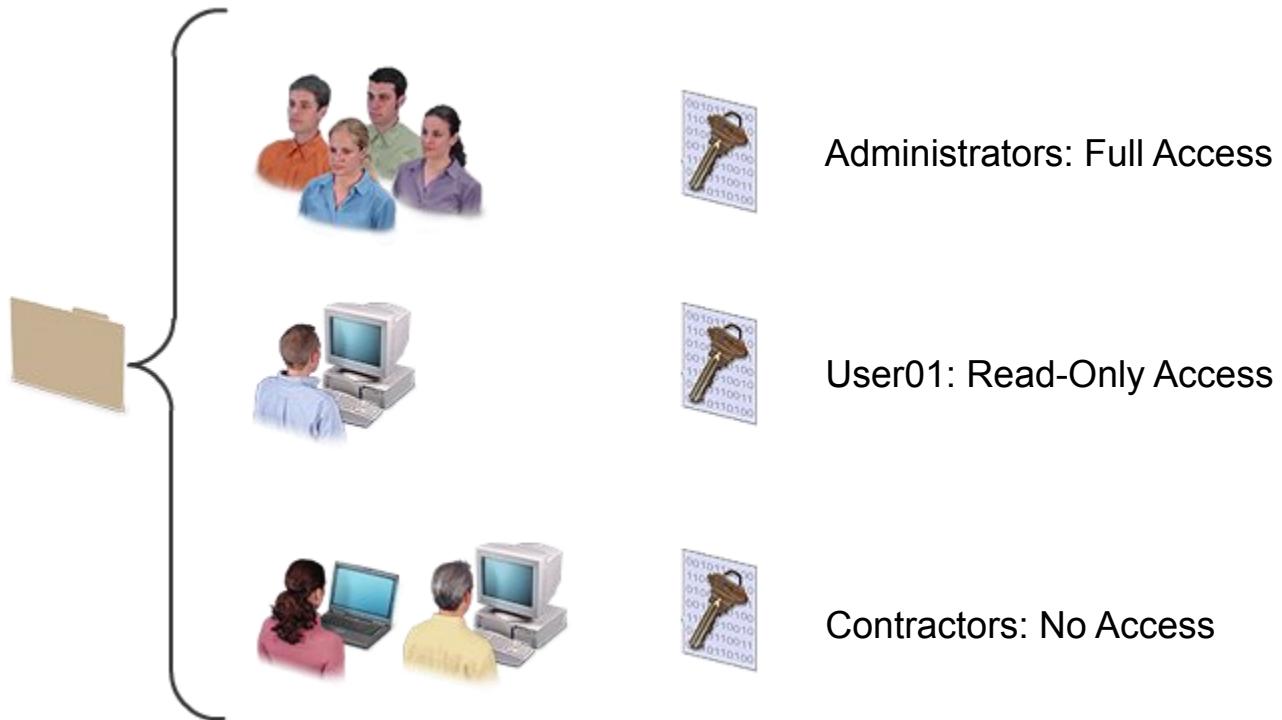
Information Security Management



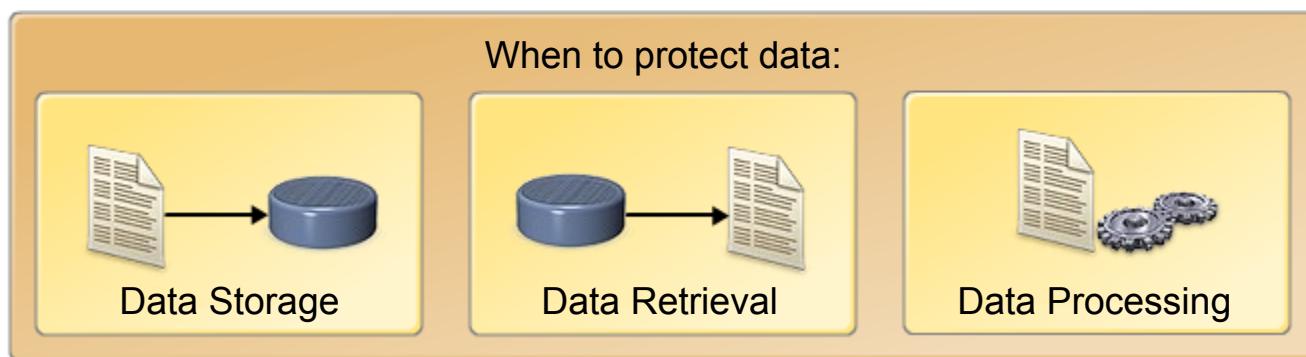
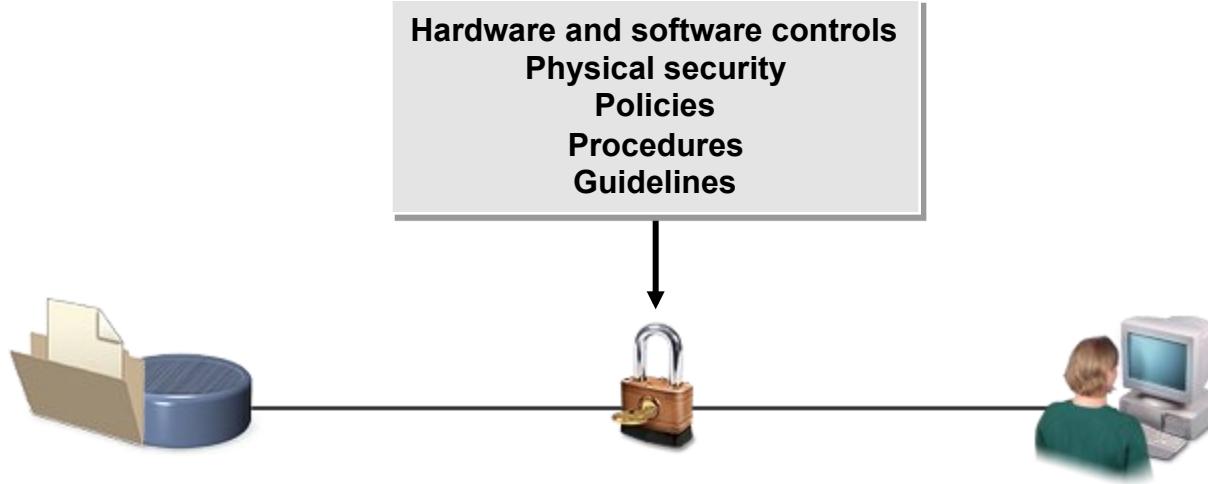
Identity Management



Access Management



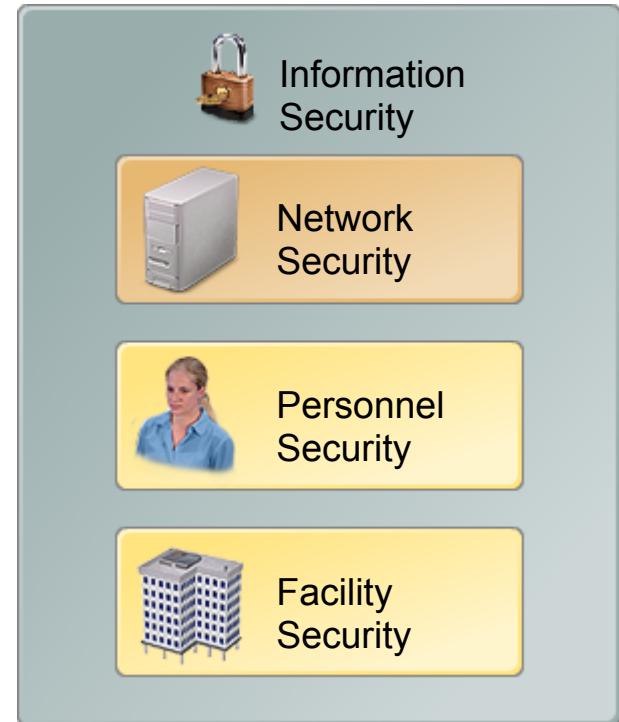
Data Protection



Network Security

Network security includes:

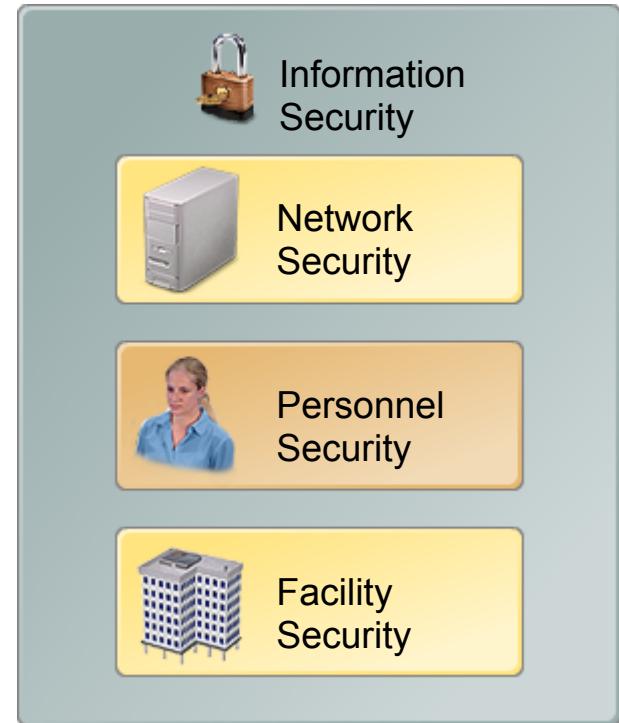
- The protection of networks and services from:
 - Unauthorized modification.
 - Destruction.
 - Disclosure.
- Assurance that the network performs critical functions.
- Data integrity and availability.



Personnel Security

Personnel security:

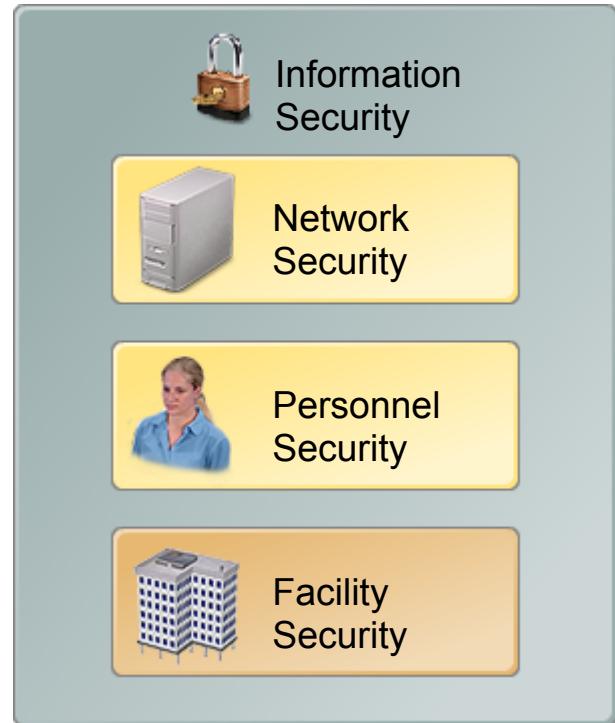
- Is the set of procedures to control access to assets.
- Ensures the right person is in the right position with the right qualifications.
- Begins at the pre-employment state.
- Continues with principles of separation of duties and least privilege.
- Includes a comprehensive training program.
- Should be addressed in organizational policies and procedures.



Facility Security

Facility security:

- ❑ Is the implementation of control mechanisms to restrict physical access.
- ❑ Involves assuring the reliability of critical infrastructure elements.
- ❑ May be challenged by:
 - Facilities intrusions.
 - Electrical grid failures.
 - Fire.
 - Personnel illnesses.
 - Data network interruptions.



Security Compliance and Standards

Area of Concern	Description
Government regulations	<ul style="list-style-type: none"><input type="checkbox"/> HIPAA<input type="checkbox"/> FISMA<input type="checkbox"/> SOX<input type="checkbox"/> New York State Information Breach and Notification Act<input type="checkbox"/> Additional state and local regulations within the U.S.<input type="checkbox"/> Additional national and local regulations outside of the U.S.
Industry standards	<ul style="list-style-type: none"><input type="checkbox"/> COBIT<input type="checkbox"/> ISO<input type="checkbox"/> IEC 27002<input type="checkbox"/> SABSA<input type="checkbox"/> GASSP<input type="checkbox"/> GAISP

Information Security Strategy



Inputs and Outputs of the Information Security Strategy

Subset	Description
Inputs	<p>Dictated by executive management, CISO, ISSG, or other senior management.</p> <ul style="list-style-type: none"><input type="checkbox"/> Business drivers and objectives<input type="checkbox"/> Current state of information security<input type="checkbox"/> Current business processes<input type="checkbox"/> Current risk assessment analyses<input type="checkbox"/> Regulatory, legal, or standards requirements<input type="checkbox"/> Inventory and valuation of information assets<input type="checkbox"/> Estimated timeline for implementation
Outputs	<ul style="list-style-type: none"><input type="checkbox"/> Clearly defined goals and objectives for the strategy<input type="checkbox"/> Strategic alignment for organizational and security objectives<input type="checkbox"/> Effective risk management<input type="checkbox"/> Value delivery<input type="checkbox"/> Clear definition of success<input type="checkbox"/> Guidelines for reporting and metric generation

Processes in an Information Security Strategy



Information Security
Strategy Processes

Risk Management Policy

Incident Response Policy

Information Classification Policy

Implement Specific Goals or Conditions

Reporting and Tracking Metrics

Managing Identities and Permissions

Education and Training Programs

People in an Information Security Strategy



Board of
Directors



Executive
Management



Information Security
Oversight Group



CISO



Information
Security
Personnel



Auditors



Individual
Contributors



Customers

Technologies in an Information Security Strategy

Information security strategy technologies include:

- Physical and logical access controls.
- Physically redundant systems (power and HVAC).
- Network firewalls.
- Physical and network IDSSs.
- Anti-virus and anti-spyware.
- Data encryption techniques.
- Remote access and VPNs.
- Digital signatures.
- Facility and network state monitoring.



Logical and Physical Information Security Strategy Architectures

Architecture Type	Description
Physical architecture	<ul style="list-style-type: none">❑ Deals with physical layout❑ Locations of network resources, facility features, and physical security controls❑ Examples: location of network cables, door locks, fences, security doors, and redundant systems
Logical architecture	<ul style="list-style-type: none">❑ Refers to processes, procedures, guidelines, and software controls❑ Examples: secure destruction of documents, network access restrictions, and reporting processes

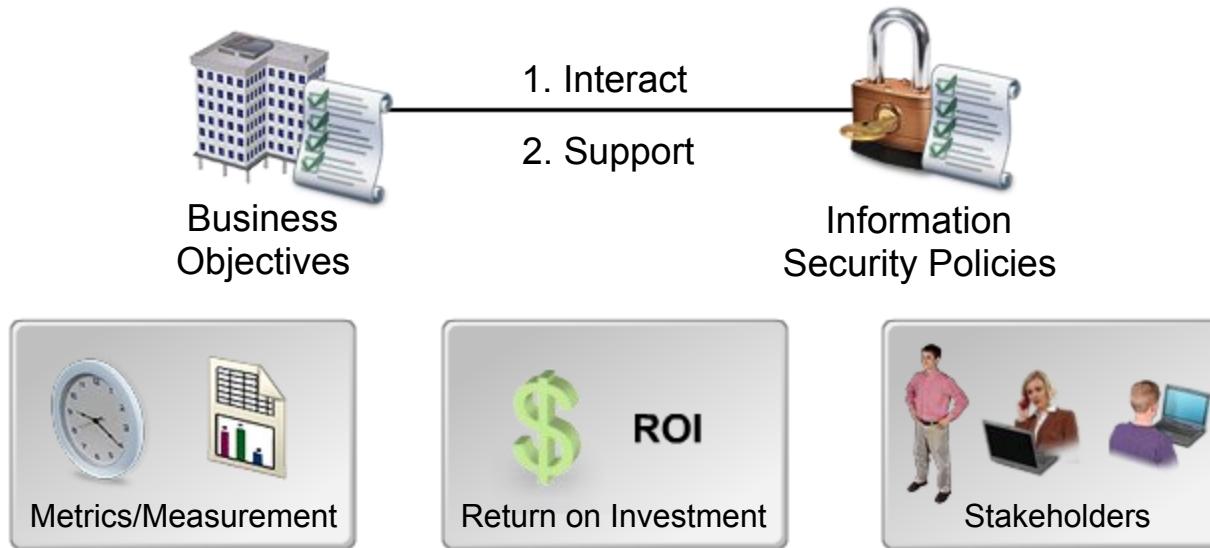
Information Security and Business Functions

Information security:

- ❑ Enables the achievement of business objectives by supporting business functions
- ❑ Must be integrated with all business functions to ensure success



Information Security Policies and Enterprise Business Objectives



Each information security solution should be directly attributable to at least one business goal.

International Standards for Information Security Management

- ISO 27000
- COBIT
- ITIL
- GASSP/GAISP
- Common Criteria (ISO/IEC 14508)

ISO/IEC 27000 Standards



ISO/IEC 27000
Standards

ISO - International Organization for Standardization

IEC - International Electrotechnical Commission

International Information Governance Standards

- OCEG
- CMMI
- Balanced Scorecard
- SABSA

Information Security Governance Standards in the U.S.

- SOX
- HIPAA
- GLBA
- FISMA
- COSO
- NIST SP800 Series

Methods of Coordinating Information Security Activities

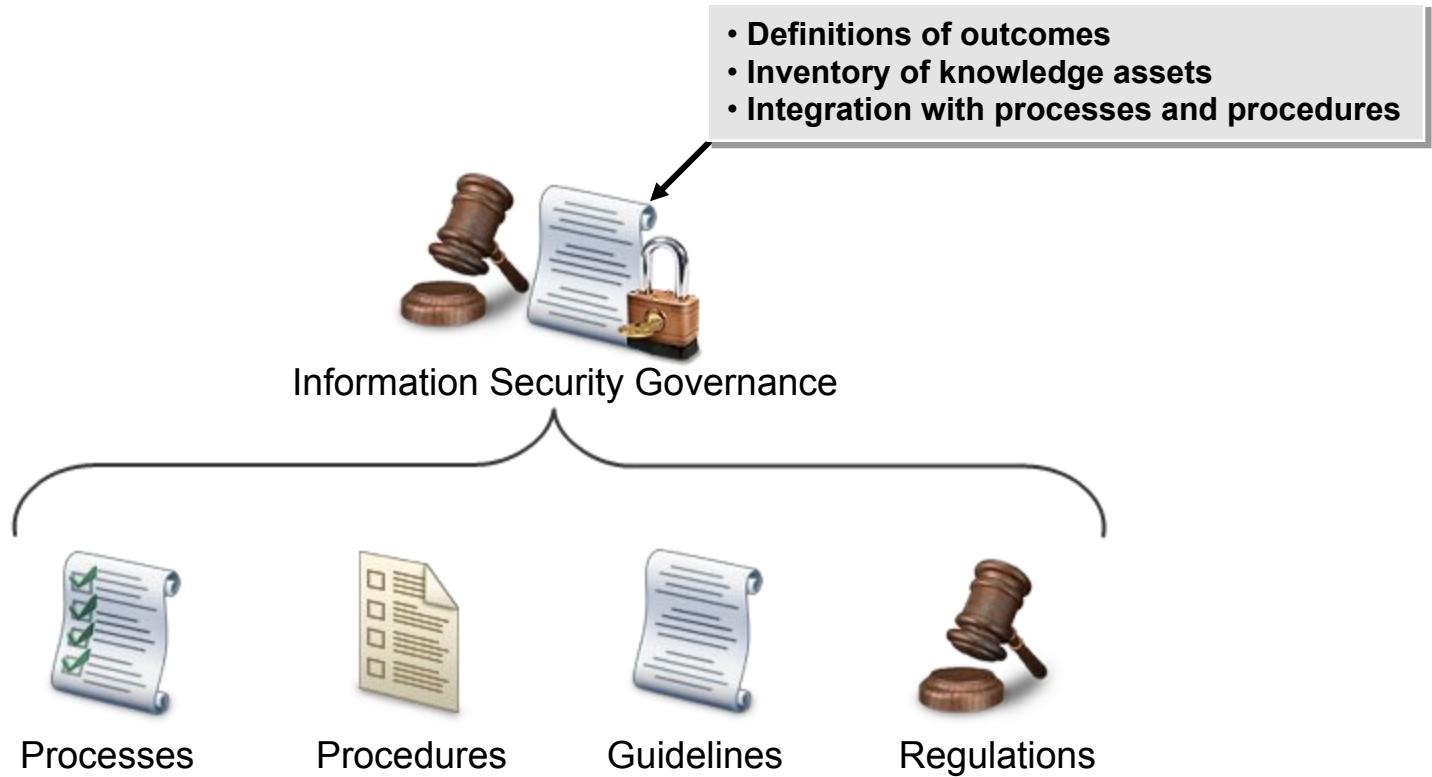


How to Develop an Information Security Strategy

To develop an information security strategy:

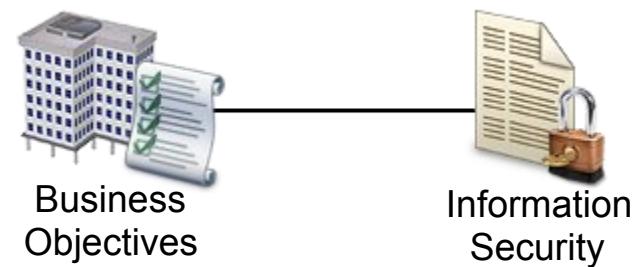
- Define the desired future state of the organization.
- Establish goals and objectives for the strategy.
- Establish objectives to define and control acceptable levels of risk.
- Define a road map for implementing the strategy.
- Locate and identify all information assets.
- Classify information assets.
- Determine the value of information assets.
- Leverage resources.
 - Policies, standards, and procedures, among others
- Be aware of constraints.
 - Legal, physical, and financial, among others

Information Security Governance



Role of Information Security in Governance

- Perform risk assessment
- Determine acceptable risk
- Integrate processes, procedures, and controls
- Plan training programs



Scope of Information Security Governance

Information security governance:

- Affects financial information, personnel files, inventory systems, workstations, access controls, and network security.
- Aims to integrate, streamline, and provide oversight.
- Increases efficiency and compliance.
- Reduces costs.



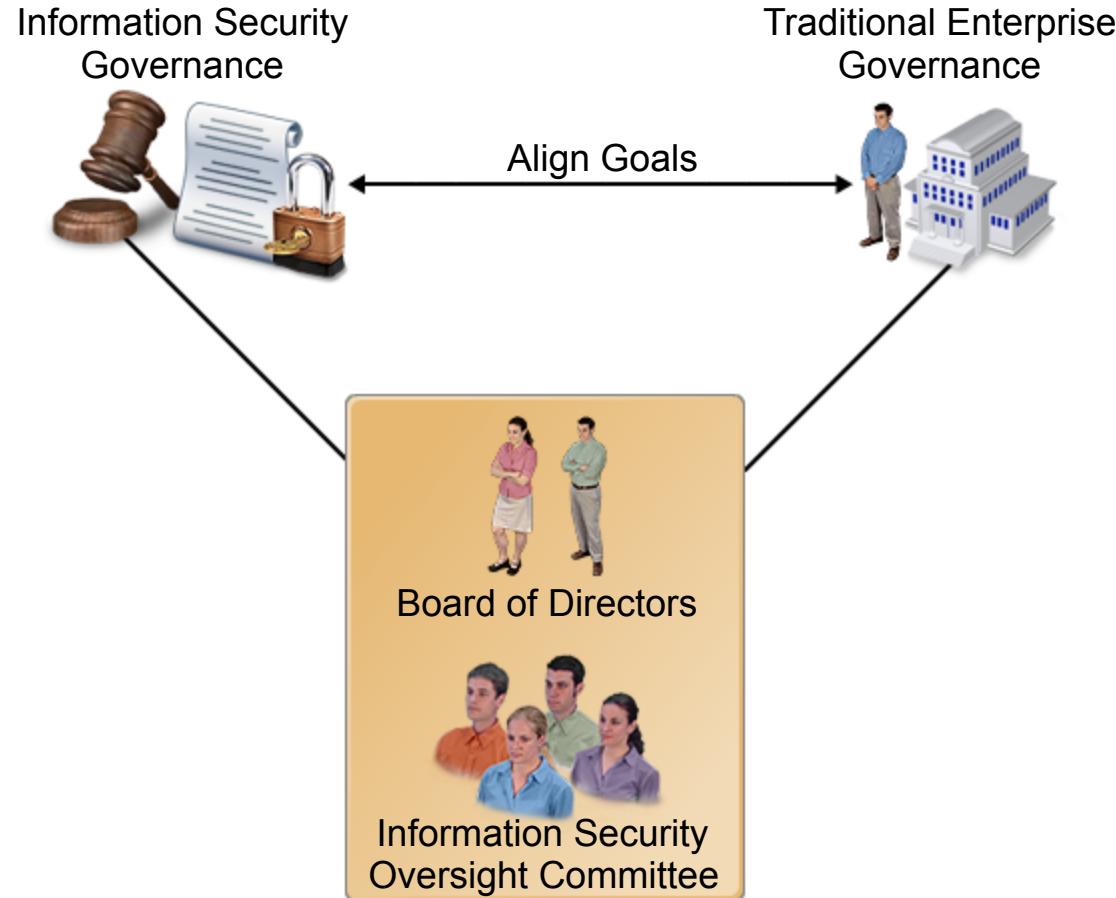
Charter of Information Security Governance

The information security governance charter:

- Describes the purpose of information security governance.
- Sets up the basic framework.
- Defines the scope of information security governance practices.
- Describes the responsibilities of the various personnel.
- Is developed at an organizational level.
- Is usually stored as an electronic document.
- Is typically distributed by the CISO on an annual basis.
- Should be reviewed and updated on an annual basis.



Information Security Governance and Enterprise Governance

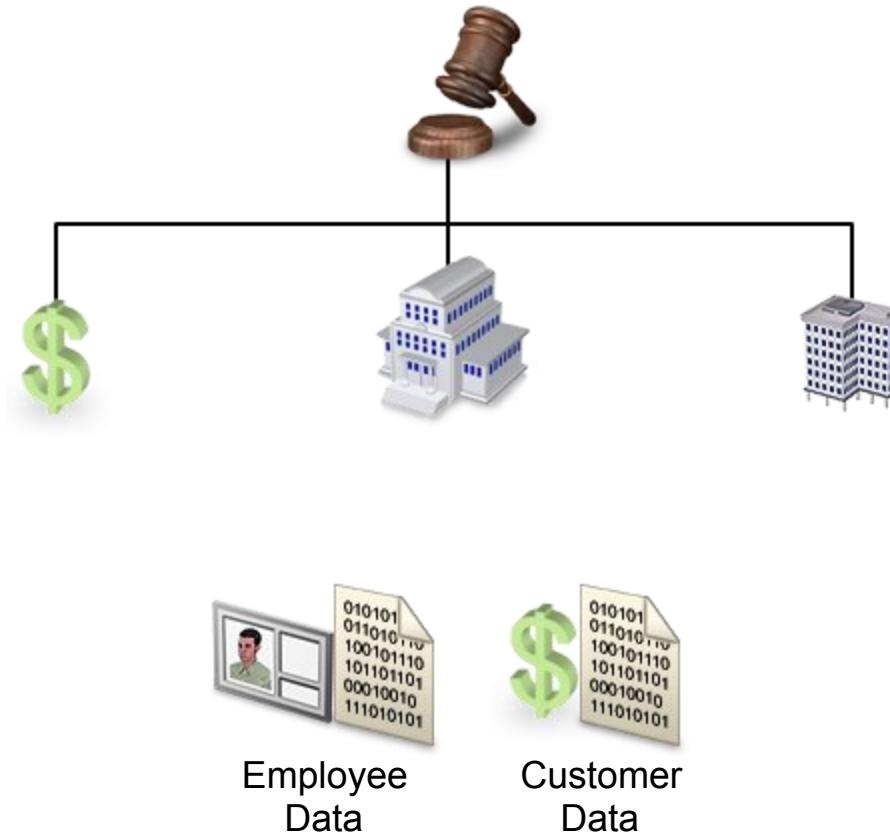


How to Align Information Security Strategy with Corporate Governance

To align information security with corporate governance:

- Obtain buy-in and support from executive management.
- Ensure that each security objective is relatable to at least one business objective.
- Establish a process for reviewing and comparing new or updated business goals with the information security strategy.
- Establish a system and standards for reporting on the state of the information security strategy implementation within the organization.
- Establish a system and standards for reporting on the current value of and ROI from information security efforts.
- Document the information security strategy and all relevant and accompanying material in an information security charter.

Regulatory Requirements and Information Security



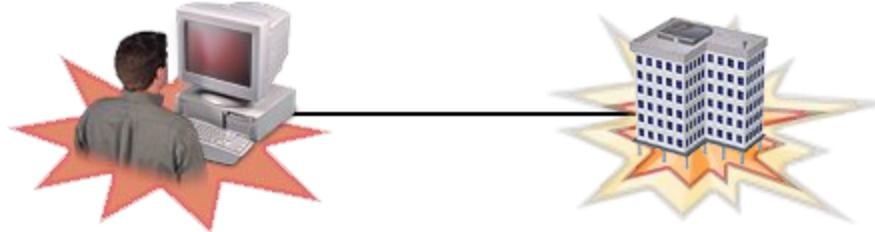
Business Impact of Regulatory Requirements



Liability Management

Goals of liability management include:

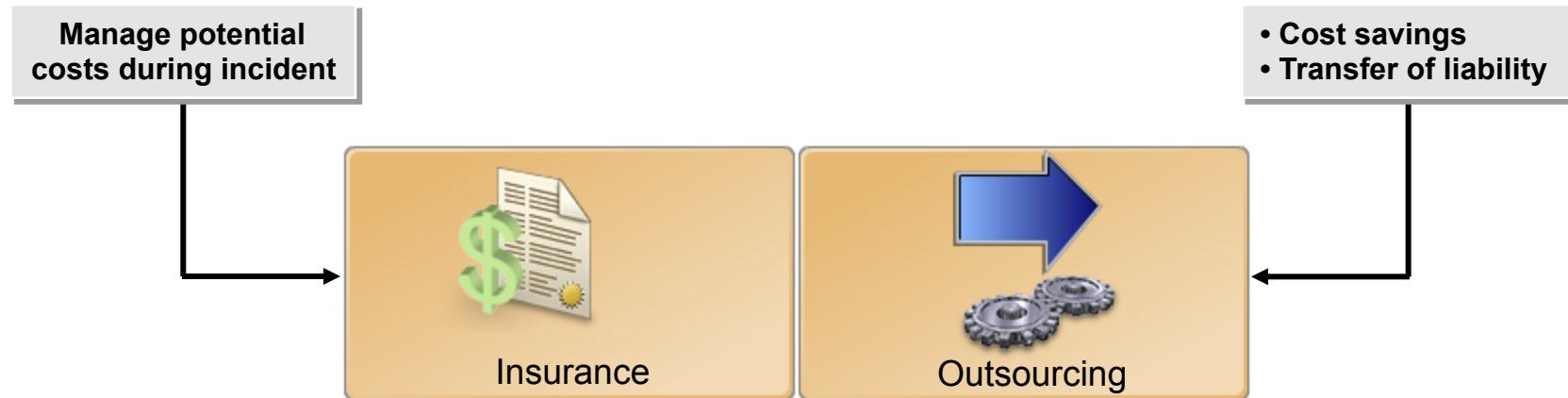
- Alignment of liability management measures with business objectives.
- Identification and documentation of potential liabilities.
- Implementation of mitigation strategies.
- Monitoring and reporting structures, measuring performance.
- Measurements of value and ROI.
- Integration with all business processes and departments.



Liability Management Strategies

Consequences of poor liability management:

- Exposure of customer information to attackers
- Legal fines and penalties
- Reputation as an uncaring or irresponsible organization



How to Identify Legal and Regulatory Requirements

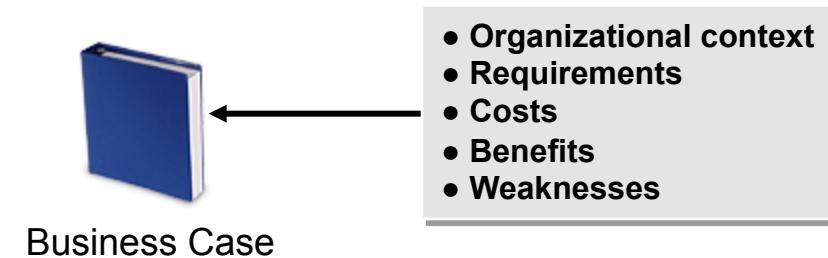
To identify legal and regulatory requirements:

- Consult with your organization's head legal counsel.
- Consult with outside legal counsel to identify potential external requirements that might not be apparent to your internal legal counsel.
- Consult with local officials.
- Review applicable national and international standards and regulations.
- Consult industry experts.
- Consult representatives in similar organizations.

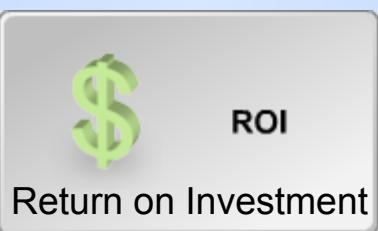
Business Case Development

Business cases typically provide:

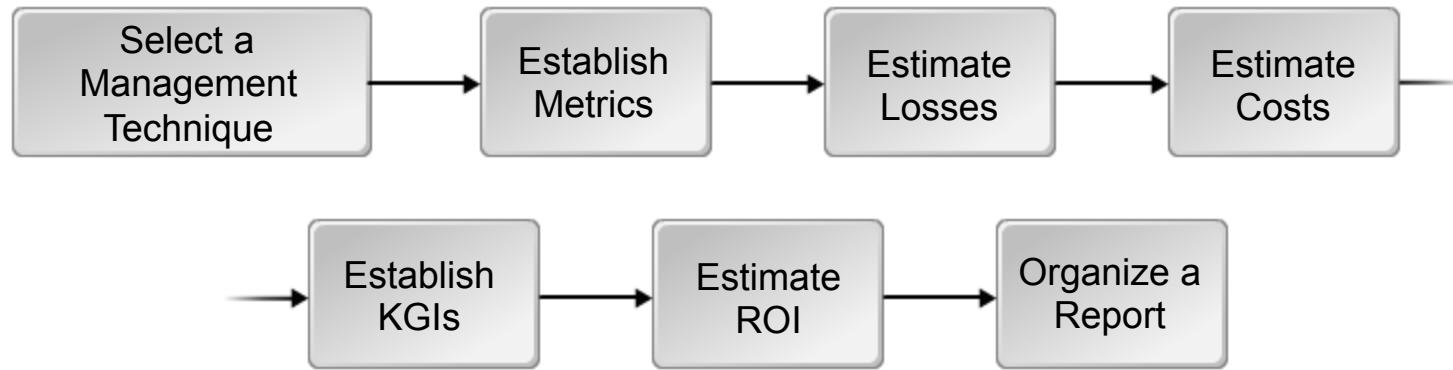
- Reference information and background information.
- A description of the problem.
- Metrics.
- Descriptions of risk tolerance.
- Specifications for expected outcomes.
- Lists of required resources and constraints.
- Budgetary information.
- Details of required commitments.



Budgetary Reporting Methods

Budgetary Reporting Methods	Description
 Resource Usage	<p>The resource usage method involves accounting for all the time, money, and other resources that are invested into a project. Reports are delivered with a level of detail specified by the accepted practices of the organization.</p>
 ROI Return on Investment	<p>Tracking ROI involves keeping track of the costs of implementation and upkeep, as compared to the actual or perceived value gained by implementing the solution.</p>
 Regulatory Compliance	<p>Tracking for regulatory compliance can vary greatly depending on the regulation(s) the organization is required to adhere to. Some regulations may require only general reports, while others may mandate a fine level of detail or an outside audit.</p>

Budgetary Planning Strategy



How to Justify Investment in Information Security

To justify investment in information security:

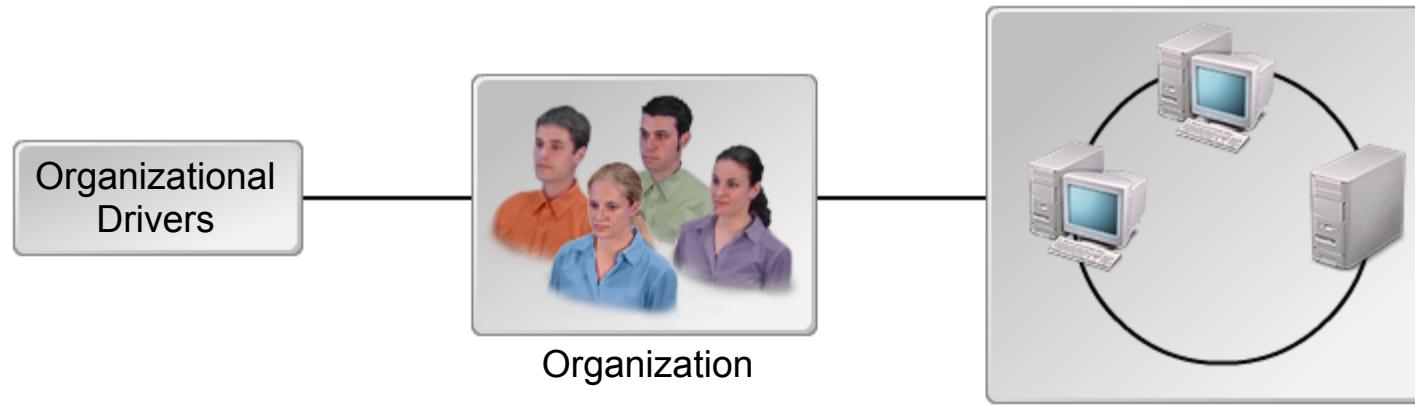
- Develop a budget.
- Analyze similar efforts within the organization.
- Develop a robust business case in support of the proposal.
- Document ROI information.
- Use business cases and industry reports to show the value of the security department.
- Demonstrate the potential downsides of not making the investment.
- Demonstrate how current funding contributes to effective security.
- Document the positive links between security investments and governance objectives.
- Use current trend and market information in business cases.
- Improve the effectiveness of the current security program.

Organizational Drivers

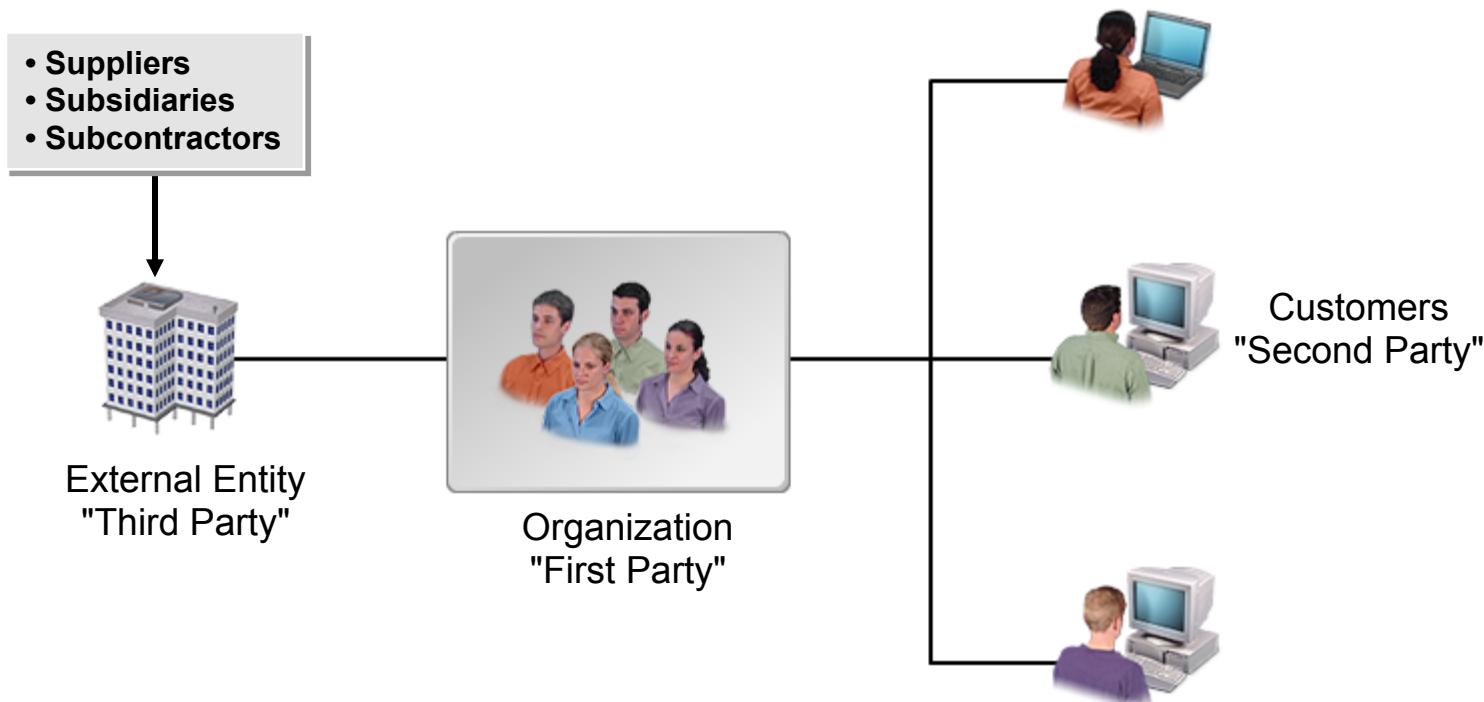
Type of Driver	Description
Organizational drivers	<p>Organizational drivers are prominent factors that drive the organization to move towards established objectives, to make changes to the way it functions, or to set new objectives.</p>
Internal drivers	<p>Internal drivers are those that come from within the organization. Types of internal drivers include:</p> <ul style="list-style-type: none"><input type="checkbox"/> Reorganizations.<input type="checkbox"/> Changes to the acceptable level of risk.<input type="checkbox"/> Security incidents.<input type="checkbox"/> New products or upgrades to existing products.<input type="checkbox"/> New or updated business goals.
External drivers	<p>External drivers are organizational drivers that originate outside the organization. Due to their nature, they can sometimes place more pressure upon an organization than internal drivers. External drivers include:</p> <ul style="list-style-type: none"><input type="checkbox"/> Technological advances.<input type="checkbox"/> New or updated laws and regulations.<input type="checkbox"/> New or updated industry standards.<input type="checkbox"/> Customer requests or new requirements.<input type="checkbox"/> Business partner requests or new requirements.

Impact of Drivers on Information Security

- New/updated business objectives
- Technology advances
- Identification of security flaws



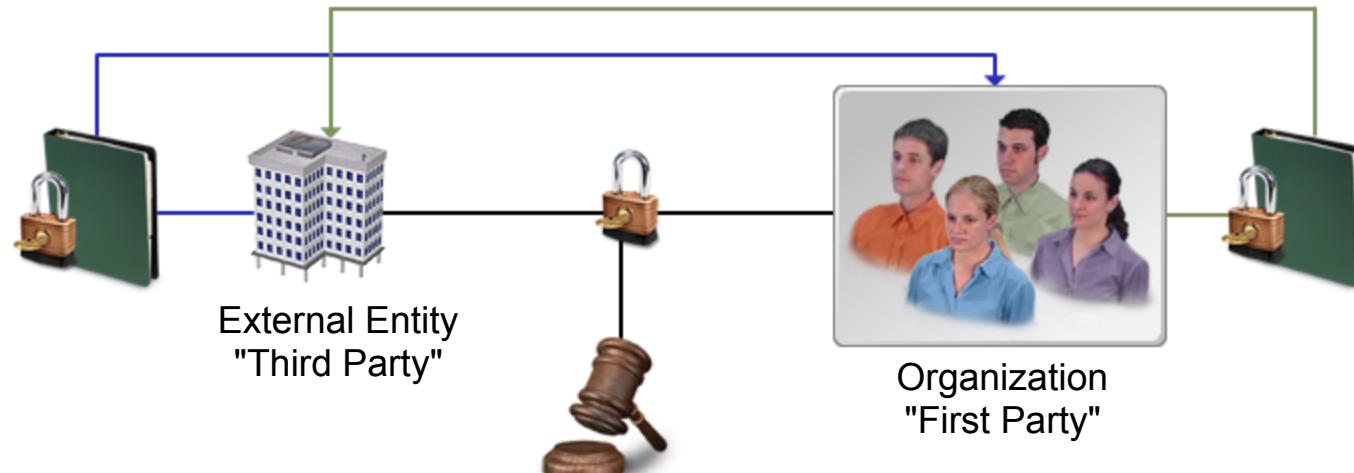
Third-Party Relationships



Impact of Third-Party Relationships on Information Security

Implementing imposed security requirements involves:

- Requirements analysis.
- Process implementation.
- Procedure implementation.
- Control implementation.

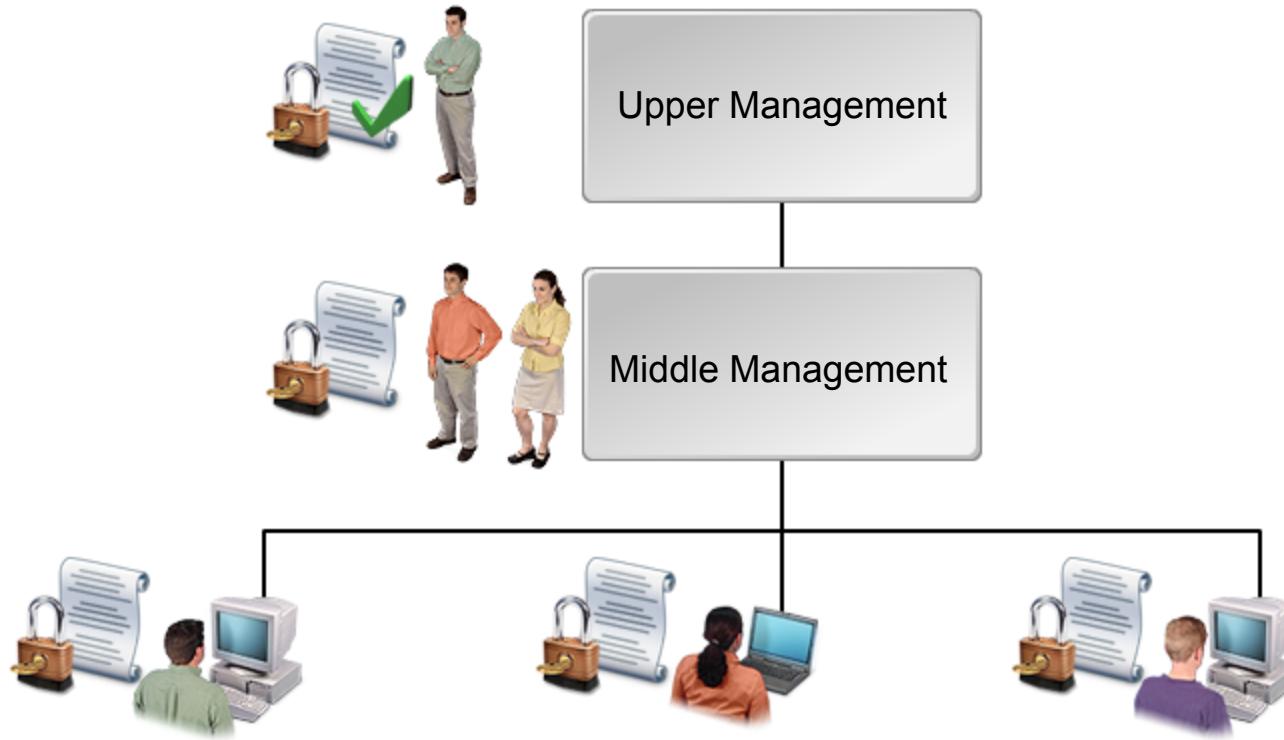


How to Identify Drivers Affecting the Organization

To identify drivers affecting the organization:

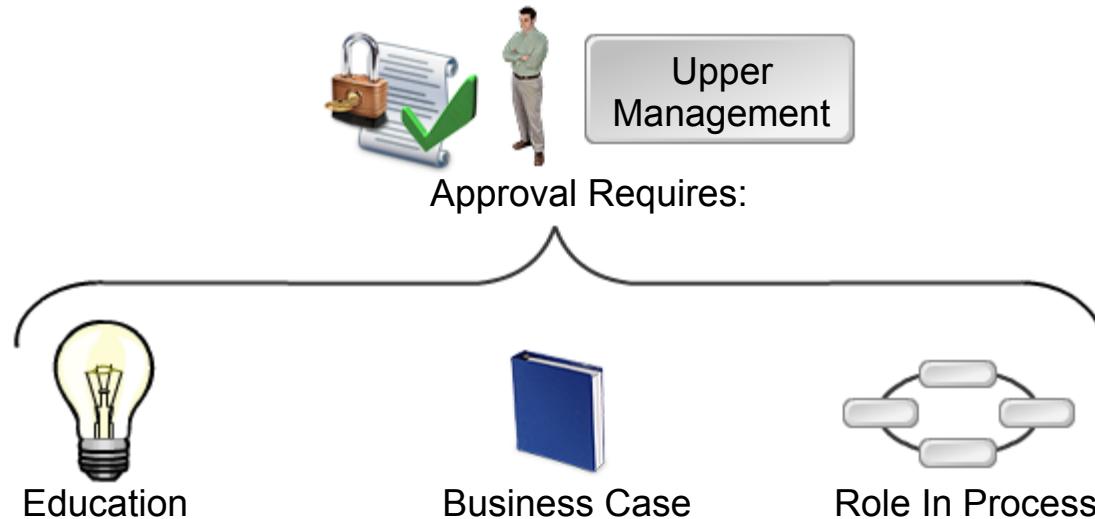
- Review the organizational goals and objectives, as well as business processes and third-party relationships, looking for internal and external drivers.
- Review current and planned future business objectives.
- Review legal and regulatory requirements.
- Analyze third-party relationships and their requirements.
- Review current industry trends.
- Review current technological trends.

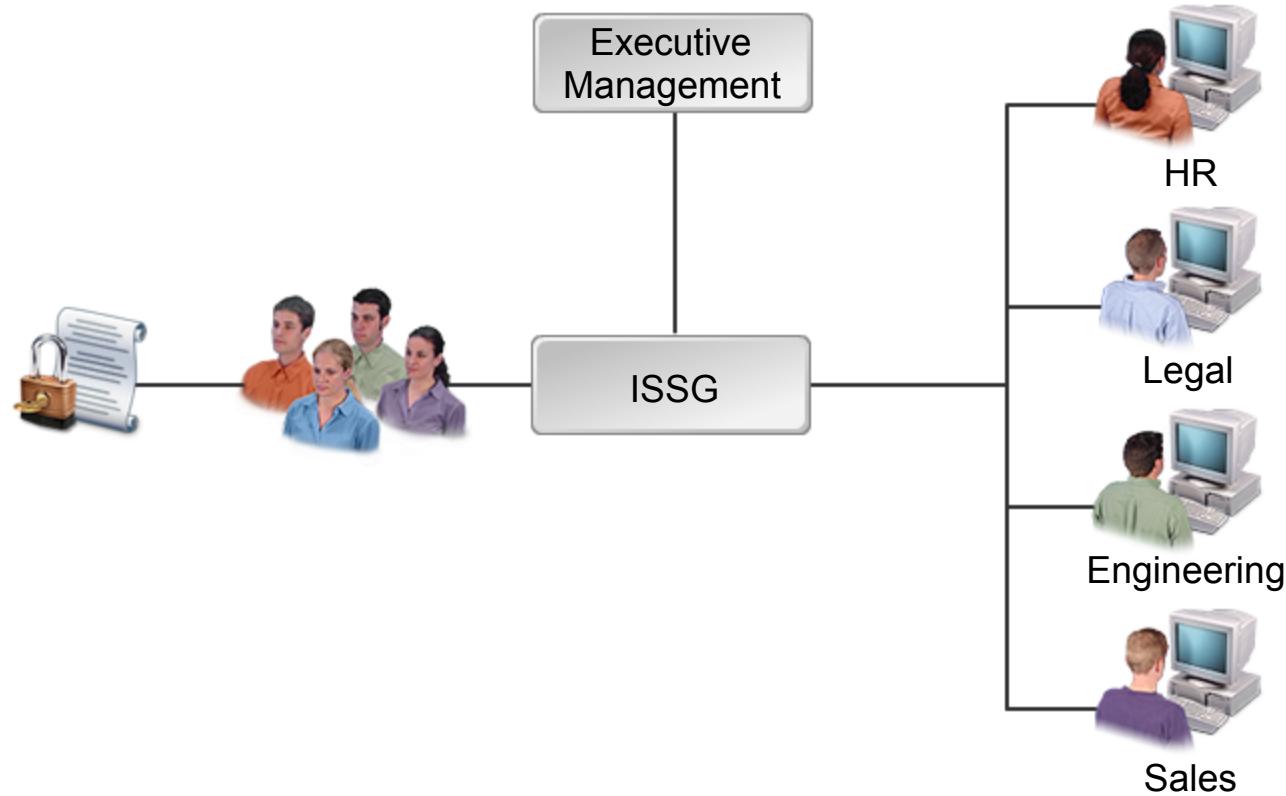
Purpose of Obtaining Commitment to Information Security



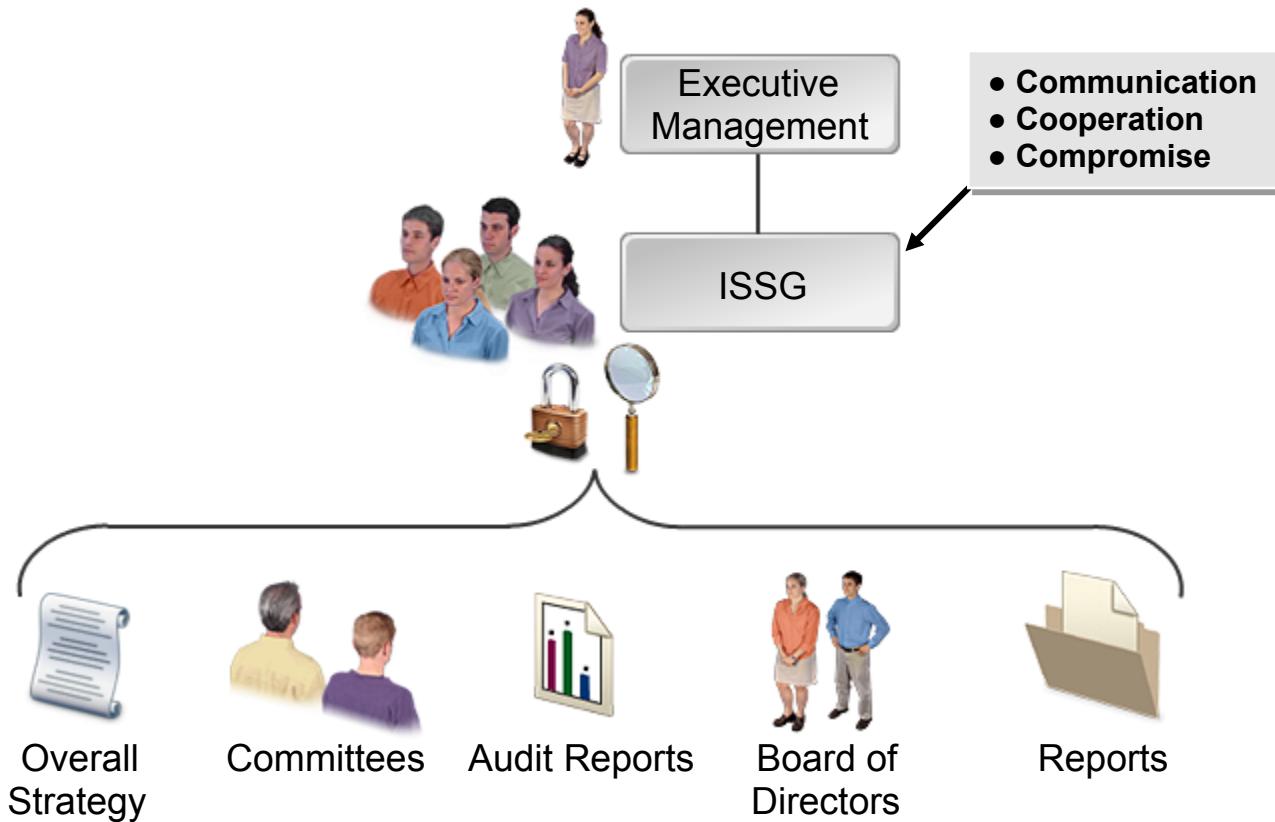
Methods for Obtaining Commitment

- ❑ Involves completion of outputs from earlier phases.
- ❑ Includes topics such as:
 - Risk management.
 - Regulatory requirements and standards.
 - Possible penalties, sanctions, and consequences of failure.
 - Value provided and return on security investment.
 - Costs and constraints.
 - Monitoring, reporting, and auditing.





ISSG Roles and Responsibilities



ISSG Operation

The ISSG should:

- Operate like any other high-level committee.
- Meet at least quarterly.
- Receive reports and presentations from all members and managers.
- Use metrics to monitor the value provided by security initiatives.
- Summarize new information and report to executive management.



ISSG

How to Obtain Senior Management's Commitment to Information Security

To obtain senior management's commitment to information security:

- Provide education on the benefits of information security.
- Describe the downsides of not implementing or improving security.
- Explain senior management's role in the security process.
- Explain the importance of risk management.
- Explain the importance of adhering to regulatory requirements and standards.
- Discuss the possible penalties, sanctions, and consequences of the failure to meet requirements or fulfill security objectives.
- Describe the value provided and return on security investment.
- Discuss technology costs and constraints.
- Describe the benefits of monitoring, reporting, and auditing.
- Dedicate time and resources to getting support from the ISSG.

Information Security Management Roles and Responsibilities



Board of Directors



Executive Management



ISSG

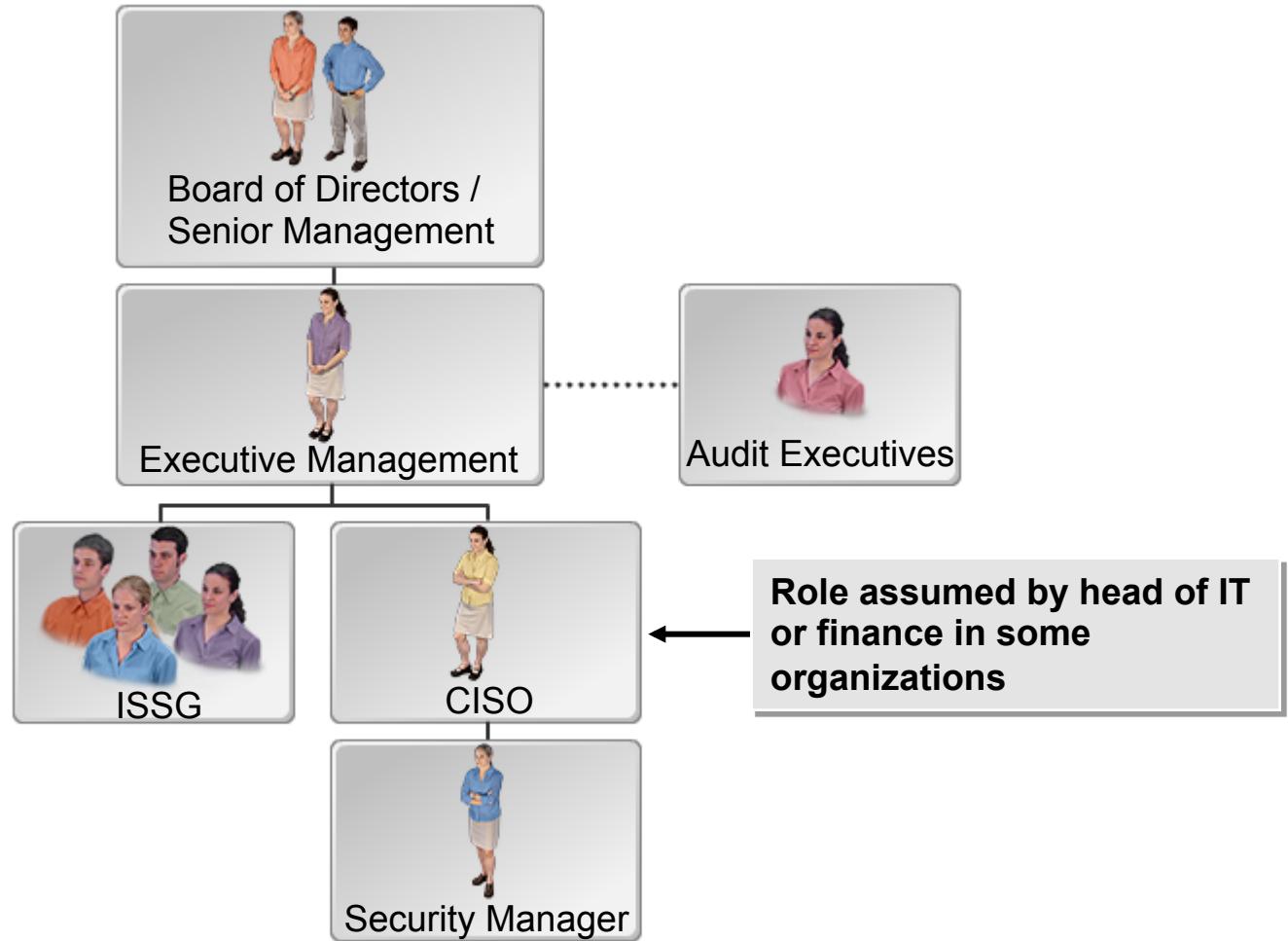


CISO



Audit Executives

Information Security Management Organizational Structures

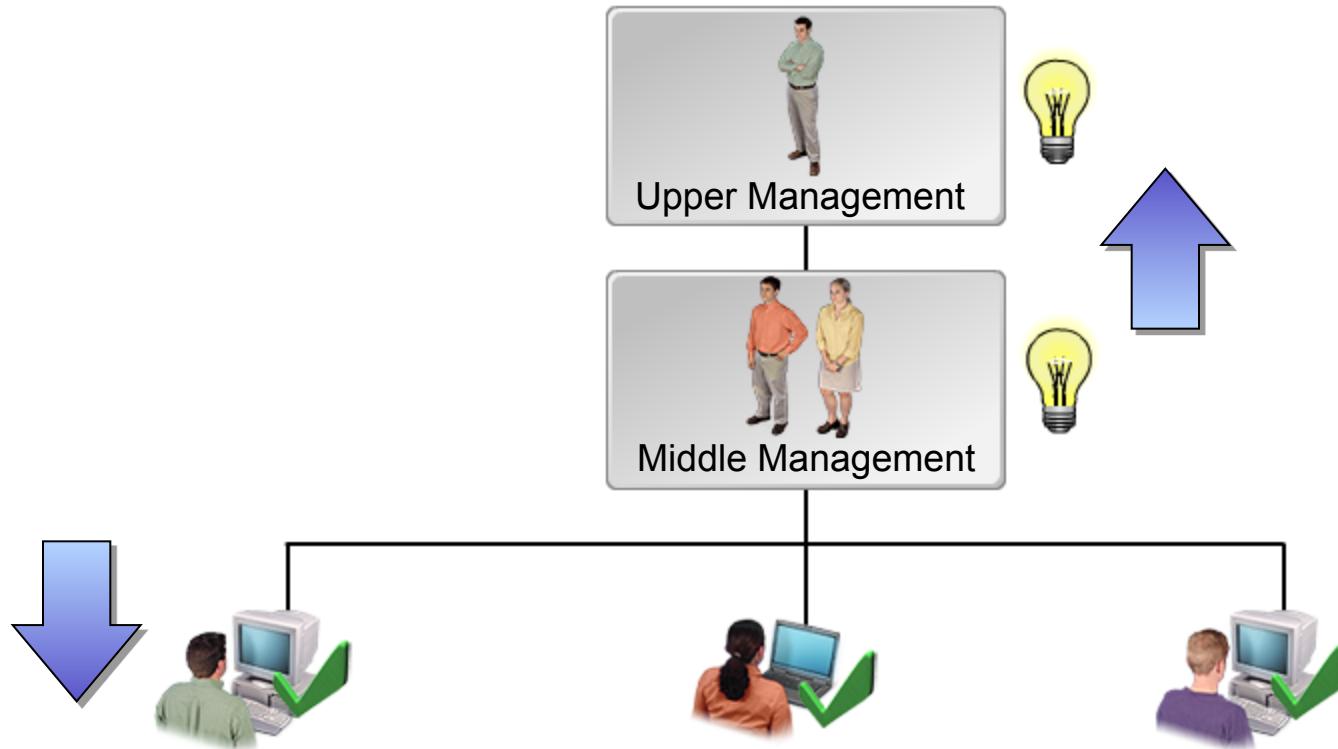


How to Define Roles and Responsibilities for Information Security

To define roles and responsibilities for information security:

- Define job titles and roles.
- Establish a hierachal relationship structure for vital security personnel.
- Empower employees to make security decisions, particularly in cases where reaction time is an important factor.
- Publish information security guidelines for the organization.
- Document and publish all security policies and procedures.
- Clarify or add specifies to policies or procedures where necessary.
- Specifically define information security roles and responsibilities for:
 - The board of directors.
 - Executive management.
 - CISO/information security management.
 - Audit executives.
 - Network and facility security personnel.

The Need for Reporting and Communication



Methods for Reporting in an Organization

Formal Communication Methods:



Email



Memo



Phone

Informal Communication Methods:



Email



Phone



Instant
Messaging



Generated
Emails



Alerts and
Logs

Methods of Communication in an Organization

Audience	Communication Suggestions
 Senior Management	<ul style="list-style-type: none"><input type="checkbox"/> Senior management is most interested in strategic information regarding current and new organizational objectives.<input type="checkbox"/> It may be beneficial to arrange meetings with security managers and business process owners to help provide insight into how these personnel are affected by security and organizational objectives.
 BPOs	<ul style="list-style-type: none"><input type="checkbox"/> BPOs need insight into the daily operations and challenges of their units.<input type="checkbox"/> BPOs should also be continuously consulted to ensure continued support of security objectives.
 Employees	<ul style="list-style-type: none"><input type="checkbox"/> When communicating with employees, it is vital that training and education take center stage.<input type="checkbox"/> Training materials should be updated to reflect the most current policies, procedures, and standards.<input type="checkbox"/> It may be helpful to appoint an information security coordinator for each functional area.

How to Establish Reporting and Communication Channels

To establish reporting and communication channels:

- Define job titles and roles.
- Establish a hierachal relationship structure for security personnel.
- Document and publish all security policies and procedures.
- Ensure that procedures include steps for reporting, including what to report and whom to report that information to.
- Define which individuals or roles should be given what information, based on the urgency of the situation and the organizational policy.
- Define preferred methods of communication, depending on the urgency of the situation and the intended audience.
- Define exactly what information is required, optional, or not needed, depending on the urgency of the situation.

Reflective Questions

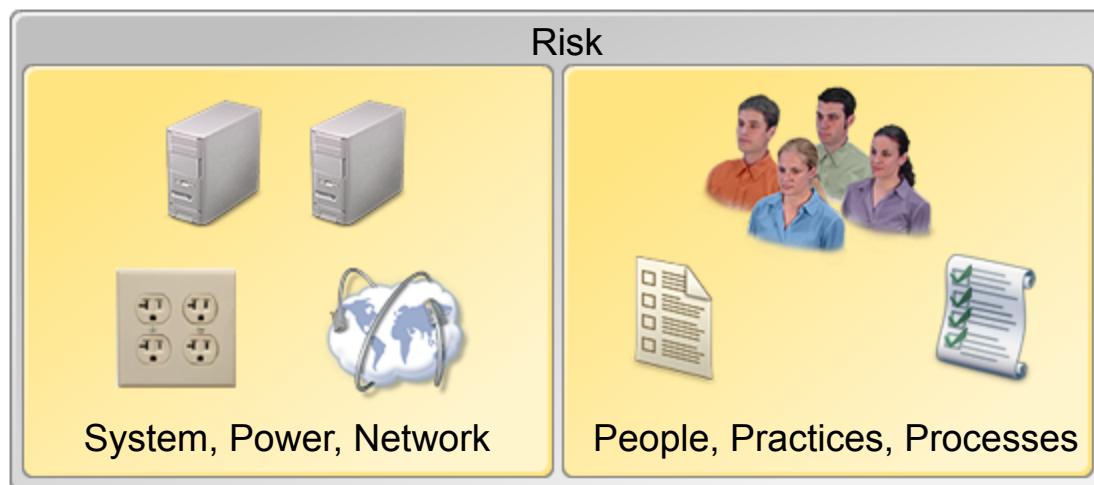
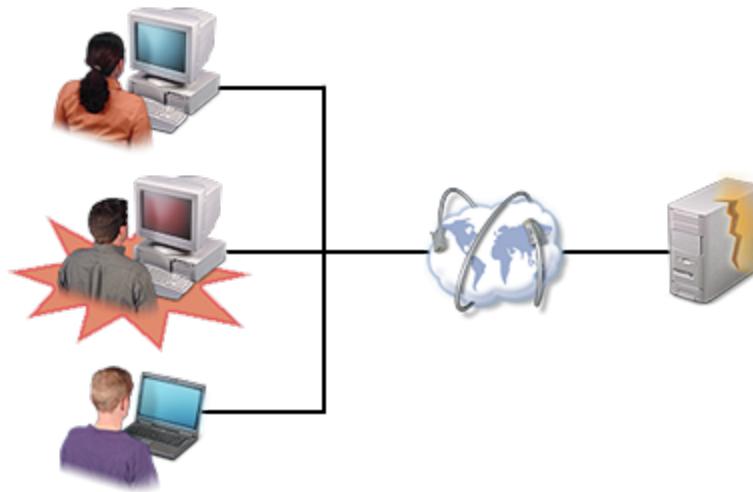
- 1.** Does your employer have a published information security policy or strategy? If so, how could it be revised to more effectively establish the domain of information security within the organization?

- 2.** What challenges could you foresee in implementing a new information security strategy in your organization?

Information Risk Management

- Implement an Information Risk Assessment Process
- Determine Information Asset Classification and Ownership
- Conduct Ongoing Threat and Vulnerability Evaluations
- Conduct Periodic BIAs
- Identify and Evaluate Risk Mitigation Strategies
- Integrate Risk Management into Business Life Cycle Processes
- Report Changes in Information Risk

Risk



Risk Assessment



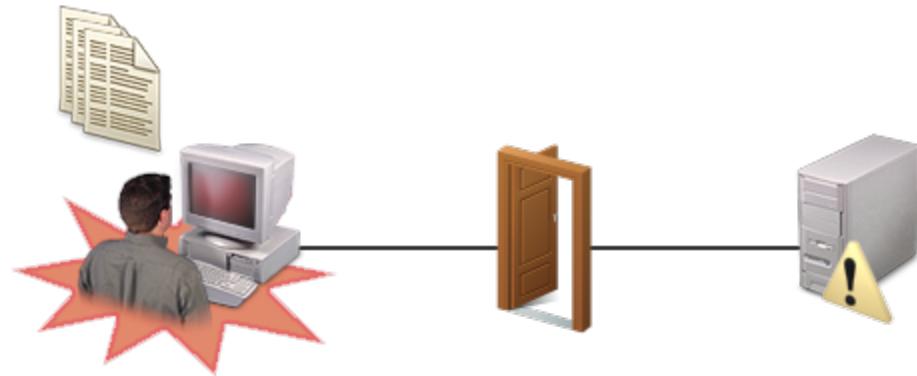
Information Threat Types



Information Vulnerabilities

Vulnerabilities and exposures are the result of:

- Improperly configured or installed hardware or software.
- Bugs in software or operating systems.
- Misuse of software.
- Poorly designed networks.
- Poor physical security.
- Insecure passwords.
- Design flaws in software or operating systems.
- Unchecked user input.



Common Points of Exposure

Exposure Area	Description
 Physical structure	Inadequate physical security includes: unlocked doors, accessible windows, easily accessible and unsecured network access points, and servers that are kept in accessible areas.
 Software	Software that threaten systems include poorly secured or unsecured code and software, worms, viruses, and Trojans. Routinely using computer virus scanners can help lessen or eliminate exposures.
 Network	Inadequate or non-existent passwords. The failure to encrypt private information as it travels across a network can heighten system exposure. The information may be intercepted and used in an unauthorized manner.
 Personnel	If key personnel that are trained to handle situations in a critical event are not available, this can cause additional corporate-wide vulnerabilities.

Information Security Controls



Types of Information Security Controls

Information security control types include:

- Deterrent
- Preventative
- Detective
- Corrective
- Compensatory



Information Security
Controls

Common Information Security Countermeasures

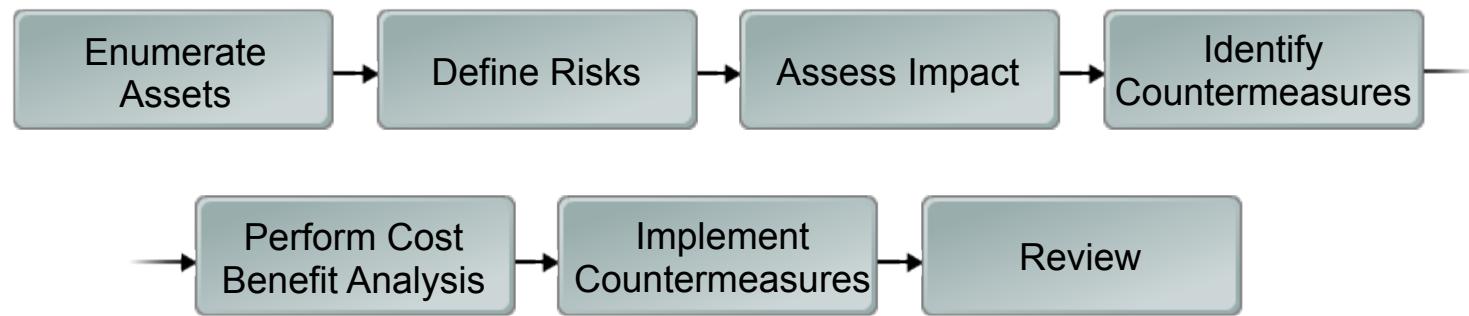
Information security countermeasures may include:

- Security policies
- Contingency planning
- Incident response
- Training and awareness
- Access control
- Physical security
- Personnel security
- Risk assessment
- Identification, authentication, authorization
- Encryption
- Perimeter protections
- IDSs/IPSs
- Anti-virus software



Information Security
Countermeasures

Overview of the Risk Assessment Process



Factors Used in Risk Assessment and Analysis



Measurability



Repeatability



Documentation

Risk Assessment Methodologies

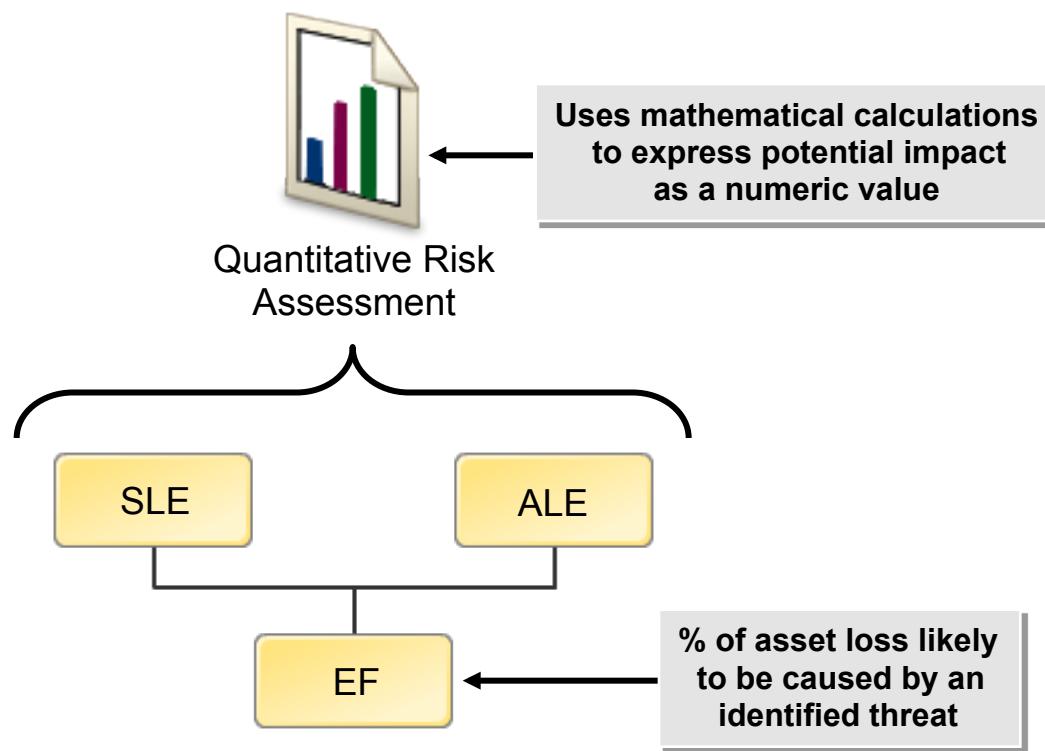
Risk assessment methodologies include:

- NIST
- COBIT
- OCTAVE
- ITIL
- CRAMM

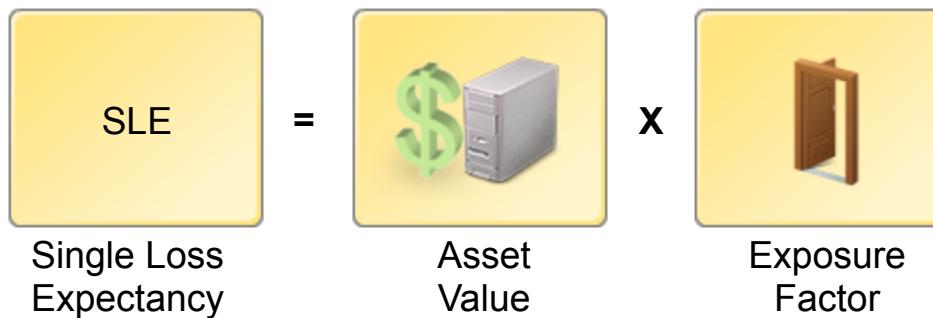
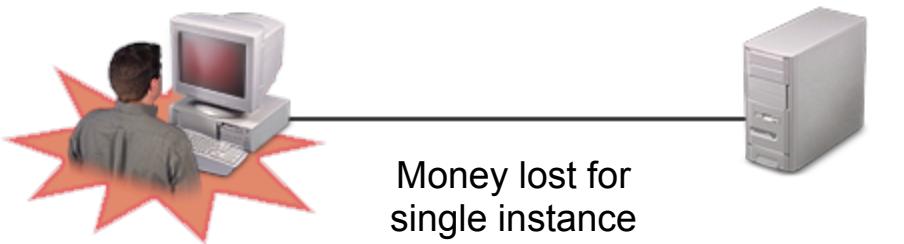


Risk Assessment

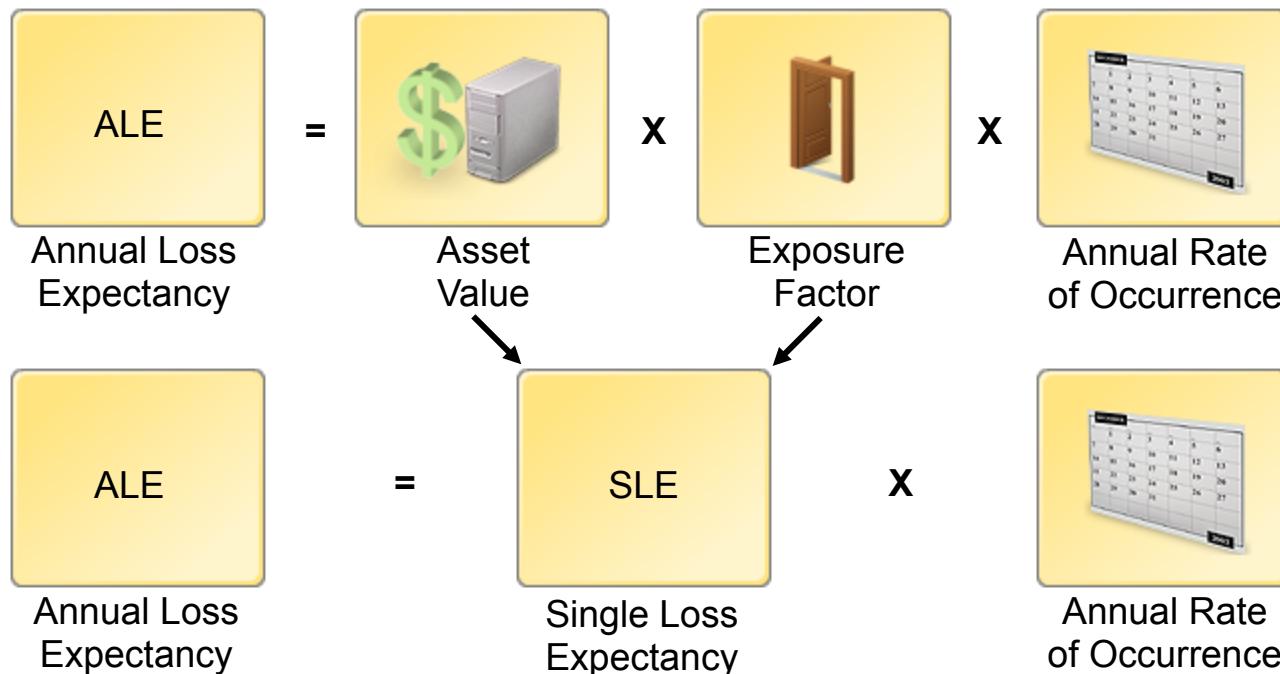
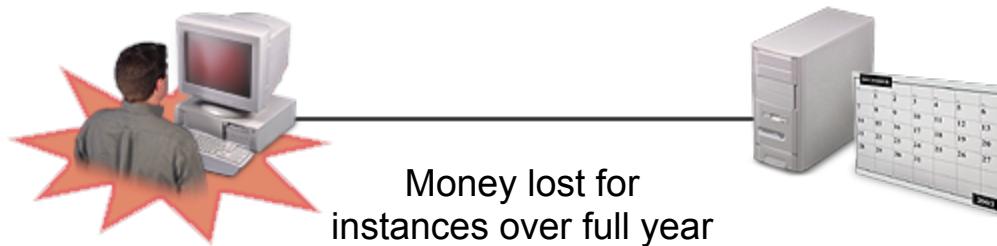
Quantitative Risk Assessment



Quantitative Risk Assessment (Cont.)



Quantitative Risk Assessment (Cont.)



Qualitative Risk Assessment

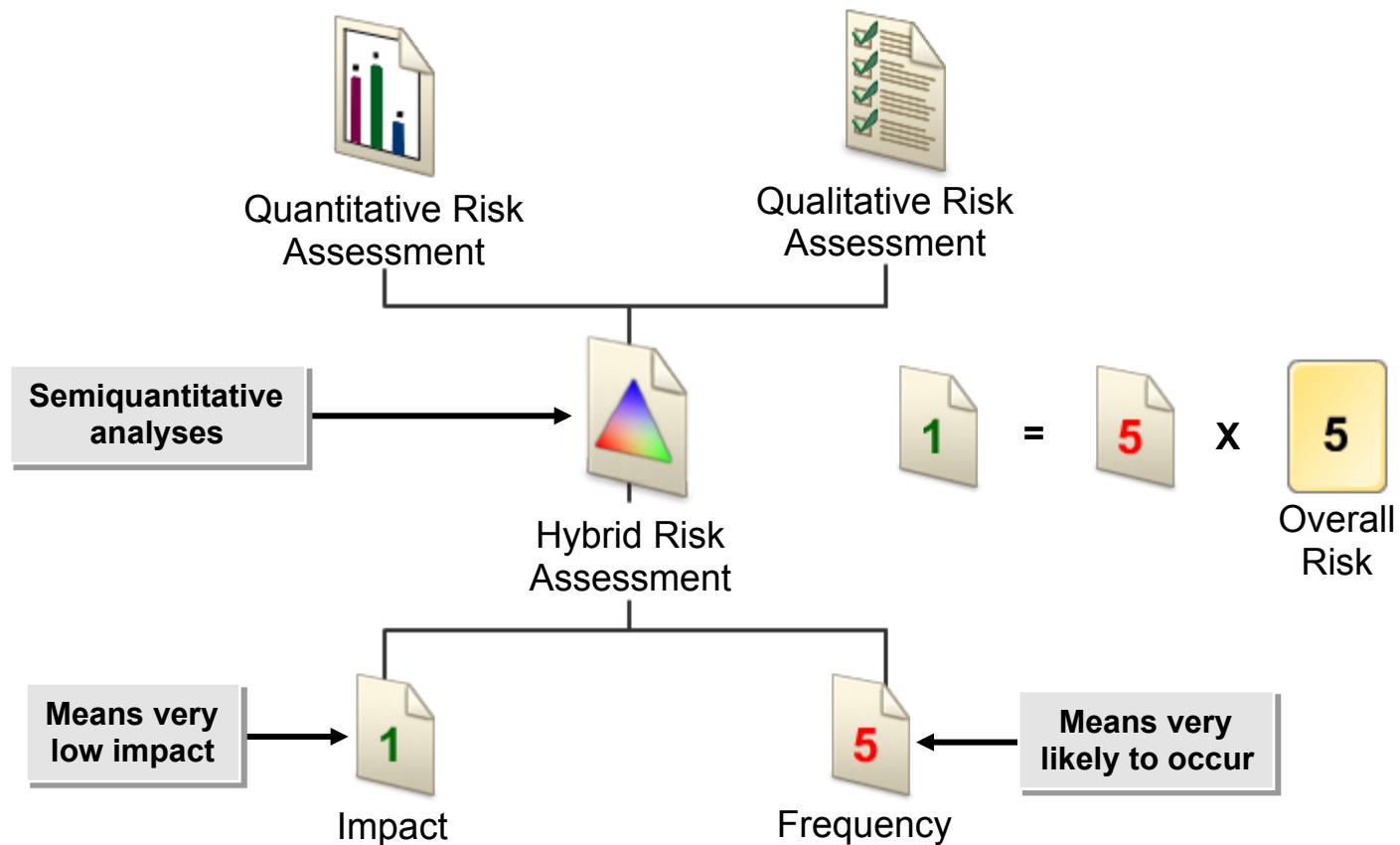
A qualitative risk assessment:

- Measures relative scope, possibility, and impact of potential consequences.
- Has less reliance on numbers, valuations, and statistics.
- Is used when non-tangible assets need to be considered.
- May include:
 - An initial assessment.
 - A detailed analysis of selected risks.
 - Surveys, questionnaires, workshops, and interviews.



Qualitative Risk
Assessment

Hybrid Risk Assessment



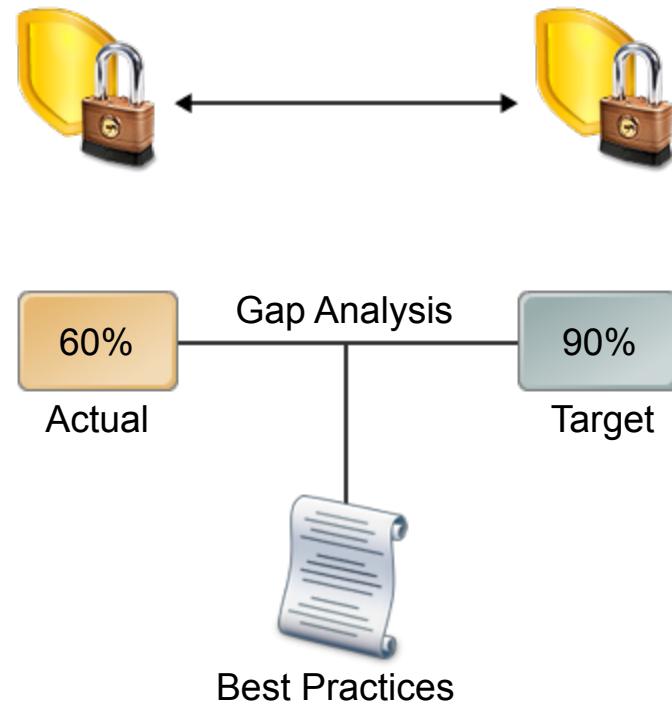
Best Practices for Information Security Management

Standards and best practices:

- COBIT
- ISO 27000
- SABSA



Gap Analysis

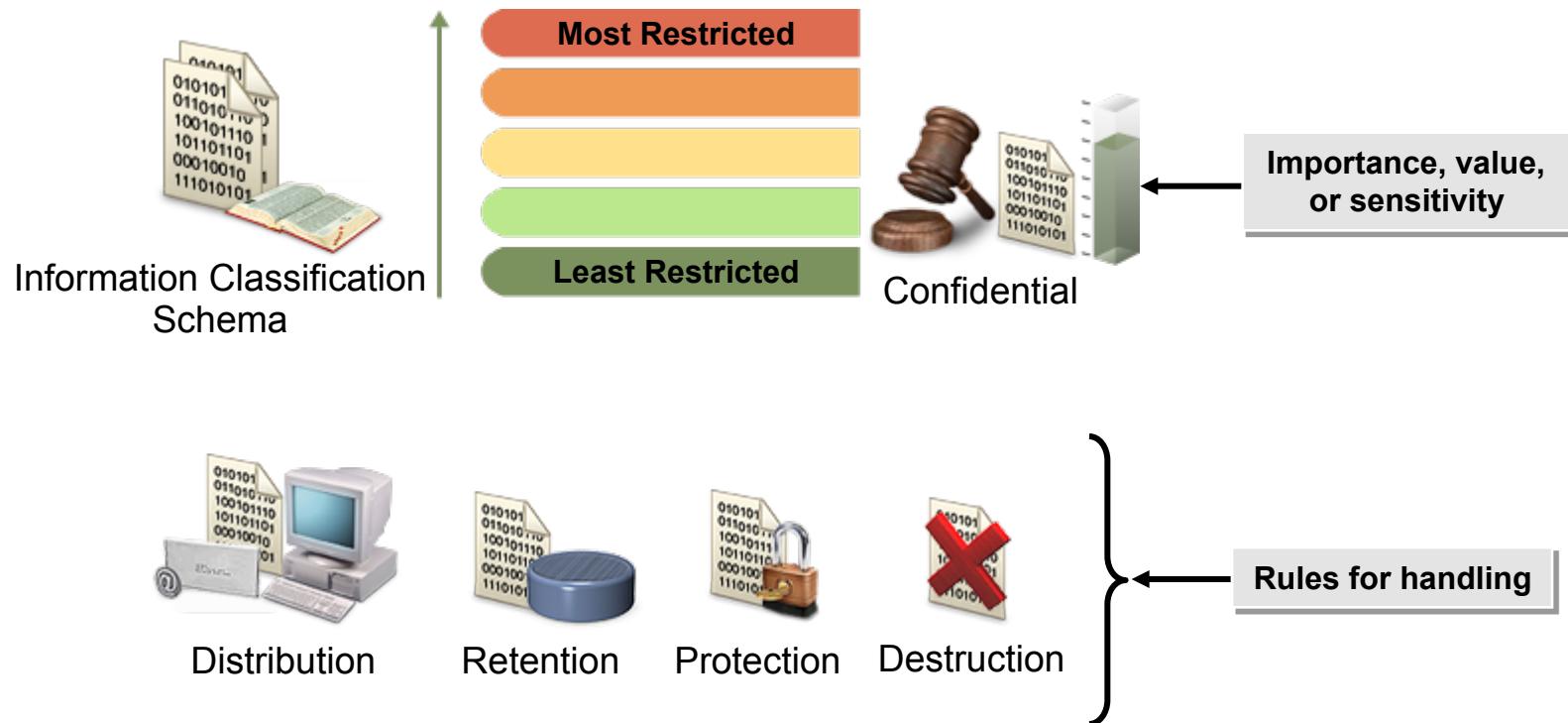


How to Implement an Information Risk Assessment Process

To implement an information risk assessment process:

- Establish the domain of risk management within the organization.
- Identify assets within the organization.
- Identify risks to those assets.
- Analyze and evaluate the identified risks.
- Assess the potential impact and likelihood of the identified risks.
- Identify potential remedies, controls, and countermeasures.
- Select and implement the most cost-effective countermeasures.
- Use gap analysis techniques to review the effectiveness of the implemented controls.
- Accept and manage any residual risk.
- Continuously communicate within the organization regarding the status of the risk assessment efforts.

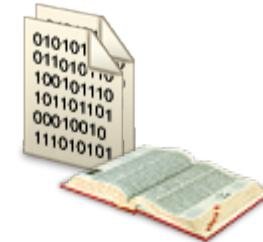
Information Classification Schemas



Components of Information Classification Schemas

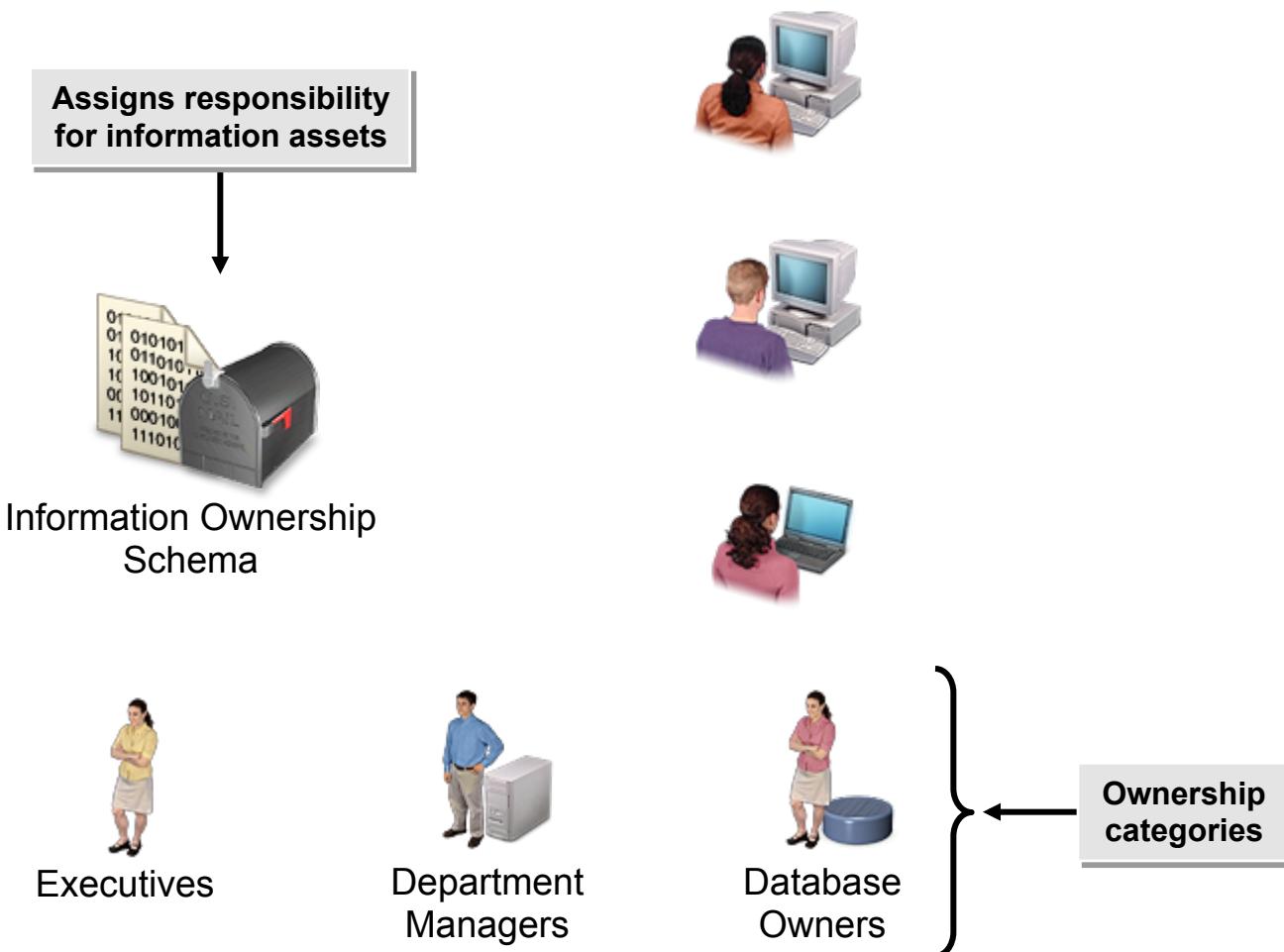
Components of information classification schemas include:

- Data categories
- Documentation
- Group definitions
- Permissions
- Controls
- Periodic review



Information
Classification Schema

Information Ownership Schemas



Components of Information Ownership Schemas



Areas of Ownership



Documentation



Group Definitions



Controls



Periodic Review

Information Resource Valuation

Assigning value to information:

- Includes cost of restoring or creating it, legal expenses, and consequences of misuse.
- Is an essential part of information security.
- Is difficult to perform accurately in most cases.



Information
Resource Valuation

Valuation Methodologies

Information valuation methodologies include:

- Price.
- Revenue generation metrics.
- Loss of reputation, trust, or customers.
- Litigation costs.
- Regulatory costs.



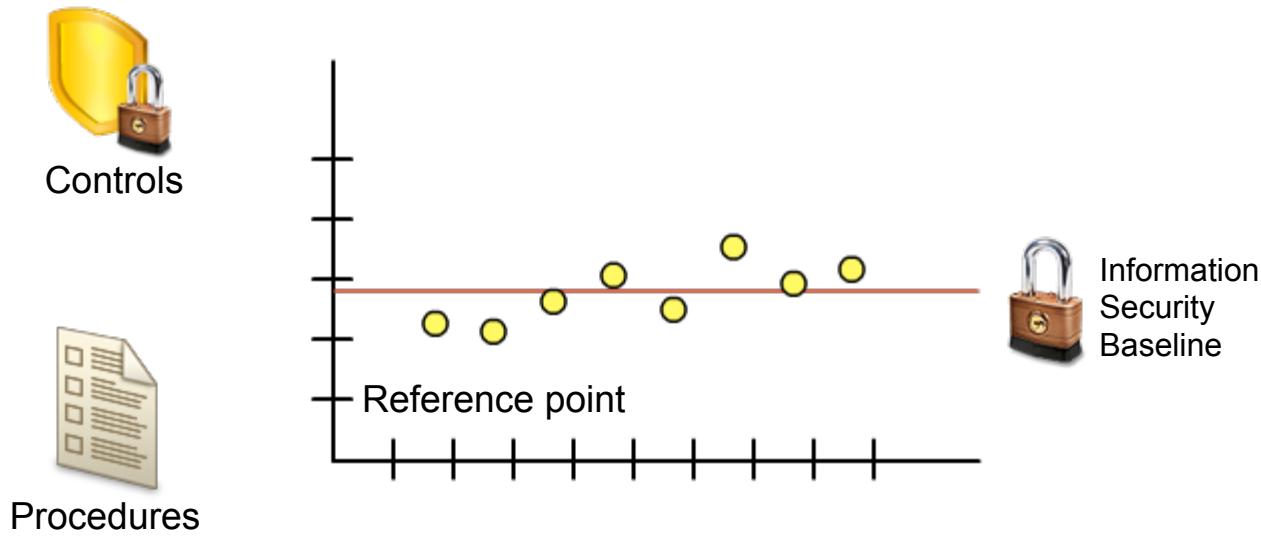
Information
Resource Valuation

How to Determine Information Asset Classification and Ownership

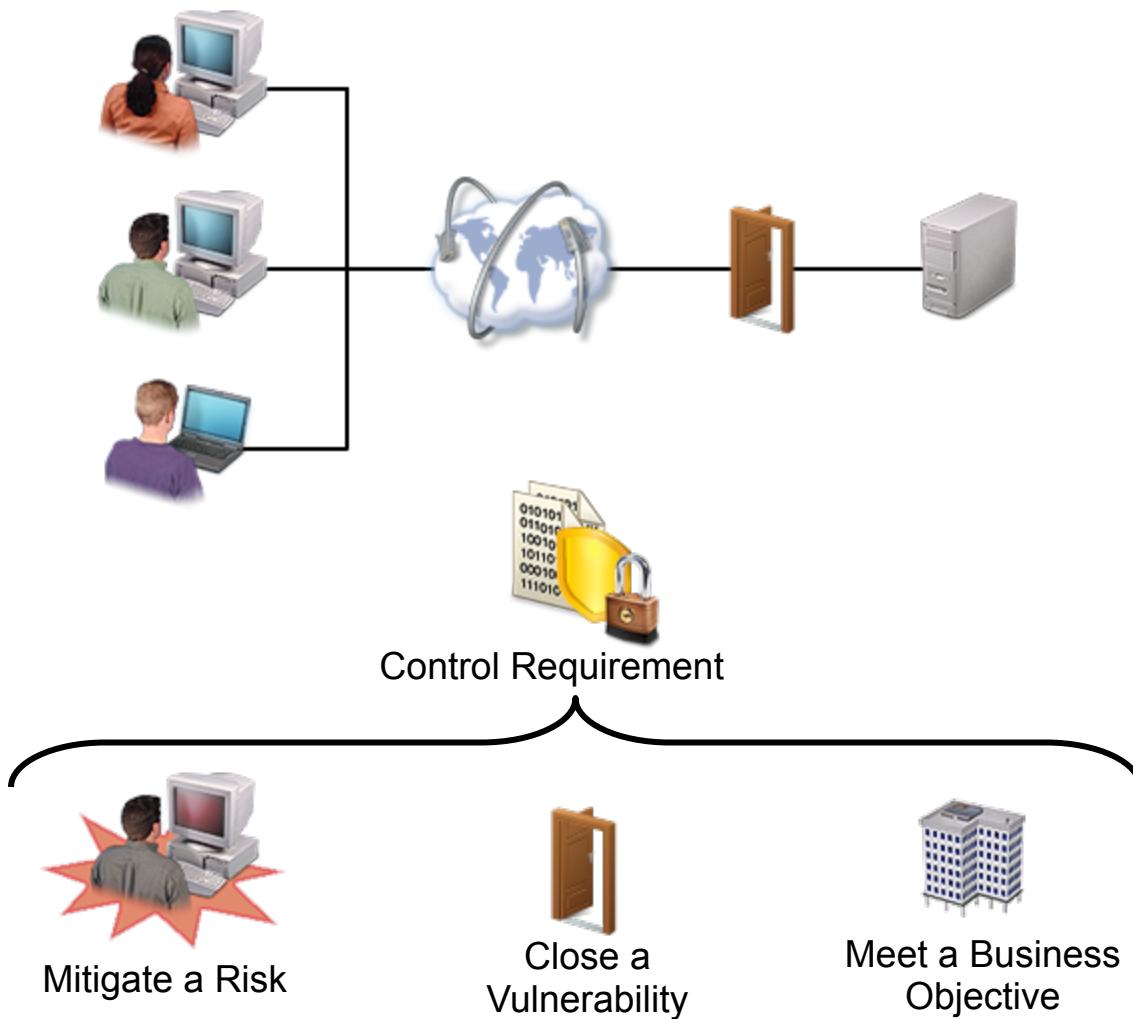
To determine information asset classification and ownership:

- Identify and document information assets within the organization.
- Establish data categories.
- Define groups and permissions.
- Define areas of ownership.
- Evaluate and select controls to enforce classification, permissions, and ownership.
- Document the classification, ownership, and valuation methodologies.
- Conduct periodic reviews to ensure that the schemas are being used and that policies are current.

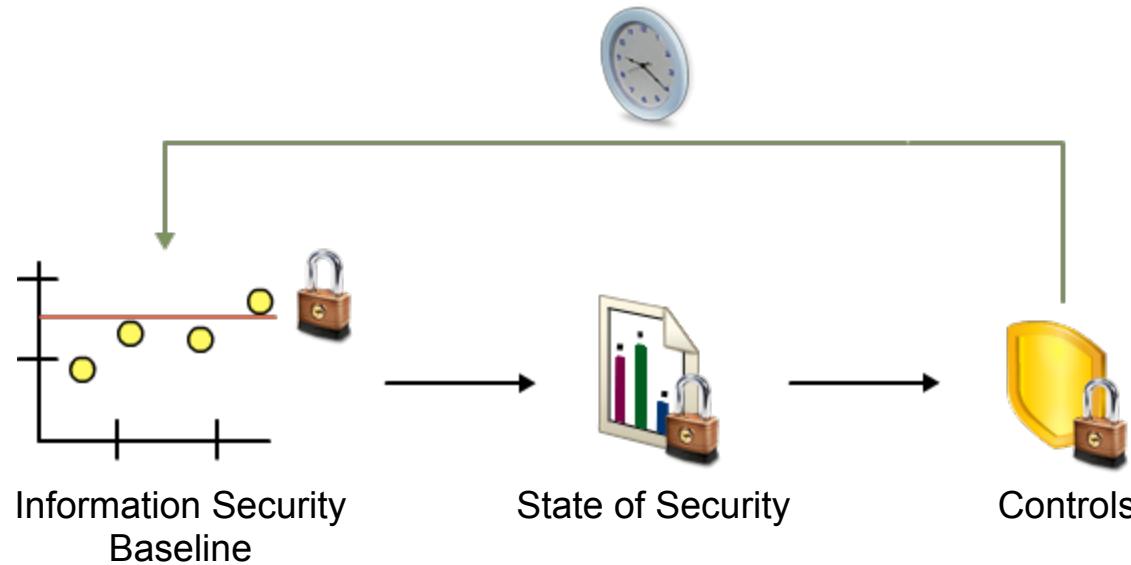
Baseline Modeling



Control Requirements



Baseline Modeling and Risk-Based Assessment of Control Requirements



Cost Benefit Analysis

How to Conduct Ongoing Threat and Vulnerability Evaluations

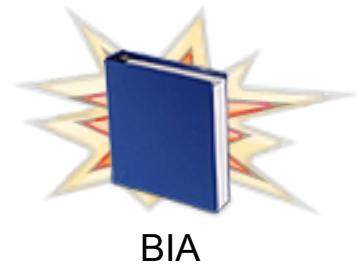
To conduct ongoing threat and vulnerability evaluations:

- Select and implement an information security management strategy.
- Select and establish a risk assessment methodology.
- Establish metrics that can be used to effectively and repeatedly measure the effectiveness of controls.
- Establish an information security baseline across all business units, business processes, and controls in the organization.
- Periodically repeat the measurements defined in the baseline and compare the results against the standard.
- Establish procedures for identifying gaps in the current control set.
- Identify potential remedies, controls, and countermeasures.
- Assess the potential impact and likelihood of the identified risks.
- Select and implement the most cost-effective countermeasures.
- Continuously communicate within the organization regarding the status of the risk assessment efforts.

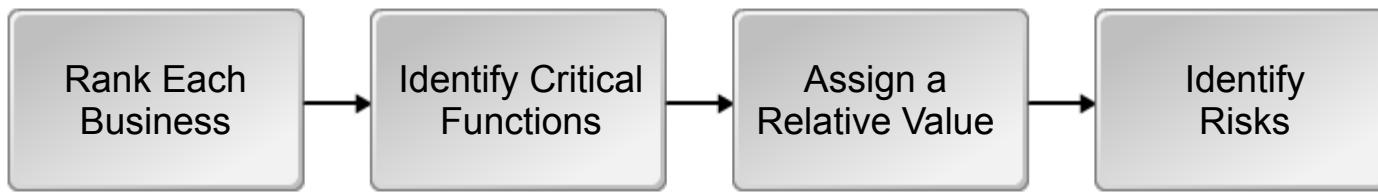
BIAs

A BIA:

- Estimates the consequences of loss.
- Provides a means of determining order of recovery.
- Determines priority of applying mitigations.
- Considers both fiscal and intangible losses.
- Prioritizes the application of controls.
- Provide a foundation for making business decisions to minimize risk.
- Is conducted by the committee responsible for assessing the risk.
- Has standards established by COBIT, ISO 27001, OCTAVE, and NIST.



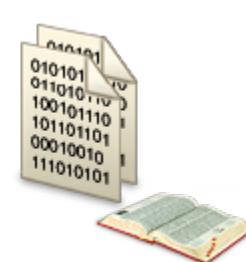
BIA Methods



Factors for Determining Information Resource Sensitivity and Criticality

Factors for determining information sensitivity:

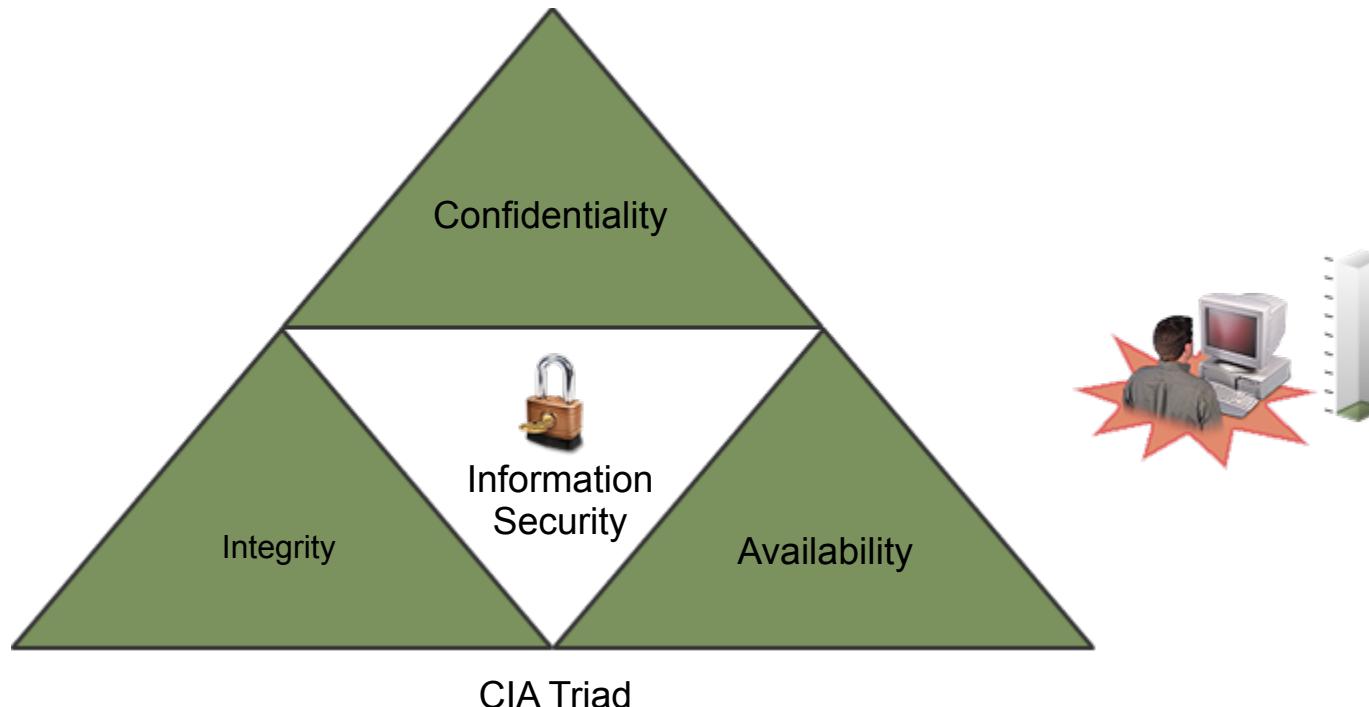
- Replacement costs.
- Costs of loss of availability and lost productivity.
- Cost of loss of integrity and restoring damaged data.
- Loss of confidentiality and consumer confidence.



Impact of Adverse Events

Questions that determine the impact of an event:

- What is the system's mission?
- How critical is the system and the information it holds?
- How sensitive is the organization to the loss of the system and data?

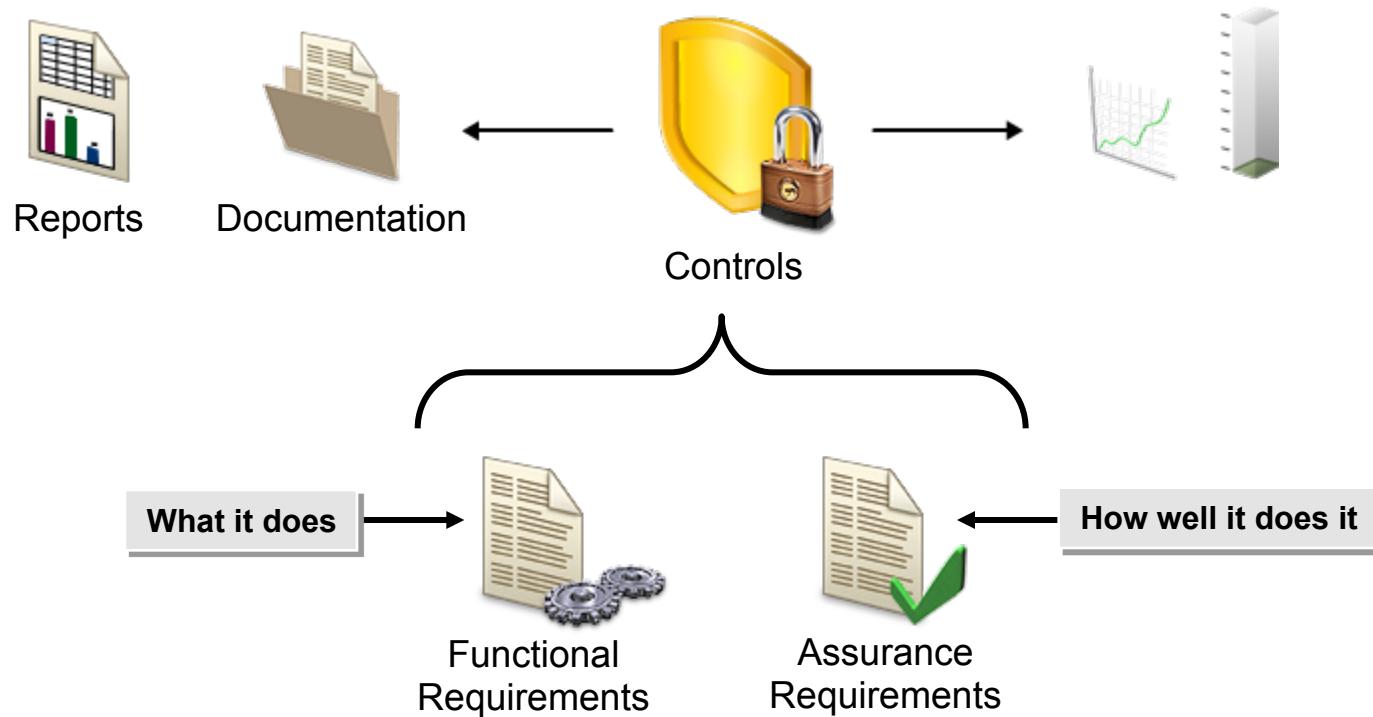


How to Conduct Periodic BIAs

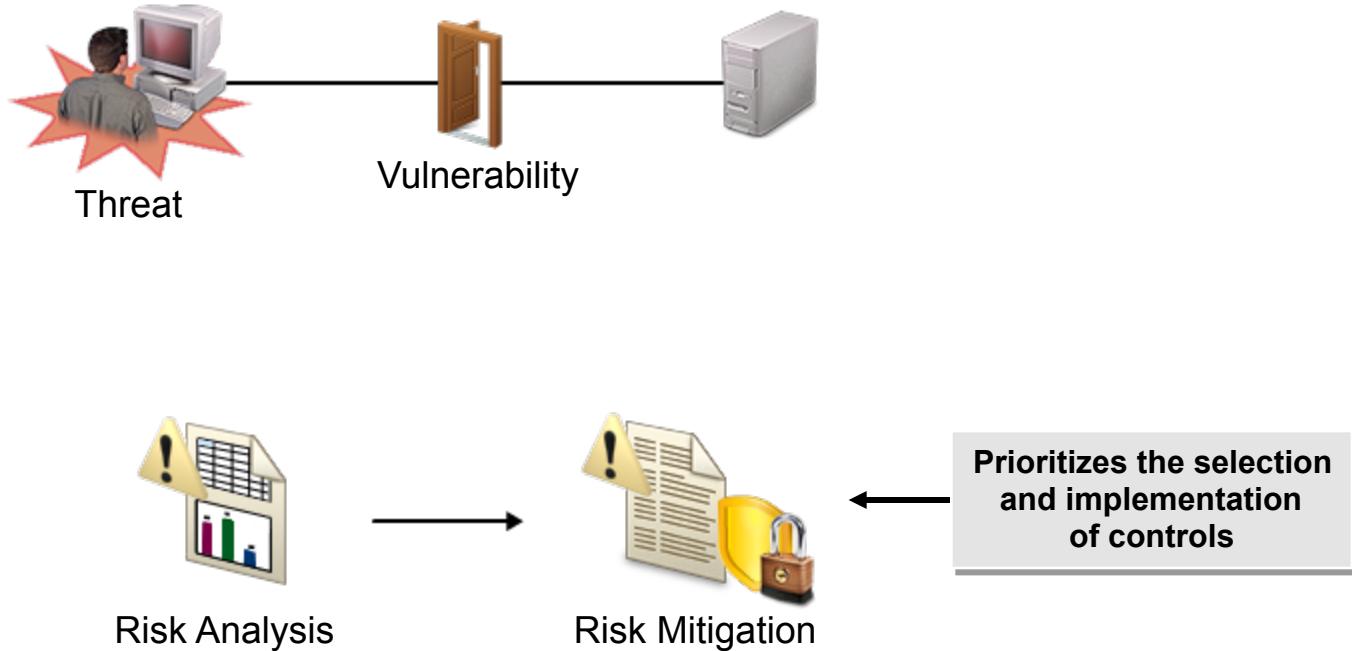
To conduct periodic BIAs:

- Select and implement an information security management methodology.
- Select and establish an impact assessment methodology.
- Perform a BIA using established processes.
- Establish metrics that can be used to effectively and repeatedly estimate the consequences of the loss of information resources.
- Periodically repeat assessments and compare the results against previous assessments.
- Establish procedures for identifying significant changes to the BIA for a particular risk.
- Consider revising BIAs when major changes are made to the organization, or when the technologies or process controls it employs change significantly. Additionally, a small sample set of analyses should be reviewed for accuracy on a yearly basis.
- Continuously communicate with interested parties regarding the status of BIA efforts.

Methods for Measuring Effectiveness of Controls and Countermeasures



Risk Mitigation



Risk Mitigation Strategies

Options for risk mitigation include:

- Risk acceptance
- Risk termination
- Risk reduction
- Risk transference
- Risk avoidance



Risk Mitigation

Effect of Implementing Risk Mitigation Strategies

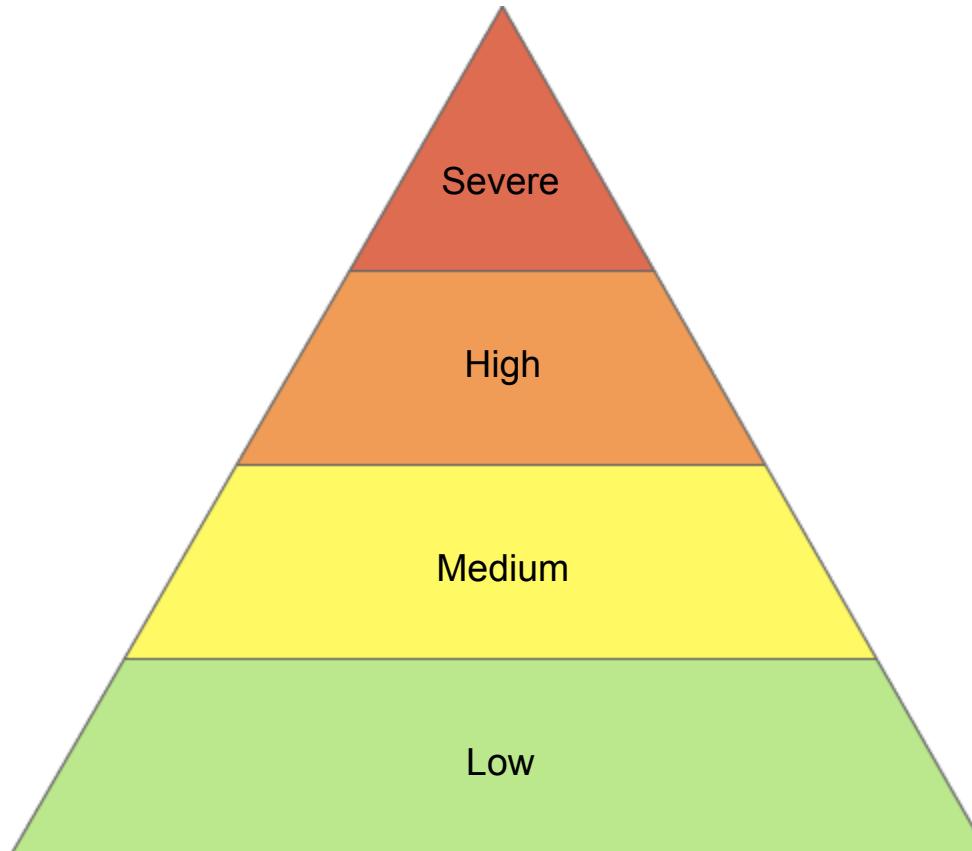
Effective risk mitigation results in:

- Reducing the impact of individual incidents.
- Reducing the number of incidents impacting the organization.
- A reduction in the number of vulnerabilities.
- An increase in confidence that goals of CIA will be met.

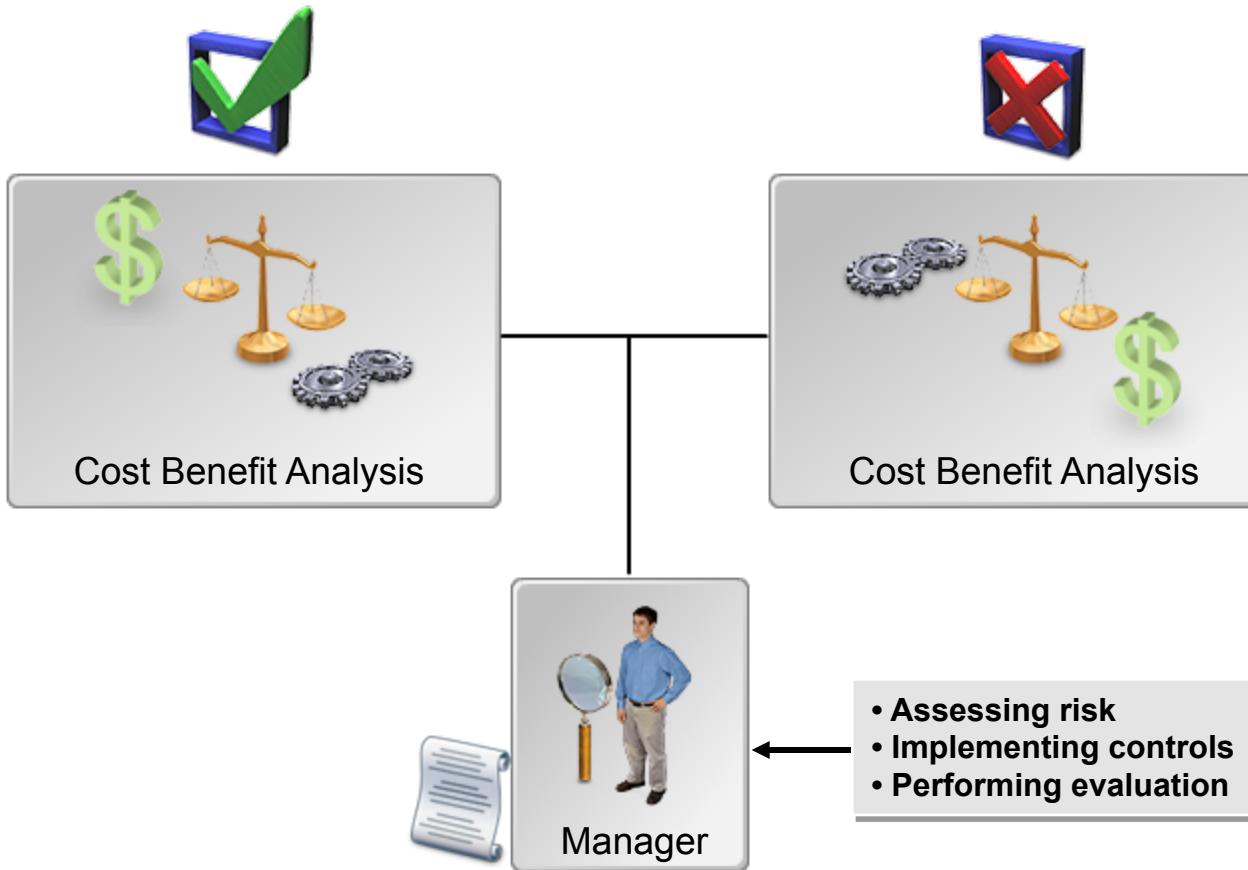


Risk Mitigation

Acceptable Levels of Risk



Cost Benefit Analysis

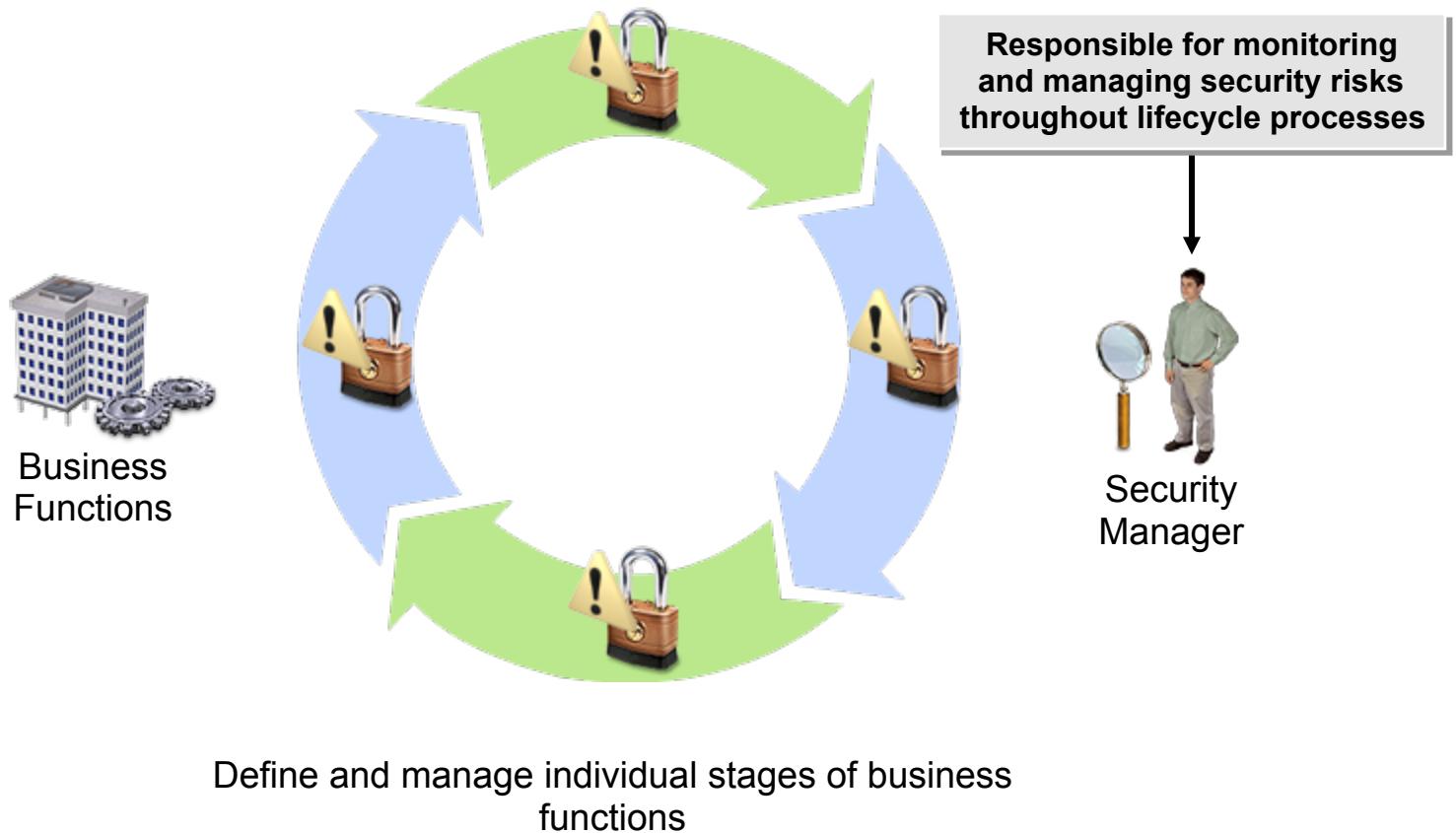


How to Identify and Evaluate Risk Mitigation Strategies

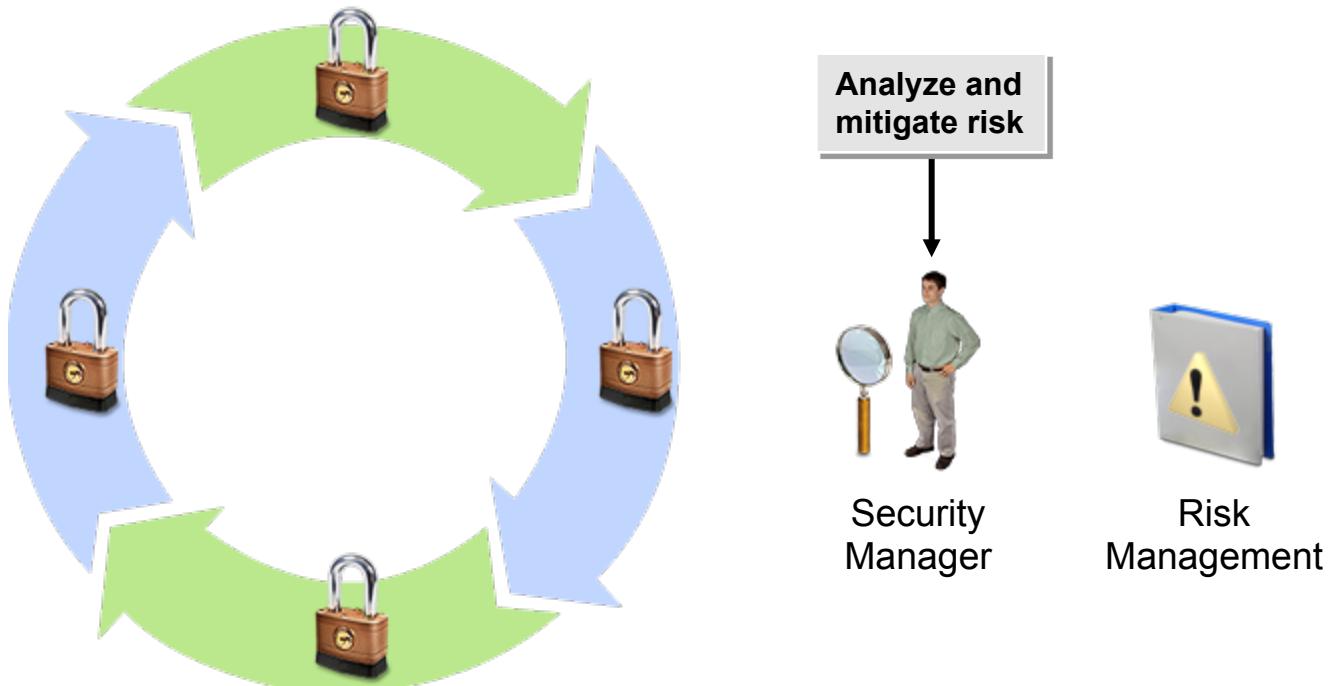
To identify and evaluate risk mitigation strategies:

- Select and implement an information security management methodology.
- Select and establish an impact assessment methodology.
- Define and document methods for measuring the effectiveness of controls and countermeasures.
- Establish metrics that can be used to effectively and repeatedly measure the effectiveness of controls.
- Identify and document acceptable levels of risk.
- Define and document general risk mitigation strategies for the organization.
- Identify potential remedies, controls, and countermeasures.
- Perform a cost benefit analysis on proposed and current controls.
- Establish procedures for identifying gaps in the current control set.
- Continuously communicate within the organization regarding the status of the risk management efforts.

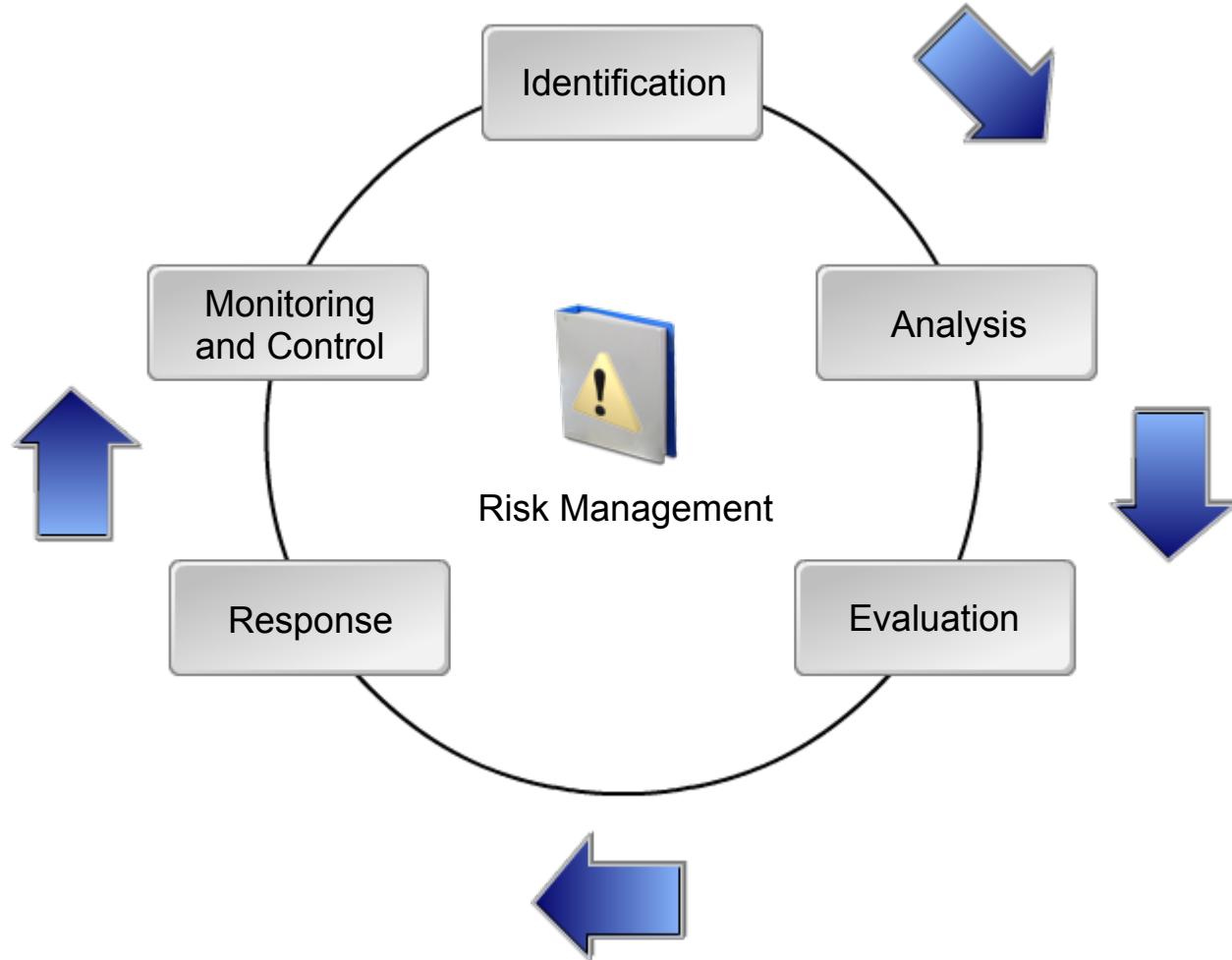
Life Cycle Processes



Life Cycle-Based Risk Management



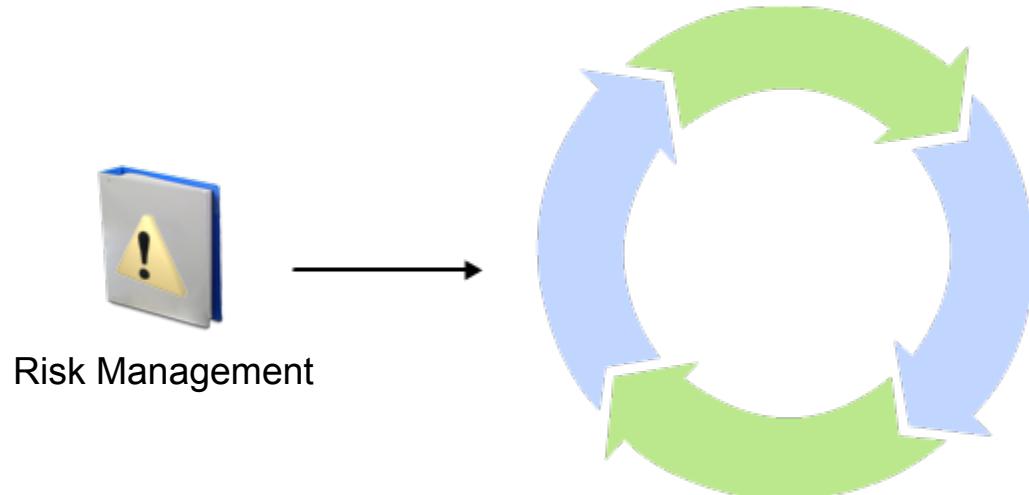
The Risk Management Life Cycle



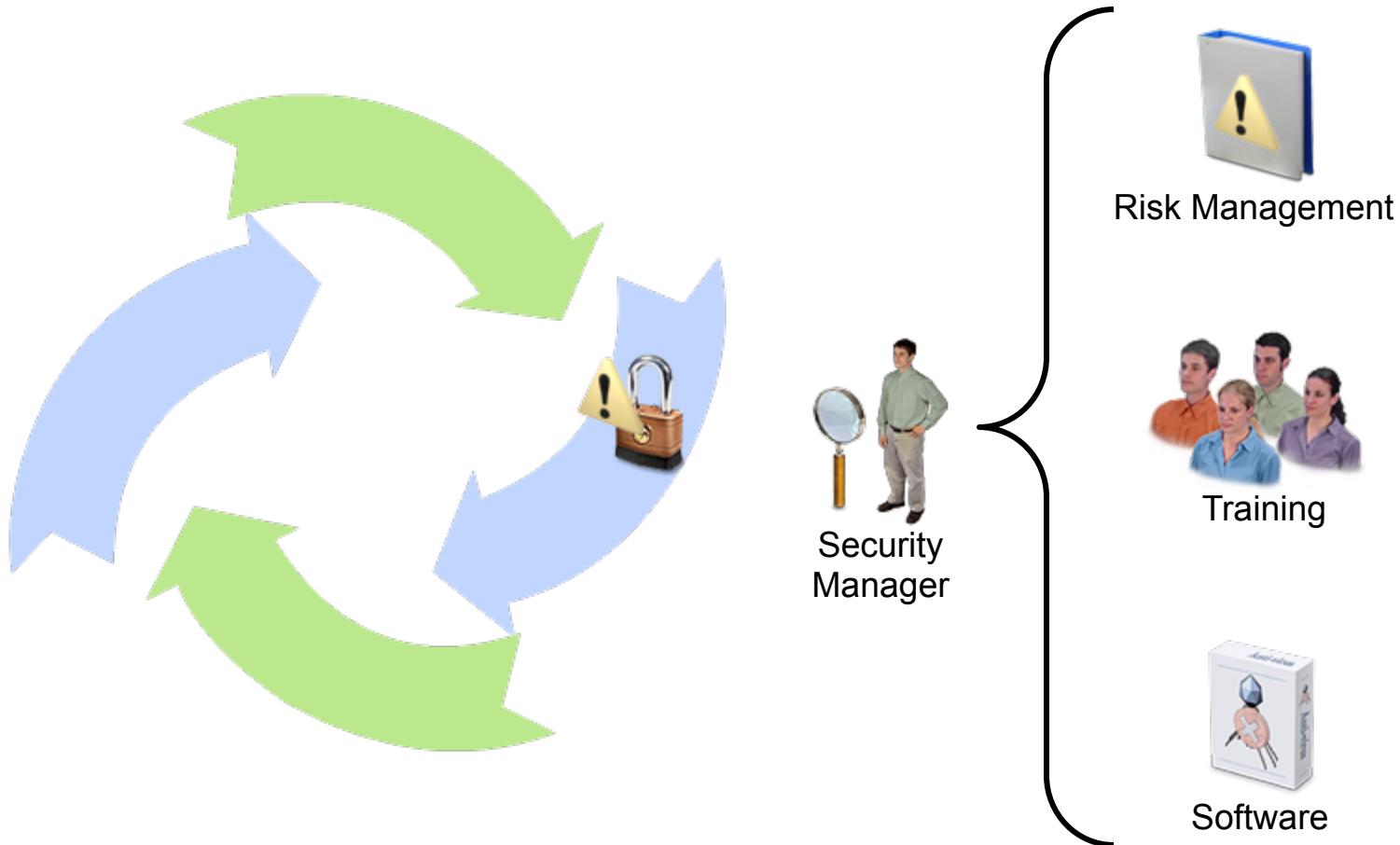
Business Life Cycle Processes Affected by Risk Management

Risk management should be integrated for:

- The change management life cycle.
- The SDLC.
- The project management life cycle.



Life Cycle-Based Risk Management Principles and Practices



How to Integrate Risk Management into Business Life Cycle Processes

To integrate risk management into business life cycle processes:

- Identify the stages in the life cycle processes that require implementation of risk management strategies.
- Use accepted practices to mitigate security risks introduced to the organization through a business life cycle process.
- Monitor changes in the organization's business life cycle processes.

Significant Changes

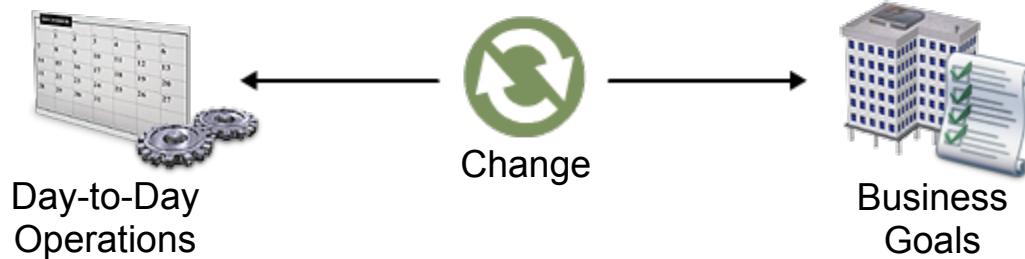
A risk assessment is needed for change in:

- Structure.
- Business processes.
- Tools and technologies.
- Interactions with third parties.

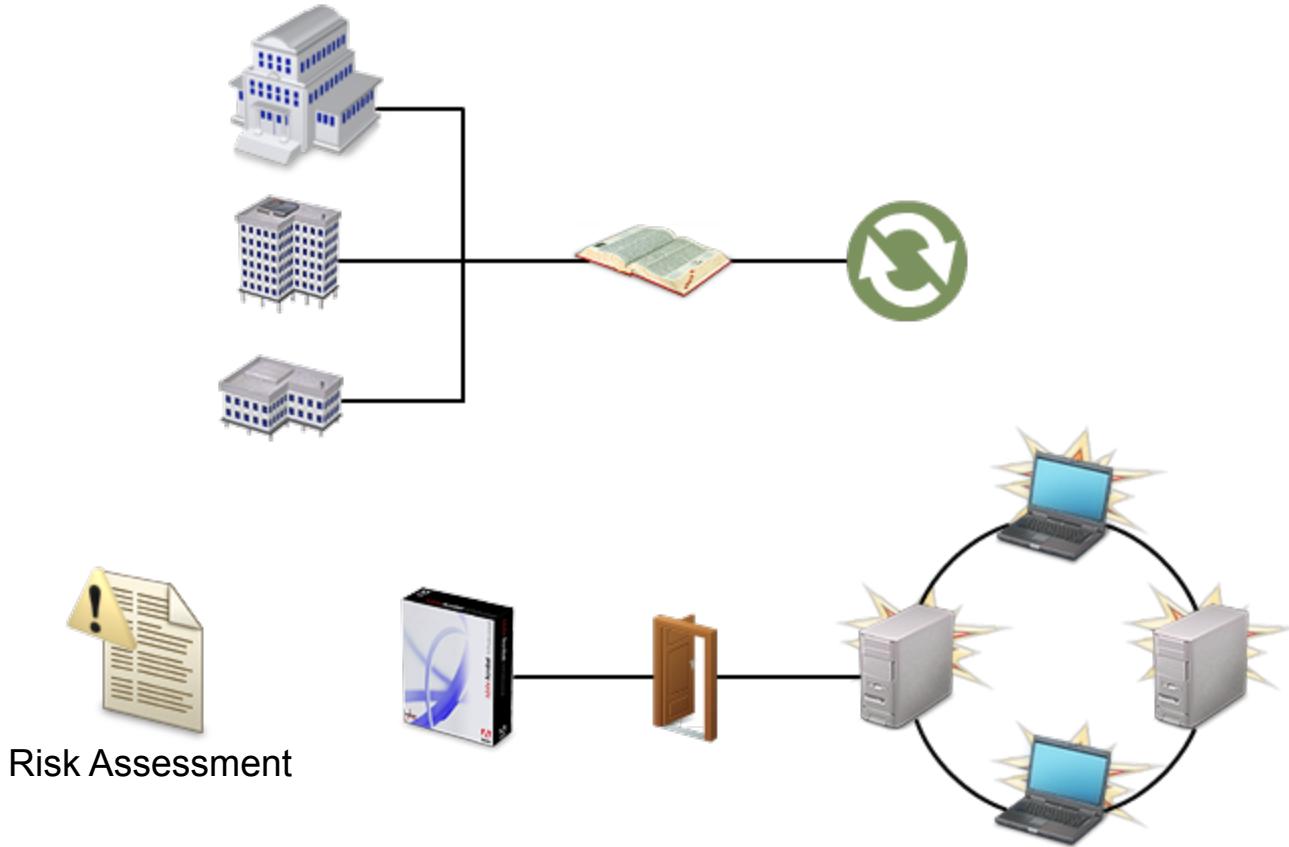
Complete as soon as possible



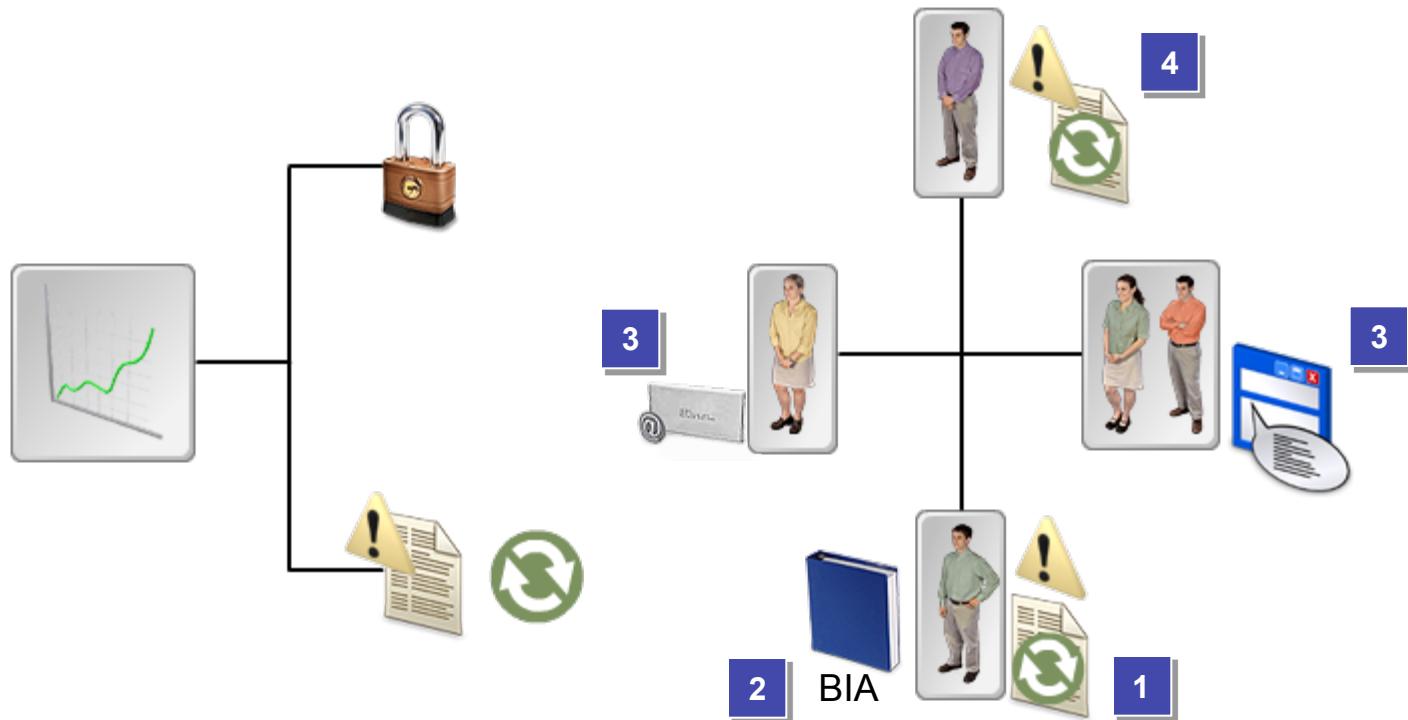
Risk Assessment



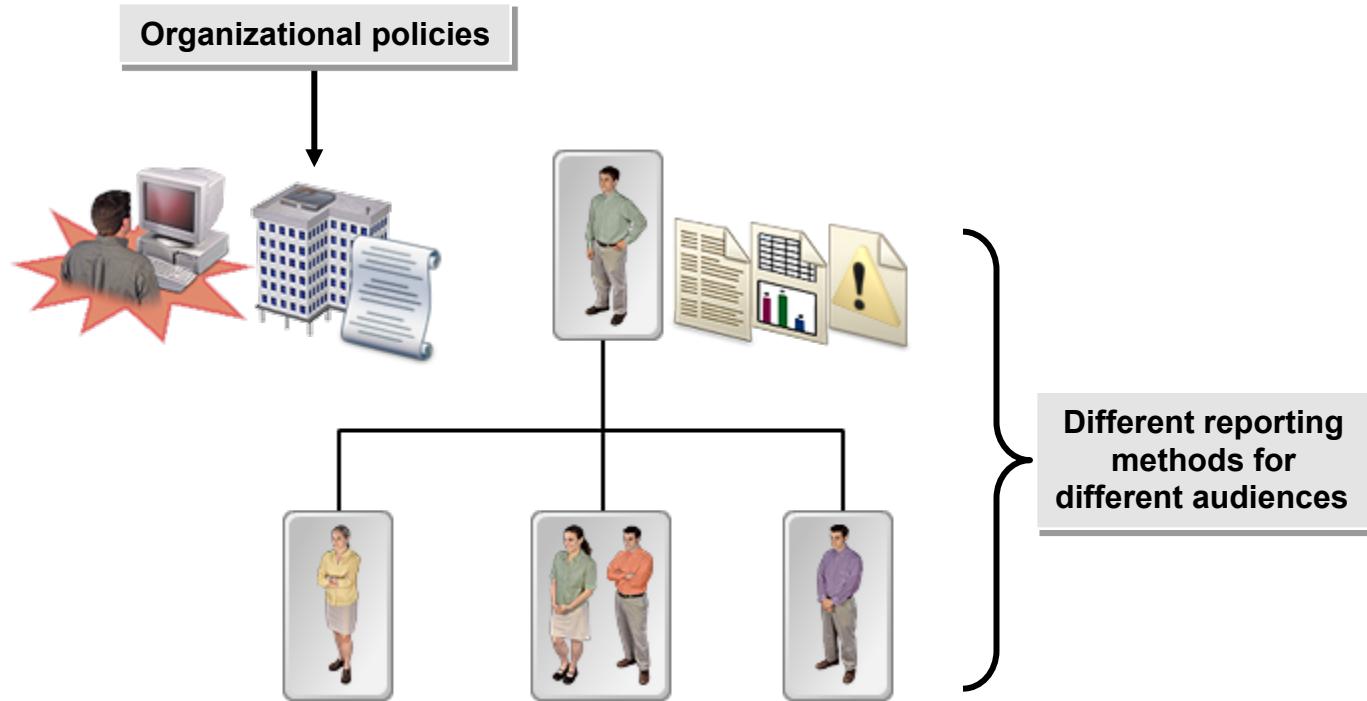
Significant Changes (Cont.)



The Risk Reporting Process



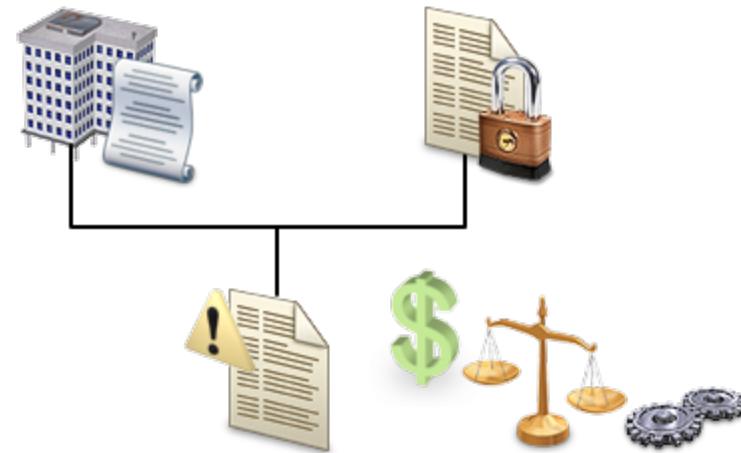
Risk Reporting Methods



Components of Risk Reports

A risk report should include:

- An objective describing the purpose of the report.
- Who the intended audience is.
- What information resources were utilized.
- Which information resources are, were, or will be affected.
- Descriptions of any assumptions made.
- Details of any decisions made.



How to Report Changes in Information Risk

To report changes in information risk:

- Include the documentation and reporting process in the organizational risk management policy.
- Establish a definition and scale for what qualifies as a significant change.
- Develop a risk reporting structure and a chain of communication.
- Define the required contents of risk reports.
- Establish a review schedule and procedures for urgent or emergency reporting.

Reflective Questions

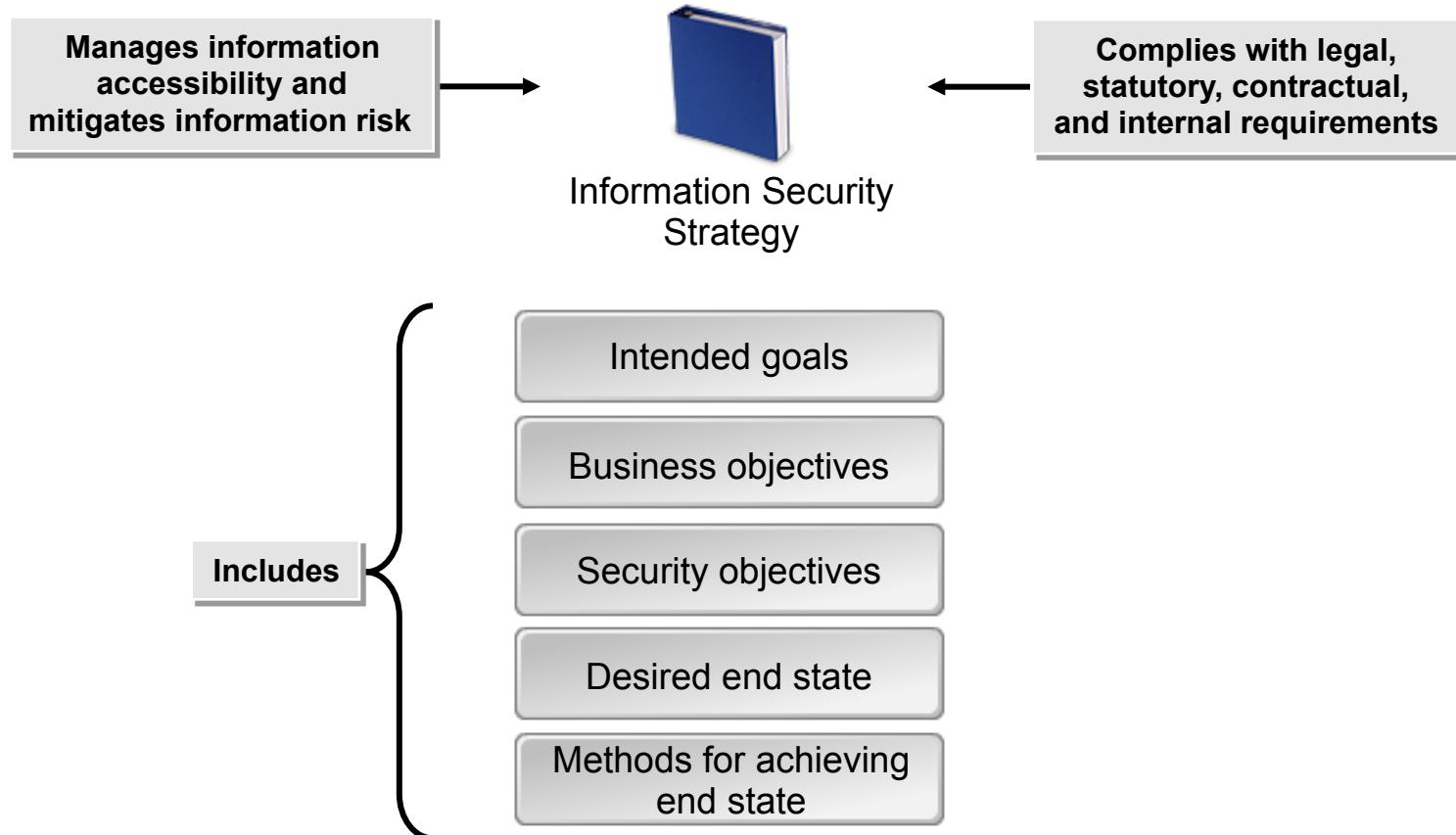
- 1.** In what ways do you feel a BIA can help you in your organization?

- 2.** Have you ever participated in or conducted a risk assessment? If so, what were the steps you took? If not, what steps would you take if you did need to conduct one?

Information Security Program Development

- Develop Plans to Implement an Information Security Strategy
- Security Technologies and Controls
- Specify Information Security Program Activities
- Coordinate Information Security Programs with Business Assurance Functions
- Identify Resources Needed for Information Security Program Implementation
- Develop Information Security Architectures
- Develop Information Security Policies
- Develop Information Security Awareness, Training, and Education Programs
- Develop Supporting Documentation for Information Security Policies

Information Security Strategies



Common Information Security Strategies

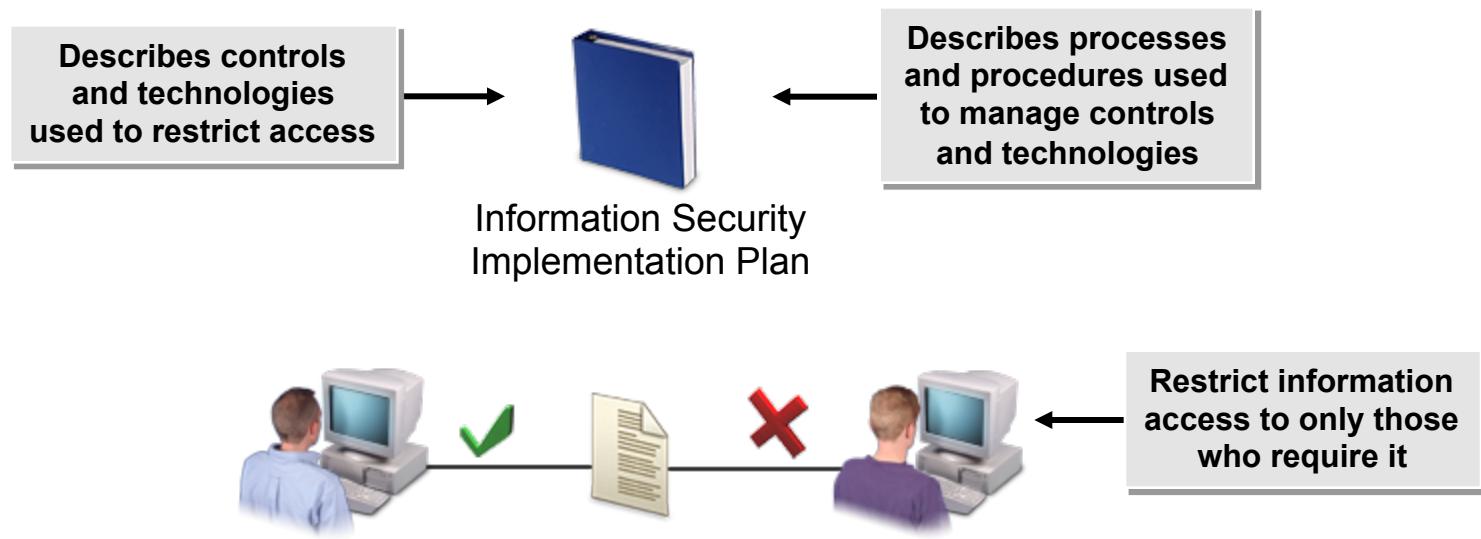
Information security strategies:

- Are based on processes, roles, or best practices
- Include:
 - Building a business case
 - Implementing a risk management process
 - Identifying baseline controls
 - Managing information security initiatives
 - Monitoring the effectiveness of initiatives
 - Conducting security reviews and audits



Information Security
Strategy

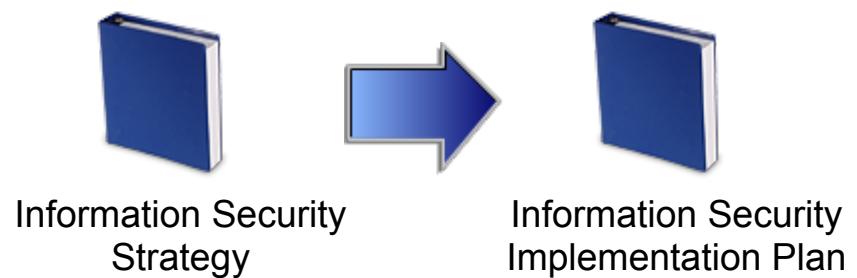
Information Security Implementation Plans



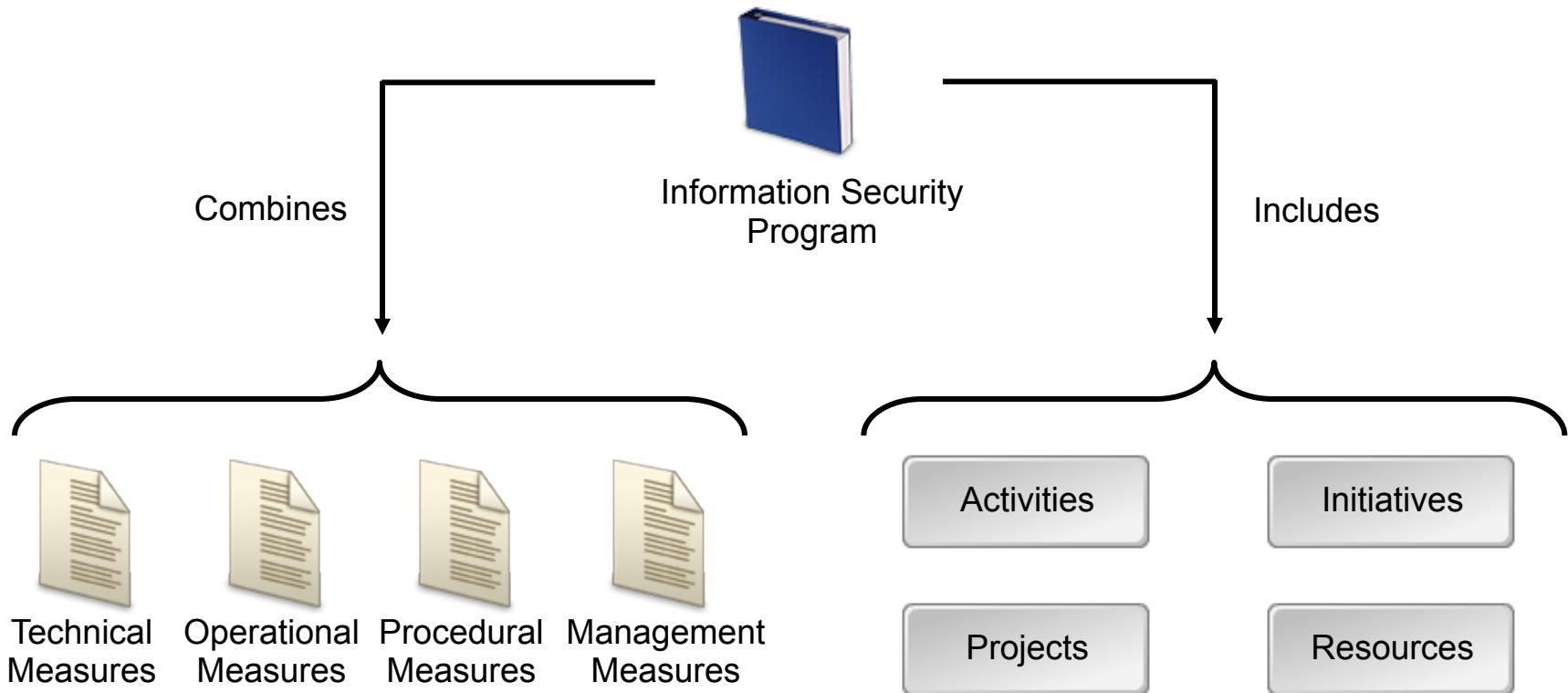
Conversion of Strategies into Implementation Plans

Conversion stages:

- Address incrementally
- Use a top-down approach
- Leverage risk management
- Ensure accountability
- Schedule security reviews
- Assess periodically
- Empower users
- Implement technology
- Determine metrics



Information Security Programs



Information Security Program Maintenance

Maintenance stages for information security programs include:

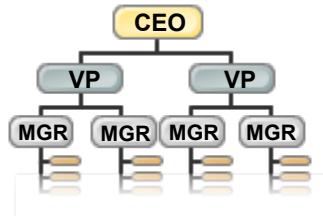
- Evaluate objectives
- Evaluate compliance conditions
- Evaluate program management
- Evaluate operations management
- Evaluate technical management
- Evaluate resources
- Conduct assessments
- Conduct reviews



Information Security
Program

Methods for Maintaining an Information Security Program

Methods for maintaining an information security program include:



Succession
Planning



Allocation
of Jobs

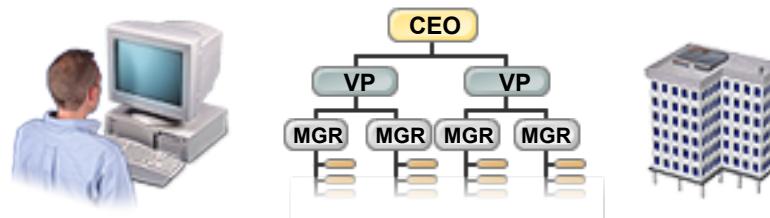


Program
Documentation

Succession Planning

Succession planning includes:

- Identifying long-term organizational goals.
- Identifying positions that require succession planning.
- Identifying potential successors.
- Evaluating the knowledge, skills, and abilities of candidates:
 - Training needed to develop these to acceptable levels.
- Implementing training and evaluating results.



Allocation of Jobs

Position	Description
 CISO	Provides executive oversight for the enterprise's information security initiatives.
 Information security department staff	Information security professionals who will write the policies, standards, guidelines, and the security awareness program. Also includes security administrators who will implement and monitor access permissions.
 Data and system owners	Determine the security requirements for their information assets.
 Asset custodians	Responsible for securing the systems and data. Includes job roles such as server operators and backup operators, information systems auditors, and users.

Program Documentation

The process of documenting an information security program includes the following stages:

- ❑ Develop policy documents:
 - ❑ Comply with organizational and regulatory objectives for data confidentiality, integrity, and availability.
- ❑ Develop standards documents:
 - ❑ Interpret the operational requirements of the policies.
- ❑ Develop processes and procedures:
 - ❑ Step-by-step instructions for complying with the standards.

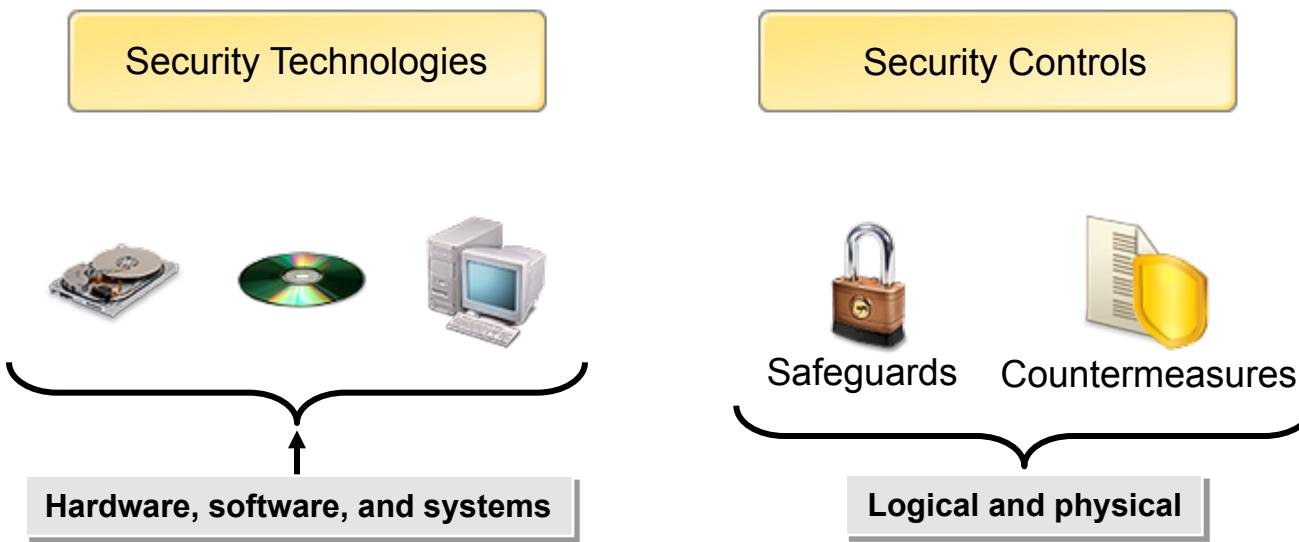


How to Develop Plans to Implement an Information Security Strategy

To develop plans to implement an information security strategy:

- Determine the activities, projects, and initiatives that are most likely to support the objectives of the information security strategy.
- Consider developing an enterprise security architecture at the logical and physical levels.
- Identify technical, procedural, and physical controls to be used in activities, projects, and initiatives.
- Determine which controls need to be developed and implemented in the existing infrastructure, and identify plans for developing and implementing new or revised controls.
- Identify the order in which the controls should be implemented.
- Develop program documentation, including policy documents, standards documents, and processes and procedures.
- Determine and document the resources necessary to implement the plan.

Security Technologies and Controls



Cryptographic Techniques

Common cryptographic techniques include:



Symmetric, or
Shared, Key

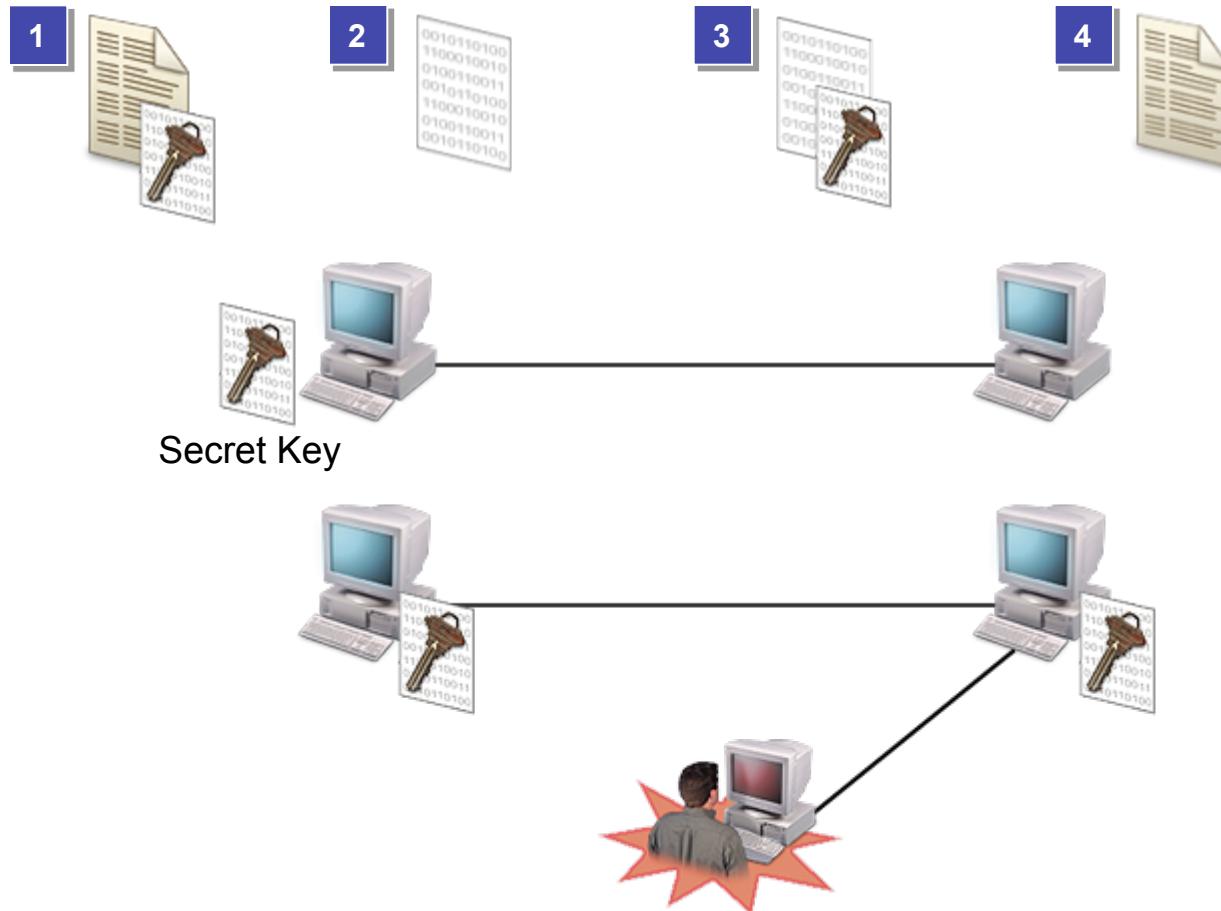


Asymmetric,
or Public, Key



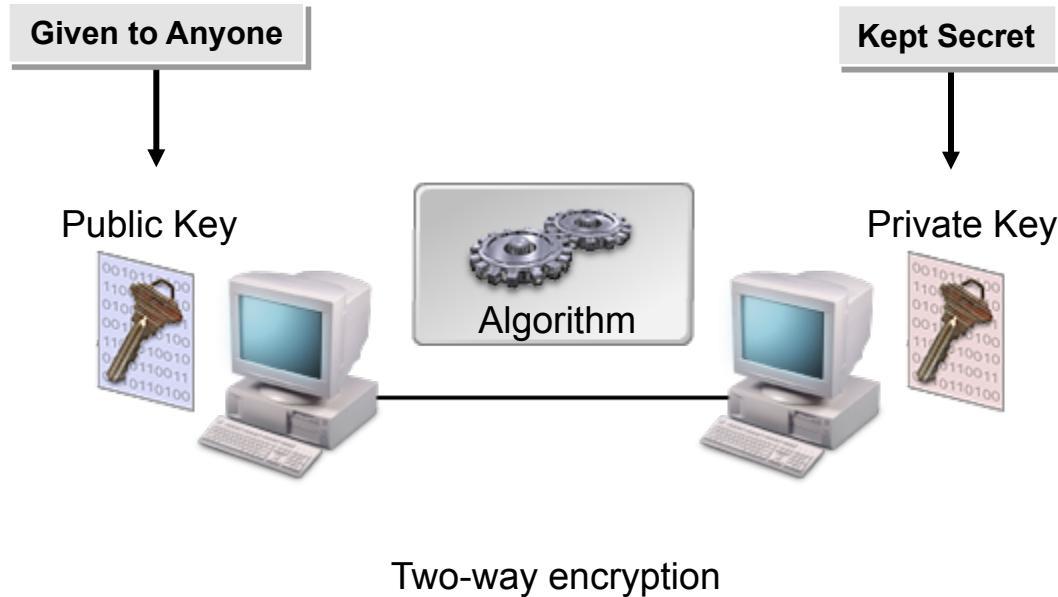
Hashing

Symmetric Cryptography



Fast, but vulnerable if key is lost or compromised

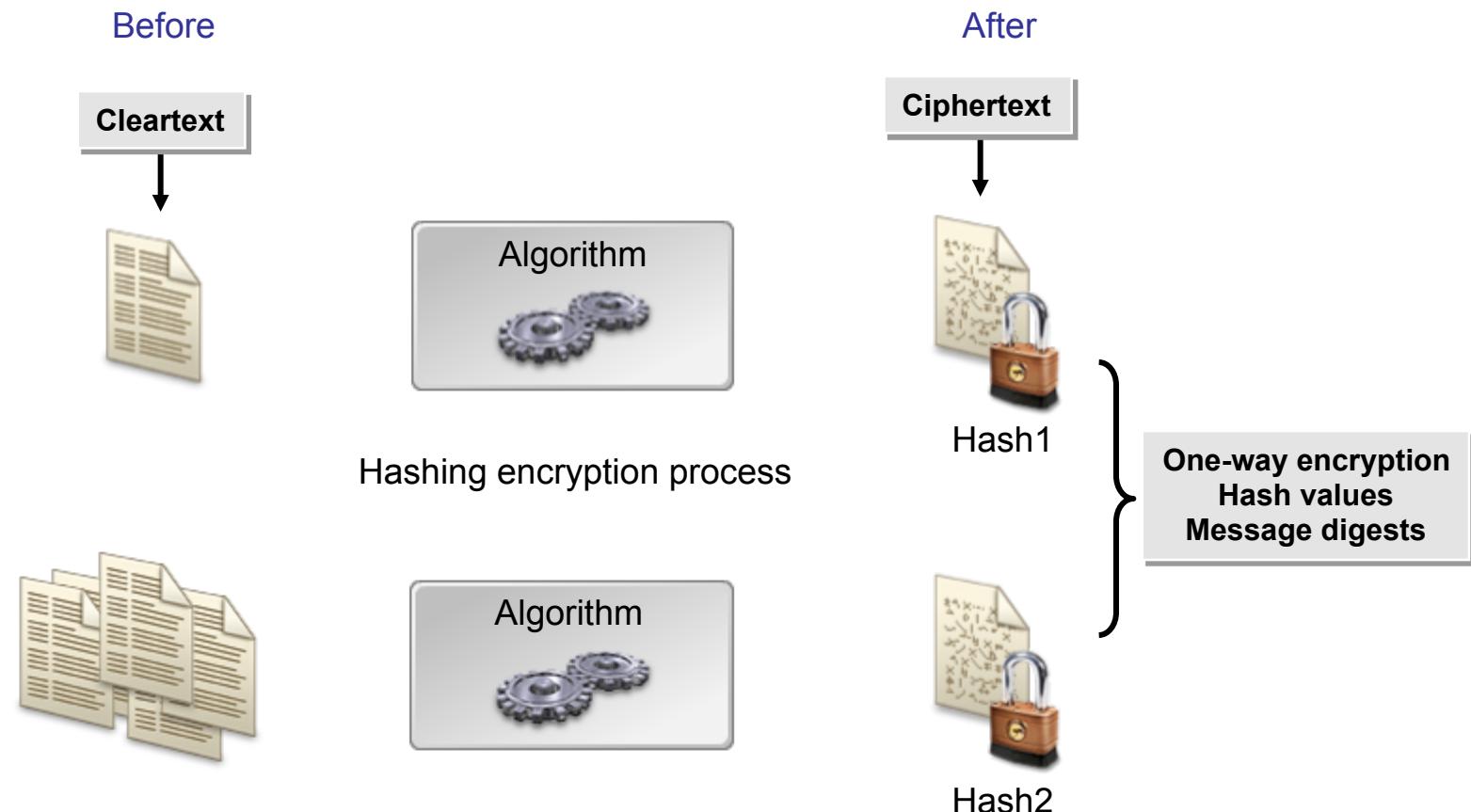
Public Key Cryptography



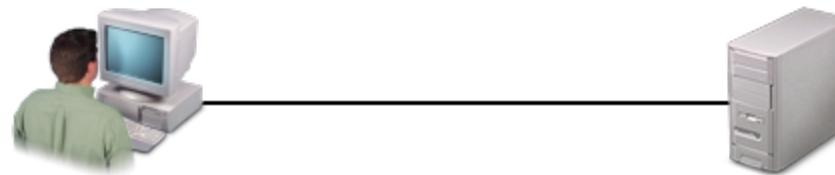
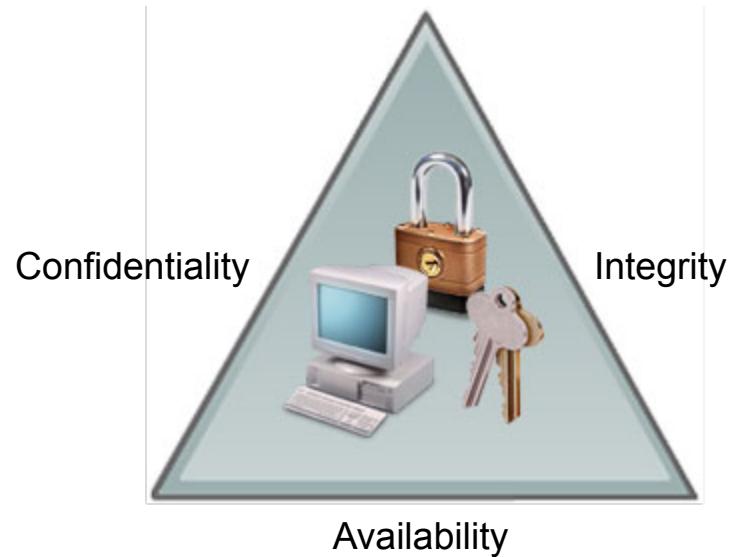
Hashes

Compare Hash1 and Hash2:

- Matching = Secure information
- Different = Possibly altered information



Access Control



Subject = Entity requesting access

Object = Entity being accessed

Access Control Categories

Access control:

- Prevents unauthorized access to facilities, systems, network resources, and information
- Is enforced through individual and organizational accountability
- Requires identification and validation before permitting or limiting access to information or network resources
- Can be categorized several ways

Access control categories include:

- Management approach
- Focus

Physical Access Controls

Physical access controls include:

- Locks and locked rooms and buildings.
- Alarm systems.
- Surveillance cameras.
- Electronic access control systems.

Technical Access Controls



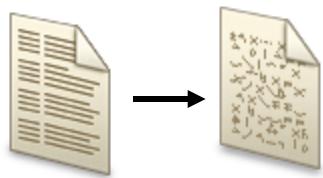
Authentication systems



Anti-virus systems



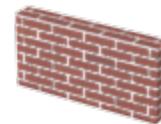
Role-based rights assignments



Encryption



VPNs



Firewalls

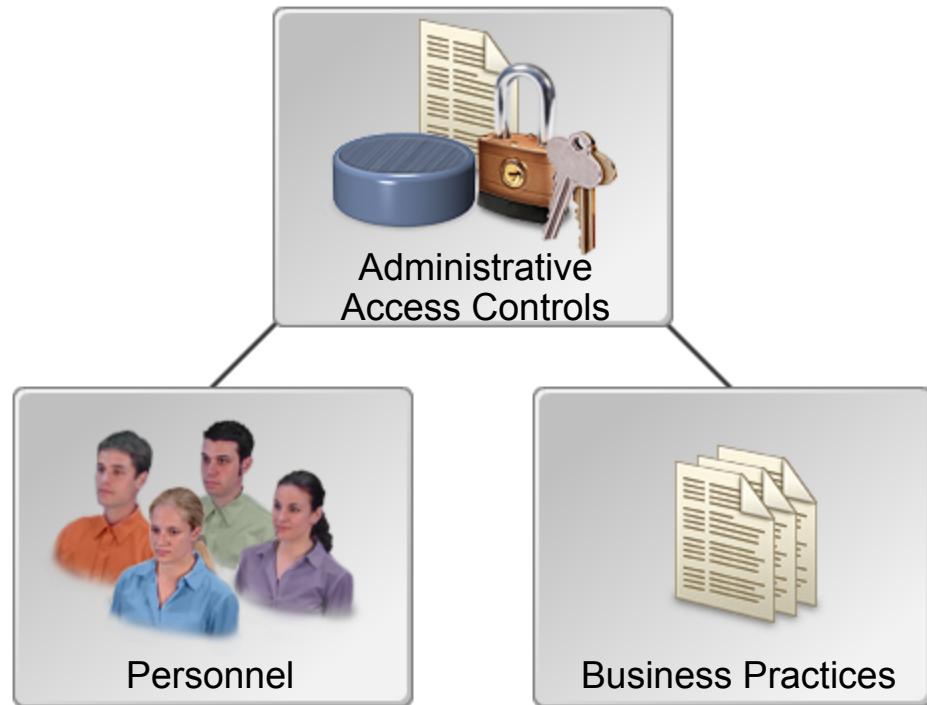


Routers

Administrative Access Controls

Administrative access controls include:

- Policies.
- Procedures.
- Hiring practices.
- Background checks.
- Data classification.
- Training.
- Personnel reviews.



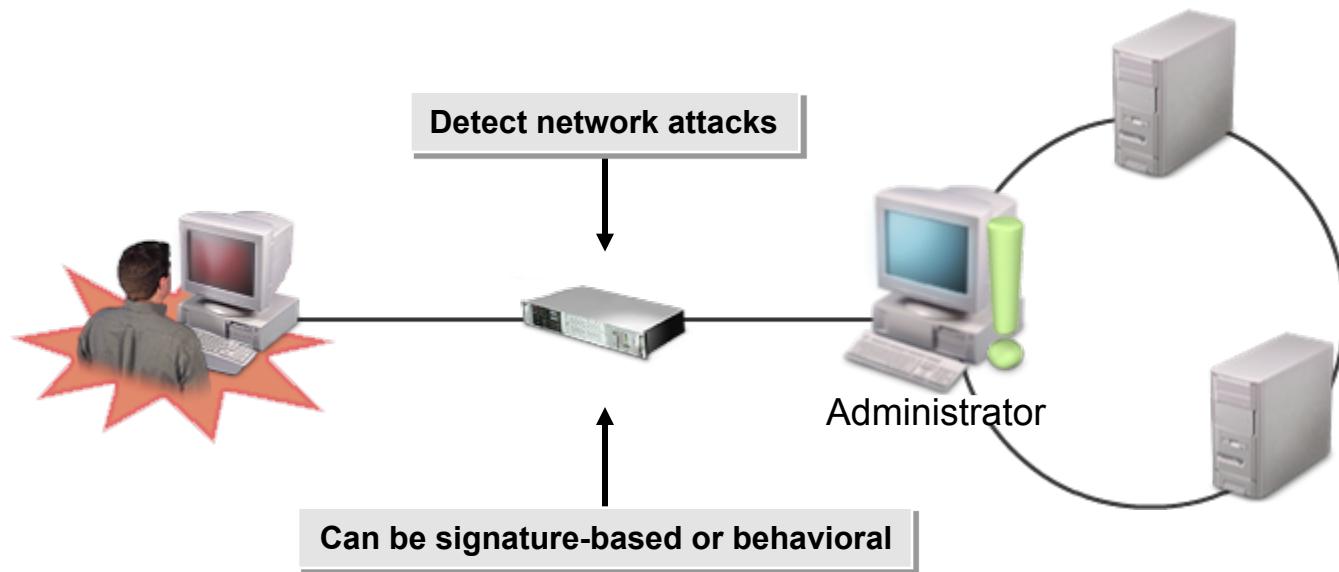
Monitoring Tools

Monitoring tools include:

- Network security scanners.
- Alarm monitoring systems.
- IDSs.
- Web security utilities.



IDSs



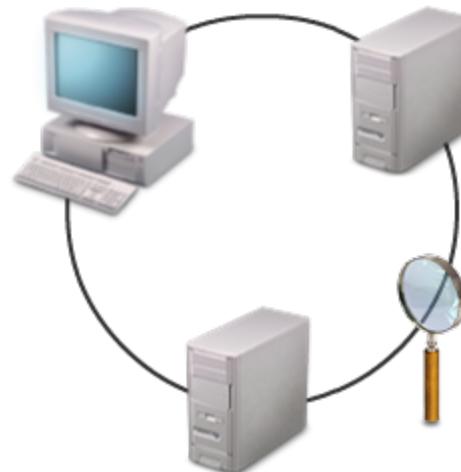
Common IDSS

IDSS can be:

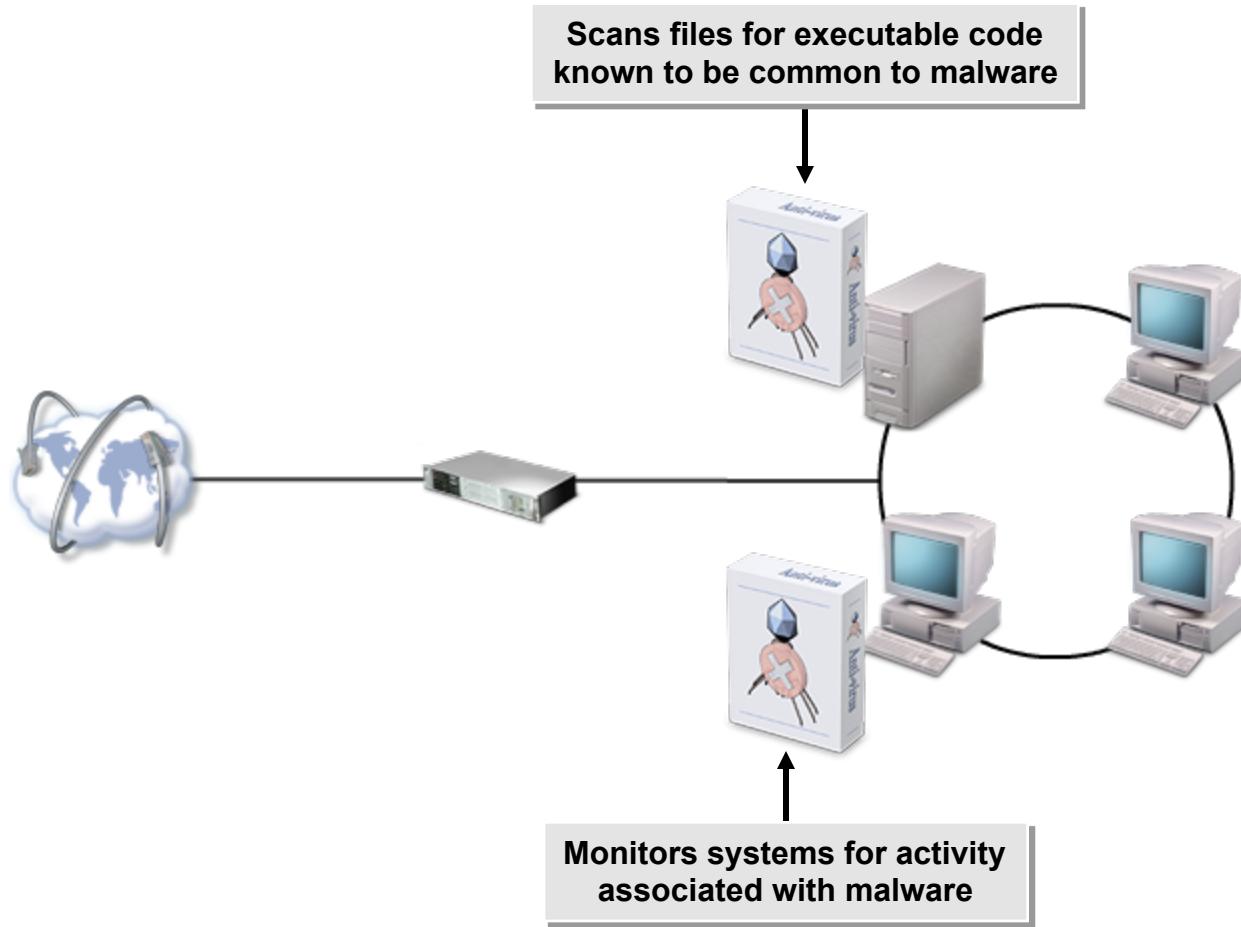
- Network-based
- Protocol-based
- Application-based
- Host-based

IDSS can also be:

- Passive
- Reactive



Anti-virus Systems



Common Anti-virus Systems

Common anti-virus systems manufacturers include:

- McAfee®
- Symantec™
- BitDefender®
- AVG®
- avast!®
- CA®

Mobile Devices

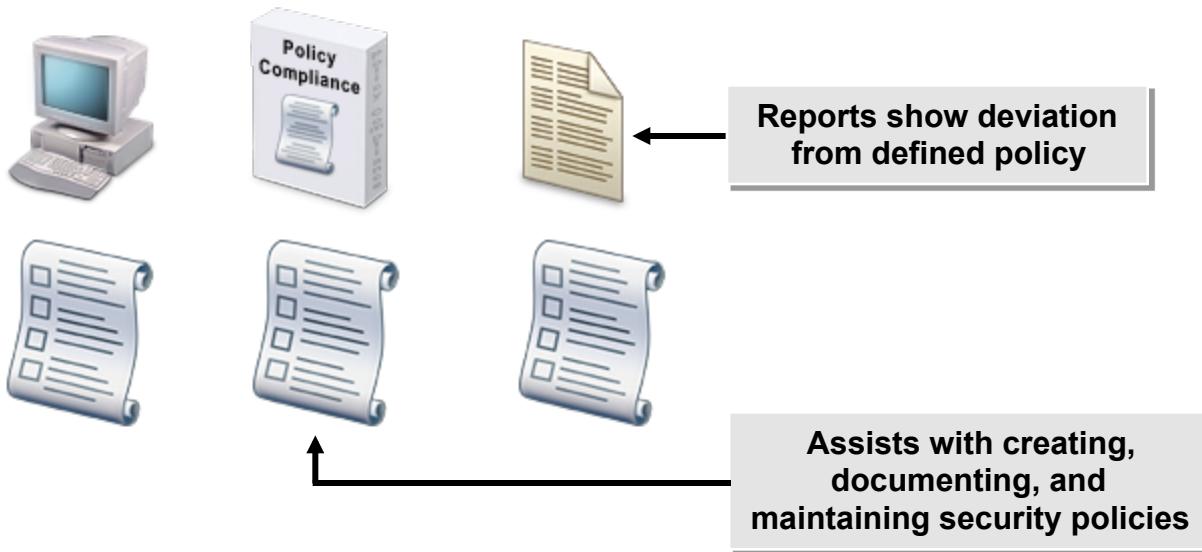


Computers



Servers

Policy-Compliance Systems



Common Policy-Compliance Systems

Common policy-compliance systems include:

- Bsafe
- nCircle
- Group Policies in the Microsoft® Windows® Active Directory® service
- Policy Auditor



Common Activities Required in Information Security Programs

Activities commonly required in information security programs include:

- Continuity planning.
- Anti-virus protection initiatives.
- Security awareness, training, and education initiatives.
- Addressing social networking and other Web 2.0 threats.
- Incident response.
- Protecting mobile devices.
- Addressing social engineering techniques.
- Managing cryptographic keys.



Prerequisites for Implementing the Program

Implementation of the information security program can begin after:

- Security objectives are determined and approved.
- Resources are identified and available.
- Control objectives are determined, and controls design is started.
- Security reviews and audits are established.
- Management buy-in is obtained.



Implementation Plan Management

Managing the information security implementation plan includes several stages:

- Ensure policy and standards compliance
- Provide awareness, training, and educational materials
- Establish control objectives and define controls
- Implement countermeasures
- Ensure commitment of third-party service providers
- Integrate into life cycle processes
- Monitor controls



Information Security
Implementation Plan

Types of Security Controls

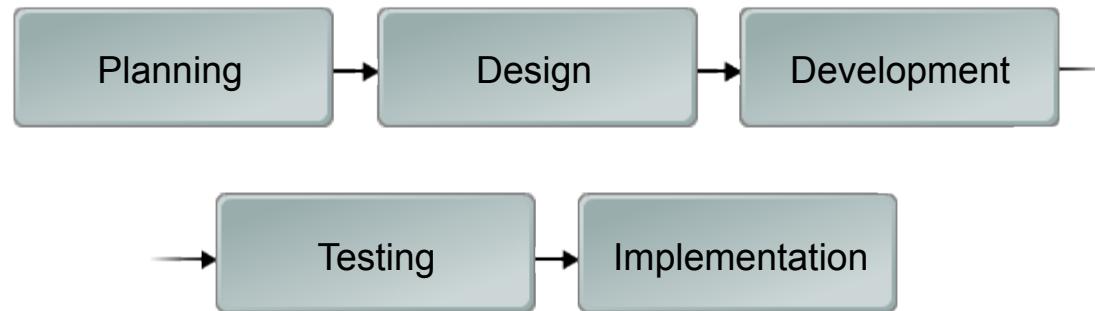
Types of security controls include:

- Preventative
- Deterrent
- Detective
- Corrective
- Recovery
- Compensating



Controls

Information Security Controls Development



How to Specify Information Security Program Activities

To specify information security program activities:

- Determine which activities, such as continuity planning and anti-virus protection initiatives, need to be included in your information security program.
- Identify the objectives in your information security strategy that are not addressed by the identified activities, and determine the possible controls that would address those objectives.
- Identify the personnel required to perform each activity.
- For each control identified as being necessary, determine whether or not existing solutions are available. If solutions are not available, they will need to be developed and tested prior to implementation.
- Document all activities, controls, and required personnel, and include this information in the information security program documentation.

Business Assurance Function

Business assurance functions:

- Are provided by departments, other organizational entities, or external entities.
- Support the enterprise by directly or indirectly affecting the security of the enterprise and its information assets.
- Help ensure compliance with legal requirements.
- Can provide services to other parts of the enterprise to support business-critical activities.



Common Business Assurance Functions

Business assurance functions to be aligned with the information security program:

- Auditing
- HR
- Risk management
- Physical security
- Privacy
- Compliance
- Legal
- Quality assurance
- IT
- Help desk

Methods for Aligning Information Security Programs with Business Assurance Functions

To align security programs with business assurance functions:

- Present the program to ISSG.
- Assign a business representative to the information security department.
- Align the program with security requirements in SLAs.



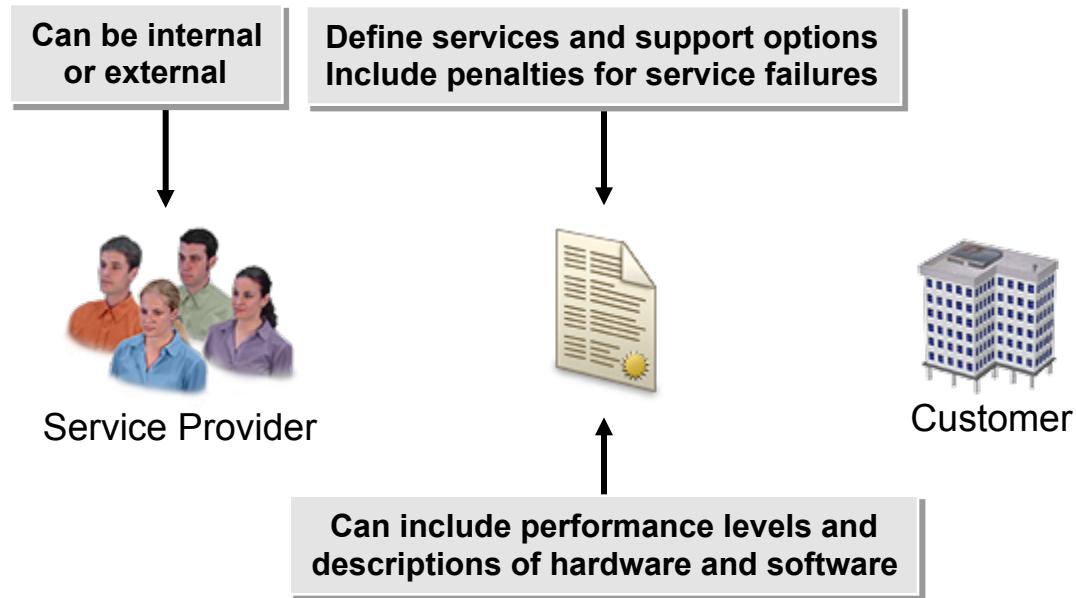
Information Security
Program

How to Coordinate Information Security Programs with Business Assurance Functions

To coordinate information security programs with business assurance functions:

- Identify the business assurance functions in your organization that will need to be aligned with the information security program.
- Meet with the managers in the identified functional areas to determine the best path for coordinating the business assurance functions with the information security program. Possible solutions include:
 - Establishing formal lines of communication between the areas.
 - Implementing reporting and monitoring processes.

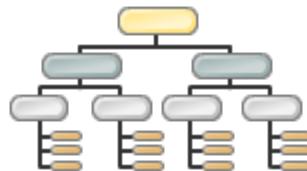
SLAs



Internal Resources



Documentation



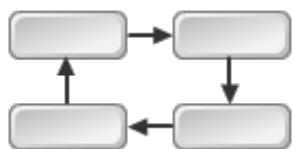
Organizational structures



Audits



Risk and business impact assessment



Architectures



Personnel



Compliance enforcement



Threat and vulnerability analysis



Controls and countermeasures



Knowledge, skills, and abilities



Resource dependency analysis

External Resources

Common external resources include:

- External security service providers
- External support organizations



Services Provided by External Resources

External security service providers:

- Business continuity planning assistance.
- Security architecture development and engineering services.
- Consulting services to define items, such as security roles and responsibilities.
- Development and documentation of control activities.
- Physical security, such as securing the perimeter of organizational properties.
- Personnel screening services.
- Auditing services.
- Security review services, including penetration testing and reporting services.
- Incident response services, such as forensic investigation and recovery services.

Services Provided by External Resource (Cont.)

External support organizations:

- ❑ Good or best practices organizations can:
 - ❑ Provide data that can be used to evaluate an information security program.
 - ❑ Help information security managers keep current with emerging threats and technologies, laws and regulations, and management techniques.
- ❑ Security networking conferences or roundtables can provide organized discussions of common security topics.
- ❑ Security training organizations can provide instruction on technical information security issues, such as the configuration of security technologies and vulnerability analysis.
- ❑ Vulnerability alerting services enable information security managers to be apprised of any vulnerabilities detected in the security technologies being used in the organization.

Skills Commonly Required for Information Security Program Implementation

Required skills and knowledge:

- Project management
- Financial management and budgeting
- Communications
- Negotiations
- Needs assessment
- Gap analysis
- Interpersonal skills

Identification of Resources and Skills Required for a Particular Implementation

Identifying required resources and skills:

- Research past implementations.
- Refer to industry standards.
- Refer to international standards.
- Review controls and technologies to be implemented.

Resource Acquisition Methods



Budgeting



Purchasing



Training existing
employees



Hiring

Skills Acquisition Methods

Skills acquisition methods:

- Borrowing employees
- Training employees
- Hiring employees
- Contracting or outsourcing



Required Skills



New Hire



On Loan



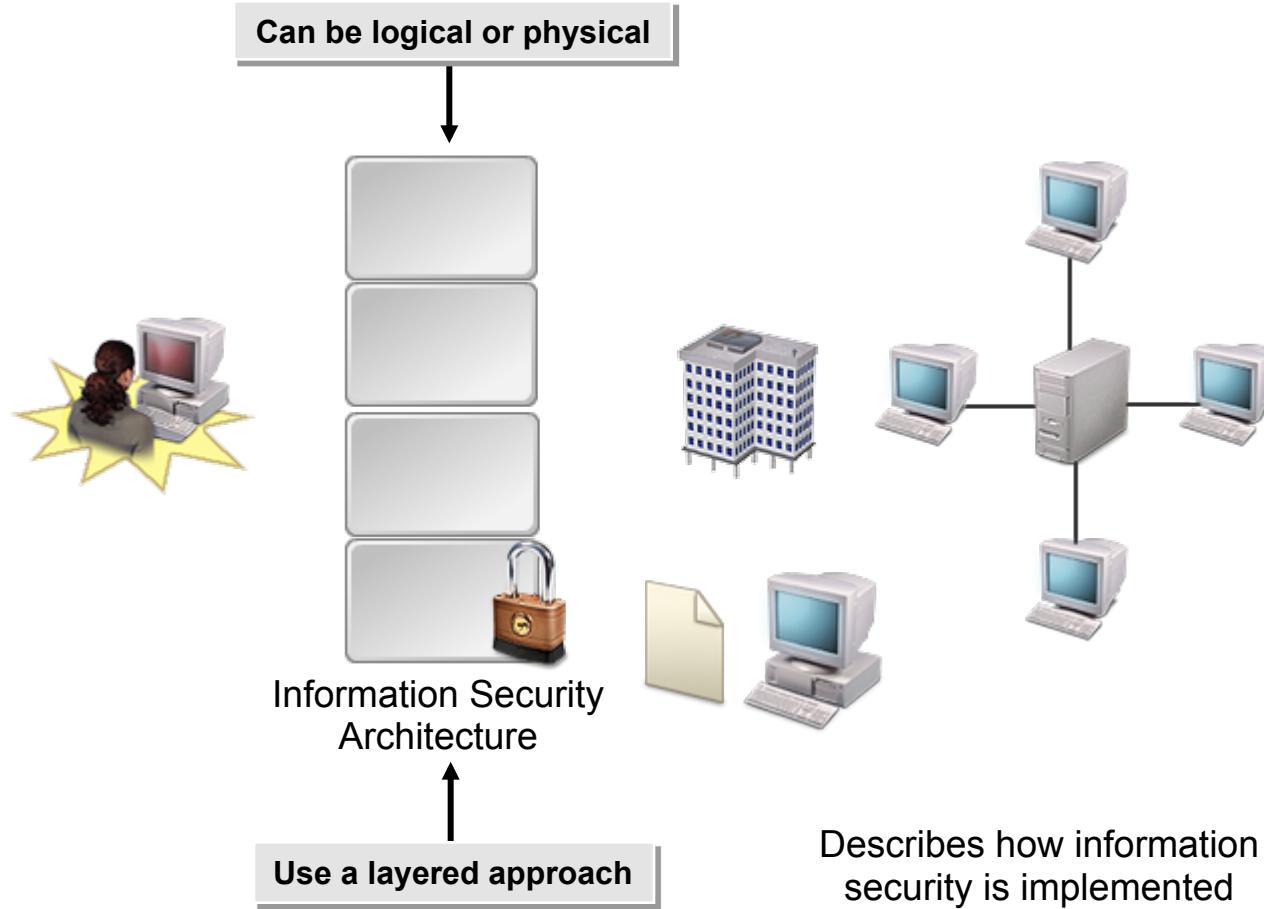
Contractor

How to Identify Resources Needed for Information Security Program Implementation

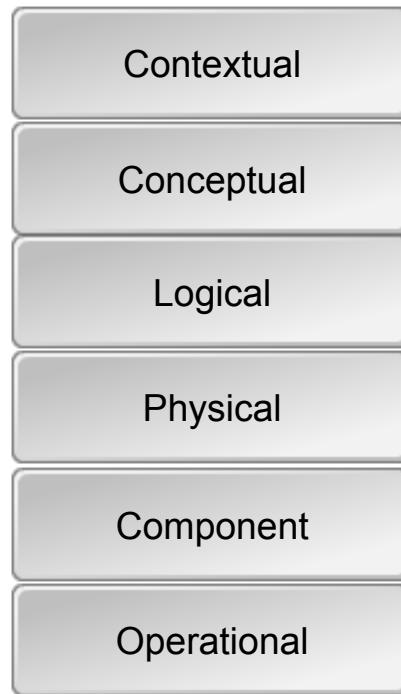
To identify the resources needed for an information security program implementation:

- Determine the internal resources needed to implement the information security program.
- Determine the external resources needed to implement the information security program.
- Determine the skills required to implement the information security controls, and compare them to the skills of existing personnel.
- Determine what training or additional staffing will be required to raise skill levels to where they need to be to implement the controls.

Information Security Architectures



The SABSA Model for Security Architecture



Deployment Considerations

Deploying information security architectures:

- Is often accomplished in phases due to cost, resource, and time constraints
- Can be phased in using implementation blueprints based on business objectives and cost

Successful implementation:

- Learn how to use the architectural components.
- Implement security procedures:
 - Protect hardware and software.
 - Use technical and procedural controls.



Information Security
Architecture

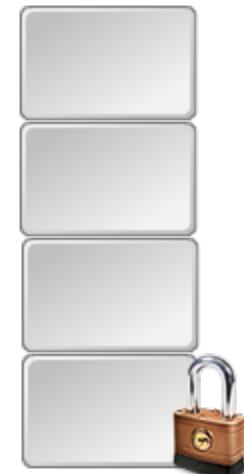
Deployment of Information Security Architectures



How to Develop Information Security Architectures

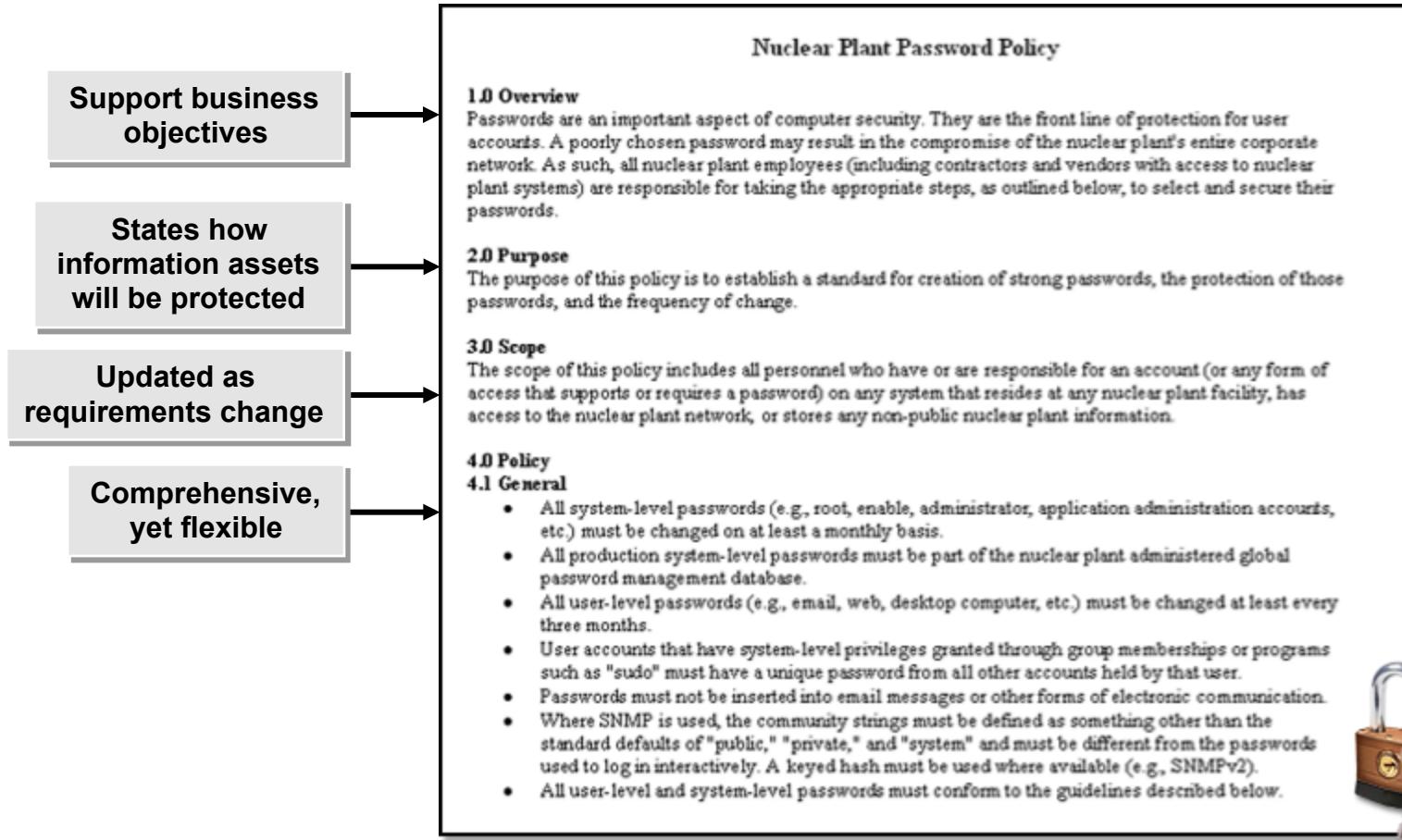
To develop information security architectures:

- ❑ Determine the information security architecture model that will provide the organization with the level of detail necessary to create an information security framework that addresses how information security is to be implemented.
- ❑ Identify the layers of the security architecture that need to be defined.
- ❑ Define the various security architectures that need to be implemented.
- ❑ For each layer of the security architecture that needs to be defined, analyze and document the following:
 - ❑ The assets to be protected.
 - ❑ The reason for the protection.
 - ❑ The process by which the protection will be implemented.
 - ❑ The personnel responsible for implementing the process.
 - ❑ The role responsible for maintaining the process.
 - ❑ The location where the protection will be applied.
 - ❑ The timeline for implementing the protection.



Information Security
Architecture

Information Security Policies



Components of Information Security Policies



Information
Security Policy



AUP



Education



Measurement

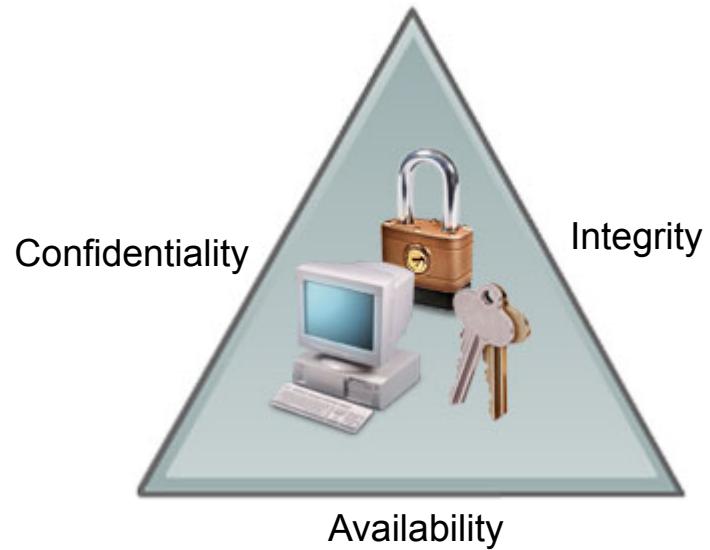


Evaluation

Information Security Policies and the Information Security Strategy



Information
Security Strategy



Policies are the practical embodiment of the security strategy.

Information Security Policies and Enterprise Business Objectives

Policies should ensure that:

- Business objectives can be achieved.
- Detrimental events can be prevented or identified and rectified.



Enterprise Business
Objectives

Information Security Policy Development

Factors



Communication



Budget constraints



Culture



Regulatory
requirements



Strategic plans



Security threats

Methods for Communicating Information Security Policies



Physical documents



Electronic documents



Formal training



Computer-based training



Login screens



Meetings and seminars

Information Security Policy Maintenance

Maintenance process:

- Periodic review
- Addition of new policies
- Revision
- Retirement
- Documentation



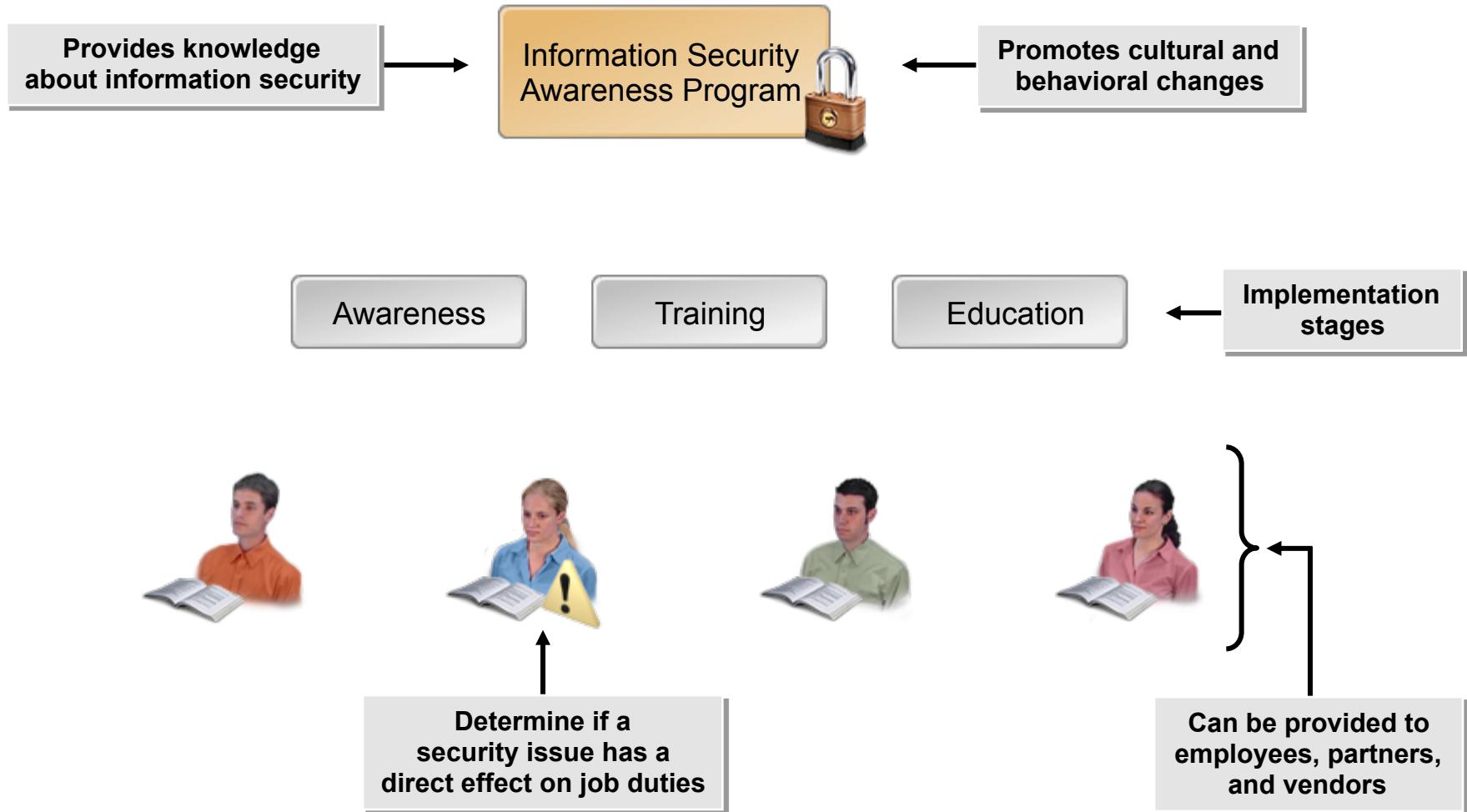
How to Develop Information Security Policies

To develop information security policies:

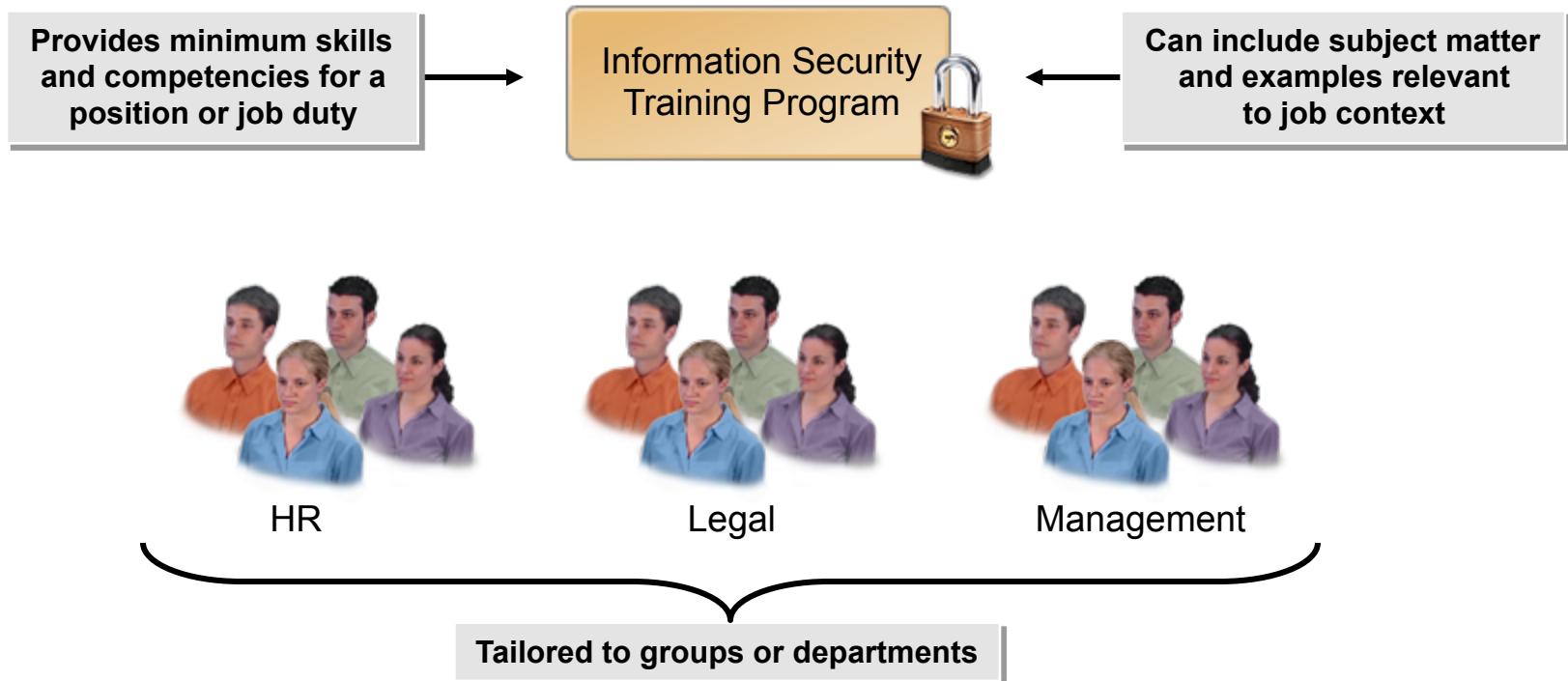
- Examine existing organizational policies to ensure that they meet and support enterprise business objectives, and revise as necessary.
- Examine the information security strategy to determine the new information security policies that are required.
- Review international, governmental, and industry standards to determine what policies need to be developed to conform to the applicable standards.
- Develop any new information security policies that are required to support the enterprise business objectives, the information security strategy, and applicable standards.
- Communicate the information security policies to all areas of the organization that will be affected by them.
- Conduct periodic reviews and revisions of information security policies to ensure that they are aligned with business objectives and the information security strategy.



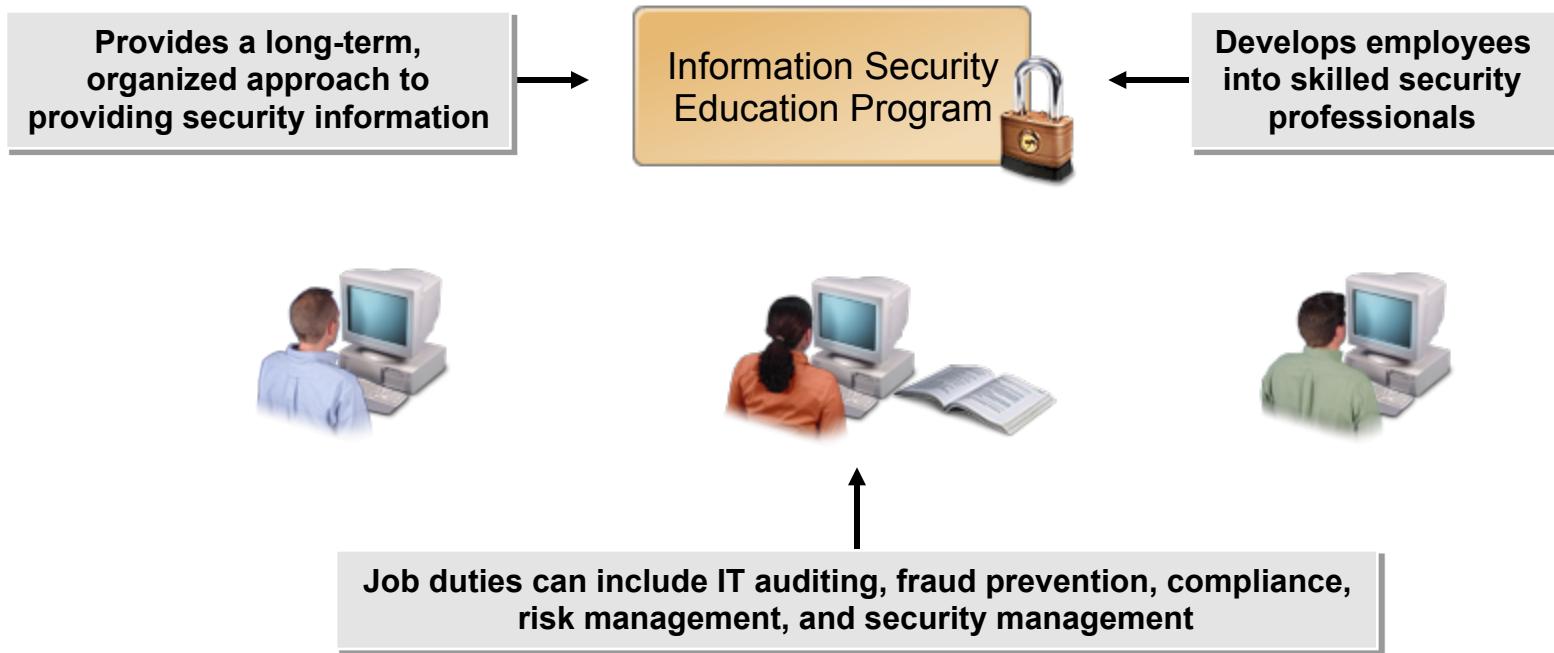
Information Security Awareness Programs



Information Security Training Programs



Information Security Education Programs



Security Awareness, Training, and Education Gap Analysis

1. Identify knowledge needed for awareness
2. Identify current proficiency levels
3. Identify knowledge needed to reach proficiency levels
4. Review violations
5. Address current alerts

Methods for Closing the Security Awareness, Training, and Education Gaps



Awareness activities



Training and education



Documentation

Security-Based Cultures and Behaviors

Security-based behavior:

- Actions performed in a manner that protects information, data, and knowledge.

Security-based culture:

- An organizational environment that practices and reinforces security-based behaviors.



Methods for Establishing and Maintaining a Security-Based Culture in the Enterprise

Establishment and maintenance of security-based cultures:

- Communicate
- Provide guidance
- Play a consultative role
- Encourage security-based behavior
- Show support from executive management
- Recognize success

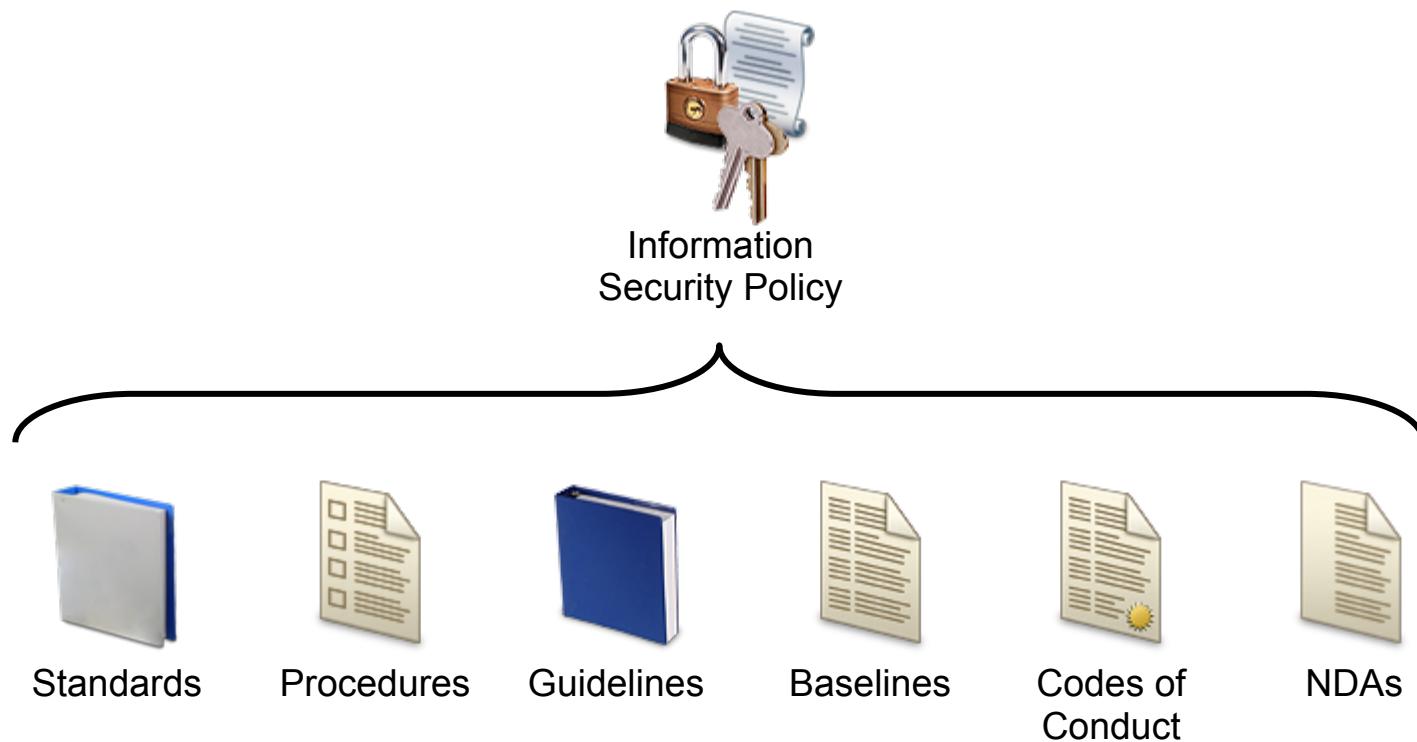


How to Develop Information Security Awareness, Training, and Education Programs

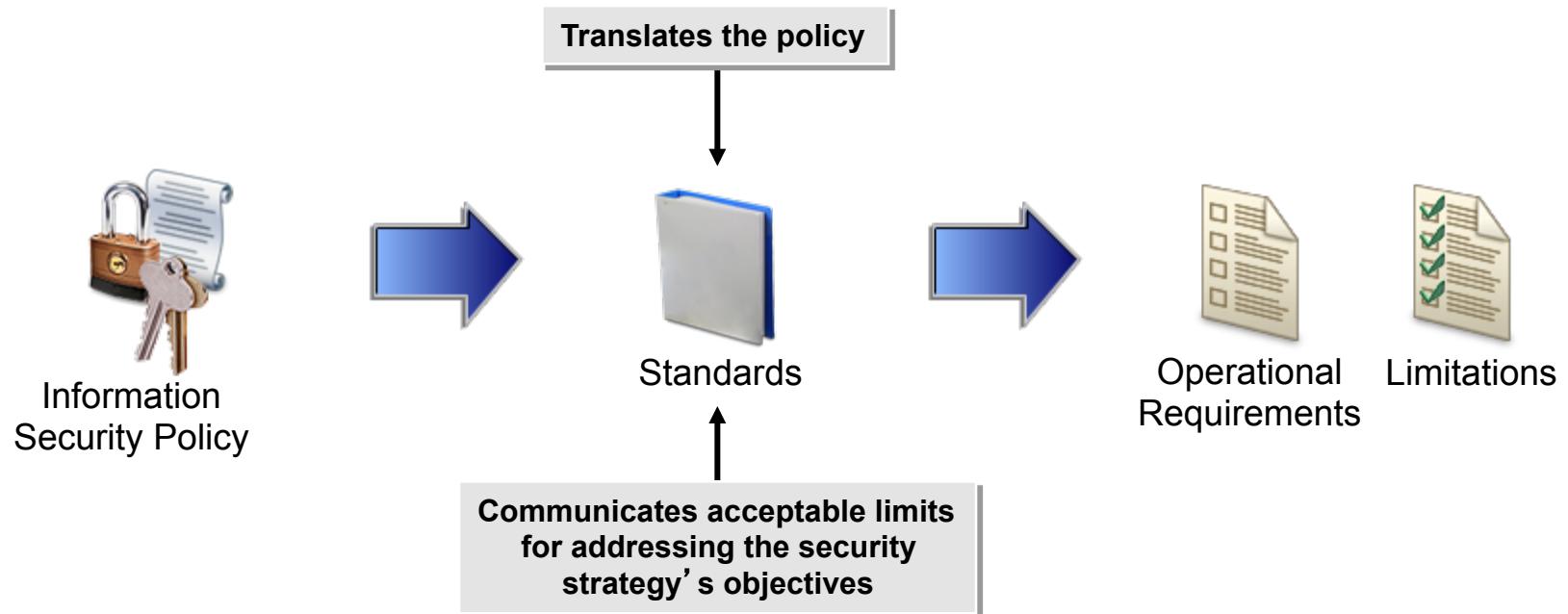
To develop information security awareness, training, and education programs:

- Analyze all job positions to determine what level of information security awareness, training, or education might be necessary.
- Identify the behaviors that are necessary for performing job duties in a manner that considers information security as an additional required outcome.
- Identify the proficiency levels of staff, and analyze the gaps between proficiency levels and the desired levels.
- Identify activities and documentation that can help close the identified gaps.
- Gather content and revise it to provide enterprise-specific information.
- Communicate the existence of information security awareness, training, and education materials to employees.
- Establish metrics for evaluating the effectiveness of the programs.
- Include security awareness in annual performance reviews.
- Encourage and support a security-based culture and behaviors.

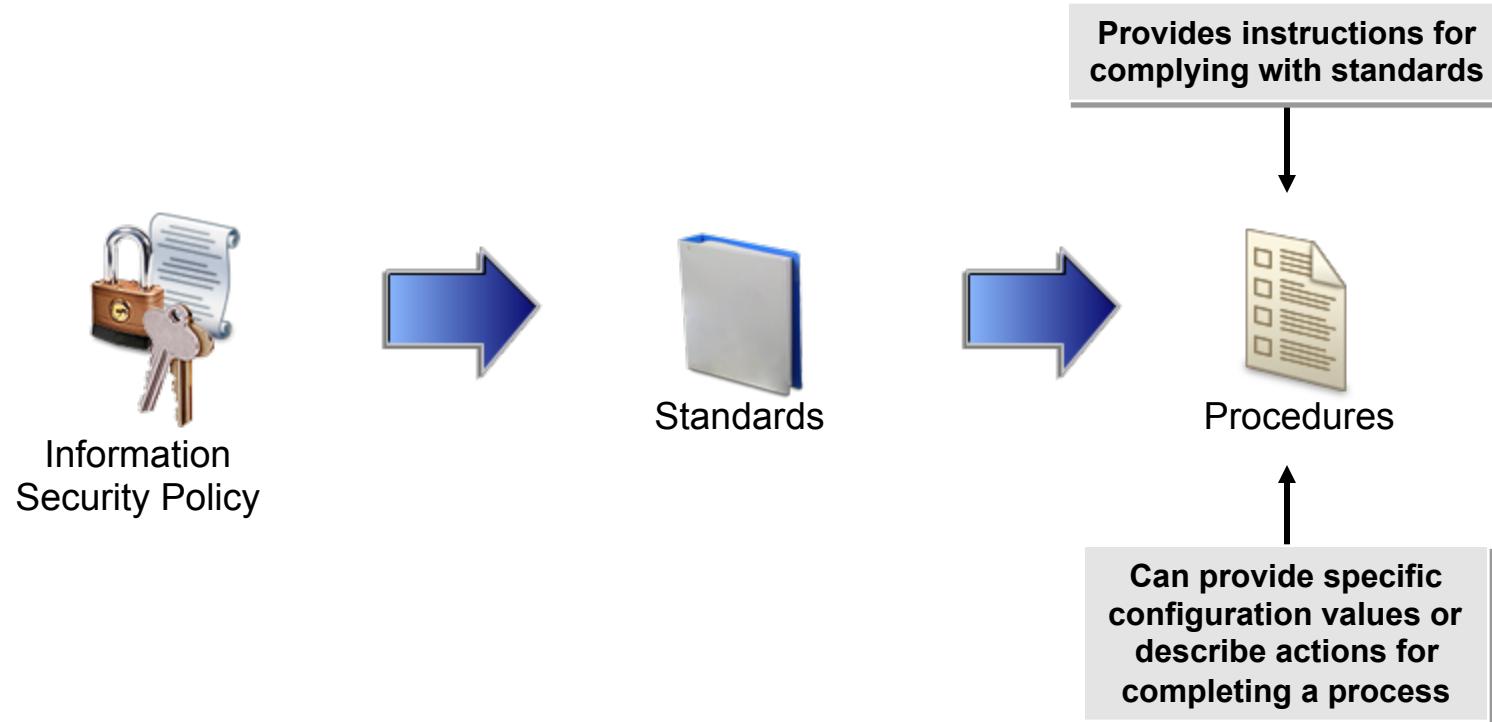
Supporting Documentation for Information Security Policies



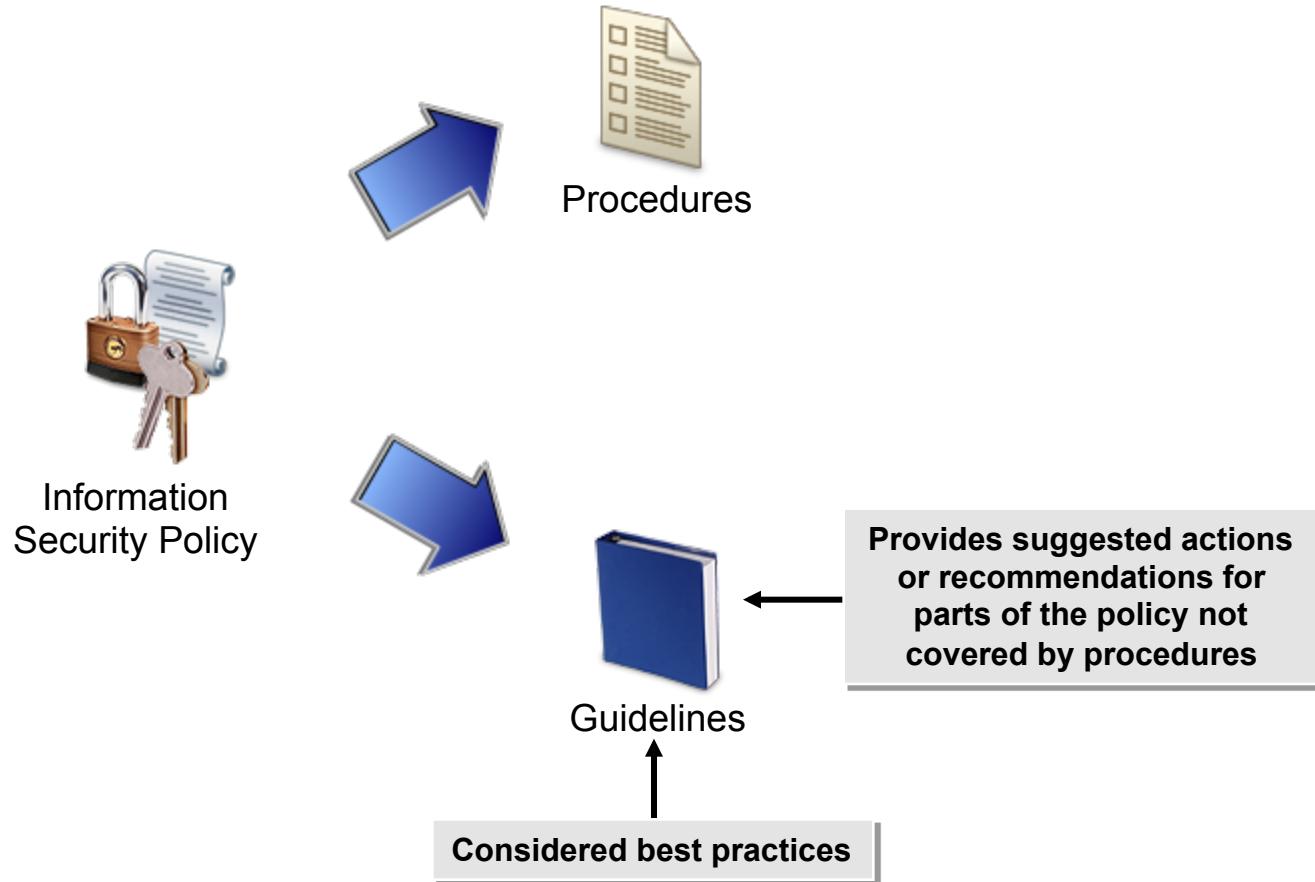
Standards



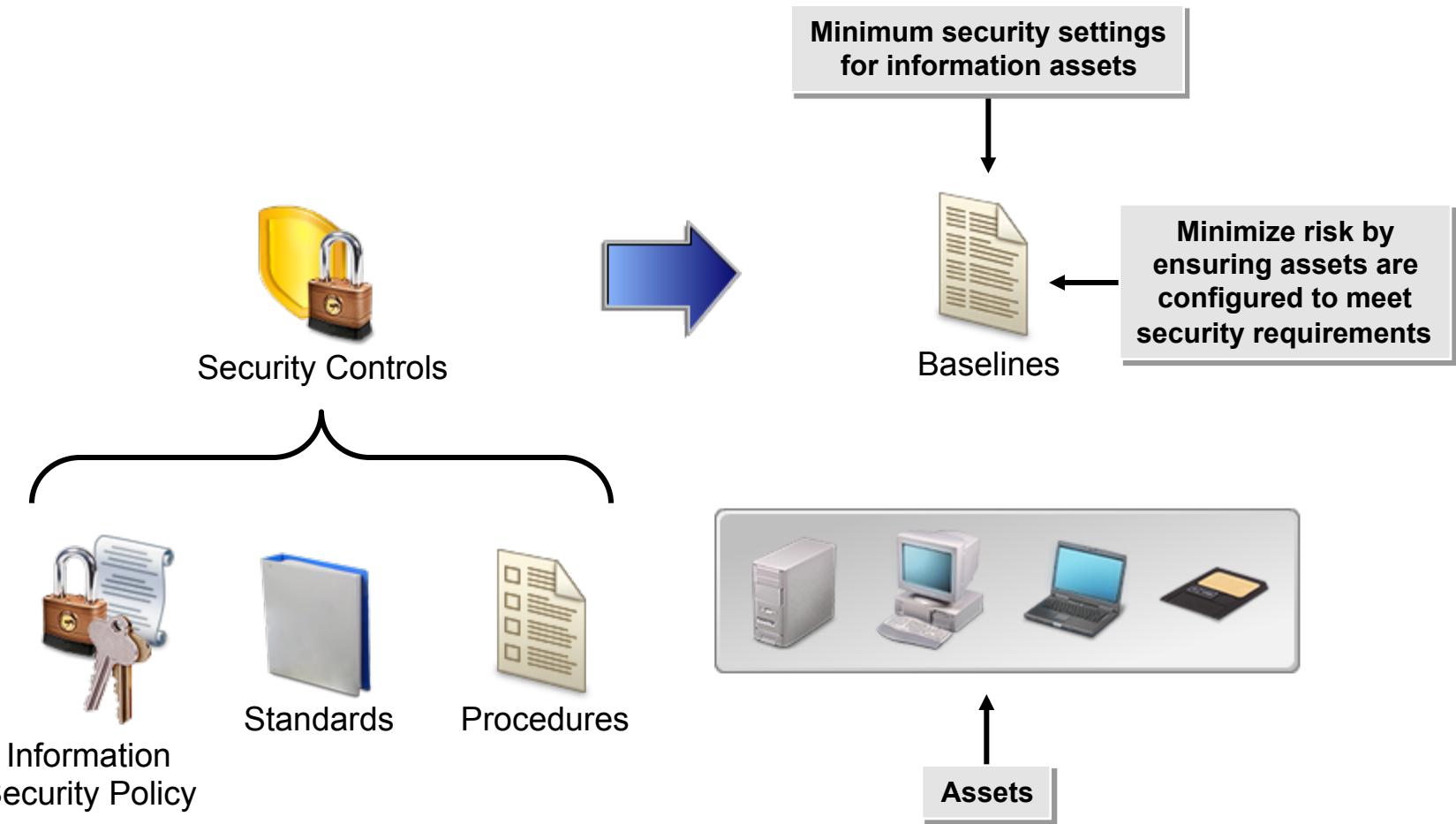
Procedures



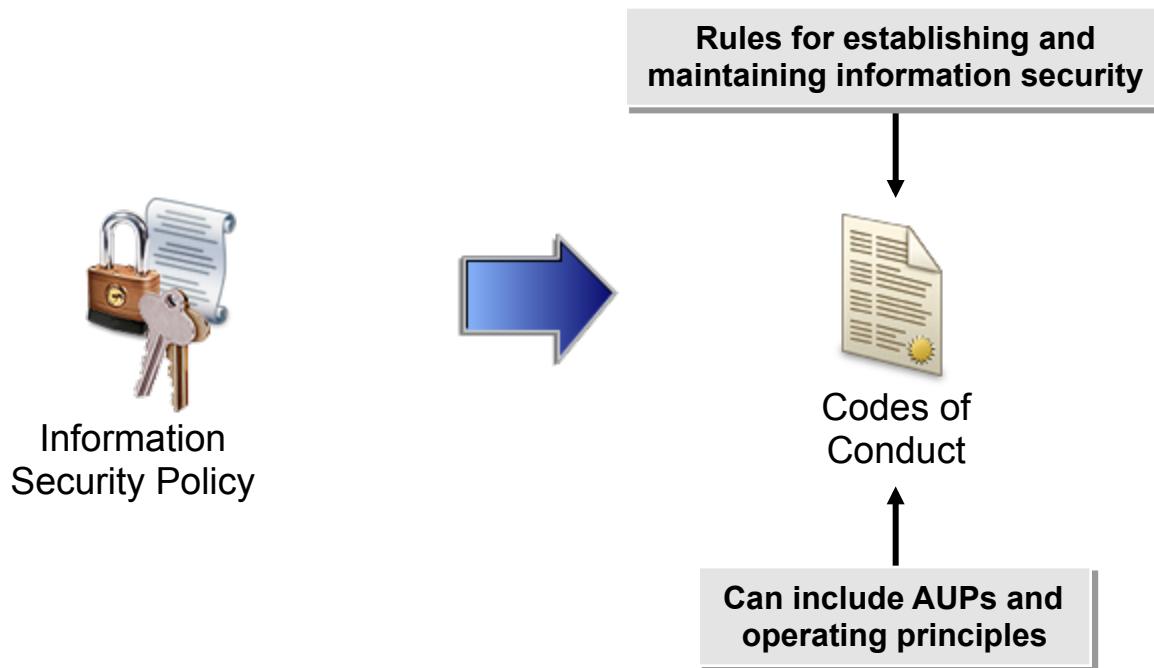
Guidelines



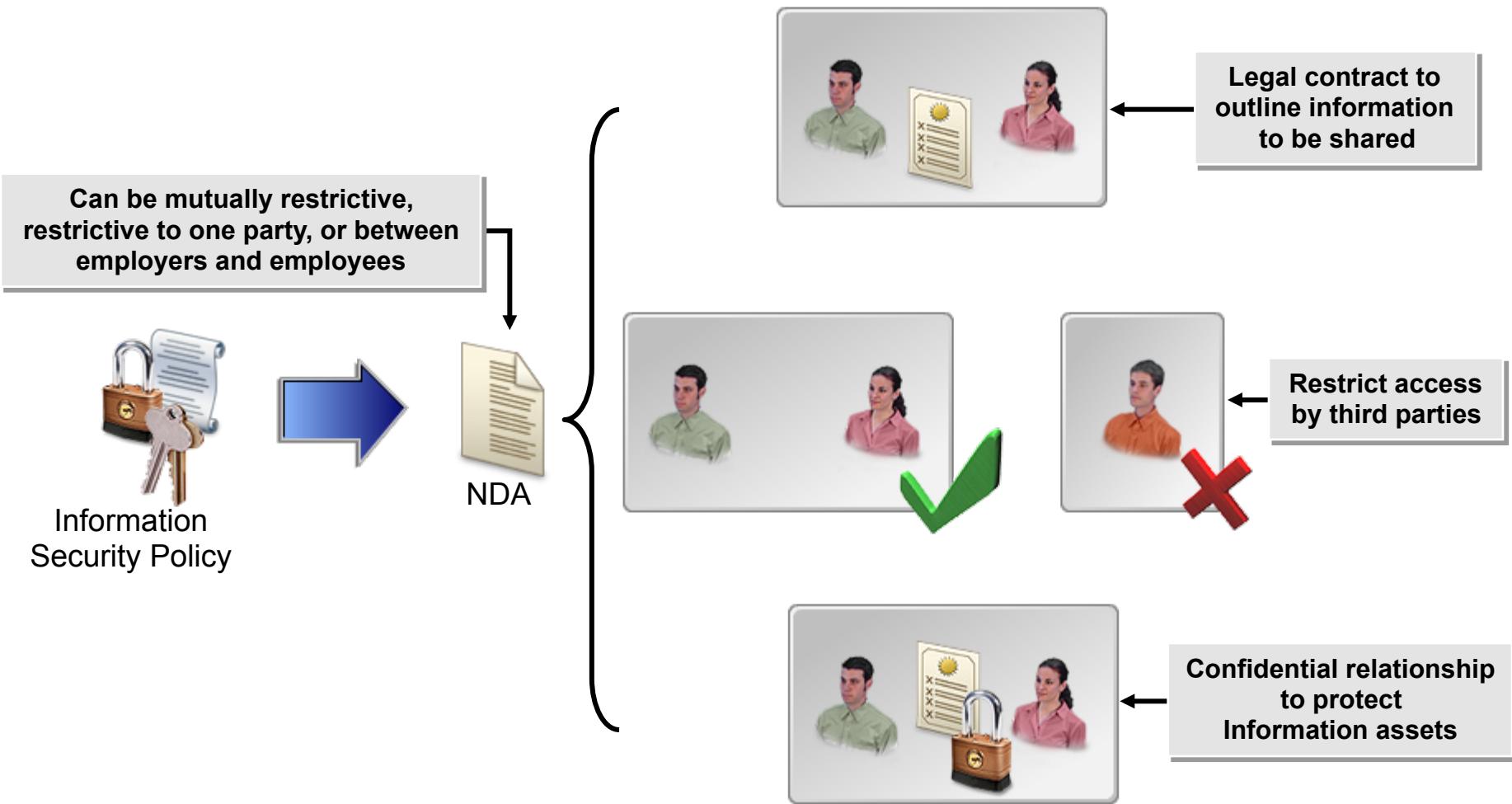
Baselines



Codes of Conduct



NDAs



Methods for Developing Supporting Documentation

Development methods include:

- Creating from scratch
- Revising existing documentation. Possible templates:
 - Existing standards and guidelines for other areas of the organization
 - NIST documents
 - Industry documents



Standards



Procedures



Guidelines



Baselines



Codes of
Conduct



NDAs

Methods for Implementing Supporting Documentation



Using the
Policy



Notification
of Availability

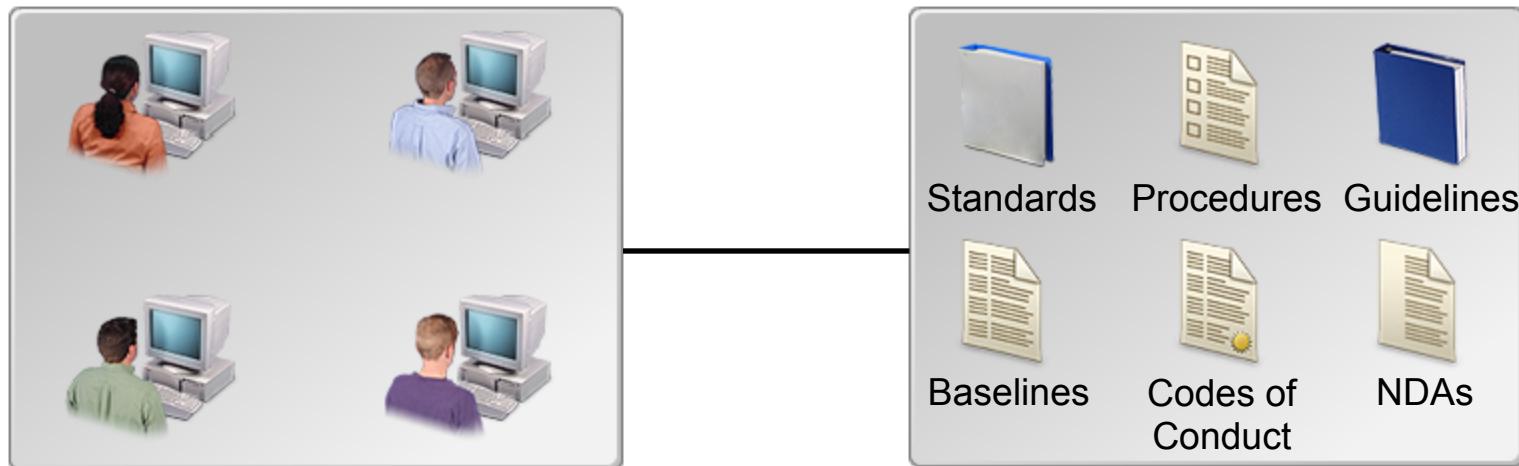


Training

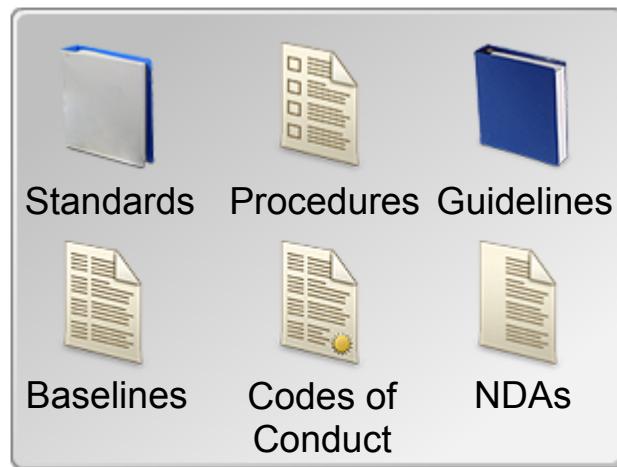
Methods for Communicating Supporting Documentation

Communication methods:

- Distributing physical copies
- Distributing electronic copies
- Storing electronic copies



Methods for Maintaining Supporting Documentation

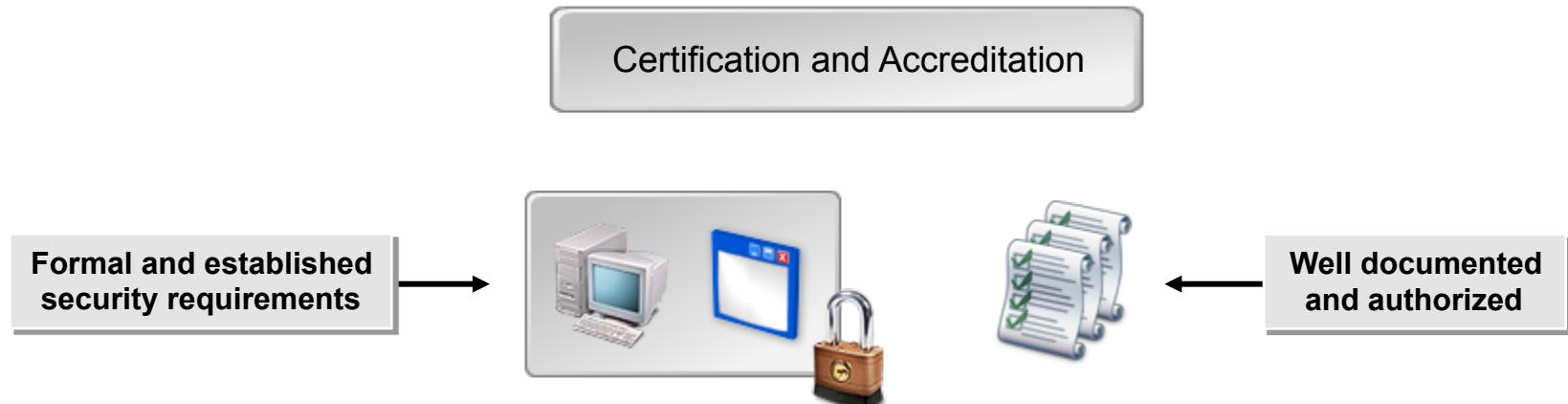


Change Management

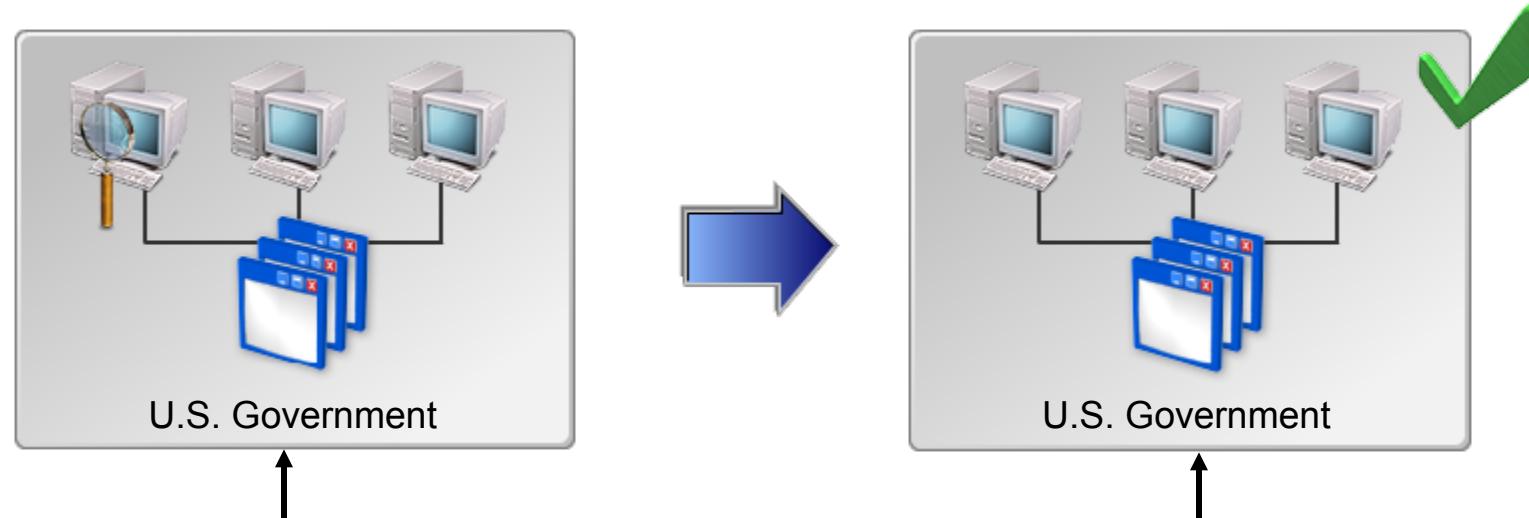


Review Date Specification

C&A



U.S. government systems and applications: C&A prior to implementation and every 3 years afterward



Certification: the technical evaluation of security components and their compliance

Accreditation: management's formal acceptance of the adequacy of the system's security

C&A Programs



How to Develop Supporting Documentation for Information Security Policies

To develop supporting documentation for information security policies:

- For each information security policy, determine what standards are necessary to support the policy.
- For each standard, determine what procedures and guidelines are necessary to support the policy.
- Identify any information security policies that require other types of documentation to support them.



Standards



Procedures



Guidelines



Baselines



Codes of
Conduct



NDAs

Reflective Questions

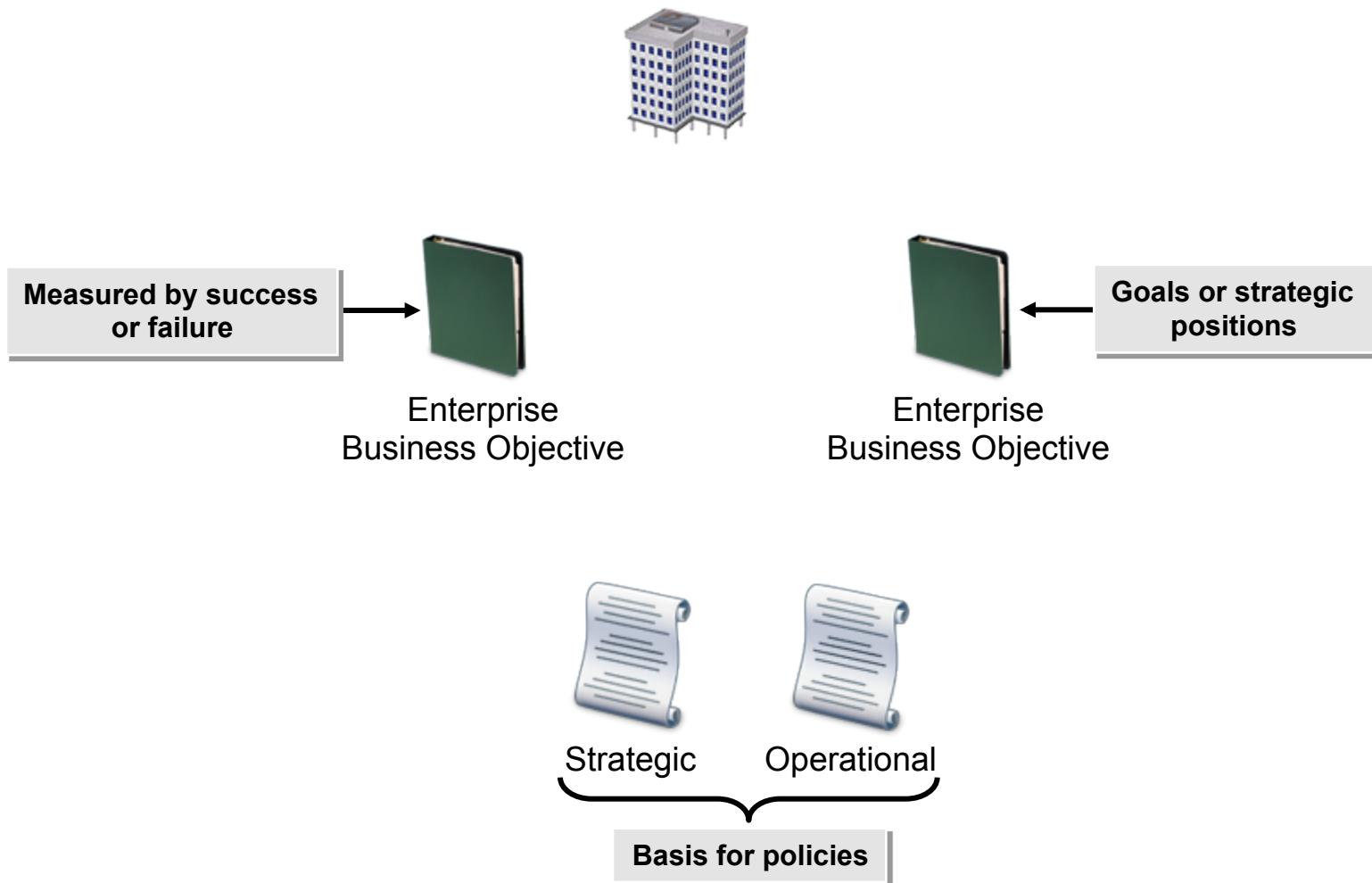
- 1.** What information security program development activities have you taken part in at your organization? Which ones do you expect to participate in?

- 2.** Which facet of information security program development do you expect to be most challenging for your organization?

Information Security Program Implementation

- Integrate Information Security Requirements into Organizational Processes
- Integrate Information Security Controls into Contracts
- Create Information Security Program Evaluation Metrics

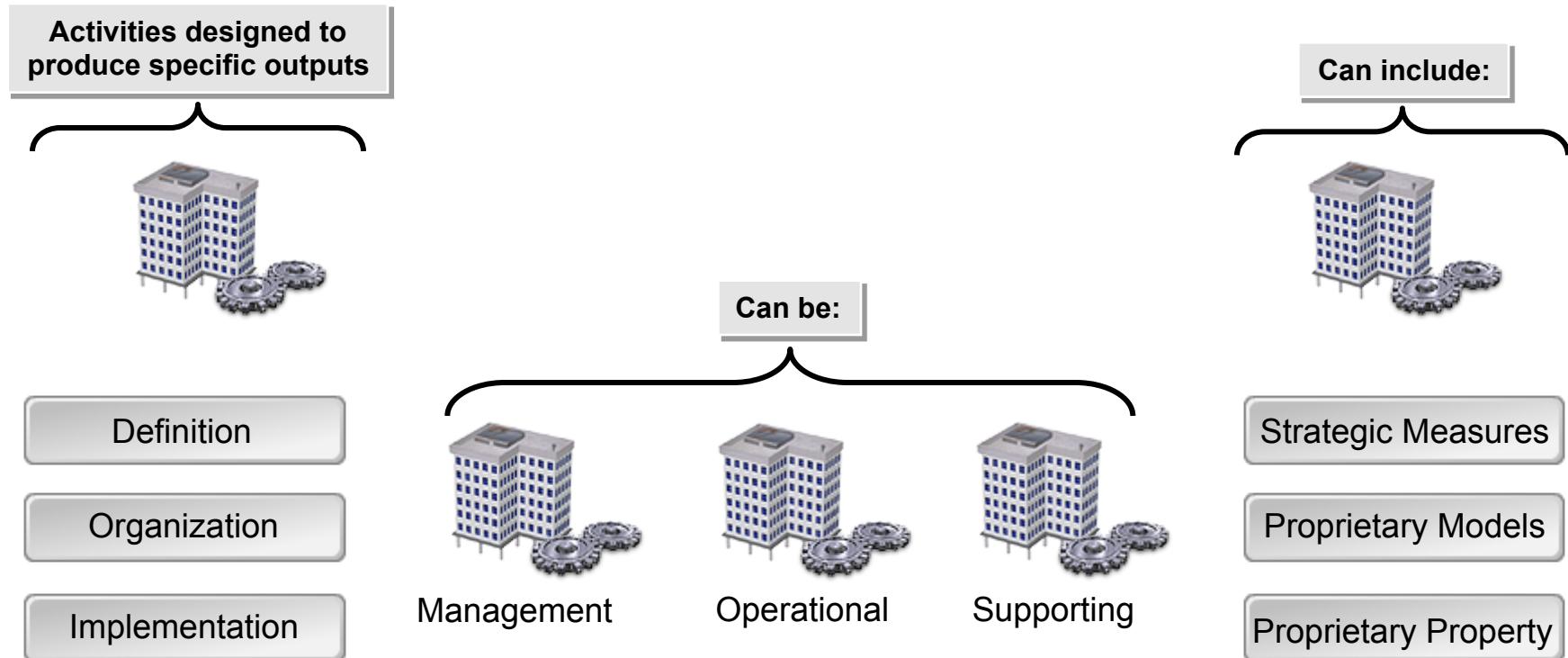
Enterprise Business Objectives



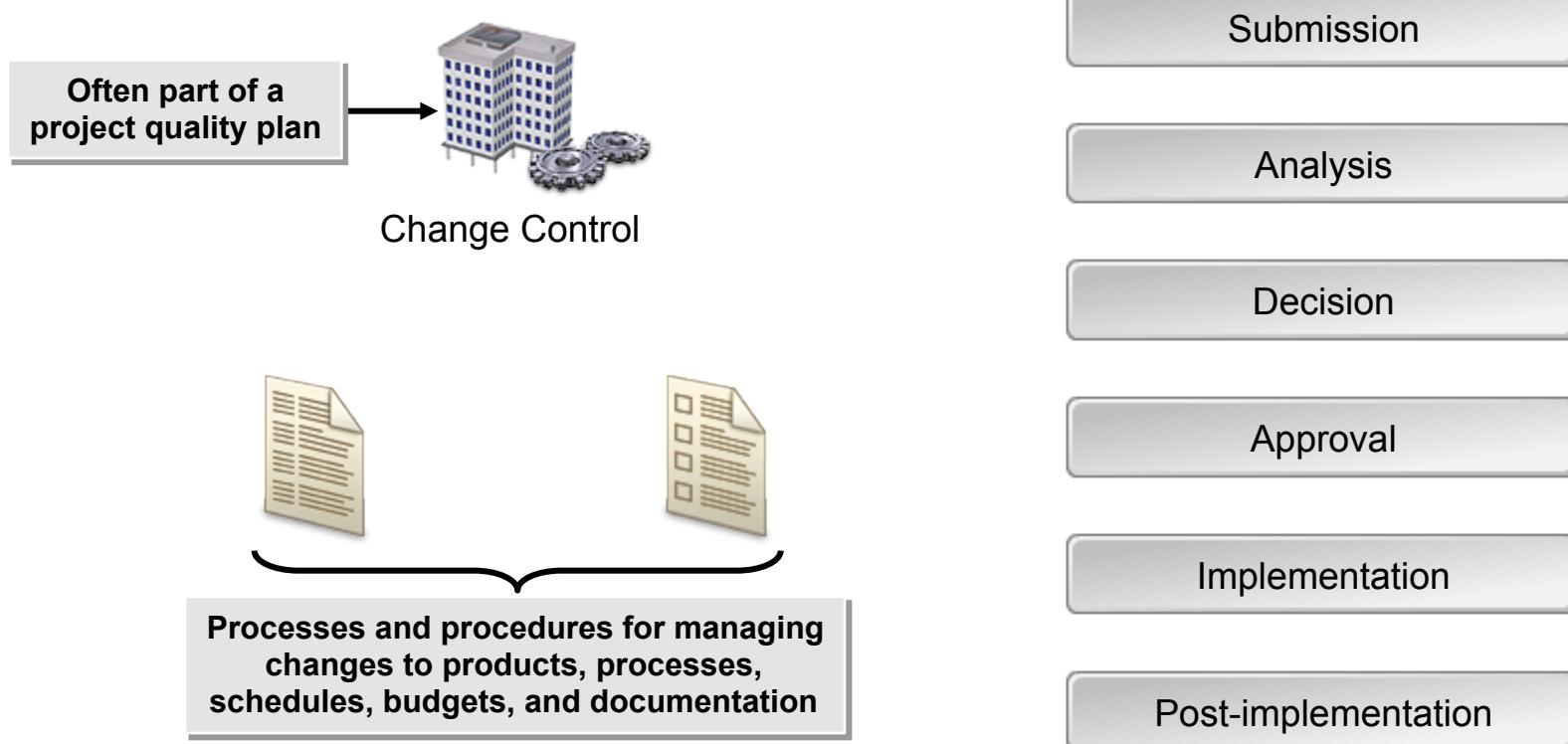
Integrating Enterprise Business Objectives and Information Security Policies

Business Objective	Information Security Policy
Traveling sales staff should have access to data stored at headquarters.	To provide secure access to data for traveling sales staff, all sales laptops will be equipped to enable VPN access to servers at headquarters.
Confidential and proprietary data needs to be protected against unauthorized access.	For confidential data access, two-factor authentication is required.
Field workers must provide timely and accurate meter readings to streamline billing processes.	Meter readers will be provided wireless access for uploading consumption data.

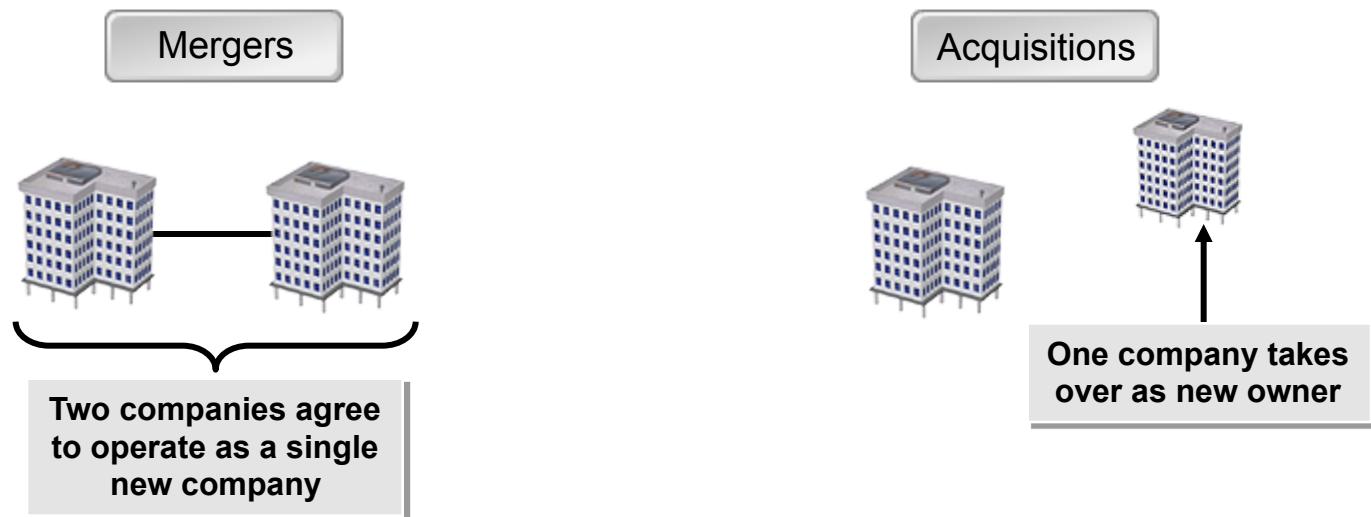
Organizational Processes



Change Control



Mergers and Acquisitions



Organizational Processes and Information Security Policies

Organizational processes such as change control and mergers can affect information security:

- If change control is not implemented with information security in mind, it can introduce vulnerabilities in the changed processes.
- Confidentiality of potential mergers and acquisitions.
- Disclosure of sensitive information during mergers and acquisitions.
- Review of security policies after mergers and acquisitions.
- Combined organization needs security technologies implemented.



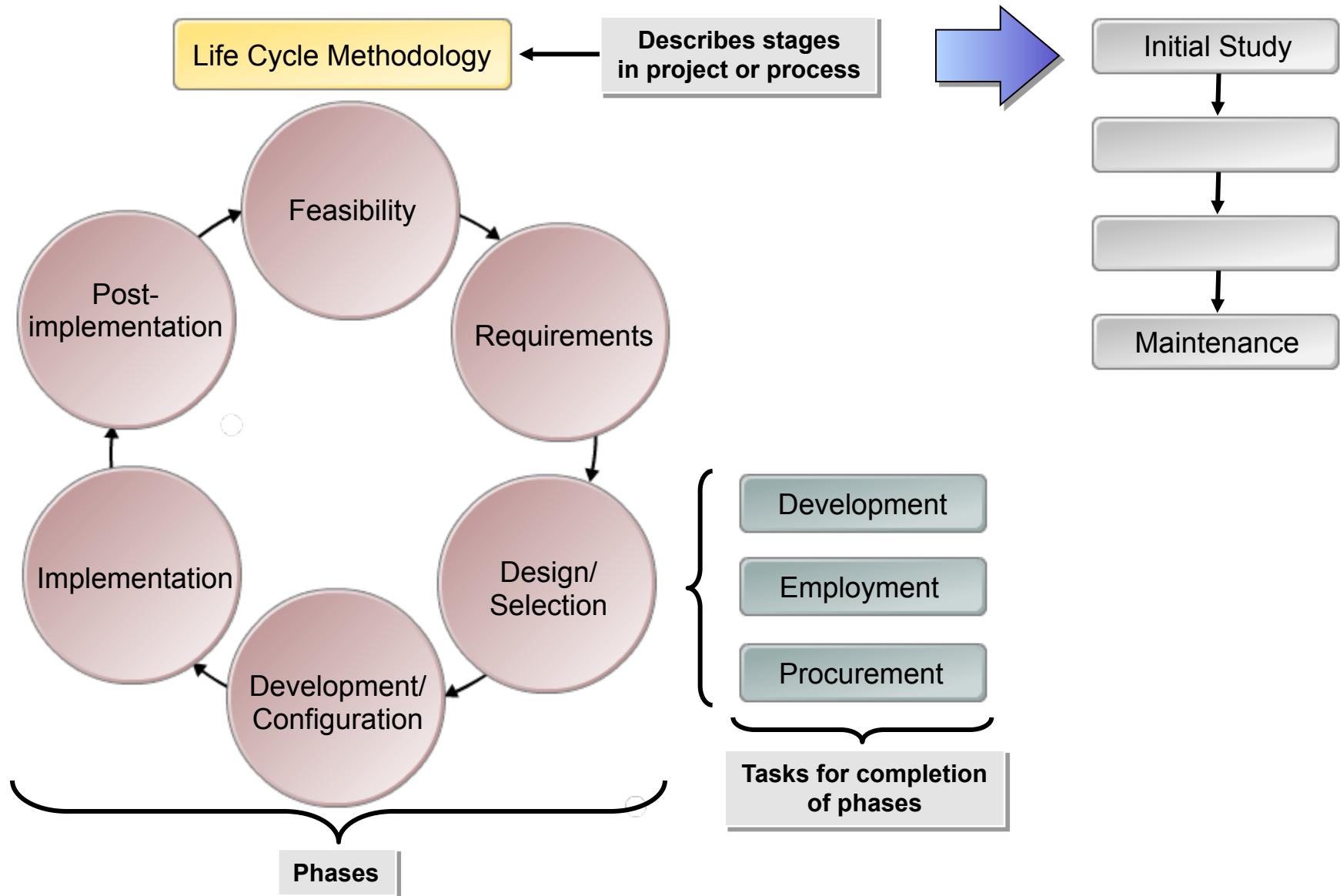
Methods for Integrating Information Security Policies and Organizational Processes

Integration methods:

- Identify organizational processes affected by change management.
- Modify the security awareness program.
- Review the information classification program.
- Reevaluate risk assessment.



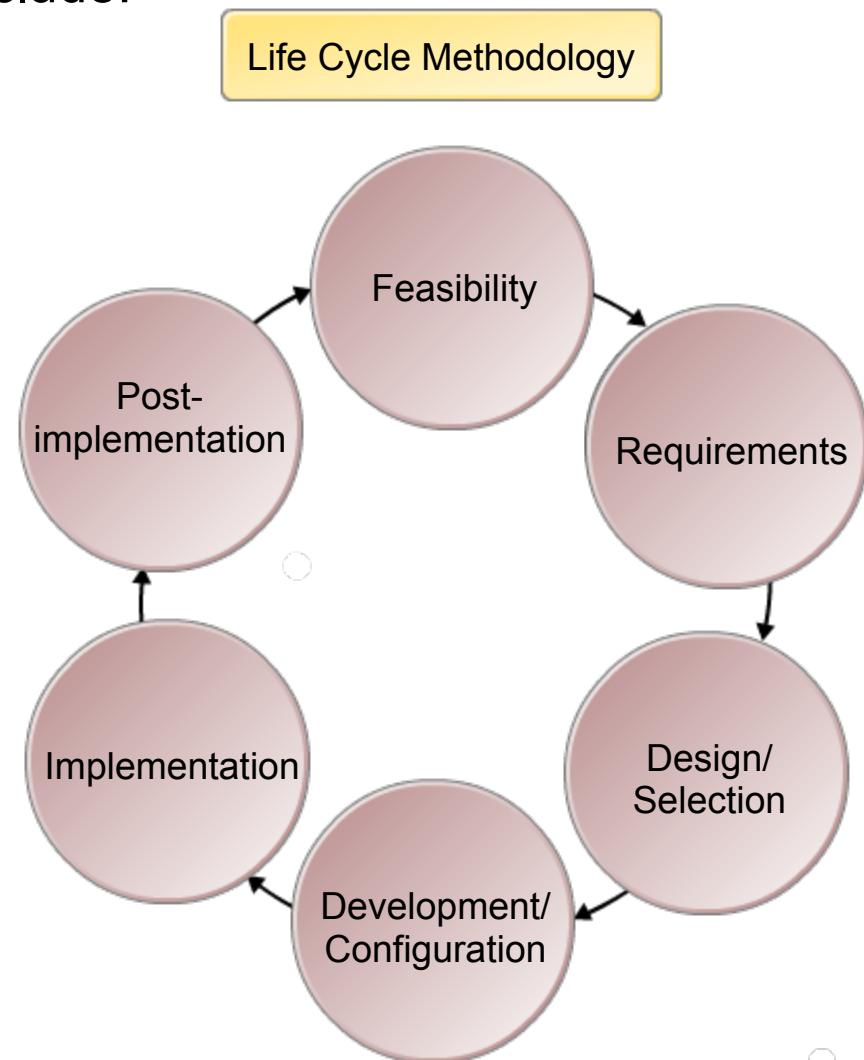
Life Cycle Methodologies



Types of Life Cycle Methodologies

Common life cycle methodologies include:

- Pure waterfall
- Spiral
- Throwaway prototyping
- Evolutionary prototyping
- Staged delivery
- U.S. Department of Justice SDLC
- PMP life cycle



How to Integrate Information Security Requirements into Organizational Processes

To integrate information security requirements into organizational processes and life cycle activities:

- Verify that the information security program addresses and supports all enterprise business objectives, organizational processes, and life cycle activities. Then, develop any new policies, procedures, and guidelines that are needed.
- Review the enterprise business objectives, organizational processes, and life cycle activities to ensure that the information security program addresses and supports them.
- Communicate with the areas of the organization that engage in life cycle activities.



Types of Contracts Affected by Information Security Programs

Type of contracts:

- Joint ventures
- Outsourced providers
- Business partners
- Customers
- Other third parties such as suppliers and subcontractors

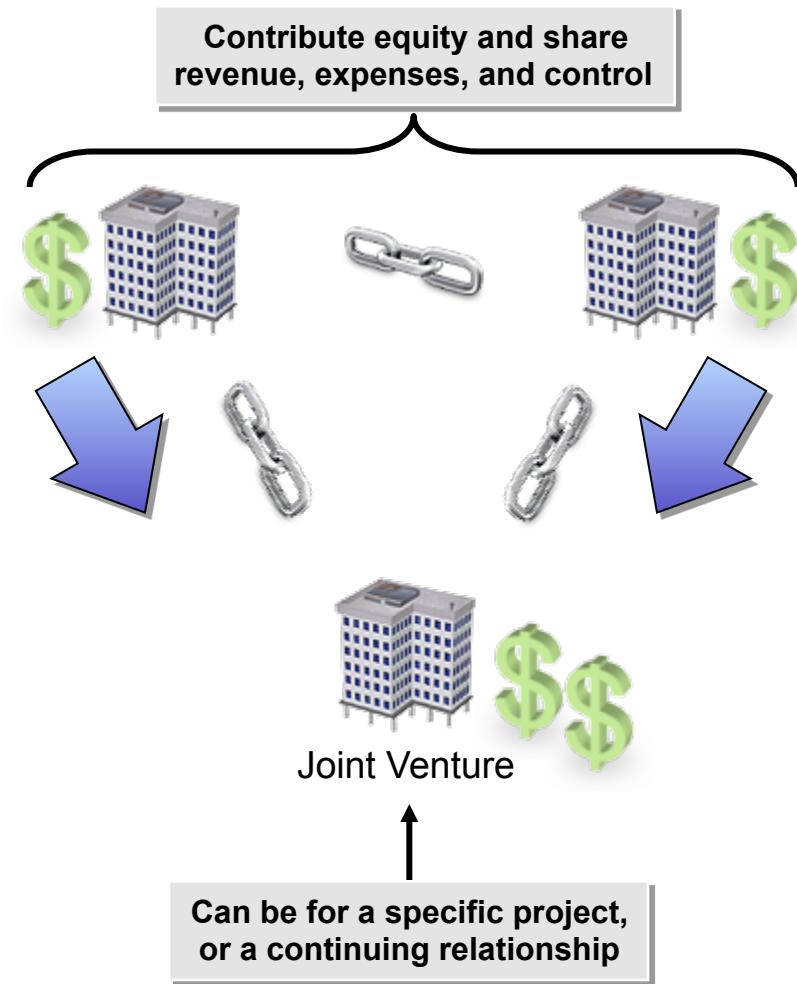


Contract

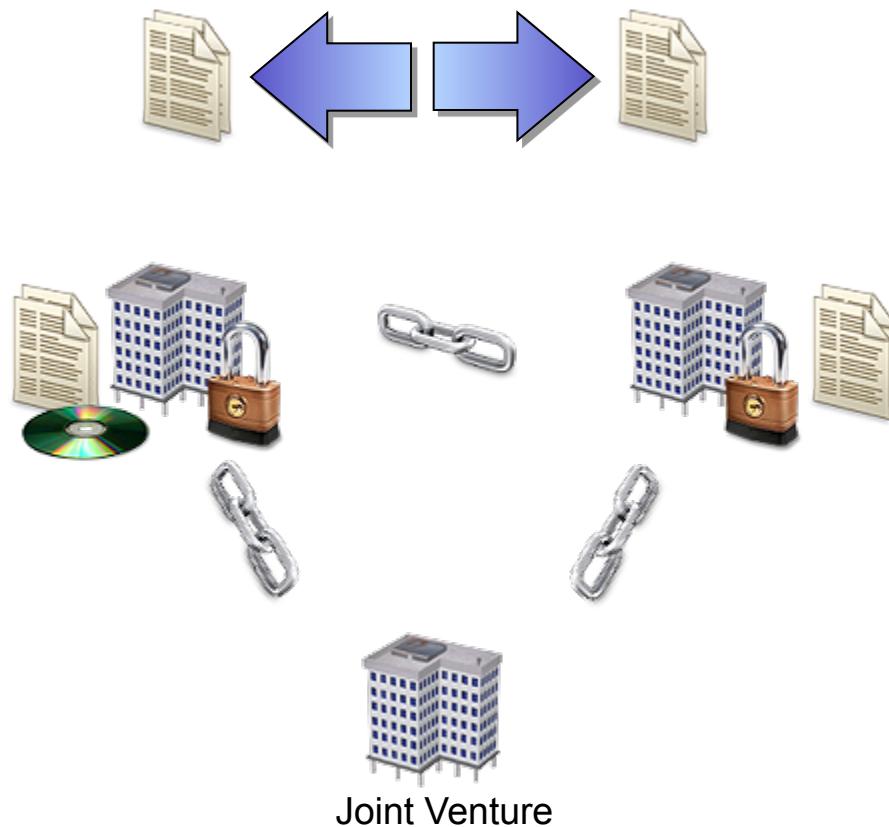


Information Security Program

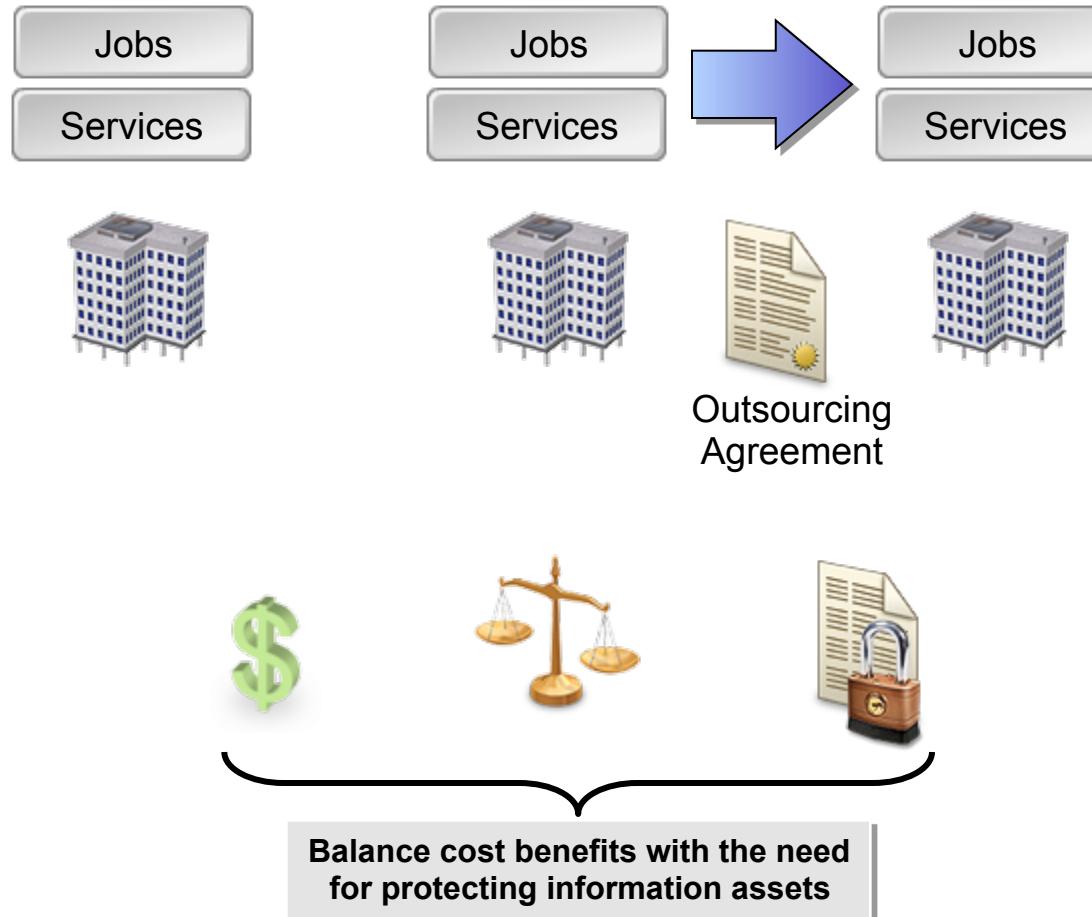
Joint Ventures



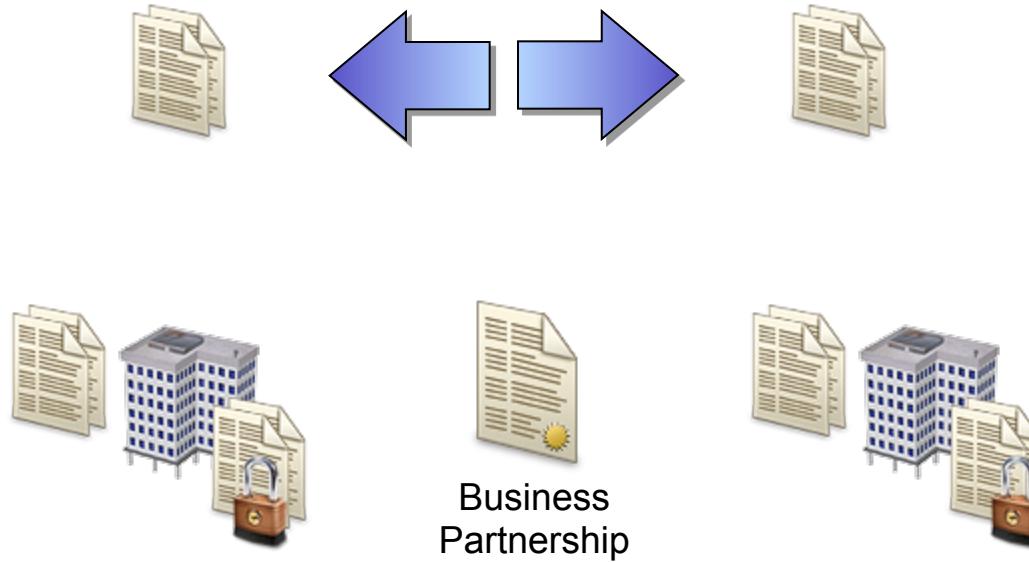
Joint Ventures and Information Security



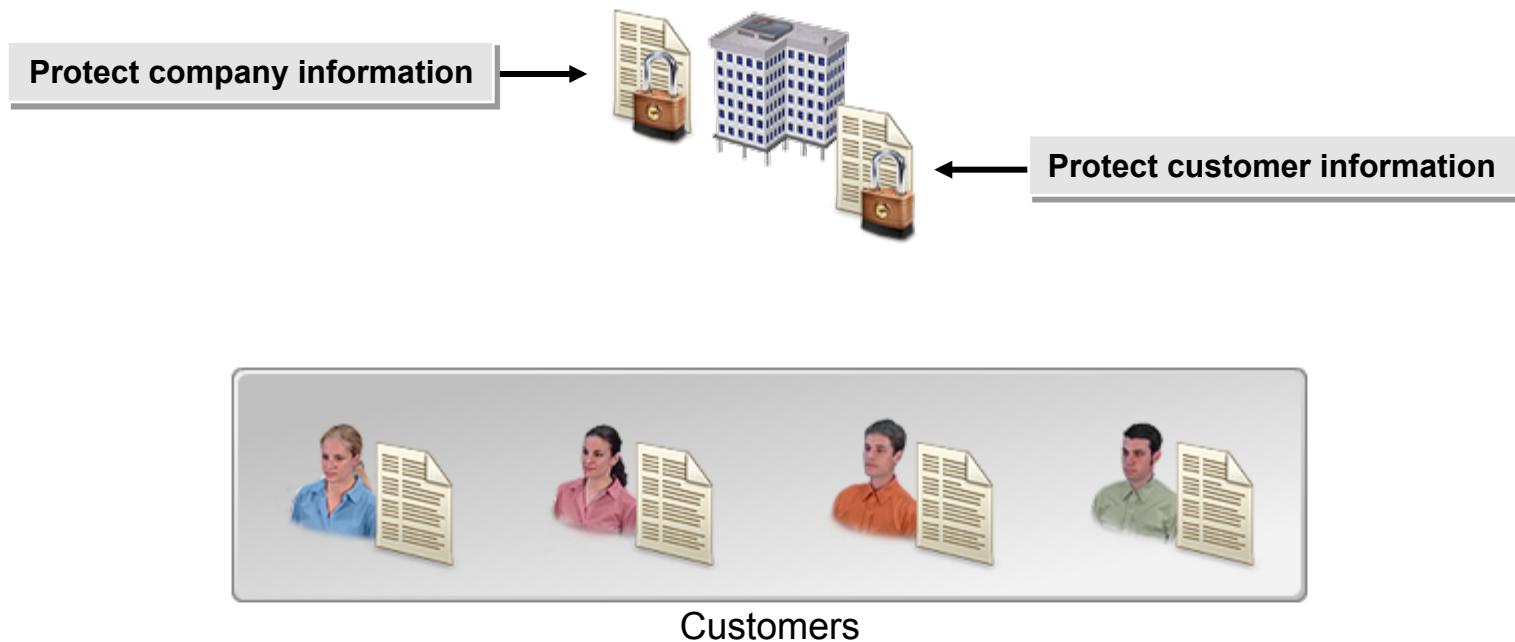
Outsourced Providers and Information Security



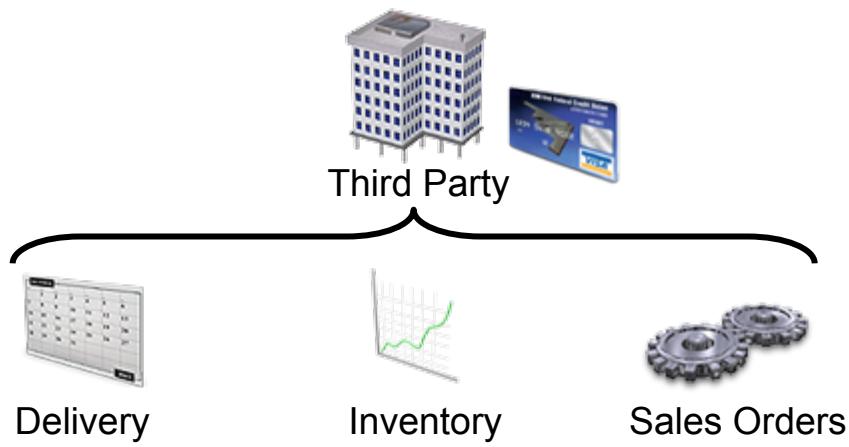
Business Partners and Information Security



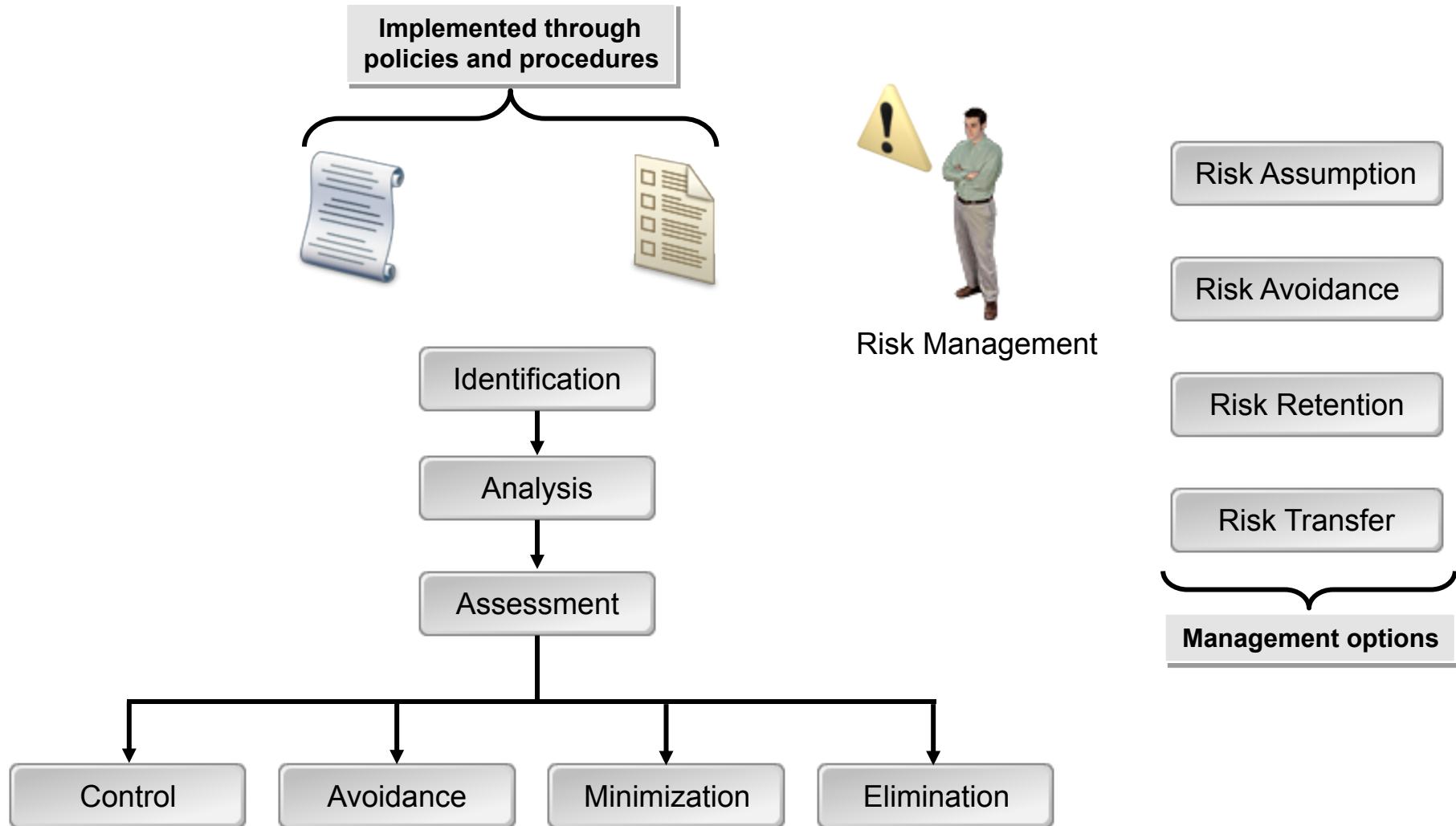
Customers and Information Security



Third Parties and Information Security



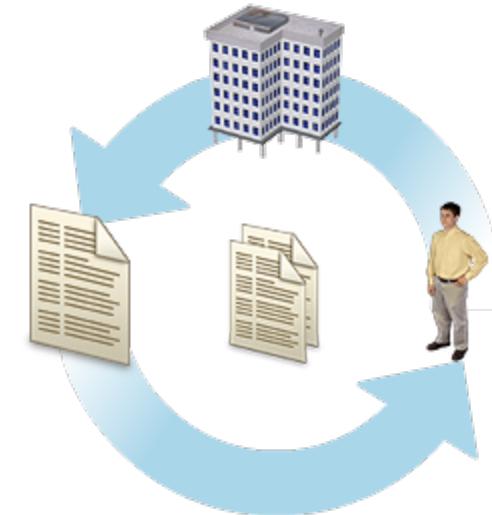
Risk Management



Risk Management Methods and Techniques for Third Parties

Risk management for third parties:

- Contractor management programs
- SLAs
- Contracts
- Due diligence
- NDAs
- Controls on subcontractors



SLAs and Information Security



Enterprise



SLA



Service Provider

Contracts and Information Security

Contract provisions:

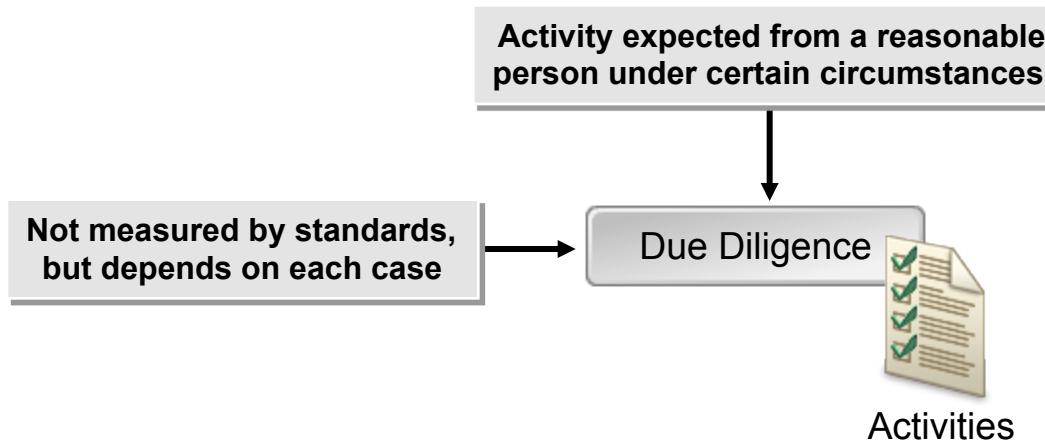
- Confidentiality, or non-disclosure
- Security rules and guidelines for the contractor
- Right-to-audit



Contract

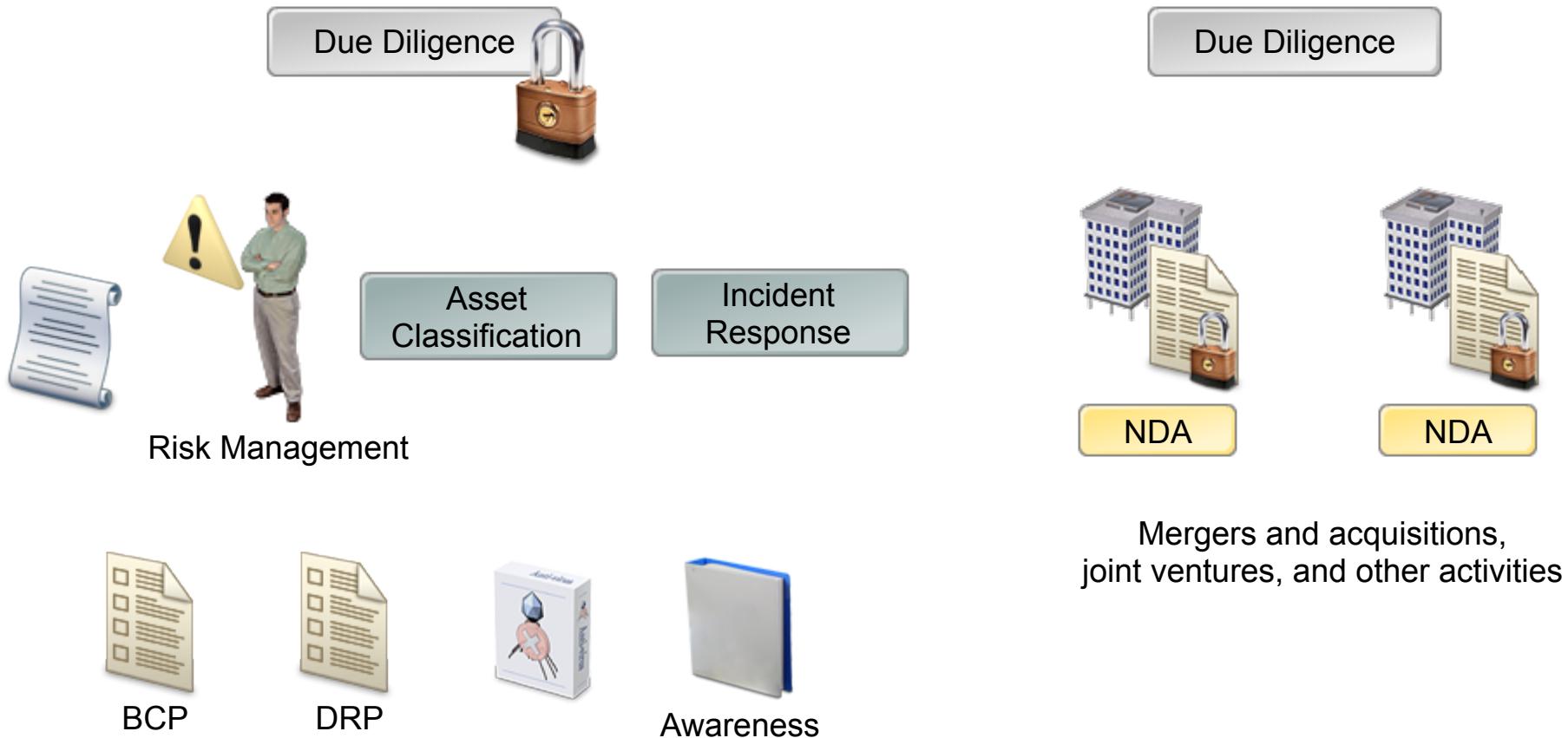


Due Diligence

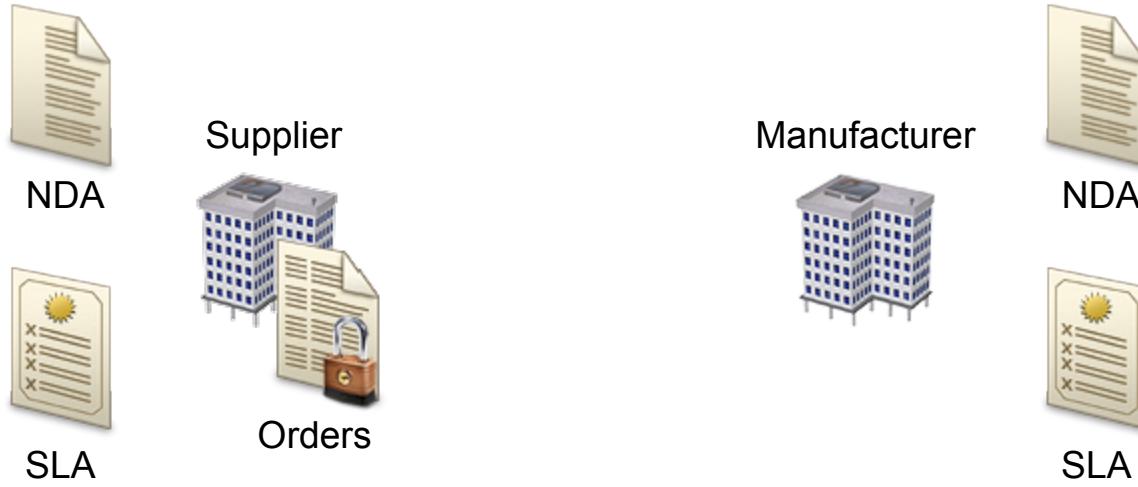


Mergers and
Acquisitions

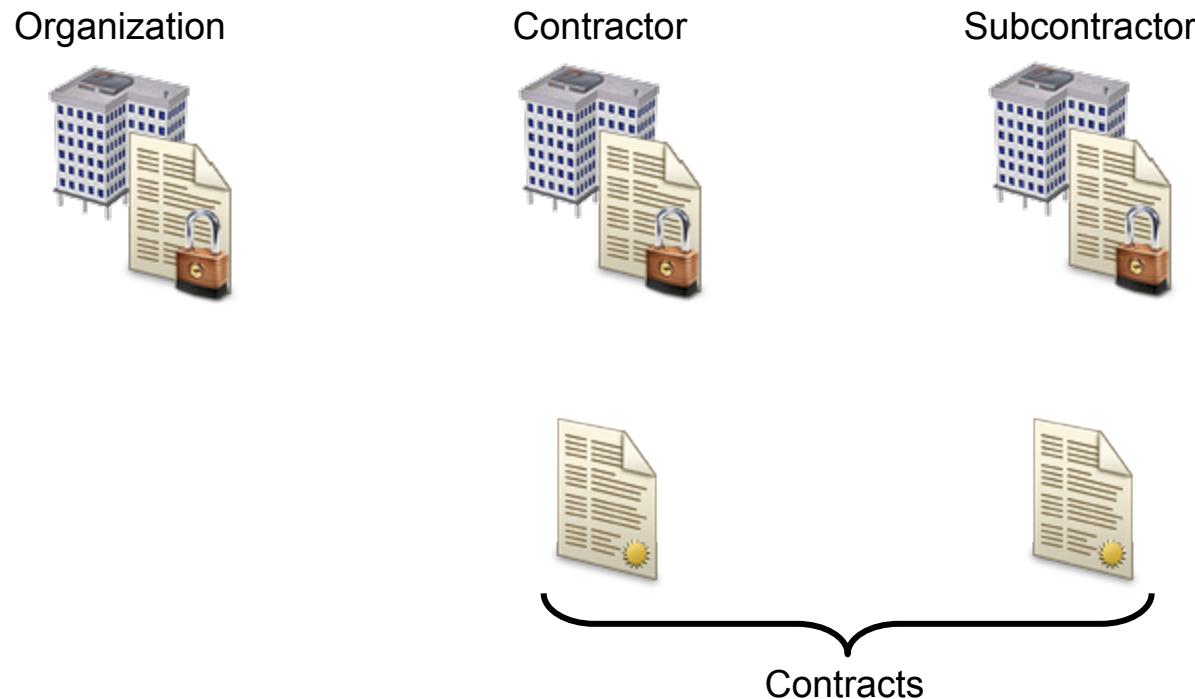
Due Diligence and Information Security



Suppliers and Information Security



Subcontractors and Information Security

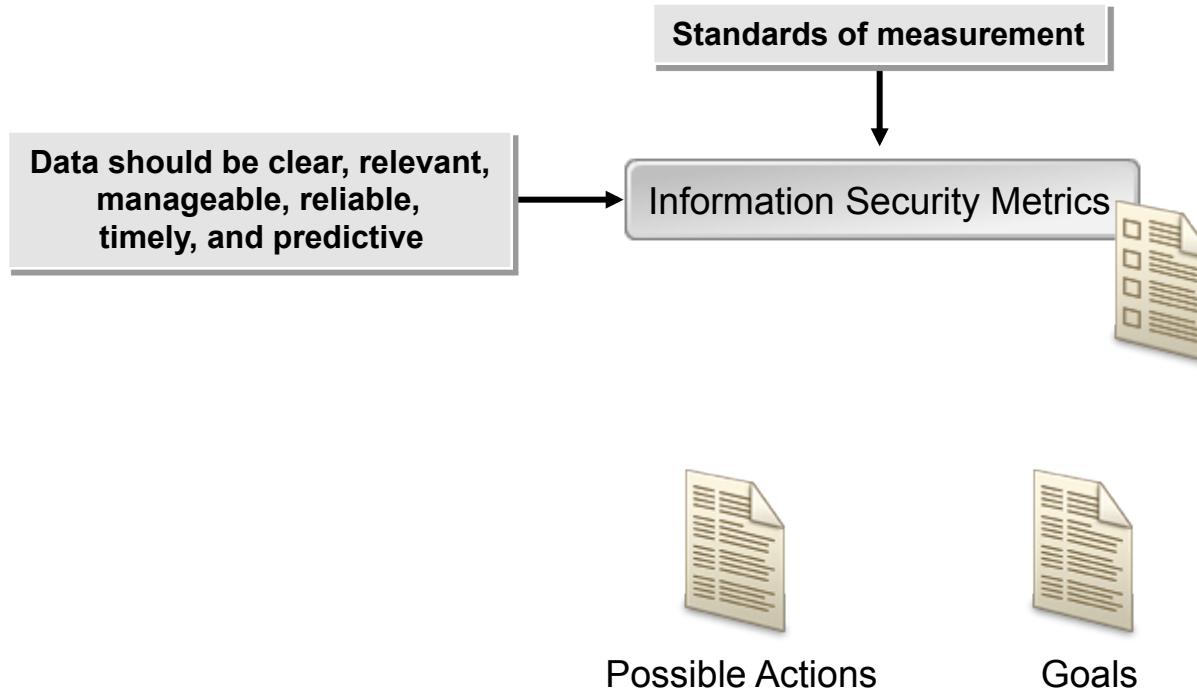


How to Integrate Information Security Controls into Contracts

To integrate information security into contracts:

- Review all relationships with contractors, outsourced providers, suppliers, and other third parties to determine which relationships need to be protected by specific contract provisions, NDAs, and SLAs.
- Work with the legal department to draft, submit, and execute the required agreements to the third parties.
- Work with the legal and human resources departments to ensure that all current information security policies address the use of contractors.
- Consider conducting security awareness training that focuses on contractors and their responsibilities.

Information Security Metrics



Types of Metrics Commonly Used for Information Security

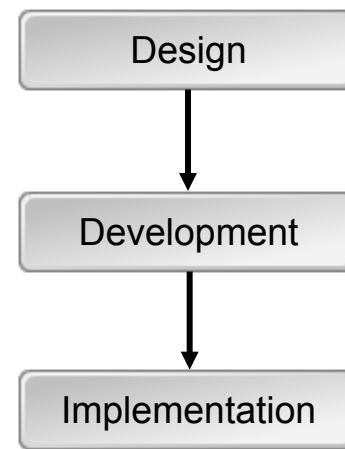
Metric categories include:

- Operational
- Managerial
- Strategic

Information Security Metrics



Metrics Design, Development, and Implementation



Goals of Evaluating Information Security Controls

Goals of evaluating controls:

- Are the controls effective?
- Are controls that are intended to enforce or satisfy a regulatory requirement successful?
- Are the controls efficient?
- Are the controls operating within established budgets and otherwise cost effective?
- Which controls can be strengthened?
- Which controls should be replaced with other controls?
- Are the controls meeting the objectives of both the information security program and the underlying business objectives?



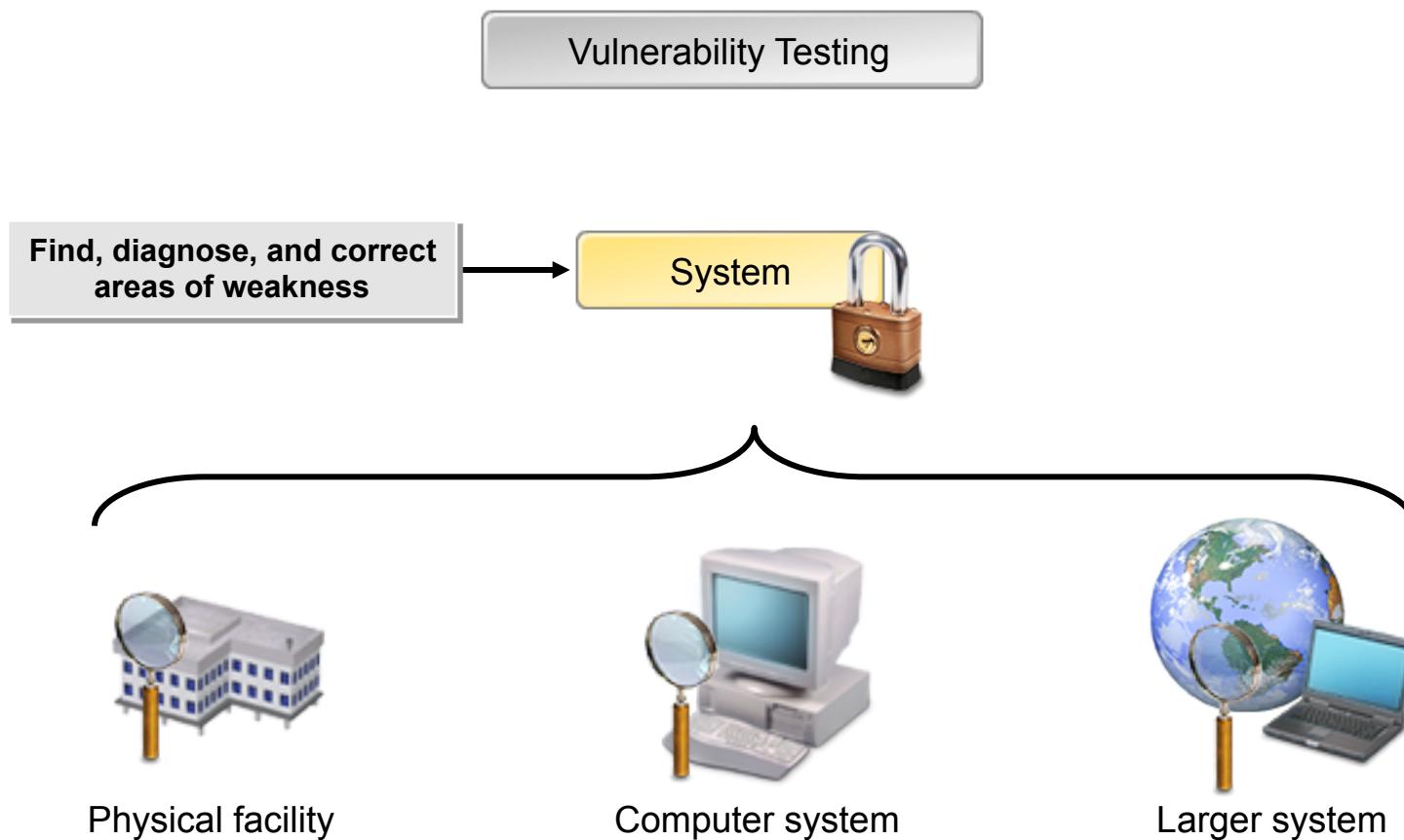
Methods for Evaluating Information Security Controls

Methods for evaluating information security controls:

- Conducting periodic vulnerability reviews and testing
- Conducting risk assessment activities
- Tracking the reduction of assessed risks



Vulnerability Testing



Types of Vulnerability Testing

Vulnerability testing types:

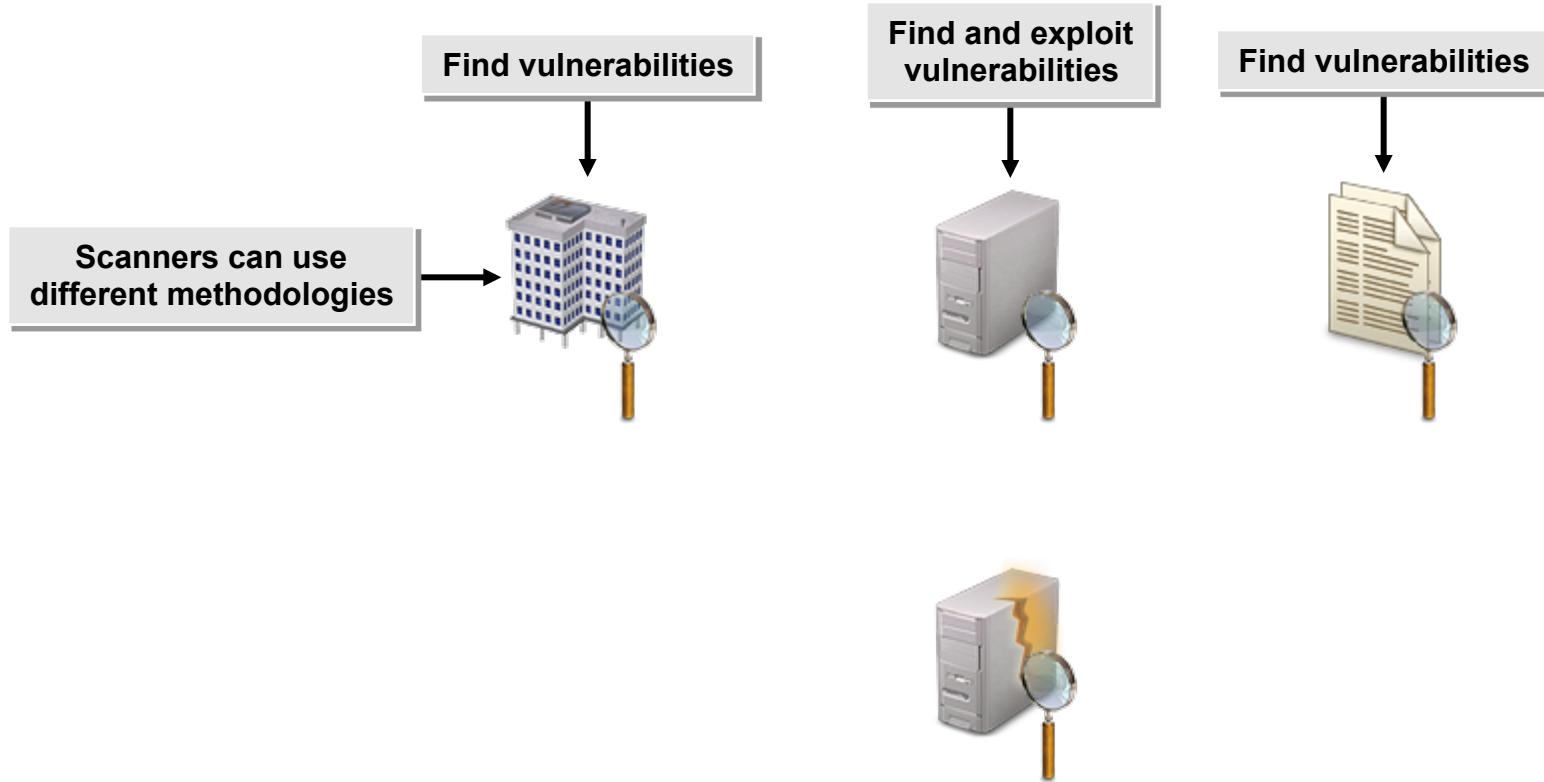
- External
- Internal

Vulnerability Testing

System

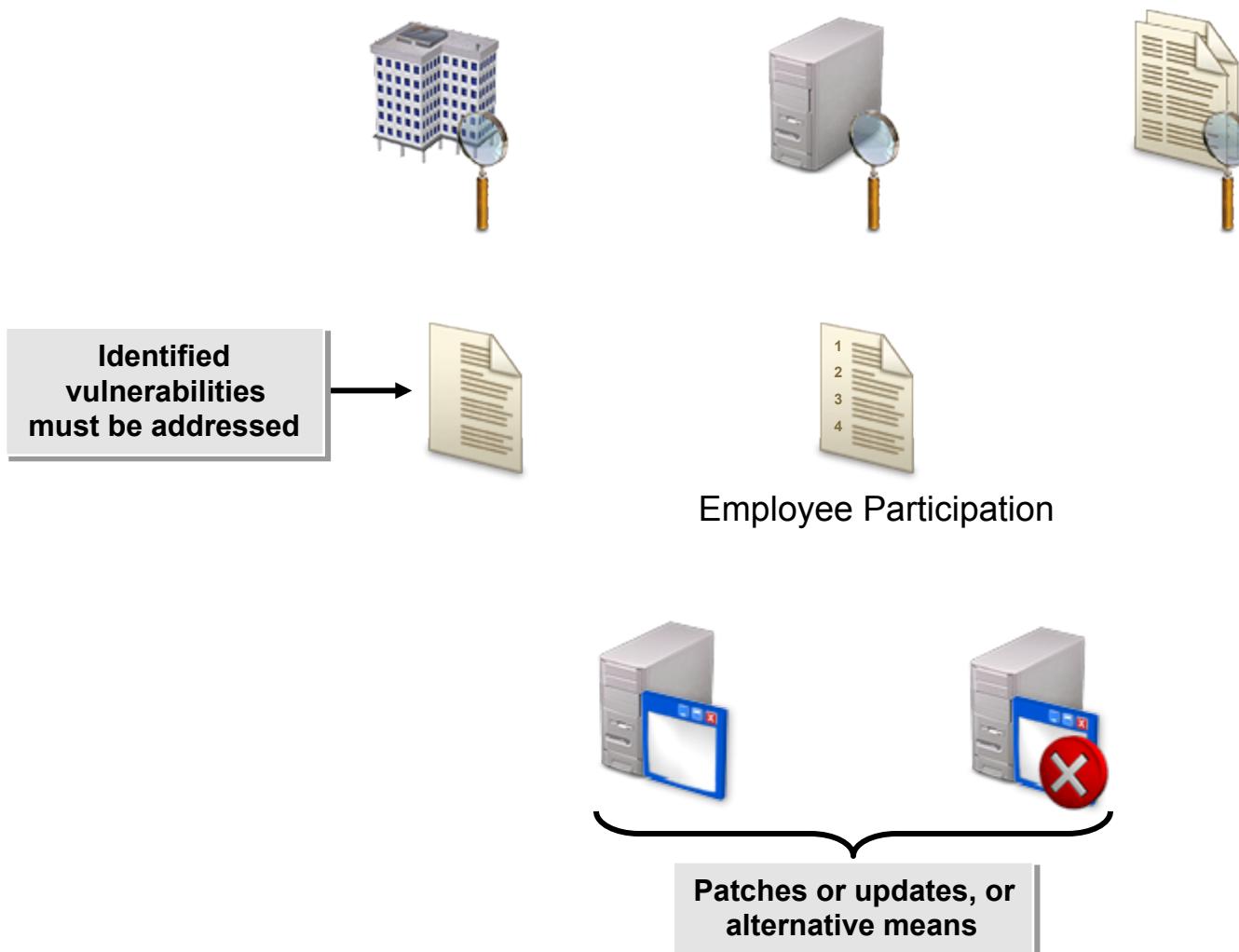


Effects of Vulnerability Assessment and Testing



Scans can be intrusive and crash a system

Vulnerability Correction



Commercial Assessment Tools

Commercial assessment tools include:

- Nessus
- SAINT®
- IBM® Internet Scanner
- Retina



Freeware Assessment Tools

Freeware assessment tools include:

- GFI LANguard™
- Windows® Vulnerability Scanner
- MBSA



Goals of Tracking Information Security Awareness, Training, and Education Programs



Awareness



Training

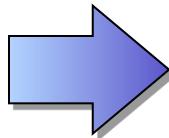


Education

**Low participation means
low success rate**



Employee Participation



Work with managers and HR to increase participation

Methods for Tracking Information Security Awareness, Training, and Education Programs

Methods for tracking information security awareness, training, and education programs:

- Establishing a database for tracking employee names and the available information security awareness, training, and education programs
- Working with an e-learning company that provides tracking services
- Establishing a paper-based record of employees and available security awareness, training, and education offerings



Awareness



Training



Education

Evaluation of Training Effectiveness and Relevance

Metrics for measuring the effectiveness of information security awareness, training, and education programs include:

- The number of security incidents reported per month prior to and after employee participation in the programs.
- The number of security incidents stopped as a result of training.
- The percentage and number of security incidents stopped as a result of training, compared to the overall number of incidents reported.
- The number of security policy violations per month prior to and after employee participation in the programs.
- The reduction in the number of security policy violations, as a percent.
- The percentage increase in the effectiveness of personnel managing security controls.
- The reduction of the impact of security incidents, as a percent.
- The percentage increase in the potential security incidents detected.

How to Create Information Security Program Evaluation Metrics

To create information security program evaluation metrics:

- Review the information security program to identify what operational, managerial, and strategic metrics might be needed.
- Determine what needs to be measured and the reason for measuring it.
- Determine the source for gathering the data.
- Work with the decision makers to agree on what the data means.
- Develop regular reports from the data.
- Review the reports with the appropriate individuals or business units.



Information
Security Program

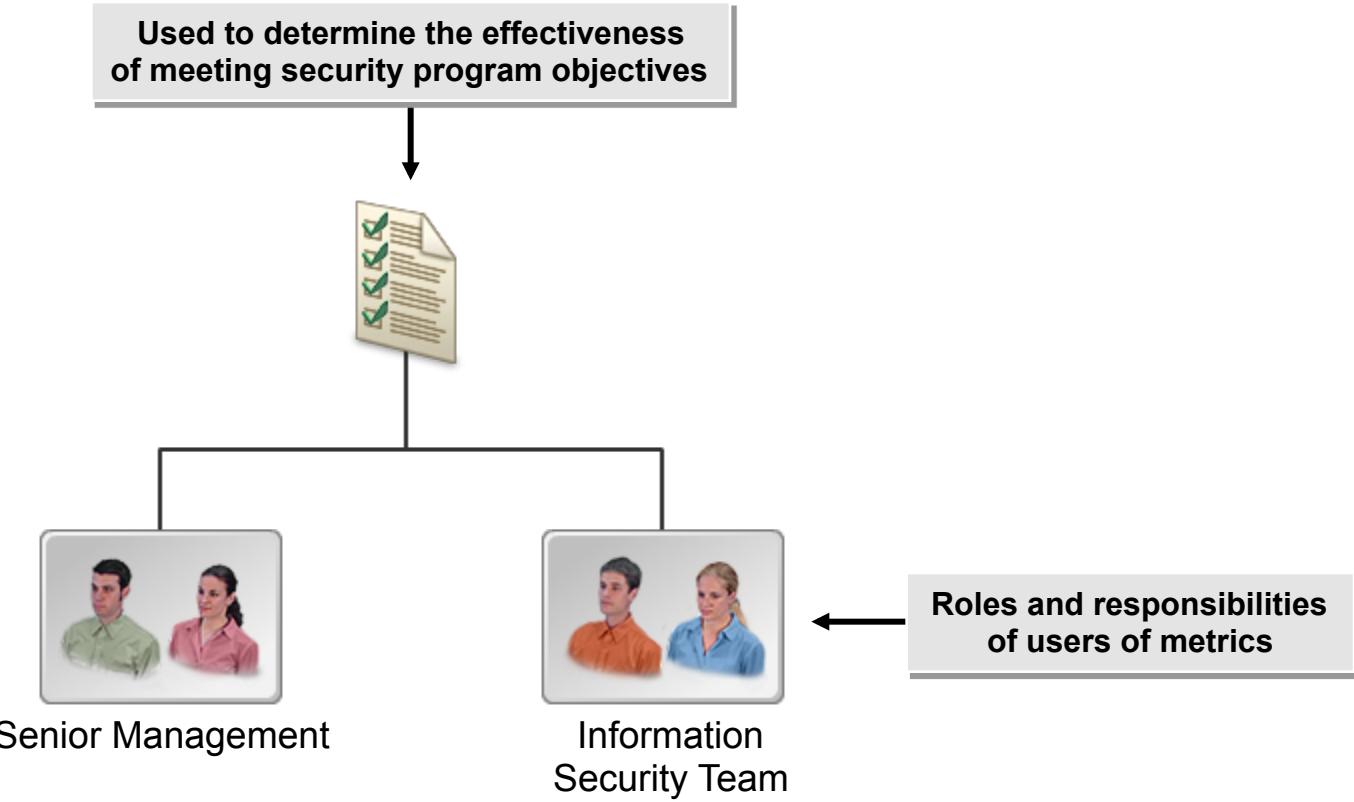
Reflective Questions

1. What information security program implementation activities have you participated in at your organization? What implementation activities do you expect to perform in the future?
2. Which part of implementing an information security program do you think you would find the most challenging?

Information Security Program Management

- Manage Information Security Program Resources
- Enforce Policy and Standards Compliance
- Enforce Contractual Information Security Controls
- Enforce Information Security During Systems Development
- Maintain Information Security Within an Organization
- Provide Information Security Advice and Guidance
- Provide Information Security Awareness and Training
- Analyze the Effectiveness of Information Security Controls
- Resolve Noncompliance Issues

Management Metrics



Specific, measurable, attainable, repeatable, and time bound

Types of Management Metrics

Management metric types include:

- Strategic
- Management
- Operational

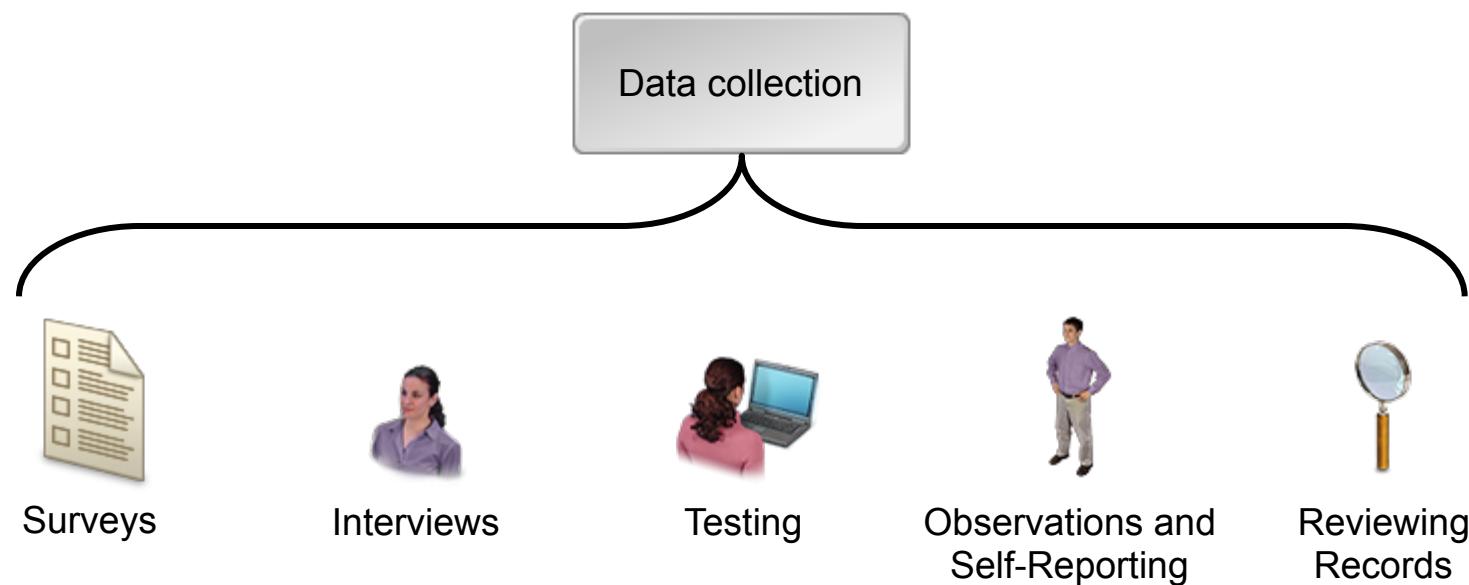
Data Collection

Quantitative data includes:

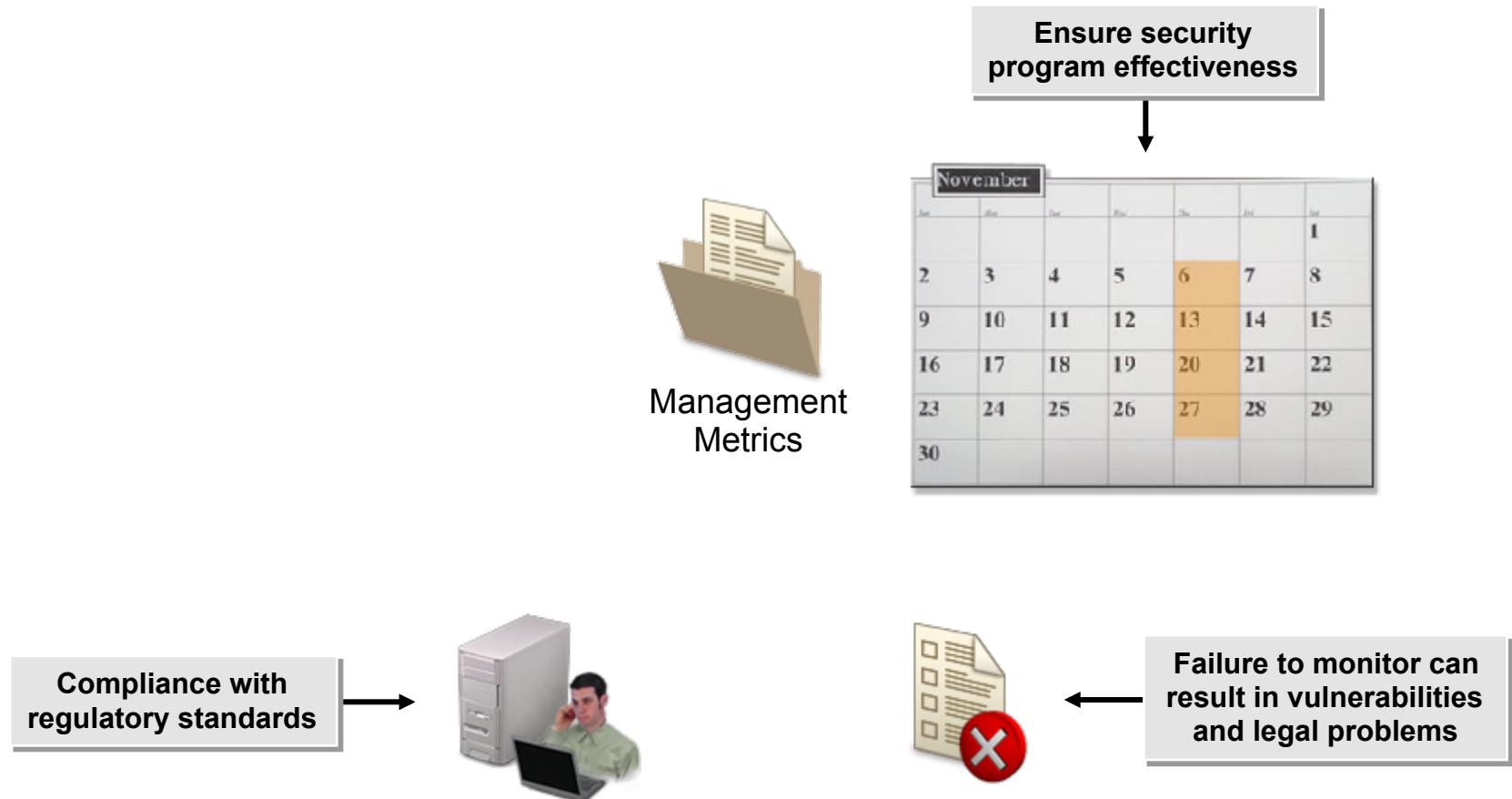
- Event logs
- Utilization reports
- Factual sources

Qualitative data includes:

- Surveys
- Observations
- Interviews



Periodic Reviews



Monitoring Approaches

For technical metrics, quantitative data will measure:

- Vulnerabilities
- Audit statistics
- Unresolved security issues

For performance statistics, qualitative data will measure:

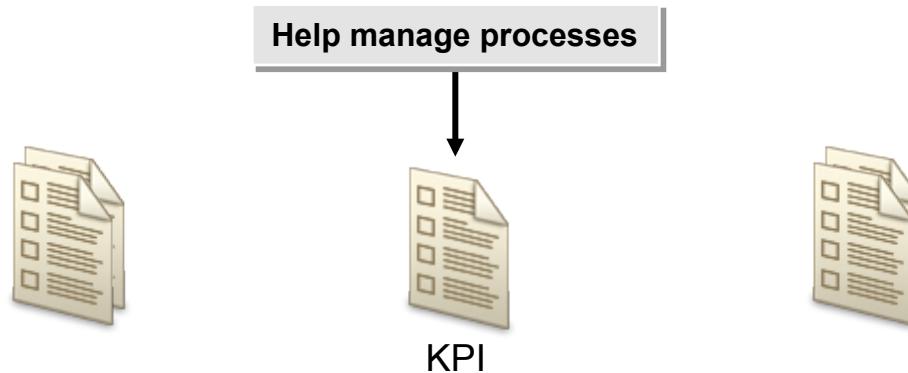
- KPIs
- KGIs
- Six Sigma
- ISO 9001 quality indicators



KPIs

Objectively measure the progress of:

- Processes
- Services
- Activities



Types of Measurements

Measurement types include:

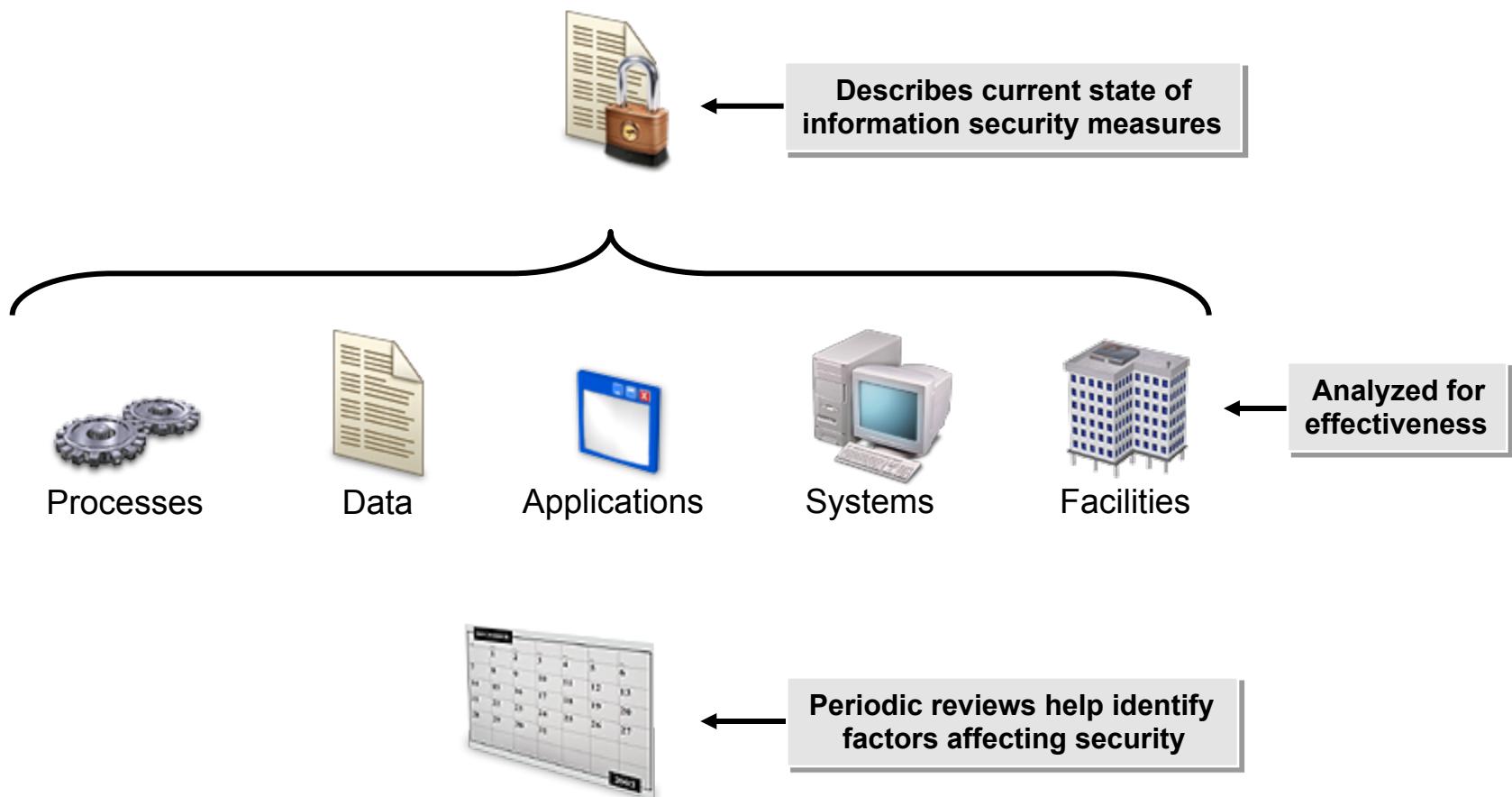
- Risk and loss
- Organizational objectives
- Regulatory standards
- Operational productivity
- Cost-effectiveness
- Organizational awareness
- Security architecture
- Management framework
- Operational performance

Other Measurements

Other measurements include:

- KGI
- Six Sigma
- ISO 9001

Information Security Reviews



The Role of Assurance Providers

Internal assurance providers come from several divisions:

- Internal audit
- Legal
- Human resources
- Risk management
- IT
- Compliance

External assurance providers can:

- Provide the same level of support.
- Often be more cost-efficient.
- Come with both advantages and disadvantages.

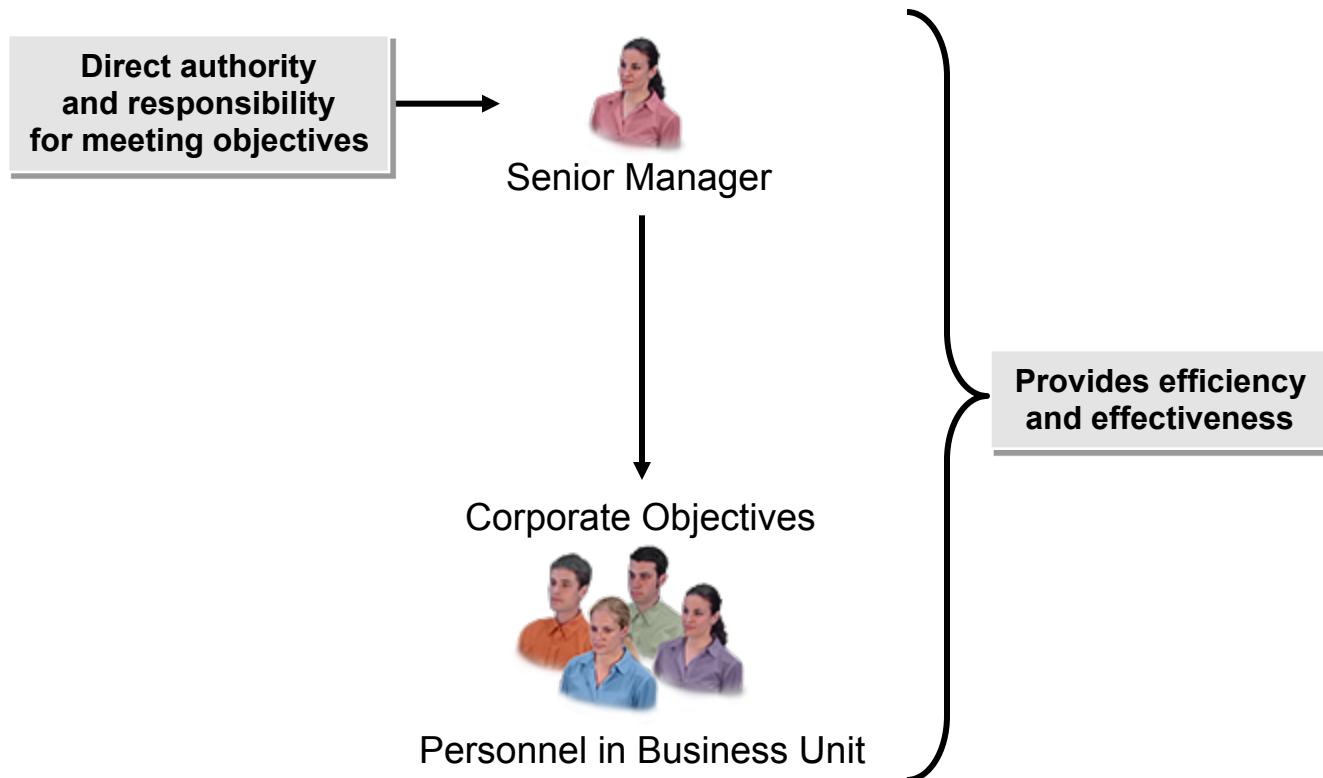


Assurance
Providers

Comparing Internal and External Assurance Providers

Assurance Provider	Advantages/Disadvantages
Internal	<p>Advantages:</p> <ul style="list-style-type: none">Ability to secure systems internally.Availability of personnel in an emergency.Control of sensitive data.Knowledge of the organization's management structure and culture. <p>Disadvantages:</p> <ul style="list-style-type: none">Varying levels of knowledge and skill.Cost of human resources.Inability to take on additional responsibilities.
External	<p>Advantages:</p> <ul style="list-style-type: none">Specialized knowledge and skills.Ability to divide labor and offload routine tasks.Availability of additional services.Cost effectiveness. <p>Disadvantages:</p> <ul style="list-style-type: none">Lack of ability to work in real-time in an emergency.Lack of access to internal resources.Possible compromises to security of sensitive data.Possible lack of security of remote access and systems.

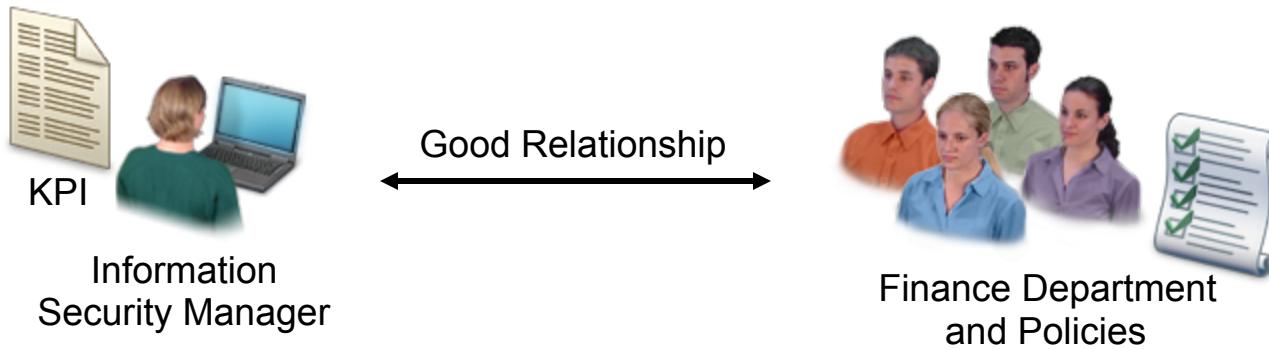
Line Management Technique



Budgeting

Budgetary responsibilities include:

- Forecasting
- Budgeting
- TCO and ROI analyses
- Inventory management



Staff Management

Roles may include:

- Security engineers
- Policy specialists
- Access administrators
- Project managers
- Compliance liaisons
- Security architects
- Awareness coordinators



Facilities

Considerations include:

- Organizational growth.
- Changes in information security standards.
- Need for new equipment.
- Financial constraints.



How to Manage Information Security Program Resources

To manage information security program resources:

- Define management metrics that will be used to measure the effectiveness of the information security program.
- Collect qualitative and quantitative data about your organization's information system.
- Use KPIs to conduct periodic information security reviews.
- Maintain the budget, staff resources, and inventory and utilization of resources.

Security Policies

Security policies:

- ❑ Describe how an organization will protect sensitive data and resources.
 - ❑ Network infrastructure
 - ❑ Physical and electronic data
 - ❑ Applications
 - ❑ Physical environment
- ❑ Can include multiple individual policies.
- ❑ Should identify conformance requirements for all implemented security measures.
- ❑ Can be used to evaluate security compliance.

Security Policy Components

Security policy components include:

- Policy statement
- Standards
- Guidelines
- Procedures



Implementation of Information Security Policies

Implementation activities include:

- Initial implementation
- Disseminating and communicating policies
- Monitoring and enforcing compliance
- Reviewing policies
- Updating policies



Administrative Processes and Procedures

Administrative process and procedures include:

- Access control
- Identity management
- Remote access

Access Control Types

Access control types include:

- Administrative
- Physical
- Technical

Bob can:

- Read People1
- Read and write to Part1, as the owner
- Read Control1

		Objects			
		Pay1	People1	Part1	Control1
Subjects	Bob		r	rwo	r
	Alice		r	r	rwo
	Boris	rw	rw		
	Natasha	rwo	rwo		r

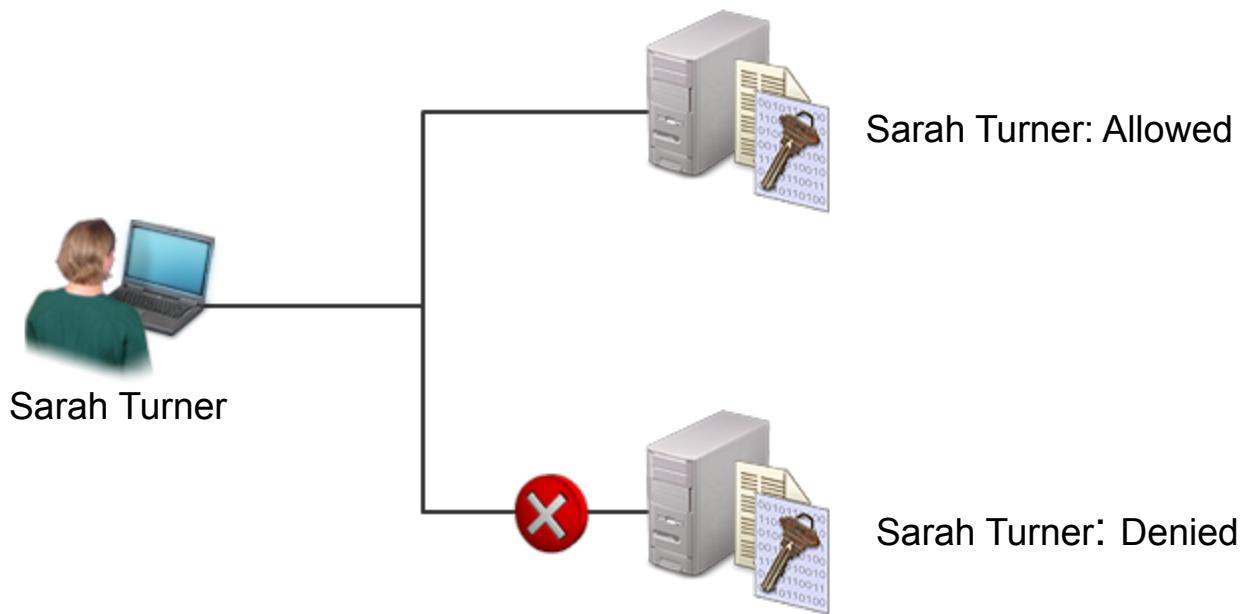
Rights ←

Access Security Policy Principles

Access security policy types include:

- Need to know
- Least privilege
- Separation of duties

Identity Management and Compliance



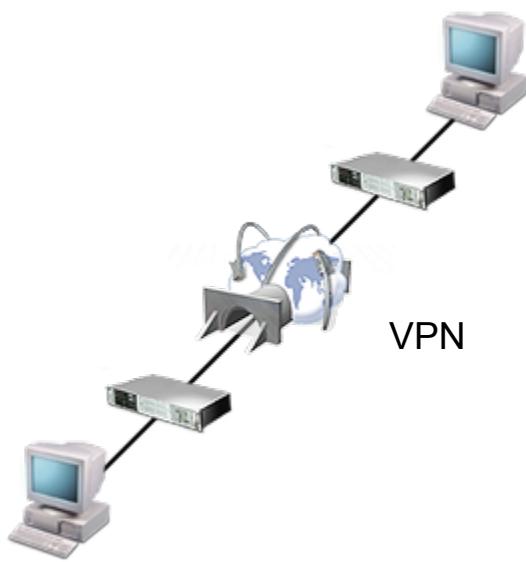
Authentication Factors

Authentication factors include:

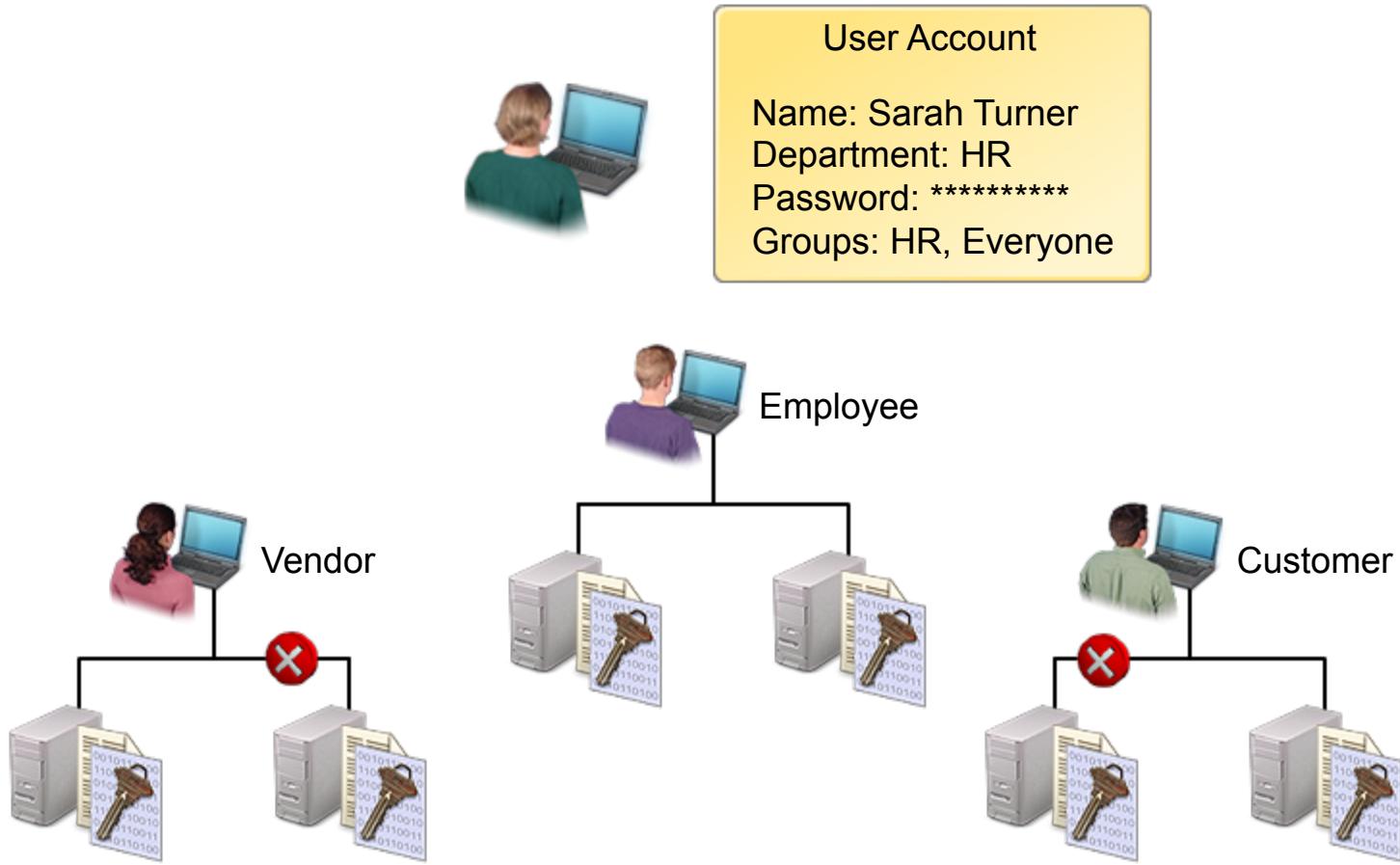
- Something you know, such as a password.
- Something you have, such as a security token.
- Something you are, such as fingerprints.



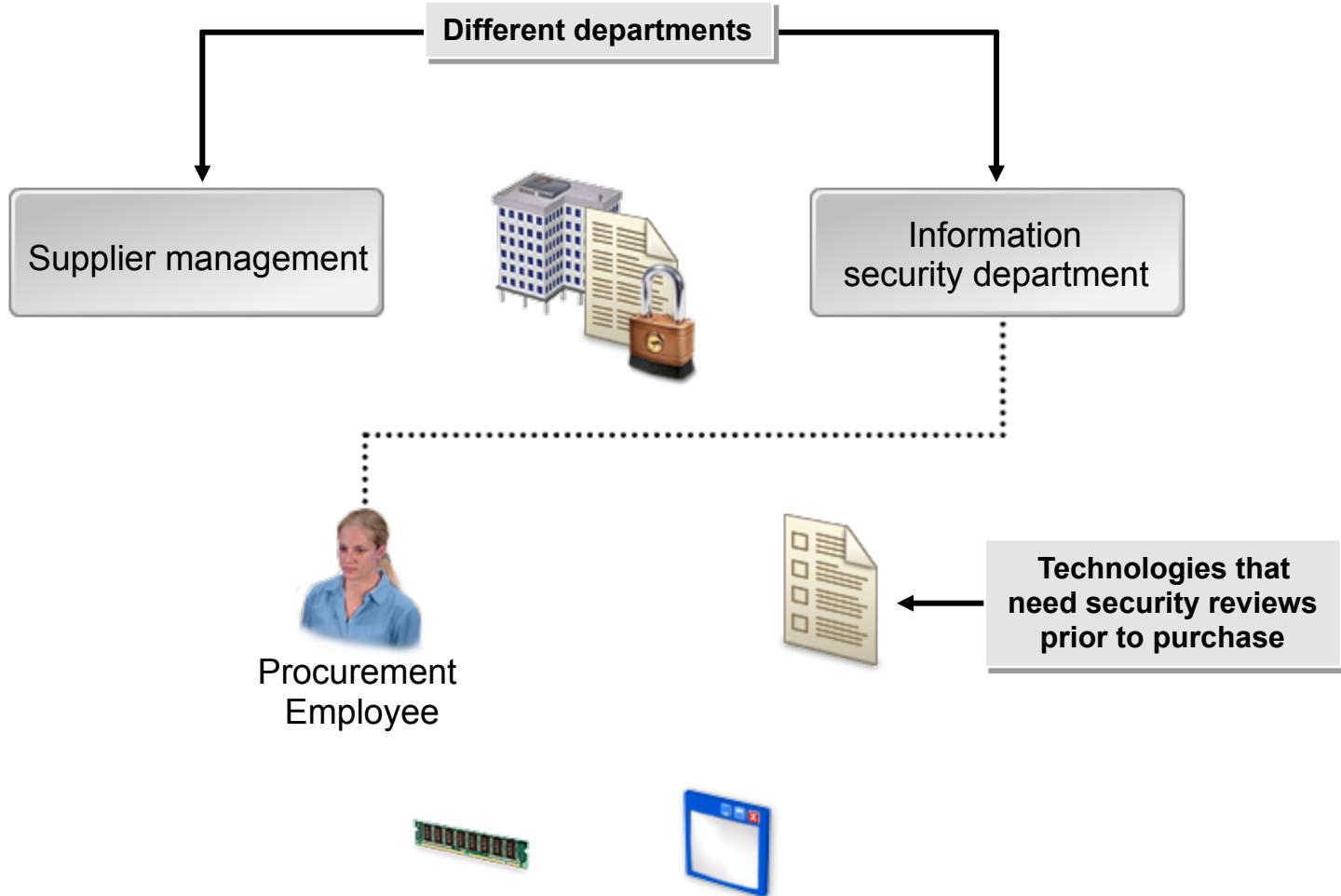
Remote Access



User Registration



Procurement



How to Enforce Policy and Standards Compliance

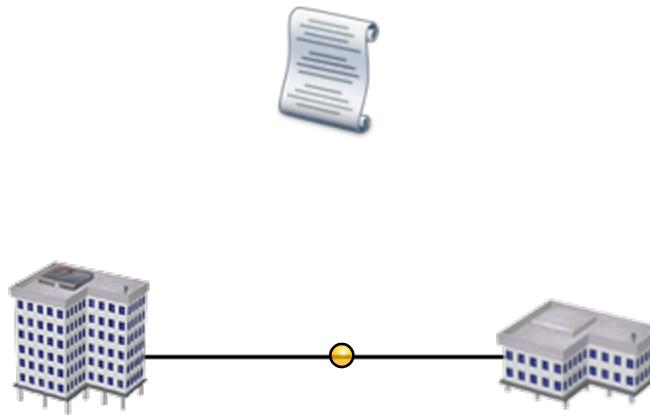
To enforce information security policy compliance:

- Create and distribute information security policy documents that include the standards and guidelines appropriate for your organization.
- Read all other applicable policy documents thoroughly so that you understand the standards and guidelines that pertain to your organization.
- Monitor security-related activities in your organization.
- When you find noncompliance with a security policy, take appropriate actions to correct the situation.
- Use available tools such as access controls and identity management to enforce compliance with the organization's security program.
- Conduct periodic reviews.

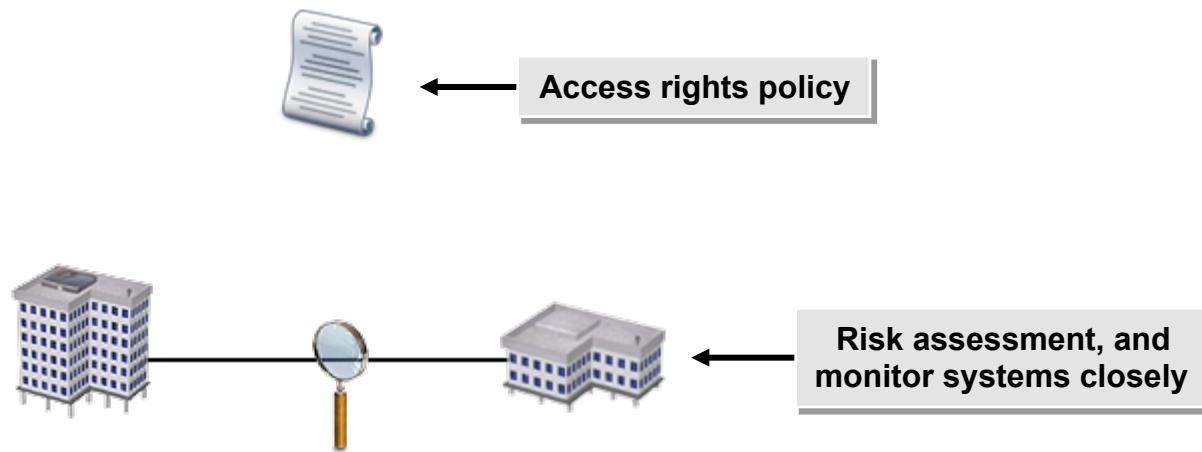
Types of Third-Party Relationships

Third-party relationships can include:

- Trade partners.
- Contractors.
- Joint ventures.
- Outsourcing providers.



Methods for Managing Information Security Regarding Third Parties



Security Service Providers

Services delivered by outsourced vendors:

- Consulting
- Security planning and design
- Auditing
- Reviewing
- Operational and forensics support

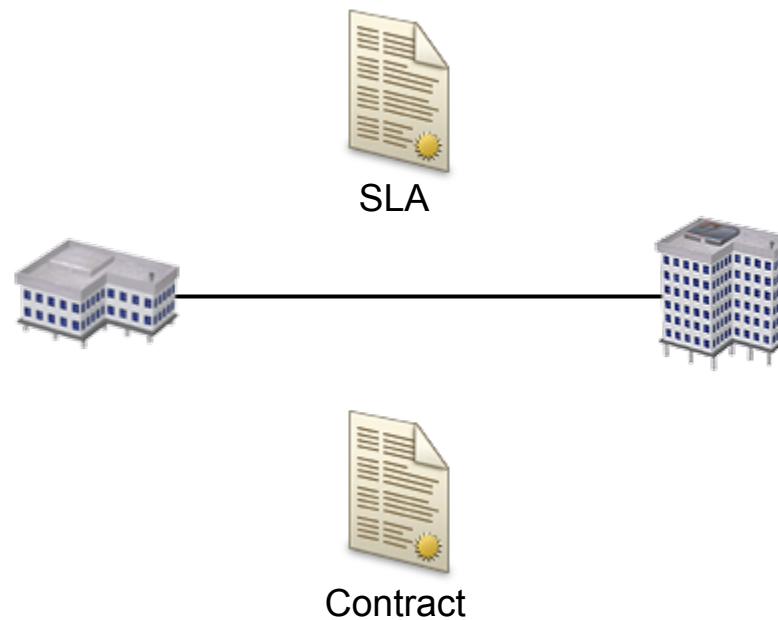


Third-Party Contract Provisions

Contract provisions include:

- Confidentiality
- Security
- Right-to-audit

Methods to Define Security Requirements in SLAs



Security Provisions and SLAs

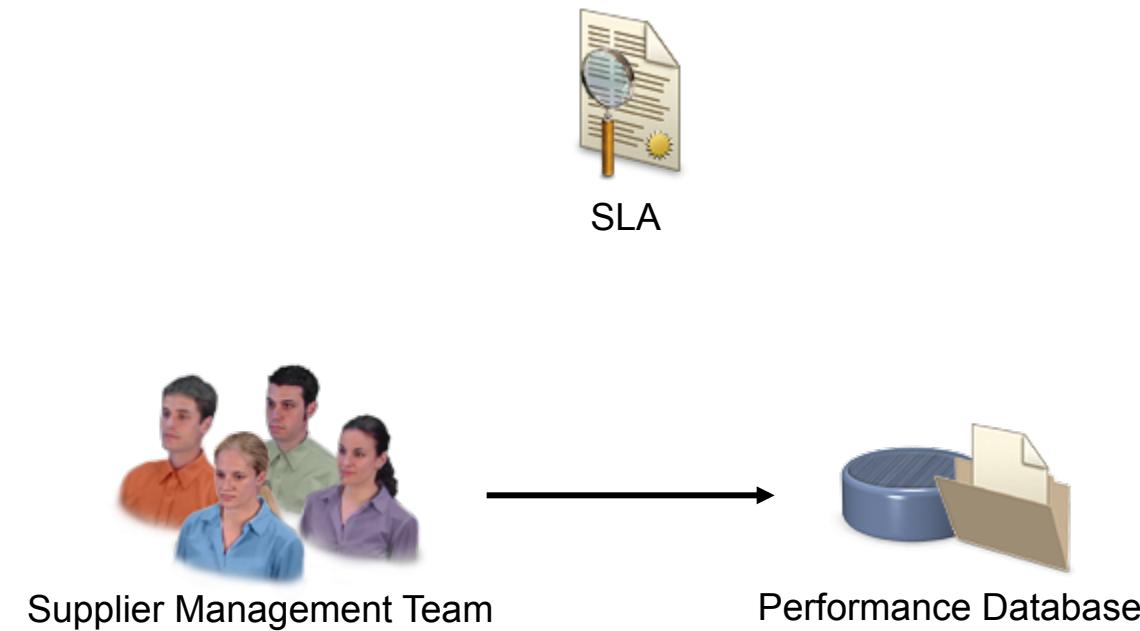
Security provisions common to SLAs include:

- Confidentiality or nondisclosure
- Destruction/disposal of information
- Security controls
- Network connectivity
- Inquiry and remediation
- Right-to-audit

Methods to Monitor Security Requirements in SLAs

The performance database tracks:

- SLA expiration and renewal dates.
- Breaches of the SLAs.
- Updates to current SLAs.

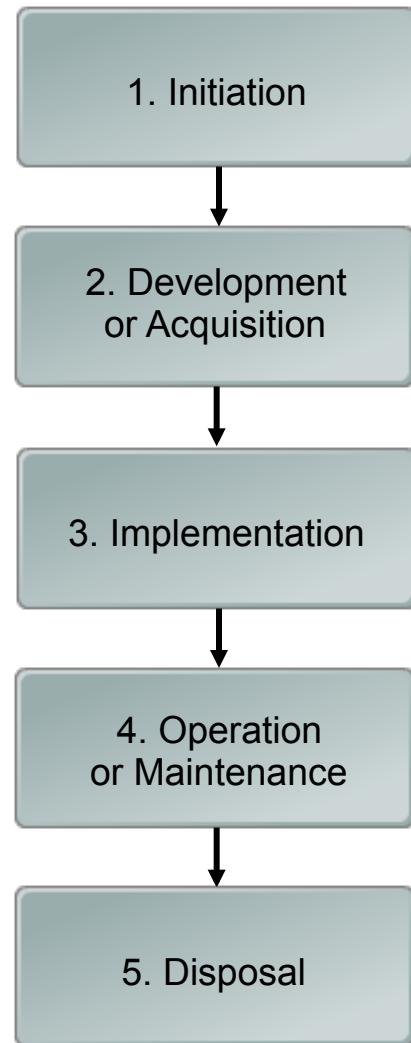


How to Enforce Contractual Information Security Controls

To enforce contractual information security controls:

- Define third-party relationships within the organization.
- Determine the level of access third-party vendors will be assigned.
- Define the provisions for information security controls that will be enforced in the organization's third-party contract.
- Define security requirements in the SLA for the third-party relationship.
- Monitor security requirements enforceable by the SLA.

The SDLC



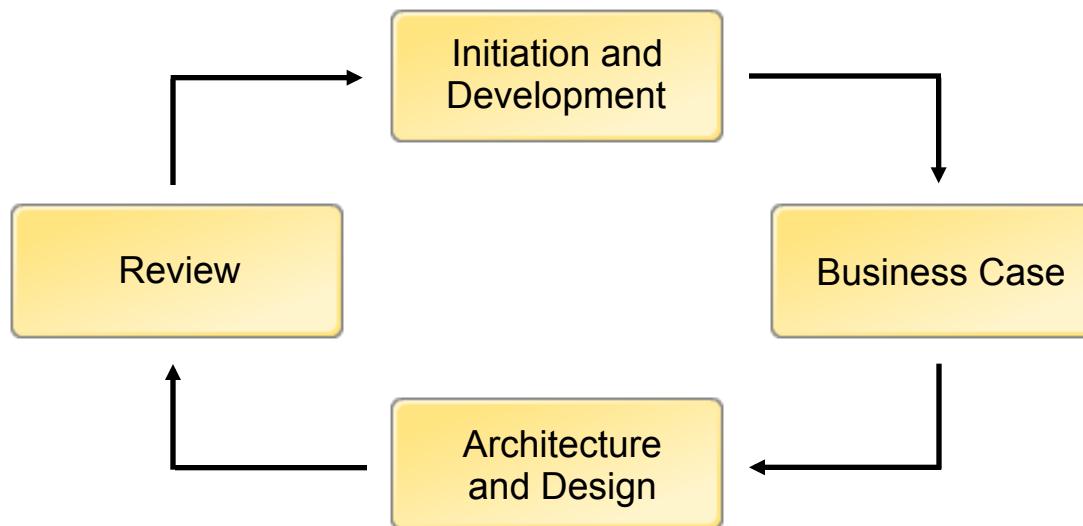
Code Development



Standards



Security Manager



Common Techniques for Security Enforcement

Common techniques include:

- Risk assessment.
- Security controls.
- Configuration management.
- Disposal of the hardware and software.

How to Enforce Information Security During Systems Development

To enforce information security during systems development:

- At the initiation phase:
 - Conduct a preliminary risk assessment.
 - Identify required security controls.
 - Define acceptable level of risk.
- At the development phase, conduct a formal risk assessment.
- At the implementation phase, implement security controls.
- During development and implementation, test that:
 - Systems meet security specifications.
 - Security controls are working.
- At the maintenance phase:
 - Implement configuration management and control.
 - Monitor.
- At the end of life phase:
 - Retain documentation.
 - Dispose of hardware and software.

Maintenance

Maintenance:

- Ensures that new life cycle activities are secure.
- Uses the same techniques as in development.



Methods of Monitoring Security Activities

Monitoring methods include:

- NIDS
- HIDS
- Honeypots
- Log reviews and reports
- Condition monitoring

Impact of Change and Configuration Management Activities



Follow the change control guidelines for all changes



Test for compliance



Security controls can be adversely affected by system changes

How to Maintain Information Security Within an Organization

To maintain information security within an organization:

- Identify the business processes of the organization.
- Identify the life cycle activities of the organization.
- Institute a change management system.
- Monitor security activities for abnormal results.

Due Diligence Activities

Due diligence activities:

- Ensure that generally expected behavior occurs.
- Can be the front line of mitigating liability.
- Can be shown by providing advice and guidance to others.



Types of Due Diligence Activities

Due diligence activities include:

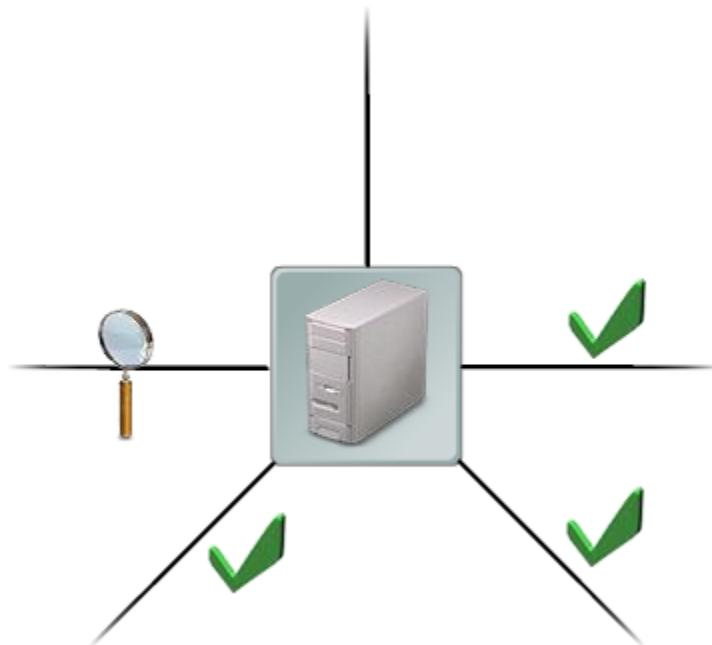
- Designing, implementing, and monitoring effective policies.
- Conducting periodic risk assessments.
- Implementing adequate security controls.
- Conducting continuous independent reviews.
- Providing security education.
- Enforcing compliance.
- Establishing effective backup and recovery processes.
- Establishing and testing BCPs and DRPs.



Reviews of Information Access

Reviews:

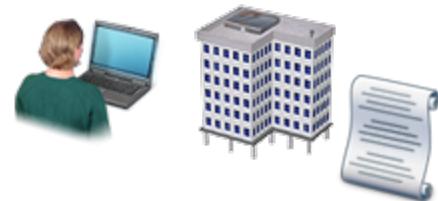
- Can be performed by employees or external service providers.
- Ensure no unauthorized access to systems.
- Show due diligence.



Standards of Managing and Controlling Information Access

Regulatory agencies include:

- The ISO.
- The OECD.
- The U.S. FERC.
- The U.S. NIST.



How to Provide Information Security Advice and Guidance

To provide information security advice and guidance:

- Review pending legislation and changing requirements in both the national and state legislature and regulatory agencies to see if they affect established security policies.
- Debrief results of risk assessments and security reviews with security stakeholders.
- Assess any due diligence issues with security stakeholders.
- Examine current information security policies and advise stakeholders of results.
- Communicate any information security issues to security stakeholders.

Information Security Awareness

To train users:

- Start with high-level security awareness education.
- Move to training in specific job roles.
- Finally, add education to provide highly skilled and competent security professionals.



Types of Information Security Stakeholders

Security stakeholders include:

- Employees
- Senior management
- BPOs

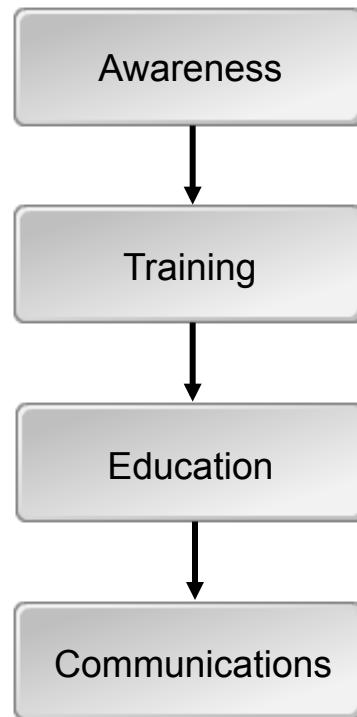
Methods of Stakeholder Education

Stakeholder education is:

- Not just for information professionals.
- Instrumental in helping everyone understand and comply with security practices.
- The responsibility of the information security manager.
- Often conducted by HR.



The Security Stakeholder Education Process



How to Provide Information Security Awareness and Training

To provide information security awareness and training:

- Train new users on how to use their computers, applications, and organizational security policies. Focus on potential security problems throughout the training.
- Post all relevant security policies so that they are easily accessible to all users.
- Notify users when changes are made to policies. Educate them on the new changes.
- Periodically test user skills after training to verify they are implementing proper security. For example, you can use planned social engineering attacks.
- Post information, such as web links, on the company website to assist users in determining whether or not an email is a hoax.

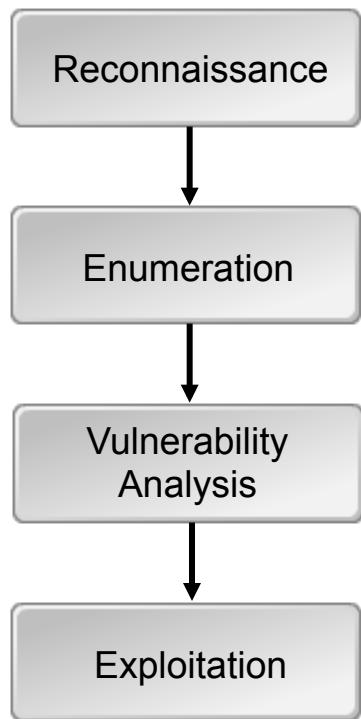
Methods of Testing the Effectiveness of Information Security Controls

Methods of testing include:

- Conducting periodic vulnerability reviews.
- Conducting and tracking risk assessments.
- Conducting penetration testing.



The Penetration Testing Process

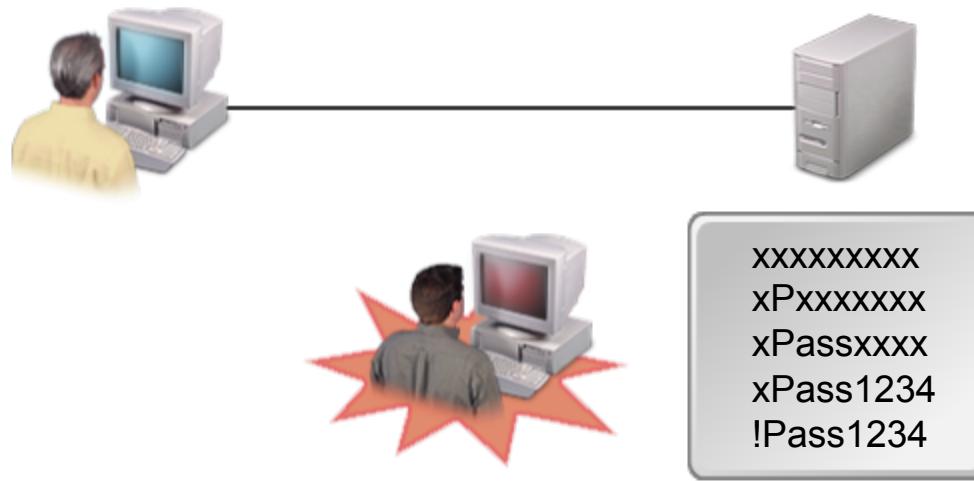


Types of Penetration Testing

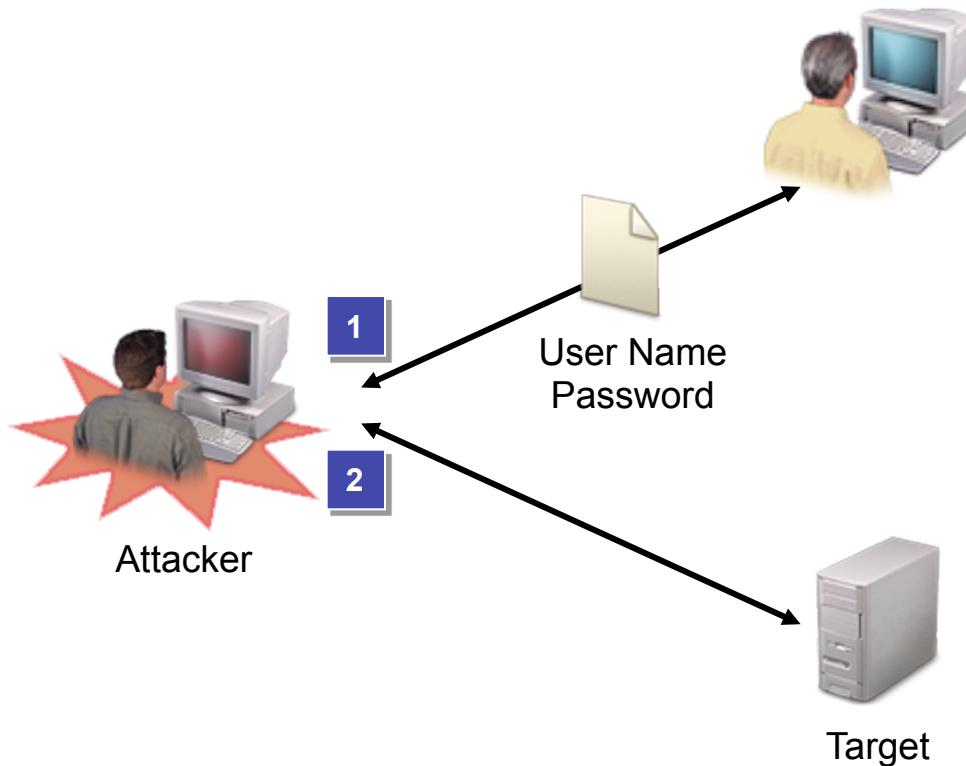
Penetration testing types include:

- White box
- Gray box
- Black hat (blind testing)
- Double blind testing

Password Cracking



Social Engineering Attacks



1. Attacker obtains credentials from user
2. Attacker uses credentials to mount attack

Social Engineering Types

Social engineering types include:

- Pretexting
- Shoulder surfing
- Dumpster diving
- Theft
- Trojan horse
- Spoofing
- Phishing

Assessment Tools

Assessment tools include:

- Tivoli® Security Compliance Manager.
- Retina Network Security Scanner.
- Symantec™ Enterprise Security Manager™.
- Symantec™ NetRecon.



External Vulnerability Reporting Sources

Vulnerability reporting sources include:

- ❑ National Vulnerability Database
 - ❑ <http://nvd.nist.gov>
- ❑ Carnegie Mellon's CERT:
 - ❑ www.cert.org
- ❑ Security advisory websites:
 - ❑ <http://secunia.com/advisories>
 - ❑ www.securityfocus.com/vulnerabilities
- ❑ The SANS Institute:
 - ❑ www.sans.org/top20



Vulnerability
Reports

Regulatory Reporting Requirements

Industry	Jurisdiction and Regulations
Healthcare	Jurisdiction: United States Regulation: HIPAA
Publicly traded companies	Jurisdiction: United States Regulation: SOX Act
Banking	Jurisdiction: International Regulation: Basel II
Financial services	Jurisdiction: United States Regulation: GLBA
Energy/infrastructure	Jurisdiction: United States Regulation: FERC Cyber Security Standard
Federal government	Jurisdiction: United States Regulation: FISMA
All industries	Jurisdiction: Canada Regulation: PIPEDA-Bill C6

Regulatory Reporting Requirements (Cont.)

Industry	Jurisdiction and Regulations
All industries	Jurisdiction: European union Regulation: EU Data Protection Directive
Security framework	Jurisdiction: International Regulations: <ul style="list-style-type: none">• ISO/IEC 17799• GAISP, Version 3.0

Internal Reporting Requirements

Internal reporting requirements:

- Vary by organization and covered by policies
- Monitors and controls costs
- Helps with decision making

Internal reports may include information about:

- Vulnerabilities
- Risk assessment
- Budget
- Utilization



How to Analyze the Effectiveness of Information Security Controls

To analyze the effectiveness of information security controls:

- Monitor the organization's information systems by completing periodic vulnerability reviews.
- Conduct and track the results of periodic risk assessments.
- Conduct penetration testing for your organization's information system.
- Report findings in accordance with your security policies.

Noncompliance Issues

Noncompliance issues can arise because of:

- An unintentional lack of awareness.
- The malicious nature of a disgruntled employee.



Noncompliance issues can be detected by:

- Monitoring tools.
- Vulnerability scans.
- System reviews.
- Due diligence.

Security Baselines



← **Assess compliance**



← **Dependent on operating system and function**



← **Different baselines for different systems**

Events Affecting the Security Baseline

Business needs that can cause a change include:

- Configuration changes needed for new hardware or software.
- Third-party access to systems.
- Mergers or acquisitions or other organizational changes.

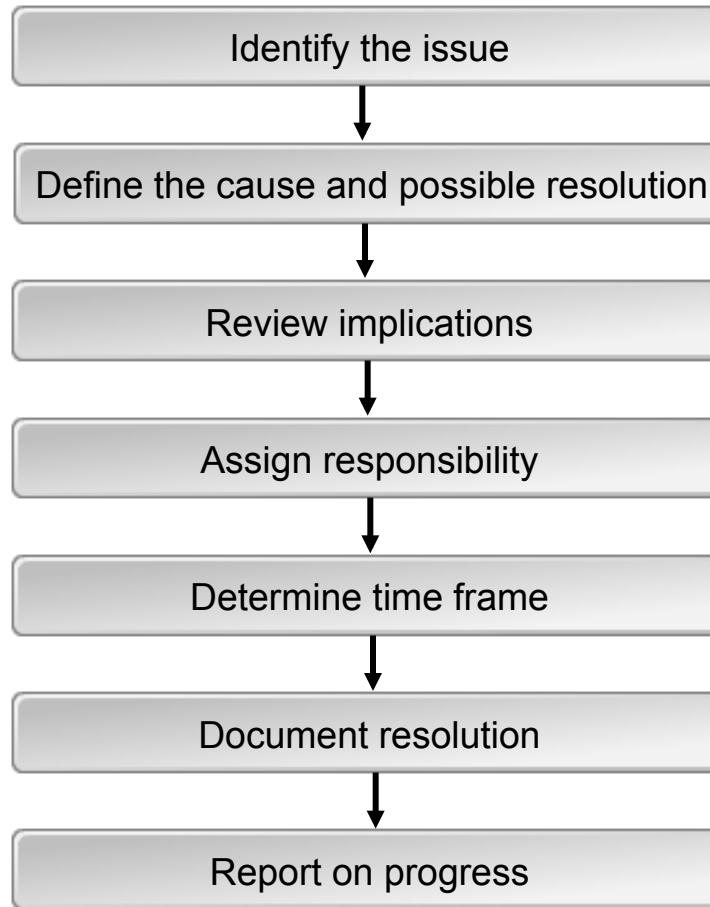
External forces can include:

- Natural disasters.
- Civil unrest.



Security Baseline

Information Security Problem Management Process



How to Resolve Noncompliance Issues

To resolve noncompliance issues:

- If multiple noncompliance issues exist, prioritize the issues based on the severity of the security threat to the organization.
- Log and track the noncompliance issue and resolution in a database designed for such information.
- Secure the organization's information systems.
- Address the current noncompliance issue to bring the issue into compliance.
- Determine the failure in the information security program and take steps to correct it.
- Test the solution to ensure it does fix the issue and that it does not create any new issues.
- Revise the solution, as needed, based on testing.

Reflective Questions

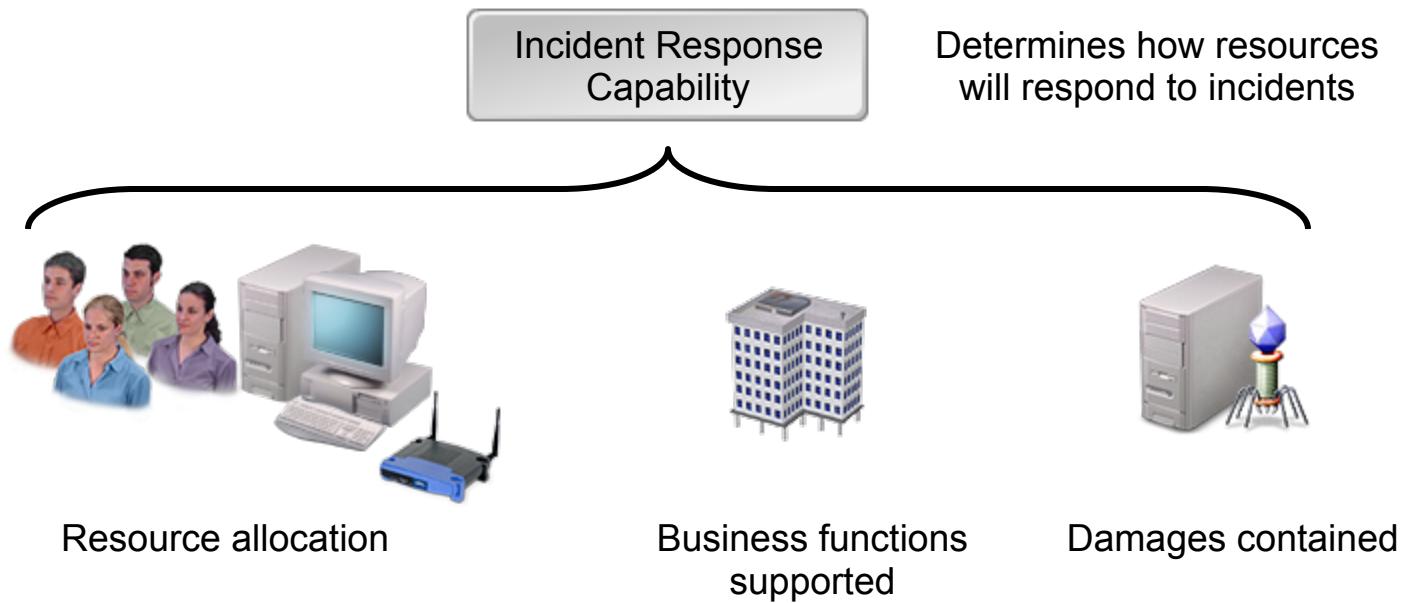
1. Which methods of managing an information security program in this lesson were familiar to you, and which were new?

2. Describe some situations in which you have practiced information security program management. If you have never experienced a situation in which you have practiced information security program management, which security component do you think you will be able to implement immediately?

Incident Management and Response

- Develop an Information Security Incident Response Plan
- Establish an Escalation Process
- Develop a Communication Process
- Integrate an IRP
- Develop IRTs
- Test an IRP
- Manage Responses to Information Security Incidents
- Perform an Information Security Incident Investigation
- Conduct Post-Incident Reviews

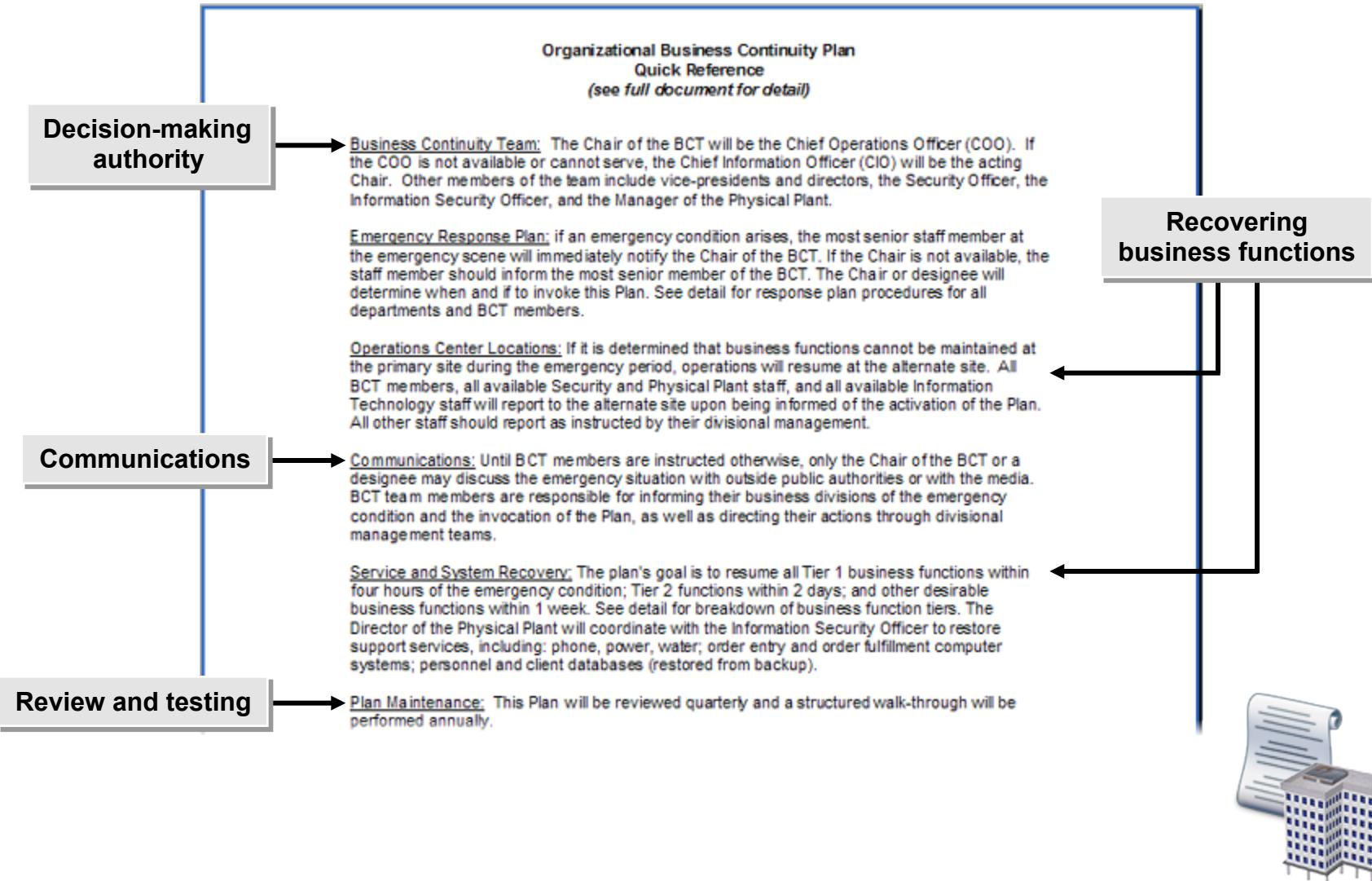
Incident Response Capability



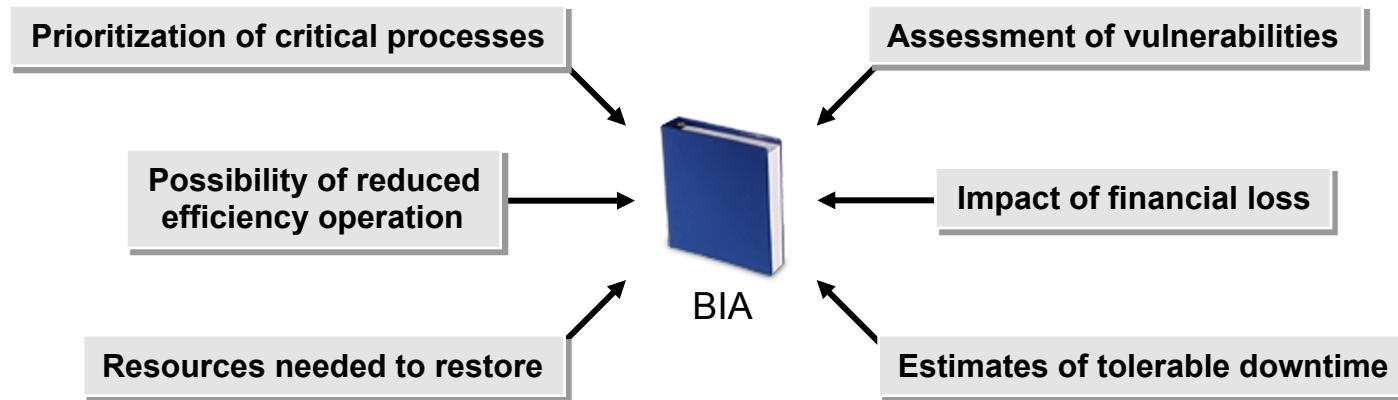
Components of Incident Response Capability

Components of incident response capability include:

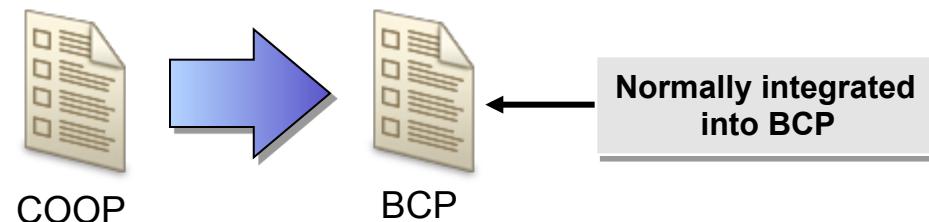
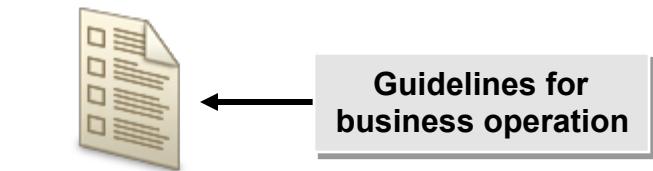
- Incident detection and monitoring capabilities
- Incident management scope
- Definition of severity criteria
- Assessment and triage
- Declaration of incident
- Response capabilities

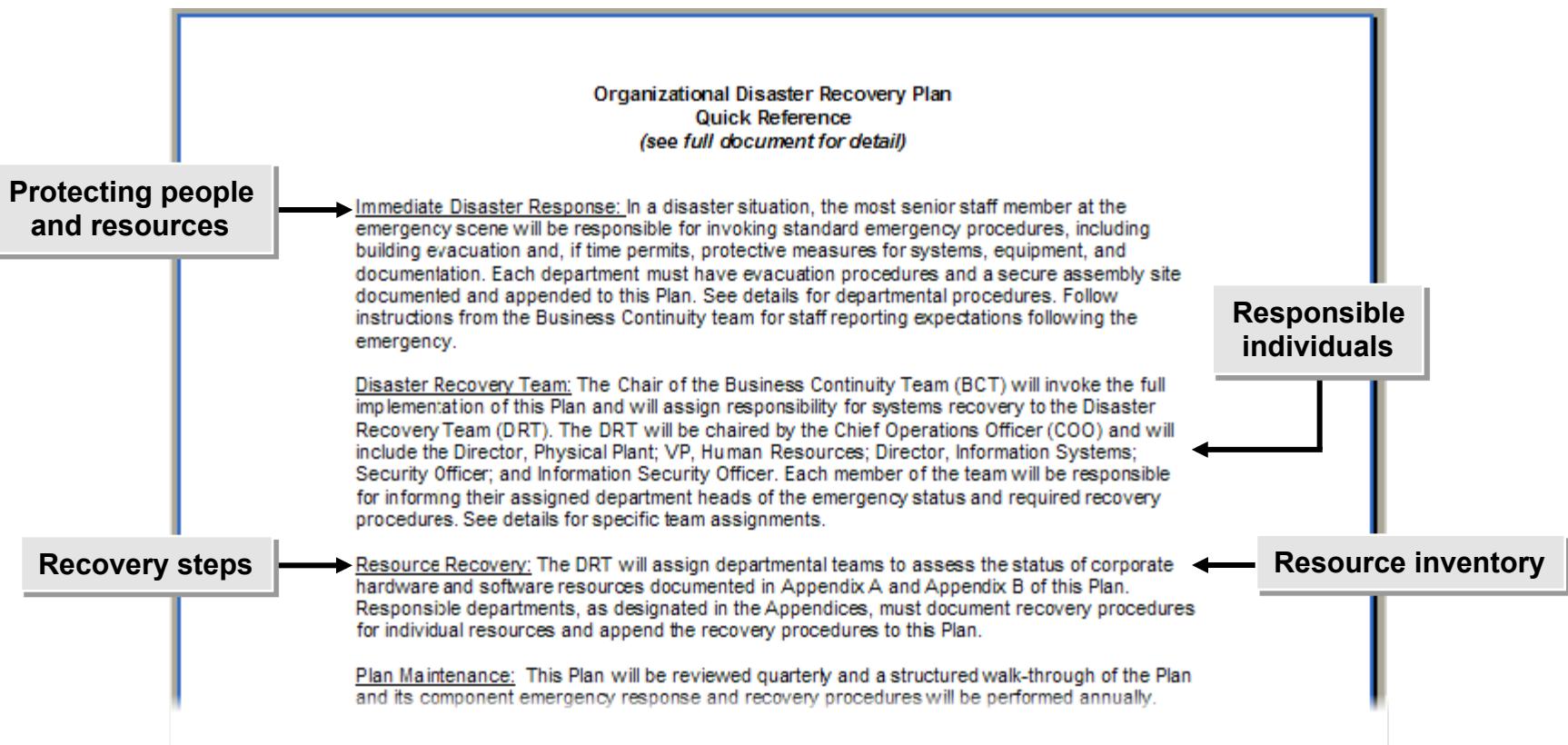


The BIA Phase



COOP



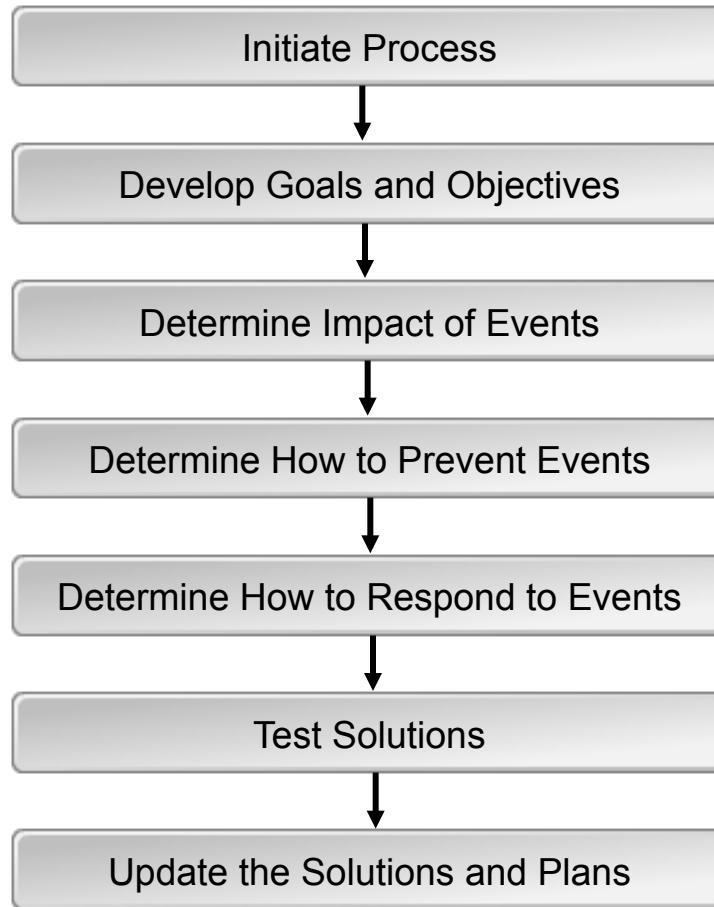


Alternate Sites

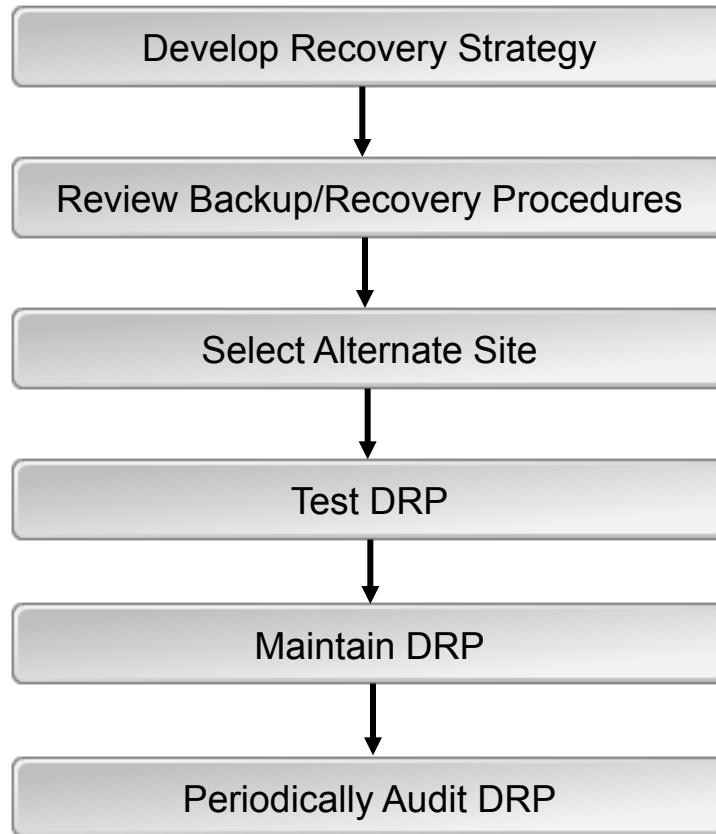
Alternate sites include:

- Hot sites
- Duplicate or mirror sites
- Warm sites
- Cold sites
- Mobile sites

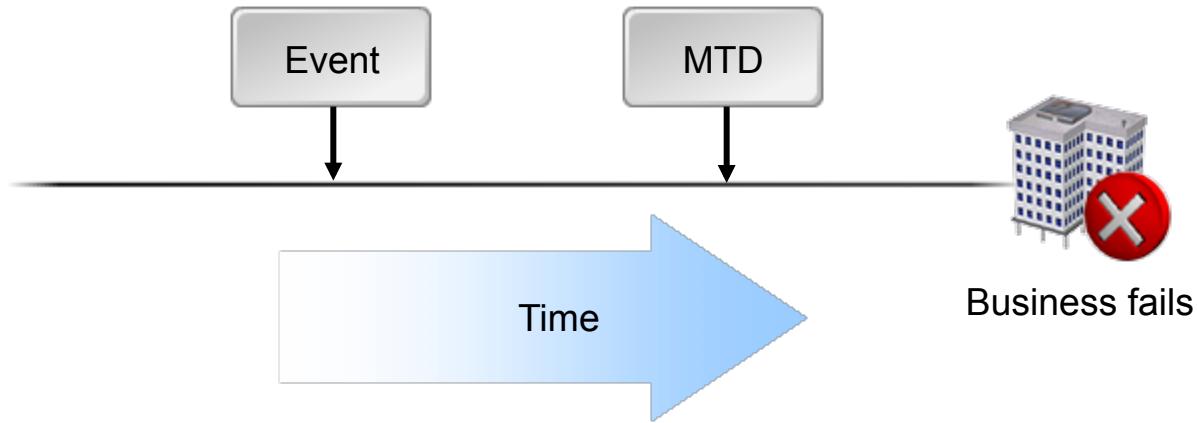
Develop a BCP



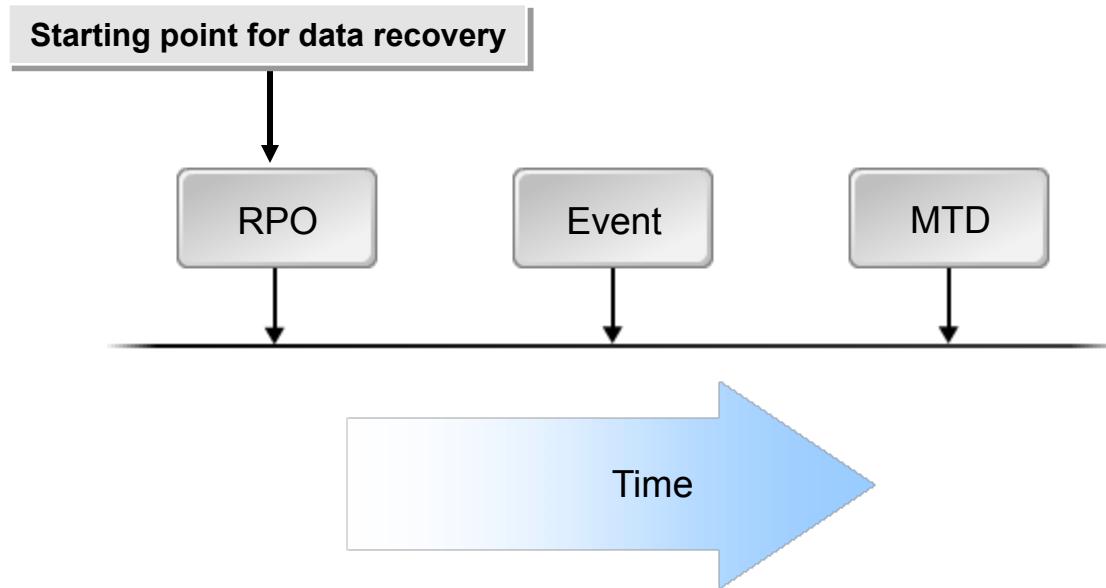
Develop a DRP



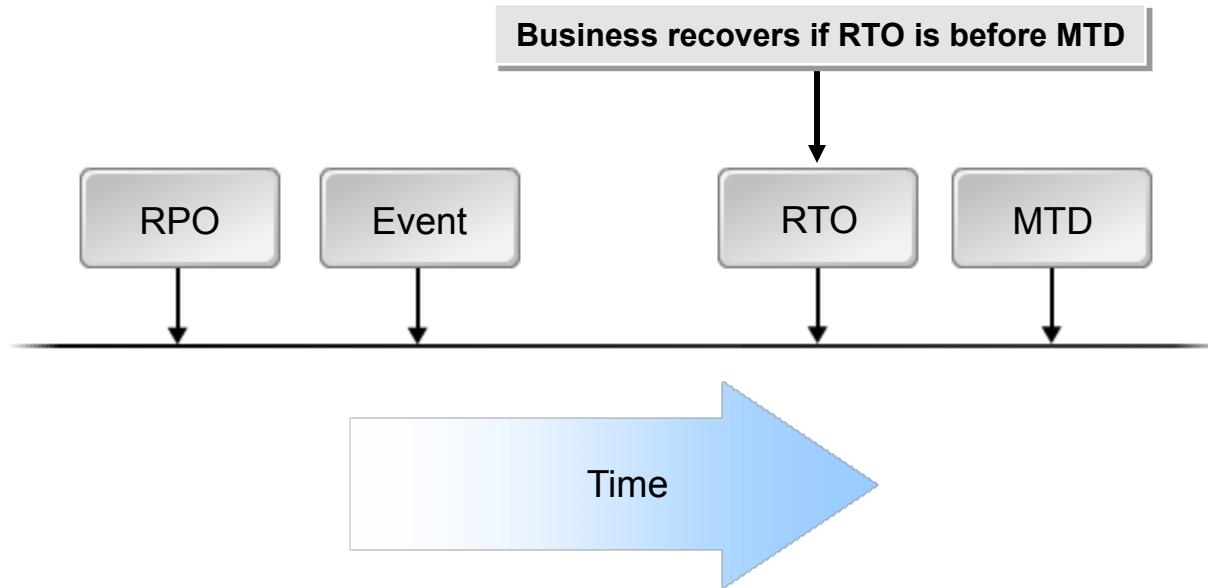
MTD



RPO



RTO



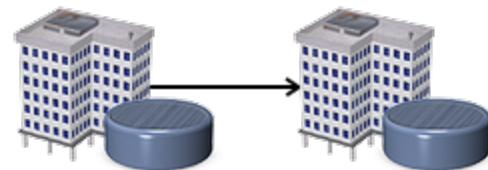
Data Backup Strategies



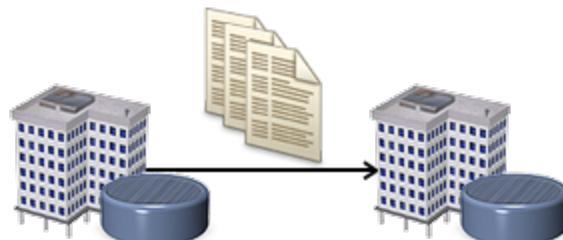
Tape/Disk Backup



Mirrored Backup



Remote Journaling



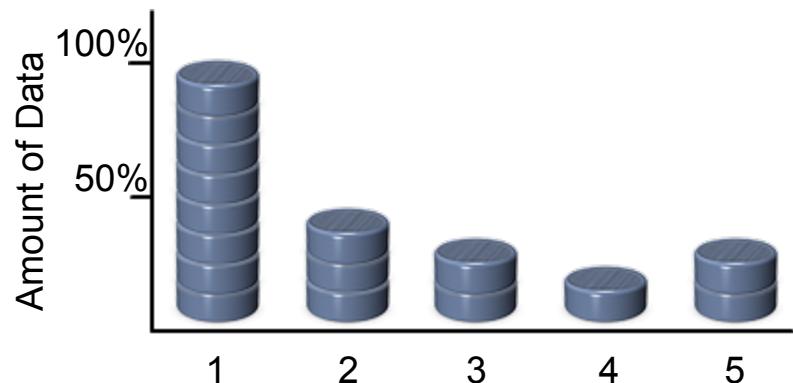
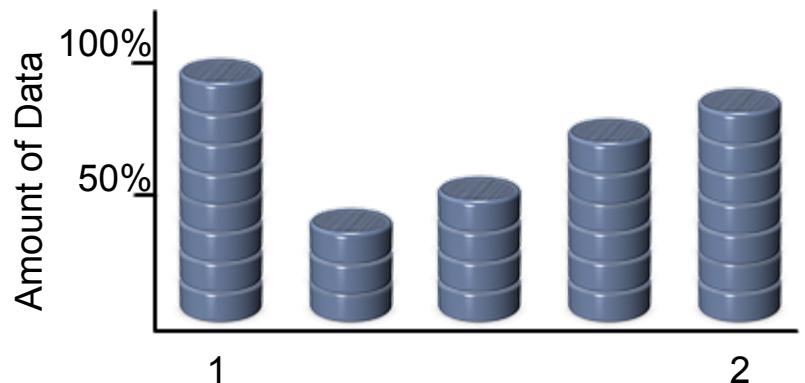
Electronic Vaulting

Data Backup Types

Backup types include:

- Full or normal
- Incremental
- Differential

Data Restoration Strategies

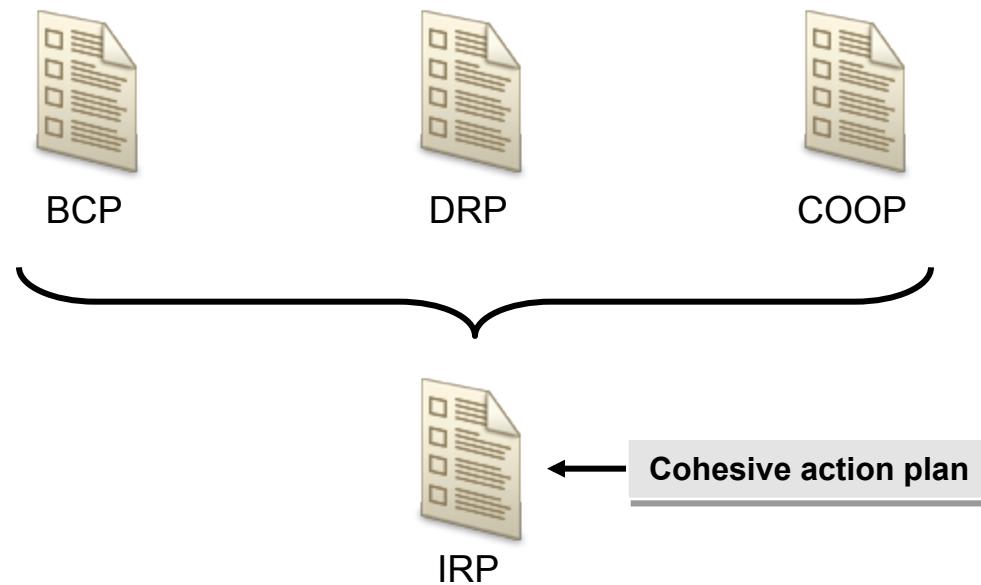


Information Incident Management Practices

Incident management practices include:

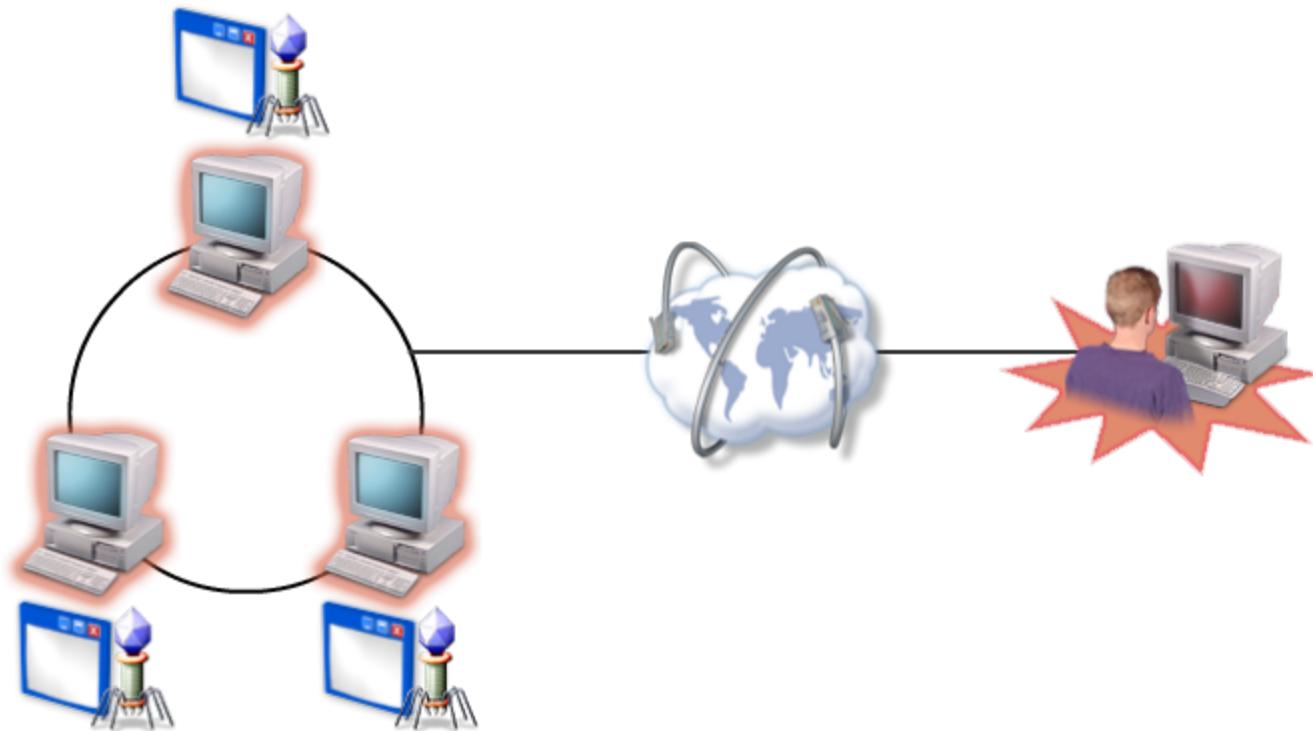
- Preparation
- Protection
- Detection
- Triage
- Respond

IRP



Trigger Events

Circumstances that set the IRP in motion



Types of Trigger Events

Trigger events include:

- Malicious code attacks
- Unauthorized access or use
- Unauthorized changes
- DoS attack
- Hoax/social engineering
- Data center failure
- Natural disaster
- Epidemic

Methods of Containing Damage

Containment methods include:

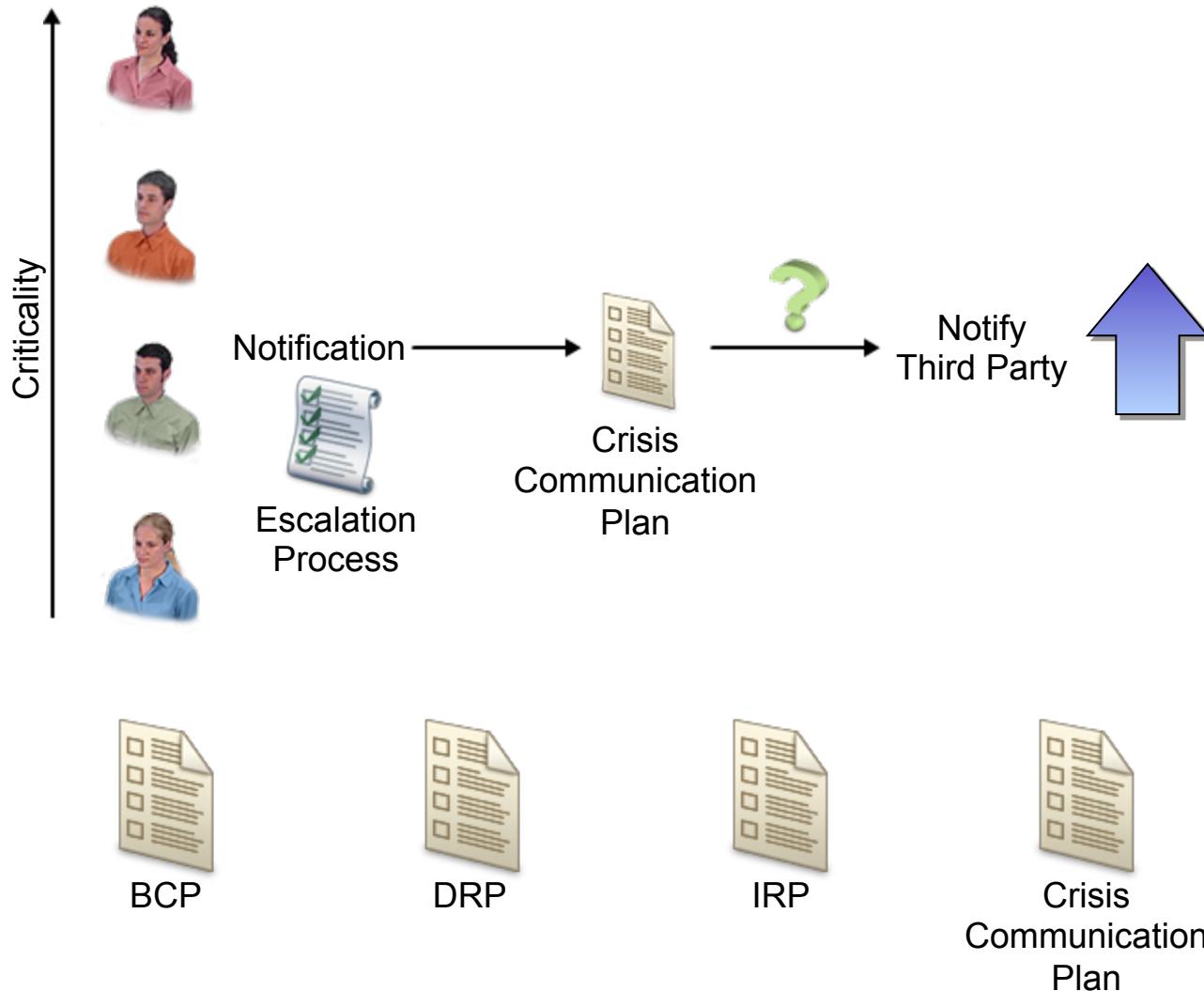
- Ensuring the safety and security of all personnel
- Removing devices from the network
- Disabling communication between network devices
- Disabling network user accounts
- Disabling email accounts
- Creating subnets on the organization ‘s network

How to Develop an IRP

To develop an IRP:

1. Conduct a BIA.
2. Study the incident response capabilities.
3. Conduct a risk assessment.
4. Develop a BCP.
5. Develop a DRP.
6. Train people to follow the plans.
7. Test the plans.
8. Revise the plans.
9. Maintain the plans.
10. Store a copy of the plans offsite.
11. Periodically audit the plans.

Escalation Process



Notification Process



Notification Process



Senior
Management



Business
Unit Leaders



HR
Representative



Info Sec
Manager



IRT
Members



Third
Parties

The IRT

Identify and manage security incidents



Business Unit Leader



Senior Manager



Business Unit Leader



Senior Manager



Security Manager



Auditor



Internal/External
Security Professional



Investigator

Crisis Communications

Vehicles:

- Scenarios
- Media relations
- News conferences

Areas:

- Organization to customer
- Within the organization
- Organization to public



How to Establish an Escalation Process

To determine the escalation process of a security event:

- Determine the business operations and systems that require an escalation process.
- Develop the escalation sequence for as many possible security events as possible that could affect the business operations and systems identified in the previous step.
- Assign responsibilities for each action in the escalation sequence.
- Assign time requirements for each action in the escalation sequence.
- Develop a notification process by:
 - Identifying the individuals or business units that need to be notified in the event of a security incident.
 - Determining when and how notifications will be made.
 - Determining who will be responsible for making the notifications.
 - Determining if any regulatory agency requires notification.

Internal Reporting Requirements

Collecting and reporting of:

- Suspicious activity.
- Inappropriate activity.
- Unauthorized activity.



Internal Reports

External Reporting Requirements

External reporting requirements are based on:

- The needs of the organization.
- Requirements of third parties.

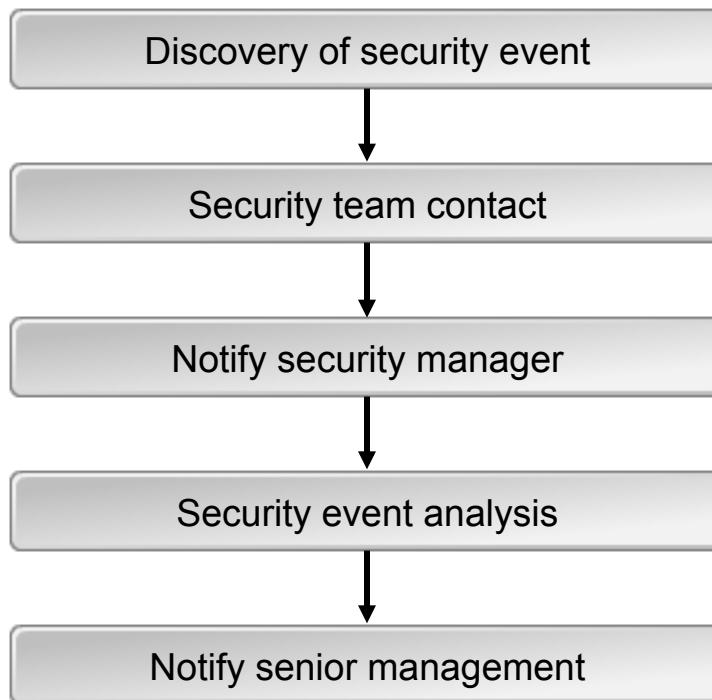
The external organizations include:

- Regulatory agencies.
- External legal counsel.
- Third-party contractual relationships.



External Reports

Communication Process



How to Develop a Communication Process

To develop a communication process:

1. Identify internal individuals to be contacted when a security incident occurs.
2. Identify external individuals to be contacted when a security incident occurs.
 - Including legal or regulatory agencies.
3. Determine when to notify the IRT members.
4. Determine the communication needed for each type of information security incident.
5. Document and train individuals in the process.
6. Test the process and revise any part of the process that fails during testing.

The IRP and DRP



IRP

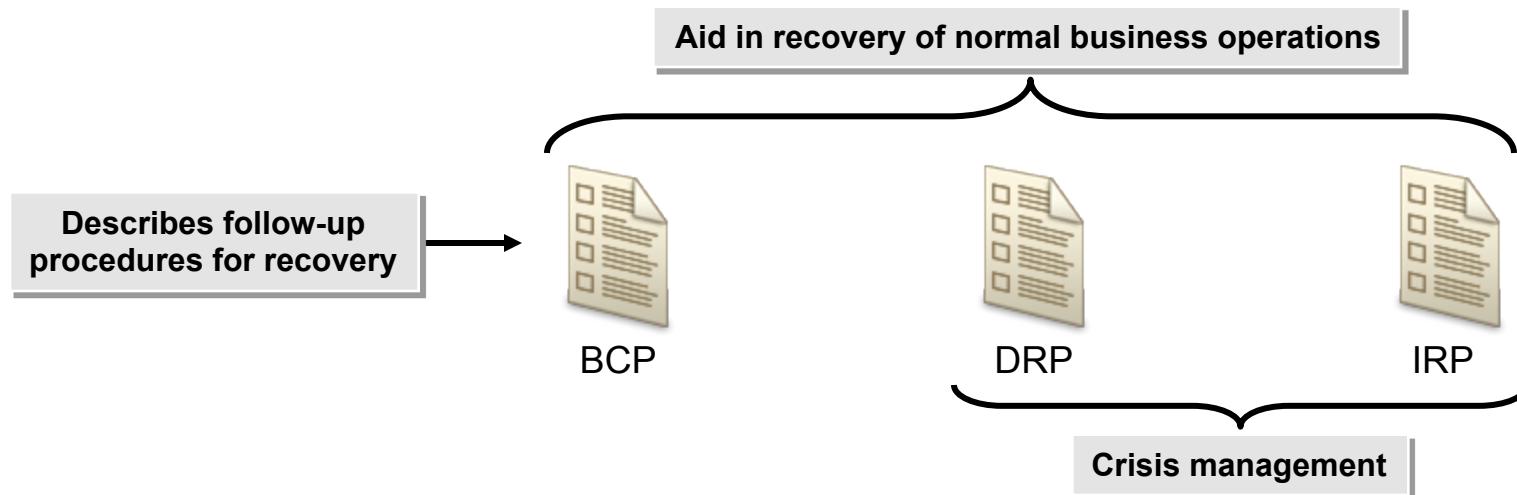


DRP

- Provide guidance for crisis situations
- Information security incidents

- Provide guidance for crisis situations
- Natural and man-made disasters

The IRP and BCP



Methods of Identifying Business Resources Essential to Recovery

Methods for identifying recovery resources include:

- Conduct a BIA
- Analyze physical aspects
- Analyze financial aspects
- Determine if staffing requirements require external resources
- Determine if recovery expertise is available

How to Integrate an IRP

To integrate an IRP:

- Manage the integration process.
 - Determine who is responsible for managing the IRP.
 - Record the activities and results of the document planning session.
 - Use a planning committee for drafting function-specific procedures.
 - Describe all roles and responsibilities.
 - Create an alert roster.
 - Identify and prioritize threats.
 - Identify the change management procedures for modifying the integration document.
- Integrate the IRP, DRP, and BCP.
 - Prepare for an incident.
 - Document activities during the incident.
 - Document post-incident activities.
 - Assemble the incident response portion of the plan.

The Role of Primary IRT Members

Primary IRT members include:

- Advisory group
- Information security manager
- Incident response manager
- Incident handler
- Investigator
- IT security specialist
- Business managers

The Role of Additional IRT Members

Additional IRT members include:

- IT specialist
- Legal counsel
- HR representative
- Public relations representative
- Risk management specialist
- Auditor

Response Team Tools and Equipment

Task	Tool or Equipment
Create disk images	AccessData® Forensic Toolkit®, EnCase® Forensic
Analyze files	AccessData Forensic Toolkit, EnCase Forensic
Display network shares	BySoft Network Share Browser, NetShareWatcher
User rights management	Novell® ZENworks® Desktop Management 7, Windows® Users and Groups control panel
Deleted data recovery	UndeletePlus™, PC Inspector™ File Recovery
Edit Windows Registry	AccessData Forensic Toolkit
Network sniffing	Wireshark, Ethereal®
Password cracking	AccessData Forensic Toolkit, John the Ripper
Active ports enumeration	Nsauditor Network Security Auditor, Nmap Security Scanner

How to Develop IRTs

To develop an IRT:

- Obtain senior management support.
- Determine the vision and operational plan for the IRT.
- Select team members to fill the roles necessary for your organization based on the skill sets and technical abilities needed.
- Train team members to follow the IRP to conduct information security incidents.
- Evaluate the effectiveness of the IRT on an ongoing basis.

BCP Testing

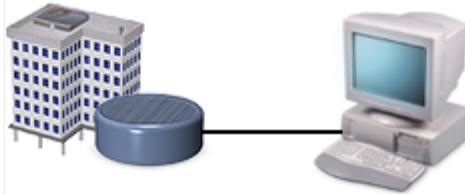
BCP testing methods include:

- Reviewing contents
- Analyzing the business continuity solution
- Using checklists
- Performing walkthroughs
- Parallel testing
- Conducting simulations
- Full interruption testing

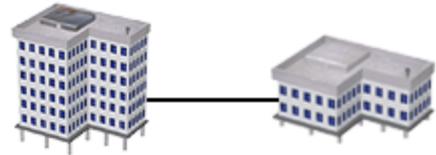
Disaster Recovery Testing



Checklist and Desktop



Offsite Restoration



Mirrored Site Cutover

Schedule Disaster Recovery Testing

Benefits of testing the DRP include:

- Ability to recover from an incident
- Identification of the effectiveness of the recovery process
- Identification of weaknesses in the DRP
- Ability to test alternate sites and backup facilities
- Ability to test business managers and IRT members
- Ability to maintain and update the DRP



DRP

Refine the IRP

Testing helps determine:

- Effectiveness of recovery
- Weaknesses needing correction



IRP

Logs should be kept by:

- IRT members
- Business managers
- Personnel



The IRT will:

- Review results
- Recommend modifications

How to Test an IRP

To test an IRP:

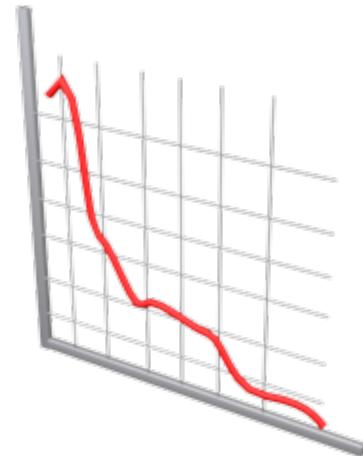
- Initiate the test with senior management approval.
- Consider following these general steps for testing an IRP:
 1. Create test objectives.
 2. Run the test.
 3. Evaluate the test results.
 4. Recommend improvements to the testing process, response plan, and recovery plan.
 5. Initiate a follow-up process.
- Select a security threat to test and create the mock conditions of the threat.
- Notify the IRT that the threat is not real, but that the IRP should be followed.
- Follow the IRP, and see if the action follows the plan.
- Analyze the response actions and times.
- Refine the IRP based on testing.
- If necessary, rewrite any IRP processes or procedures.
- Be sure to re-test any procedures or process that have been changed.

Damage Assessment

Damage assessment is necessary to:

- Determine facility damages.
- Identify the cause of the disaster.
- Estimate the expected down time.

LOSS



Business Impacts Caused by Security Incidents

Business impacts include:

- Damage to data, information systems, and resources.
- Unauthorized changes to data or systems.
- Theft of data or resources.
- Disclosure of confidential data.
- Interruption of services.



How to Manage Responses to Information Security Incidents

To manage responses to information security incidents:

- Identify the threat.
- Notify the IRT team members of the incident.
- Put the IRP into action.
- Log all actions and decisions made.
- Communicate with stakeholders following the communication plan.
- Conduct a post-incident review.
- Assess damages.
- Be sure to consider hidden costs.
- Determine the business impact of a security incident by considering both tangible and intangible impacts.

Computer and Digital Forensics

Forensic methods to obtain evidence include:

- Analyzing software for viruses or worms.
- Obtaining forensic copies of drives.
- Analyzing drives for hidden information.
- Analyzing network traffic for criminal activity.
- Shutting down systems to preserve evidence.



Forensic Requirements for Responding to Information Security Incidents

Requirements:

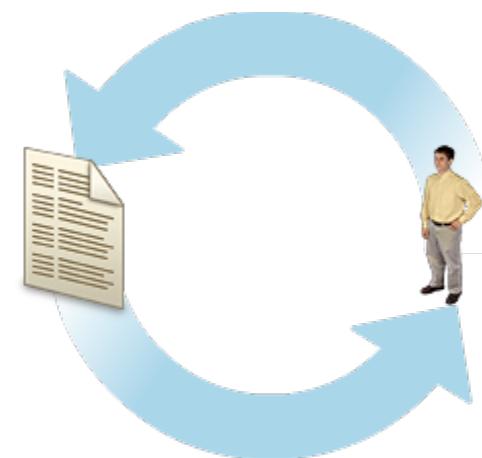
- Admissibility
- Quality
- Completeness of evidence
- Chain of custody



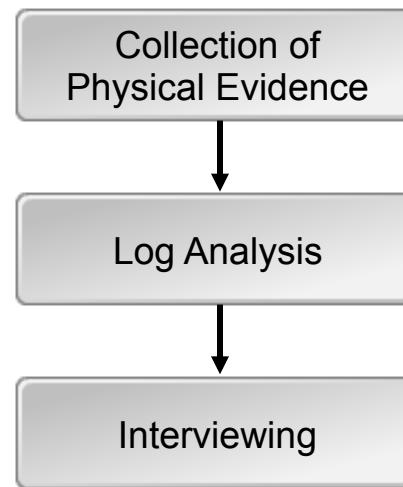
Evidence Life Cycle

Evidence life cycle steps:

1. Discovery and recognition
2. Protection
3. Recording
4. Collection
5. Identification
6. Storage and preservation
7. Transportation
8. Presentation in court
9. Return to victim or owner



Evidence Collection



Evidence Types

Evidence types include:

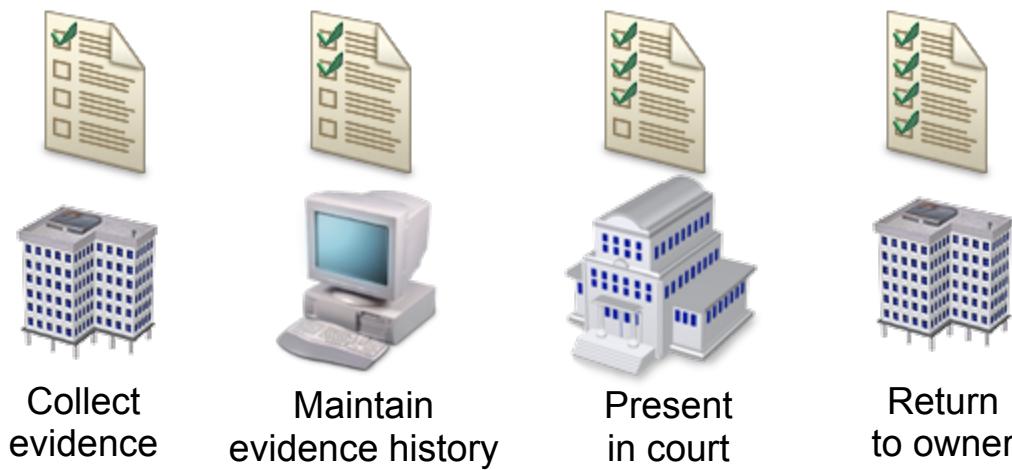
- Best
- Secondary
- Direct
- Conclusive
- Opinion
- Corroborative
- Circumstantial
- Hearsay
- Demonstrative

The Five Common Rules of Evidence

Common rules of evidence are:

- Reliable
- Preserved
- Relevant
- Properly identified
- Legally permissible

Chain of Custody



How to Investigate an Information Security Incident

To investigate an information security incident:

- If an IRP exists, follow the guidelines to respond to the incident.
- If an IRP does not exist, then determine a primary investigator who will lead the investigation process.
- Determine if the events actually occurred and to what extent a system or process was damaged.
- Document the incident.
- Assess the damage and determine the risk priority for all systems.
- Determine if outside expertise is needed, such as a consultant firm.
- Notify local law enforcement, if needed.
- Secure the scene so that the hardware is contained.
- Collect all necessary evidence, which may be electronic data, hardware components, or telephony system components.
- Interview personnel to collect additional information pertaining to the crime.
- Report the investigation findings to the required people.

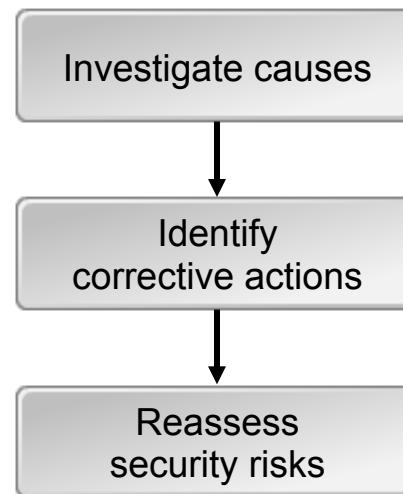
PIR Methods

PIRs:

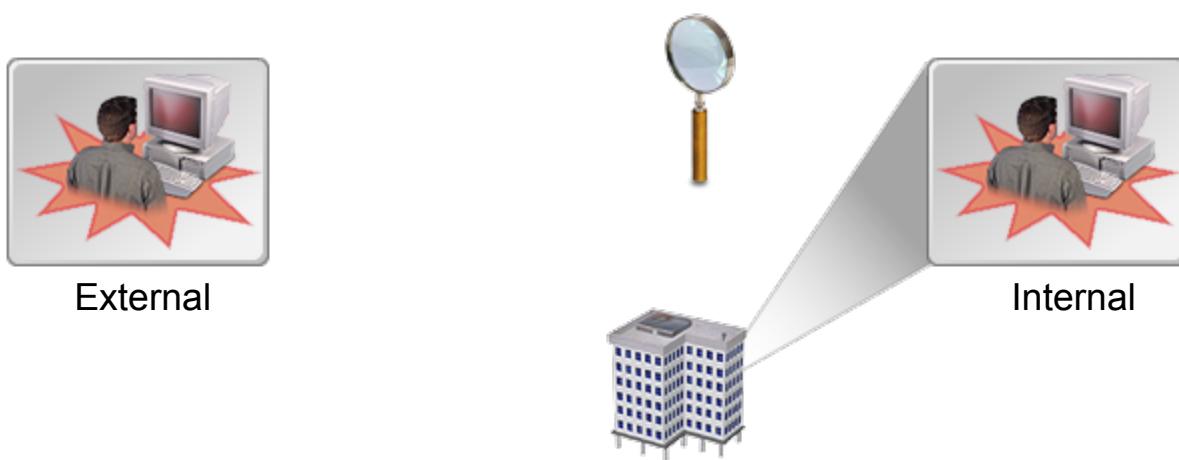
- Identify and correct weaknesses.
- Determine and highlight strengths.
- Should be conducted immediately after an incident.
- Should include questions to evaluate incident response techniques.



The Security Incident Review Process



Investigate Causes of a Security Incident

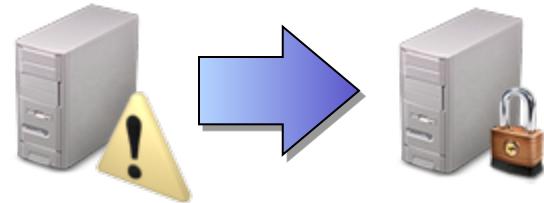


Investigating an incident's cause helps prevent reoccurrence and helps identify the source of the issue

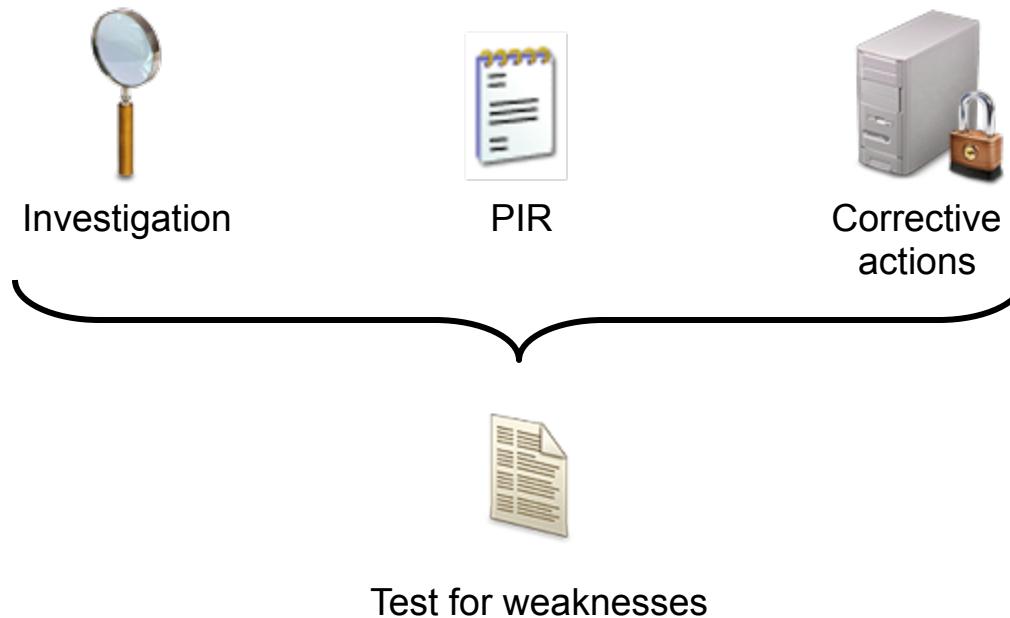
Identify Corrective Actions

Corrective actions include:

- Stronger passwords.
- Firewall rule changes.
- More security awareness workshops.



Reassess Security Risks After a Security Incident



How to Conduct a Post-Incident Review

To conduct a post-incident review:

- 1. Investigate the causes of a security incident.**
 - ❑ Determine the personnel involved with the incident.
 - ❑ Analyze the details of the incident.
 - ❑ Investigate the source of the incident.
 - ❑ Determine when the incident took place.
 - ❑ Determine the motivation for the attack.
 - ❑ Determine weaknesses in the security protocol.
- 2. Determine corrective actions.**
 - ❑ Identify the cause of the security incident.
 - ❑ Review actions and fixes made during the incident response.
 - ❑ Identify remaining weaknesses in the organization's security protocol.
 - ❑ Create recommendations based on the findings.
- 3. Reassess security risks after a security incident.**
 - ❑ Identify the risk.
 - ❑ Determine the risk tolerance.
 - ❑ Analyze the risk.
 - ❑ Evaluate the risk.

Reflective Questions

1. Which techniques of managing and responding to security incidents in this lesson were familiar to you, and which were new?

2. Have you ever had the need to respond to a security incident at your organization? If so, how did you respond? If not, how do you believe you would respond if there ever was a need?