# Principles of Information Security, Fourth Edition

*Chapter 12*

*Information Security Maintenance*

# Introduction

- Organizations should avoid overconfidence after improving their information security profile
- Organizational changes that may occur include:
  - Acquisition of new assets; emergence of new vulnerabilities; business priorities shift; partnerships form or dissolve; organizational divestiture and acquisition; employee hire and turnover
- If program does not adjust, may be necessary to begin cycle again
- More expensive to reengineer information security profile again and again

# Security Management Maintenance Models

- Management model must be adopted to manage and operate ongoing security program
- Models are frameworks that structure tasks of managing particular set of activities or business functions

# NIST SP 800-100 Information Security Handbook: A Guide for Managers

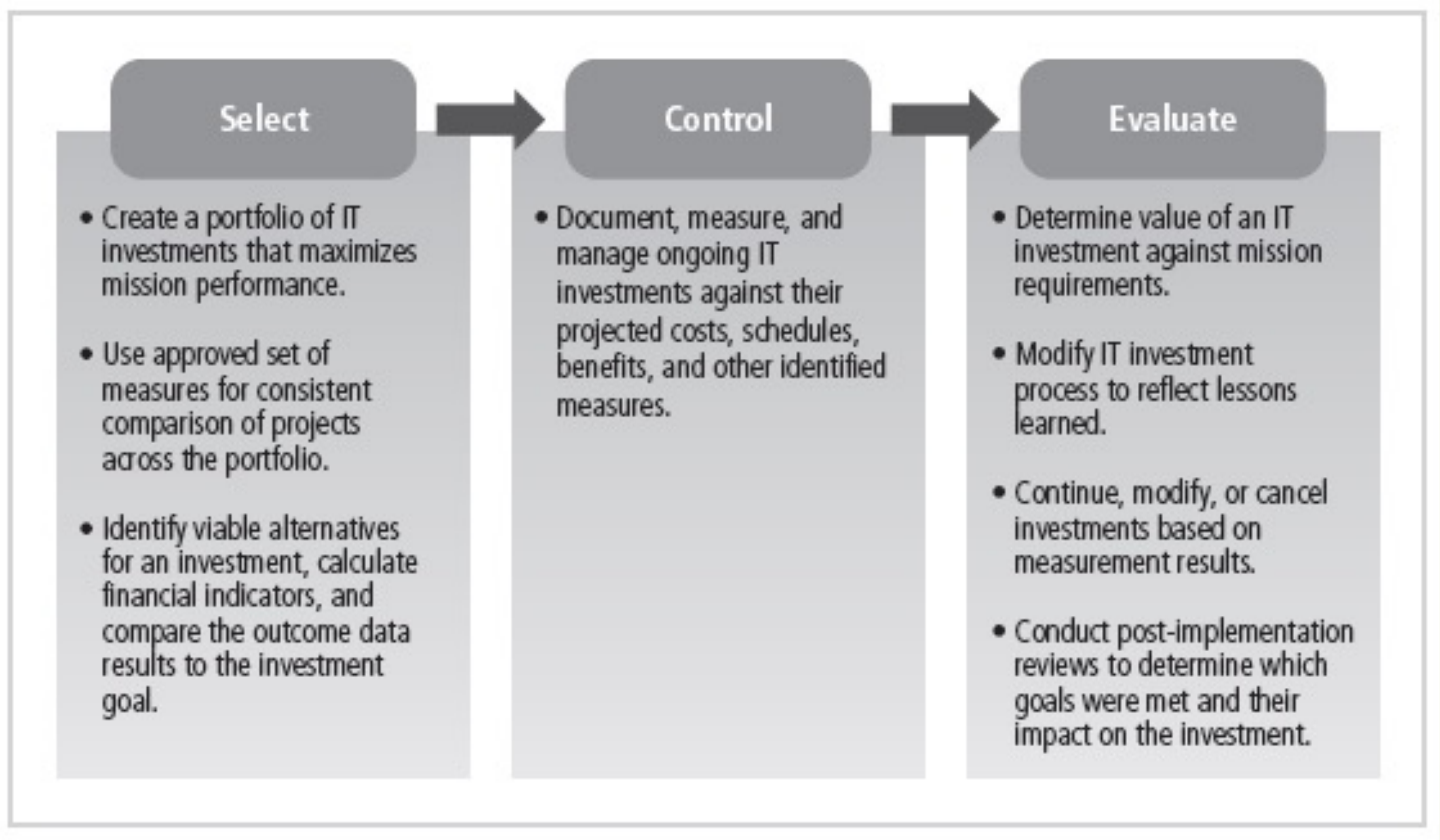
- Provides managerial guidance for establishing and implementing of an information security program
- Thirteen areas of information security management
  - Provide for specific monitoring activities for each task
  - Tasks should be done on an ongoing basis
  - Not all issues are negative

# NIST SP 800-100 Information Security Handbook: A Guide for Managers (cont'd.)

- Information security governance
  - Agencies should monitor the status of their programs to ensure that:
    - Ongoing information security activities provide support to agency mission
    - Current policies and procedures are technology-aligned
    - Controls are accomplishing the intended purpose
- System development life cycle:
  - The overall process of developing, implementing, and retiring information systems through a multistep process

# NIST SP 800-100 Information Security Handbook: A Guide for Managers (cont'd.)

- Awareness and training
  - Tracking system should capture key information on program activities
  - Tracking compliance involves assessing the status of the program
  - The program must continue to evolve
- Capital planning and investment control
  - Designed to facilitate and control the expenditure of agency funds
  - Select-control-evaluate investment life cycle



**Select**

- Create a portfolio of IT investments that maximizes mission performance.
- Use approved set of measures for consistent comparison of projects across the portfolio.
- Identify viable alternatives for an investment, calculate financial indicators, and compare the outcome data results to the investment goal.

**Control**

- Document, measure, and manage ongoing IT investments against their projected costs, schedules, benefits, and other identified measures.

**Evaluate**

- Determine value of an IT investment against mission requirements.
- Modify IT investment process to reflect lessons learned.
- Continue, modify, or cancel investments based on measurement results.
- Conduct post-implementation reviews to determine which goals were met and their impact on the investment.

Figure 12-1 Select-Control-Evaluate Investment Life Cycle

# NIST SP 800-100 Information Security Handbook: A Guide for Managers (cont'd.)

- Interconnecting systems
  - The direct connection of two or more information systems for sharing data and other information resources
  - Can expose the participating organizations to risk
  - When properly managed, the added benefits include greater efficiency, centralized access to data, and greater functionality
- Performance measures
  - Metrics: tools that support decision making
  - Six phase iterative process

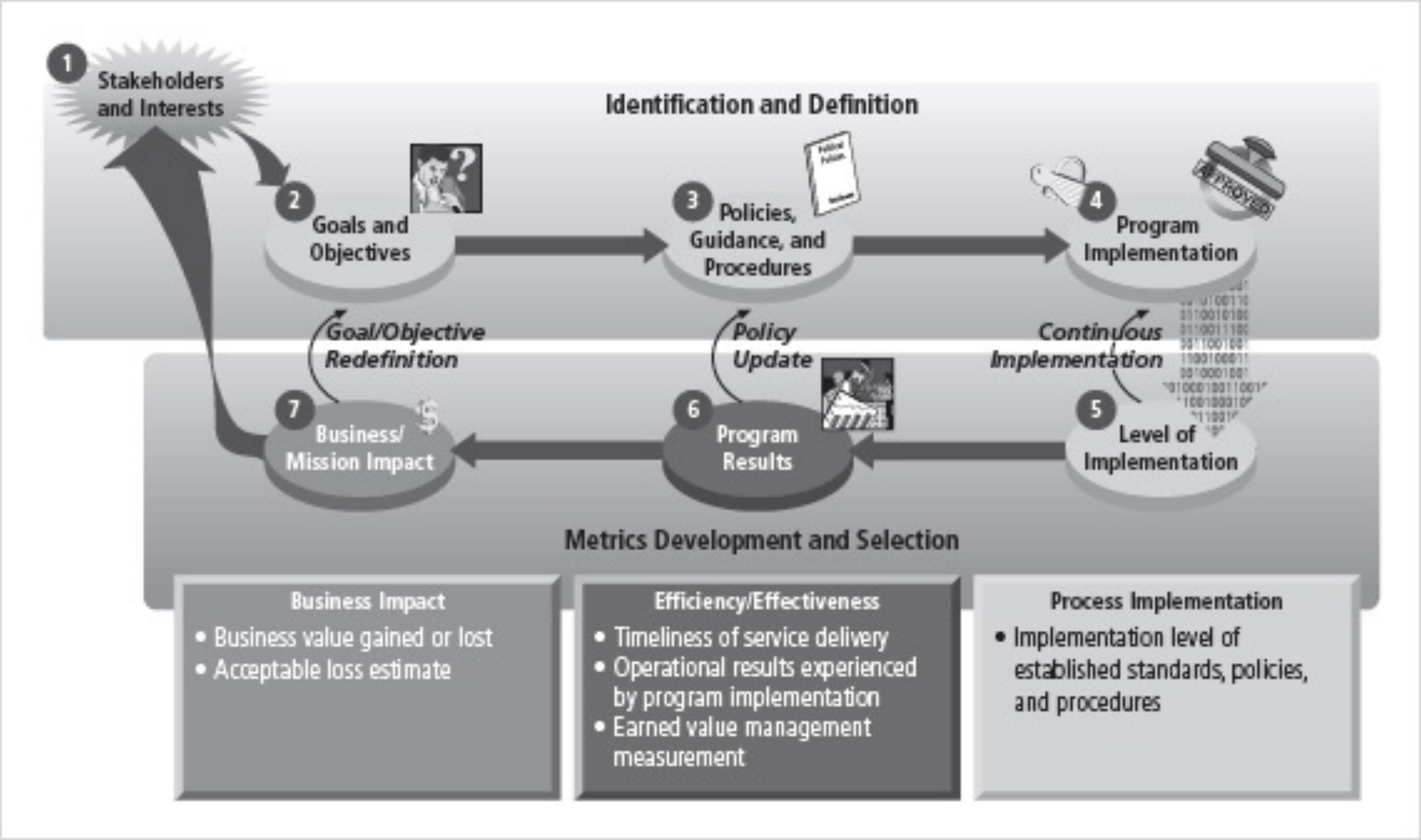

1 Stakeholders and Interests
Identification and Definition
2 Goals and Objectives
3 Policies, Guidance, and Procedures
4 Program Implementation
Goal/Objective Redefinition
Policy Update
Continuous Implementation
7 Business/ Mission Impact
6 Program Results
5 Level of Implementation
Metrics Development and Selection
Business Impact
• Business value gained or lost
• Acceptable loss estimate
Efficiency/Effectiveness
• Timeliness of service delivery
• Operational results experienced by program implementation
• Earned value management measurement
Process Implementation
• Implementation level of established standards, policies, and procedures

Figure 12-3 Information Security Metrics Development Process

# NIST SP 800-100 Information Security Handbook: A Guide for Managers (cont'd.)

- Security planning: one of the most crucial ongoing responsibilities in security management
- Information technology contingency planning: consists of a process for recovery and documentation of procedures
- Risk management
  - Ongoing effort
  - Tasks include performing risk identification, analysis, and management

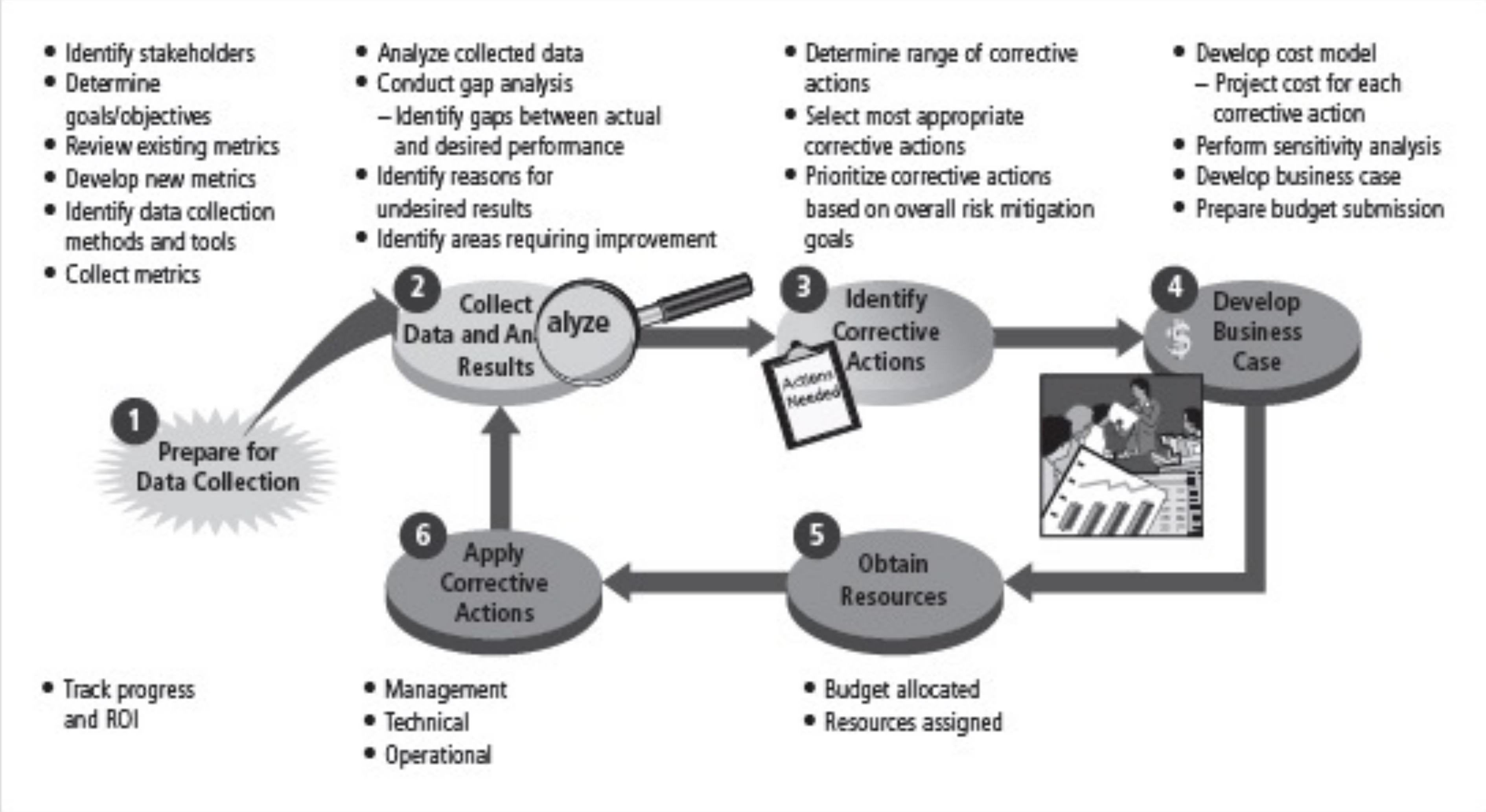
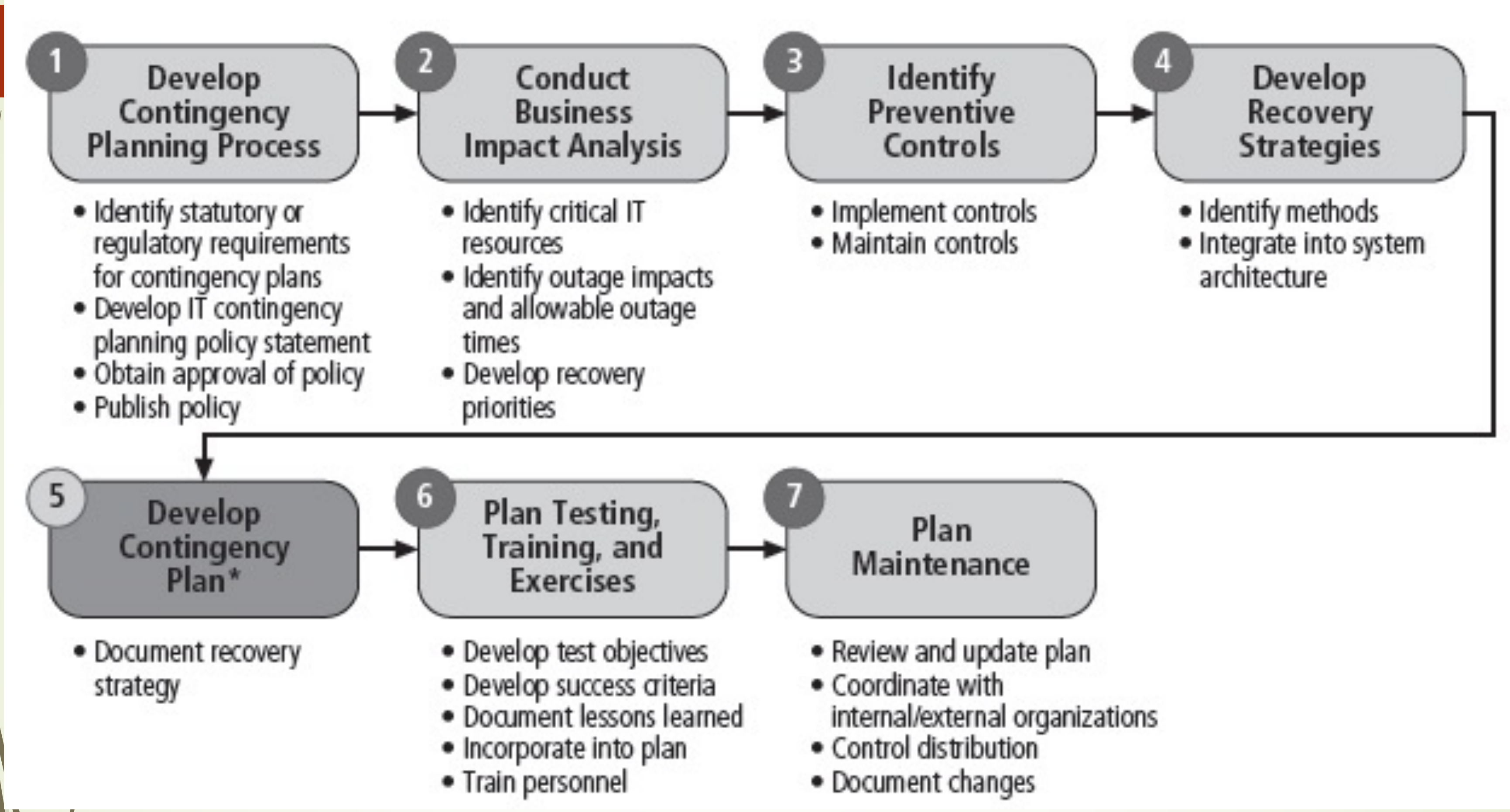

• Identify stakeholders
• Determine goals/objectives
• Review existing metrics
• Develop new metrics
• Identify data collection methods and tools
• Collect metrics
• Analyze collected data
• Conduct gap analysis
– Identify gaps between actual and desired performance
• Identify reasons for undesired results
• Identify areas requiring improvement
• Determine range of corrective actions
• Select most appropriate corrective actions
• Prioritize corrective actions based on overall risk mitigation goals
• Develop cost model
– Project cost for each corrective action
• Perform sensitivity analysis
• Develop business case
• Prepare budget submission
1 Prepare for Data Collection
2 Collect Data and Analyze Results
3 Identify Corrective Actions
Actions Needed
4 Develop Business Case
$
5 Obtain Resources
6 Apply Corrective Actions
• Track progress and ROI
• Management
• Technical
• Operational
• Budget allocated
• Resources assigned

Figure 12-4 Information Security Metrics Program Implementation Process



1 Develop Contingency Planning Process

- Identify statutory or regulatory requirements for contingency plans
- Develop IT contingency planning policy statement
- Obtain approval of policy
- Publish policy

2 Conduct Business Impact Analysis

- Identify critical IT resources
- Identify outage impacts and allowable outage times
- Develop recovery priorities

3 Identify Preventive Controls

- Implement controls
- Maintain controls

4 Develop Recovery Strategies

- Identify methods
- Integrate into system architecture

5 Develop Contingency Plan*

- Document recovery strategy

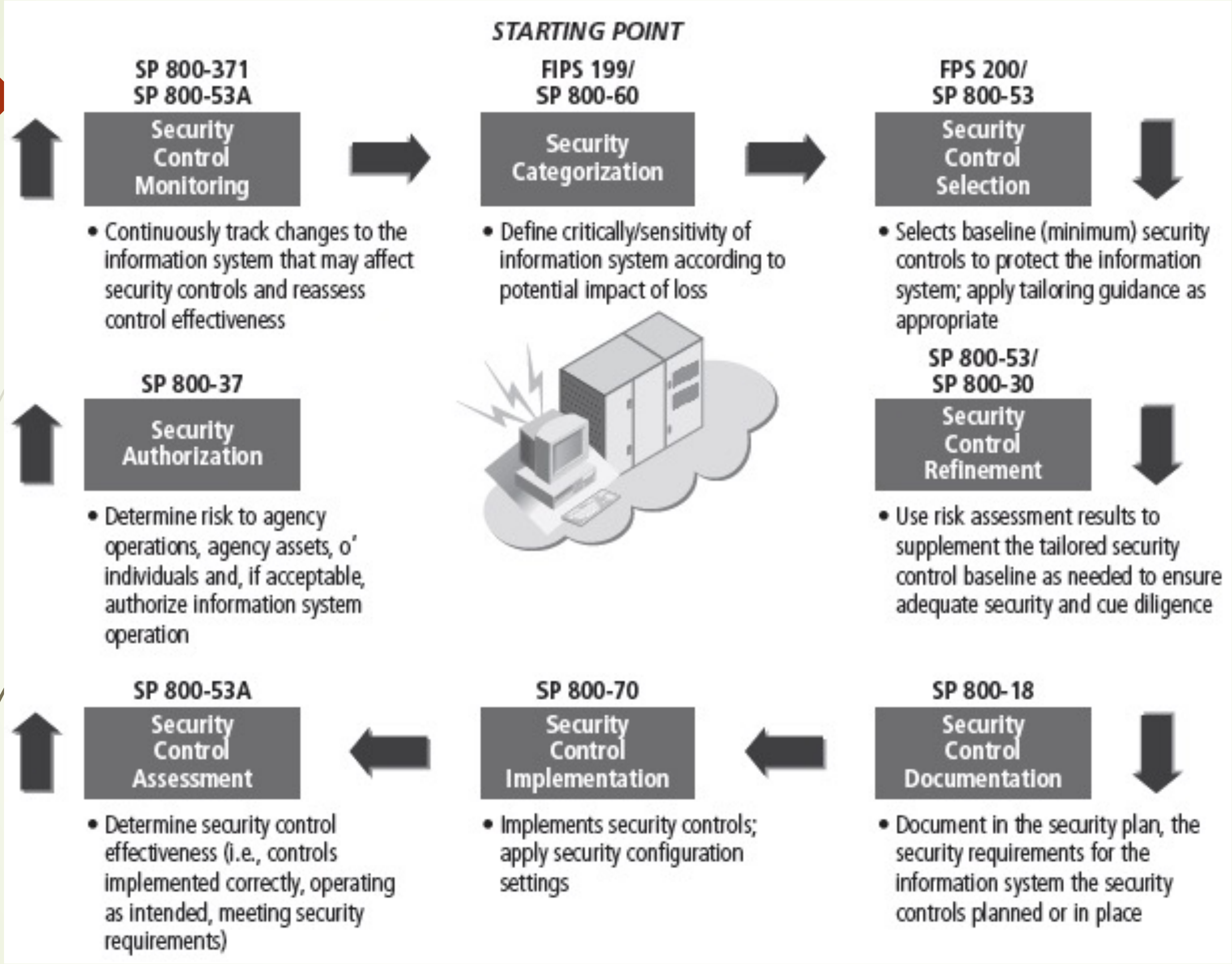
6 Plan Testing, Training, and Exercises

- Develop test objectives
- Develop success criteria
- Document lessons learned
- Incorporate into plan
- Train personnel

7 Plan Maintenance

- Review and update plan
- Coordinate with internal/external organizations
- Control distribution
- Document changes

Figure 12-5 The NIST Seven-Step Contingency Planning Process



*STARTING POINT*

SP 800-371
SP 800-53A
**Security Control Monitoring**

- Continuously track changes to the information system that may affect security controls and reassess control effectiveness

FIPS 199/
SP 800-60
**Security Categorization**

- Define critically/sensitivity of information system according to potential impact of loss

FPS 200/
SP 800-53
**Security Control Selection**

- Selects baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

SP 800-37
**Security Authorization**

- Determine risk to agency operations, agency assets, o' individuals and, if acceptable, authorize information system operation

SP 800-53/
SP 800-30
**Security Control Refinement**

- Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and cue diligence

SP 800-53A
**Security Control Assessment**

- Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-70
**Security Control Implementation**

- Implements security controls; apply security configuration settings

SP 800-18
**Security Control Documentation**

- Document in the security plan, the security requirements for the information system the security controls planned or in place

Figure 12-6 Risk Management in the System Security Life Cycle

# NIST SP 800-100 Information Security Handbook: A Guide for Managers (cont'd.)

- Certification, accreditation, and security assessments
  - An essential component in any security program
  - The status of security controls is checked regularly
  - Auditing: the process of reviewing the use of a system for misuse or malfeasance
- Security services and products acquisition
- Incident response: incident response life cycle
- Configuration (or change) management: manages the effects of changes in configurations

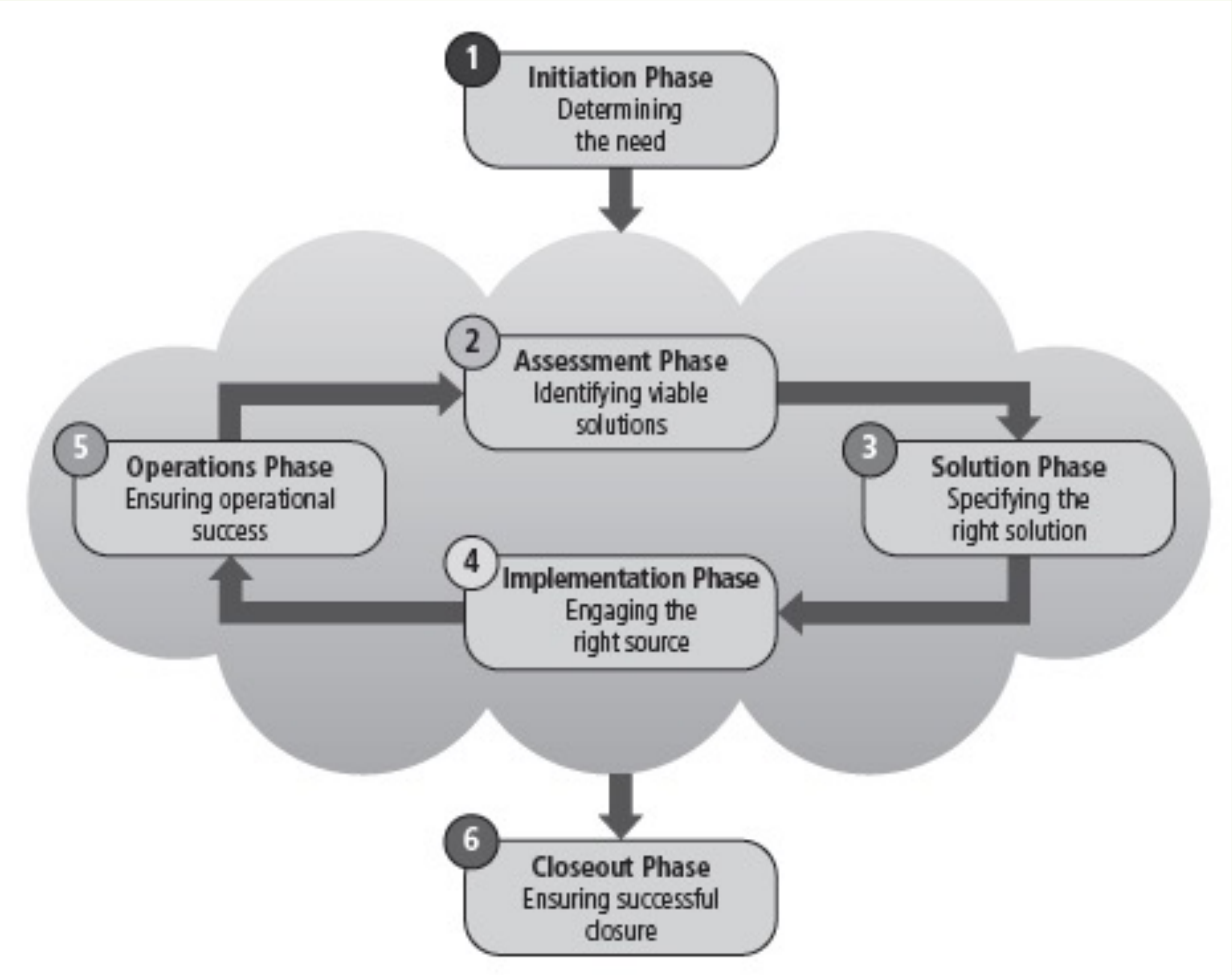

1
Initiation Phase
Determining the need
2
Assessment Phase
Identifying viable solutions
3
Solution Phase
Specifying the right solution
4
Implementation Phase
Engaging the right source
5
Operations Phase
Ensuring operational success
6
Closeout Phase
Ensuring successful closure

Figure 12-7 The Information Security Services Life Cycle

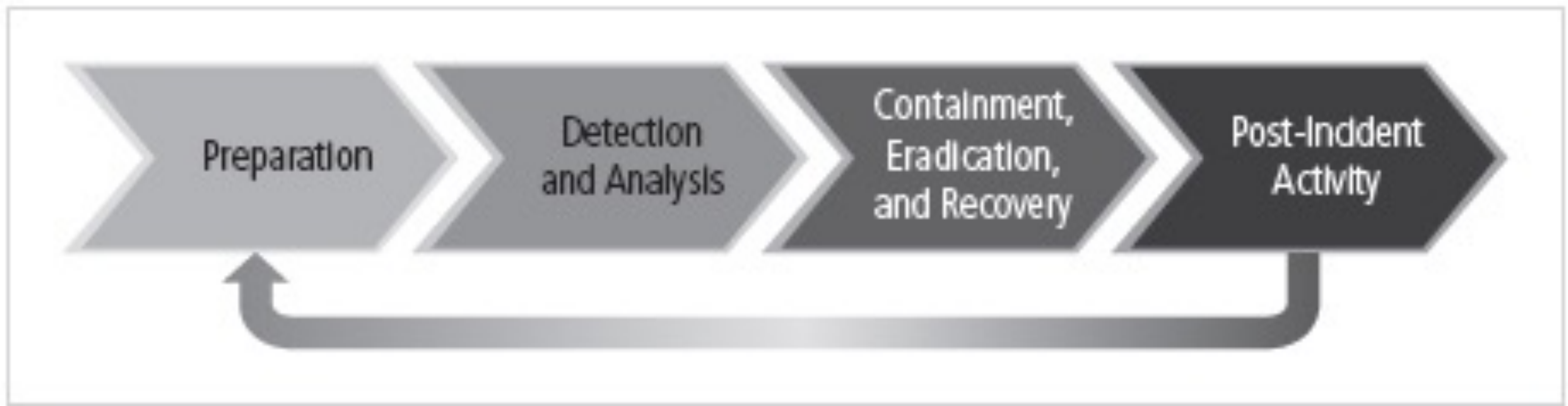


Figure 12-8 The Incident Response Life Cycle

# The Security Maintenance Model

- Designed to focus organizational effort on maintaining systems
- Recommended maintenance model based on five subject areas:
  - External monitoring
  - Internal monitoring
  - Planning and risk assessment
  - Vulnerability assessment and remediation
  - Readiness and review

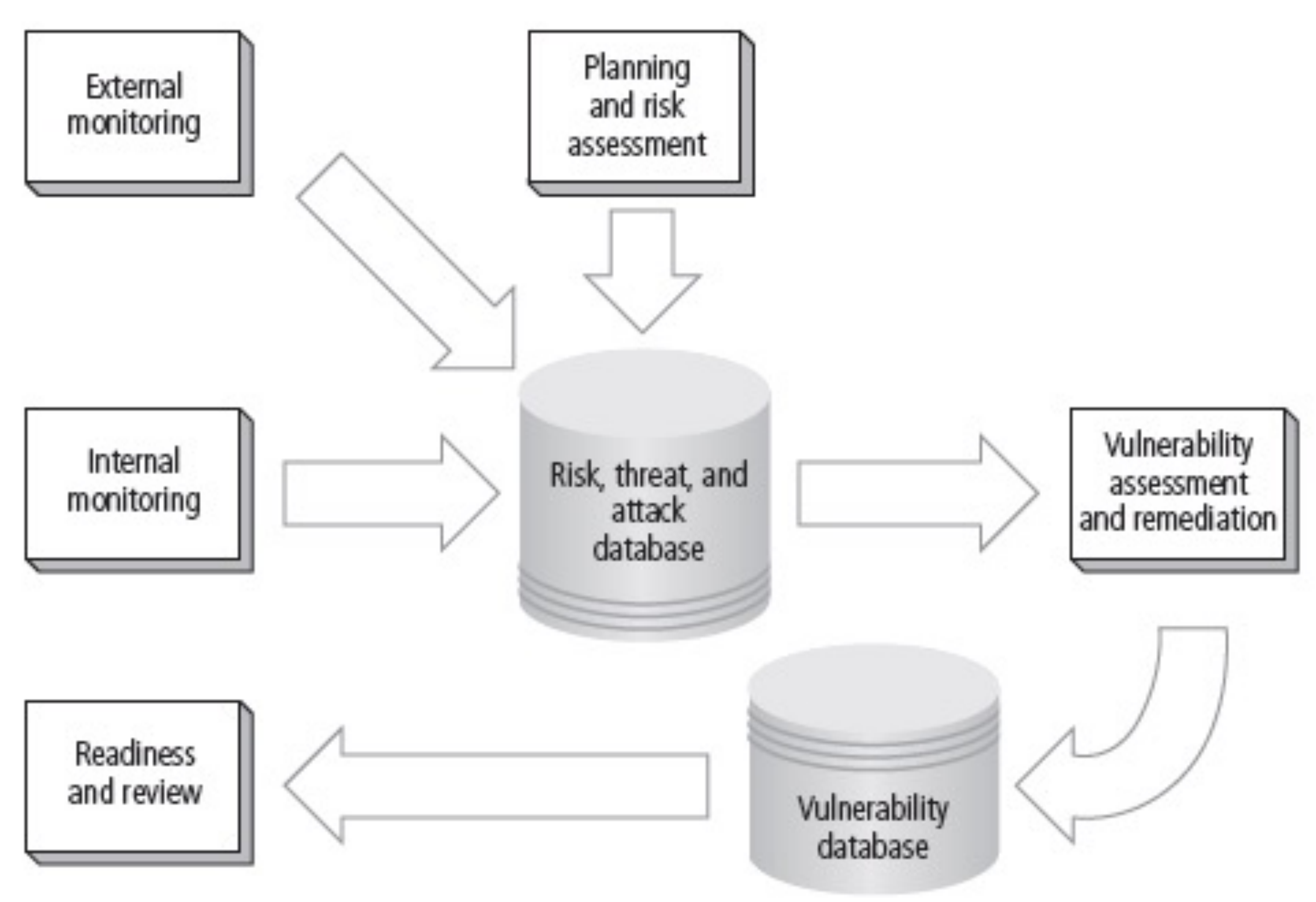

External monitoring
Planning and risk assessment
Internal monitoring
Risk, threat, and attack database
Vulnerability assessment and remediation
Readiness and review
Vulnerability database

Figure 12-10 The Maintenance Model

# Monitoring the External Environment

- Objective to provide early awareness of new threats, threat agents, vulnerabilities, and attacks that is needed to mount an effective defense
- Entails collecting intelligence from data sources and giving that intelligence context and meaning for use by organizational decision makers

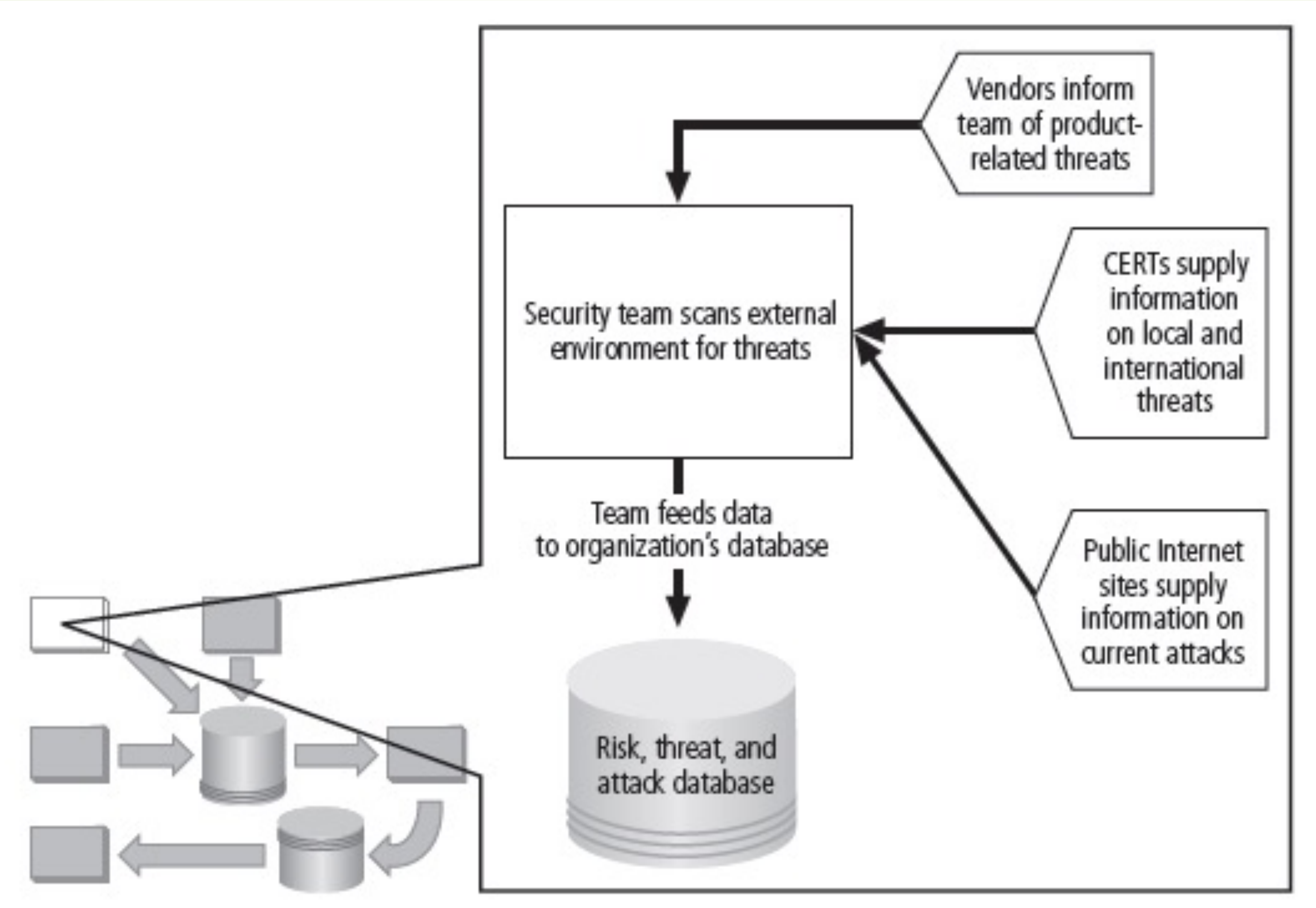

Vendors inform team of product-related threats
Security team scans external environment for threats
CERTs supply information on local and international threats
Public Internet sites supply information on current attacks
Team feeds data to organization's database
Risk, threat, and attack database

Figure 12-11 External Monitoring

# Monitoring the External Environment (cont'd.)

- Data sources
  - Acquiring threat and vulnerability data is not difficult
  - Turning data into information decision makers can use is the challenge
  - External intelligence comes from three classes of sources: vendors, computer emergency response teams (CERTs), public network sources
  - Regardless of where or how external monitoring data is collected, must be analyzed in context of organization's security environment to be useful

# Monitoring the External Environment (cont'd.)

- Monitoring, escalation, and incident response
  - Function of external monitoring process is to monitor activity, report results, and escalate warnings
  - Monitoring process has three primary deliverables:
    - Specific warning bulletins issued when developing threats and specific attacks pose measurable risk to organization
    - Periodic summaries of external information
    - Detailed intelligence on highest risk warnings

# Monitoring the External Environment (cont'd.)

- Data collection and management
  - Over time, external monitoring processes should capture knowledge about external environment in appropriate formats
  - External monitoring collects raw intelligence, filters for relevance, assigns a relative risk impact, and communicates to decision makers in time to make a difference

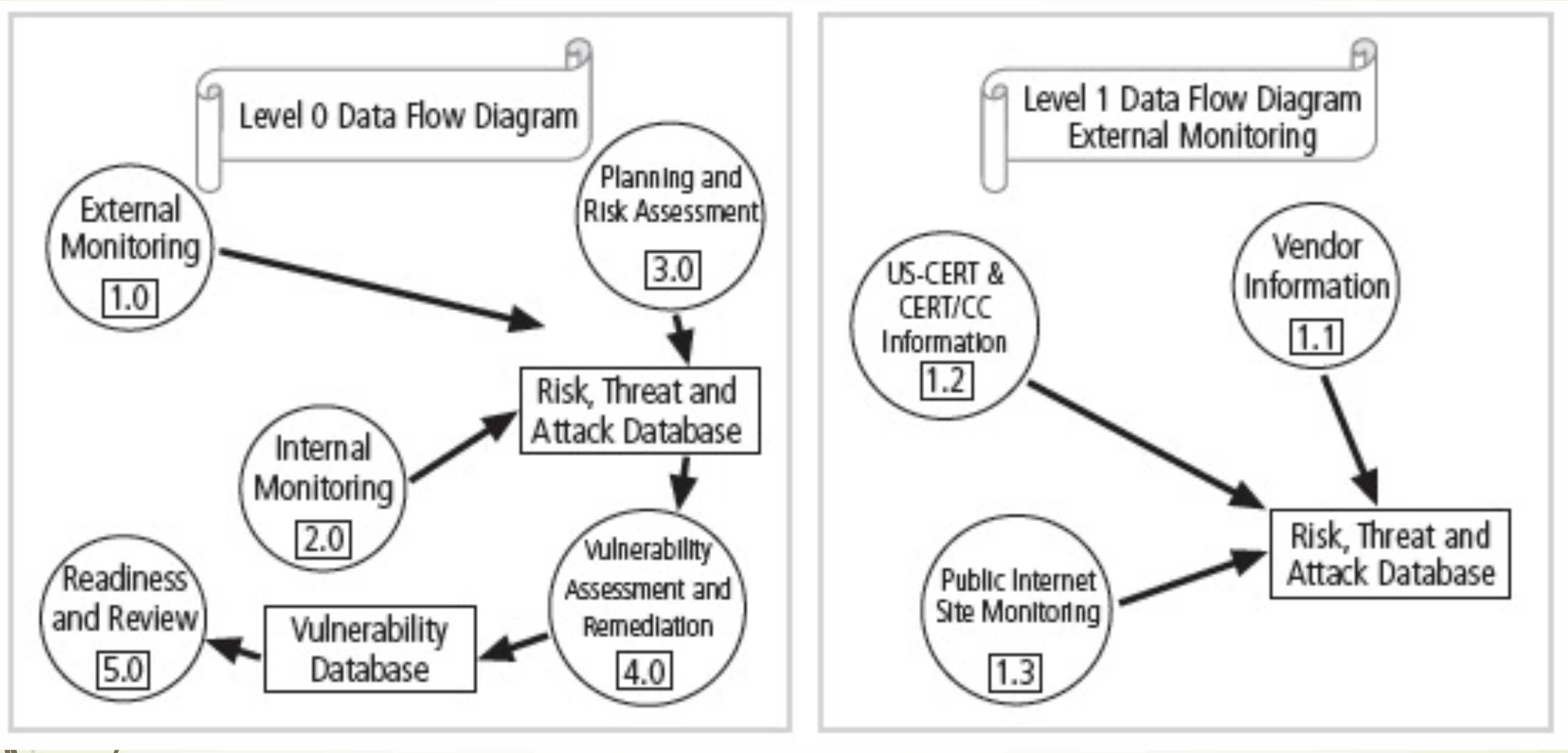

Level 0 Data Flow Diagram
External Monitoring
1.0
Planning and Risk Assessment
3.0
Risk, Threat and Attack Database
Internal Monitoring
2.0
Vulnerability Assessment and Remediation
4.0
Readiness and Review
5.0
Vulnerability Database
Level 1 Data Flow Diagram External Monitoring
US-CERT & CERT/CC Information
1.2
Vendor Information
1.1
Risk, Threat and Attack Database
Public Internet Site Monitoring
1.3

Figure 12-12 Data Flow Diagrams for External Data Collection

# Monitoring the Internal Environment

- Maintain informed awareness of state of organization’s networks, systems, and security defenses
- Internal monitoring accomplished by:
  - Doing inventory of network devices and channels, IT infrastructure and applications, and information security infrastructure elements
  - Leading the IT governance process
  - Real-time monitoring of IT activity
  - Monitoring the internal state of the organization’s networks and systems

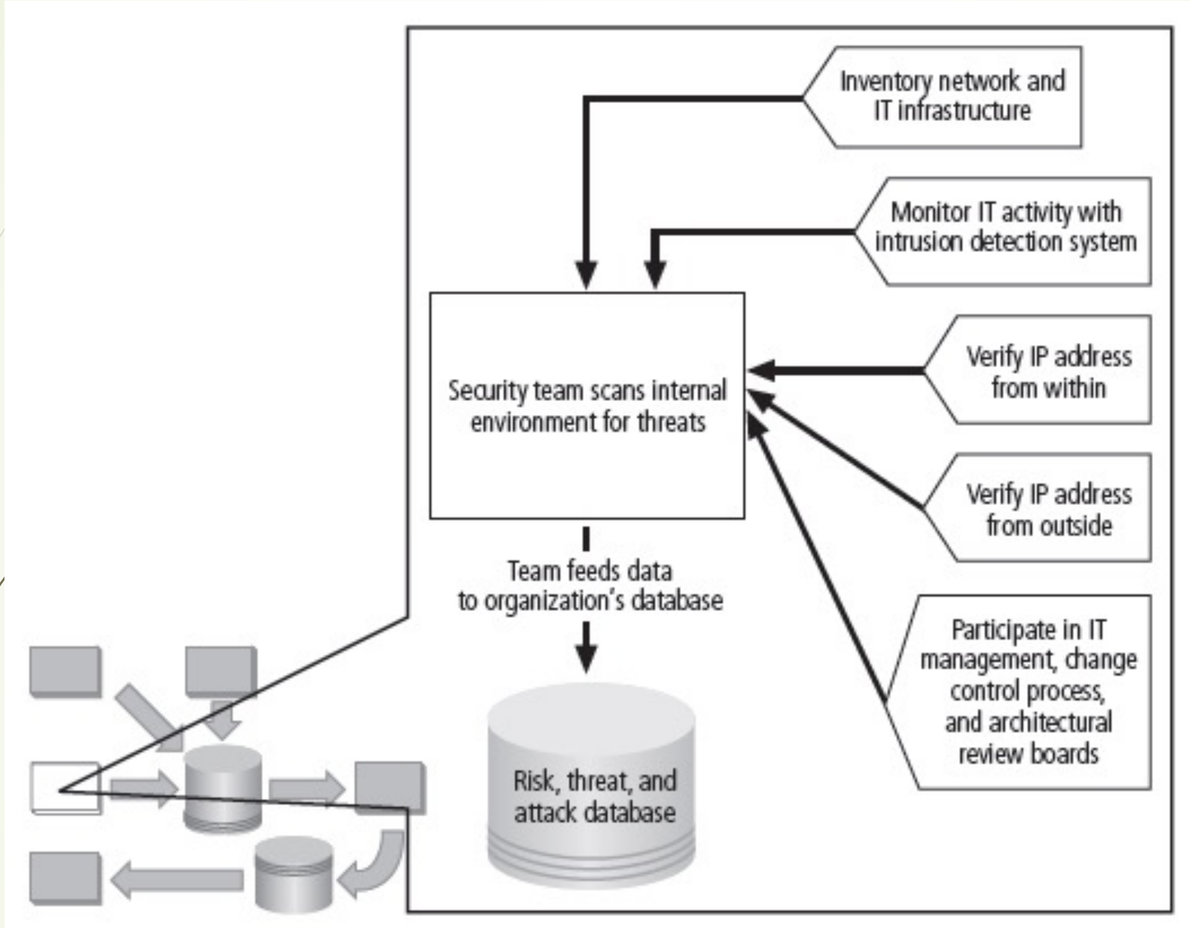

Inventory network and IT infrastructure
Monitor IT activity with intrusion detection system
Security team scans internal environment for threats
Verify IP address from within
Verify IP address from outside
Participate in IT management, change control process, and architectural review boards
Team feeds data to organization's database
Risk, threat, and attack database

Figure 12-13 Internal Monitoring

# Monitoring the Internal Environment (cont'd.)

- Network characterization and inventory
  - Organizations should have carefully planned and fully populated inventory for network devices, communication channels, and computing devices
  - Once characteristics identified, they must be carefully organized and stored using a mechanism (manual or automated) that allows timely retrieval and rapid integration of disparate facts

# Monitoring the Internal Environment (cont'd.)

- Making intrusion detection and prevention systems work
  - The most important value of raw intelligence provided by the IDS is providing indicators of current or imminent vulnerabilities
  - Log files from IDS engines can be mined for information
  - Another IDS monitoring element is traffic analysis
  - Analyzing attack signatures for unsuccessful system attacks can identify weaknesses in various security efforts

# Monitoring the Internal Environment (cont'd.)

- Detecting differences
  - Difference analysis: procedure that compares current state of network segment against known previous state of same segment
  - Differences between the current state and the baseline state that are unexpected could be a sign of trouble and need investigation

# Planning and Risk Assessment

- Primary objective is to keep lookout over entire information security program
- Accomplished by identifying and planning ongoing information security activities that further reduce risk

# Planning and Risk Assessment (cont'd.)

- Primary objectives
  - Establishing a formal information security program review
  - Instituting formal project identification, selection, planning, and management processes
  - Coordinating with IT project teams to introduce risk assessment and review for all IT projects
  - Integrating a mindset of risk assessment across organization

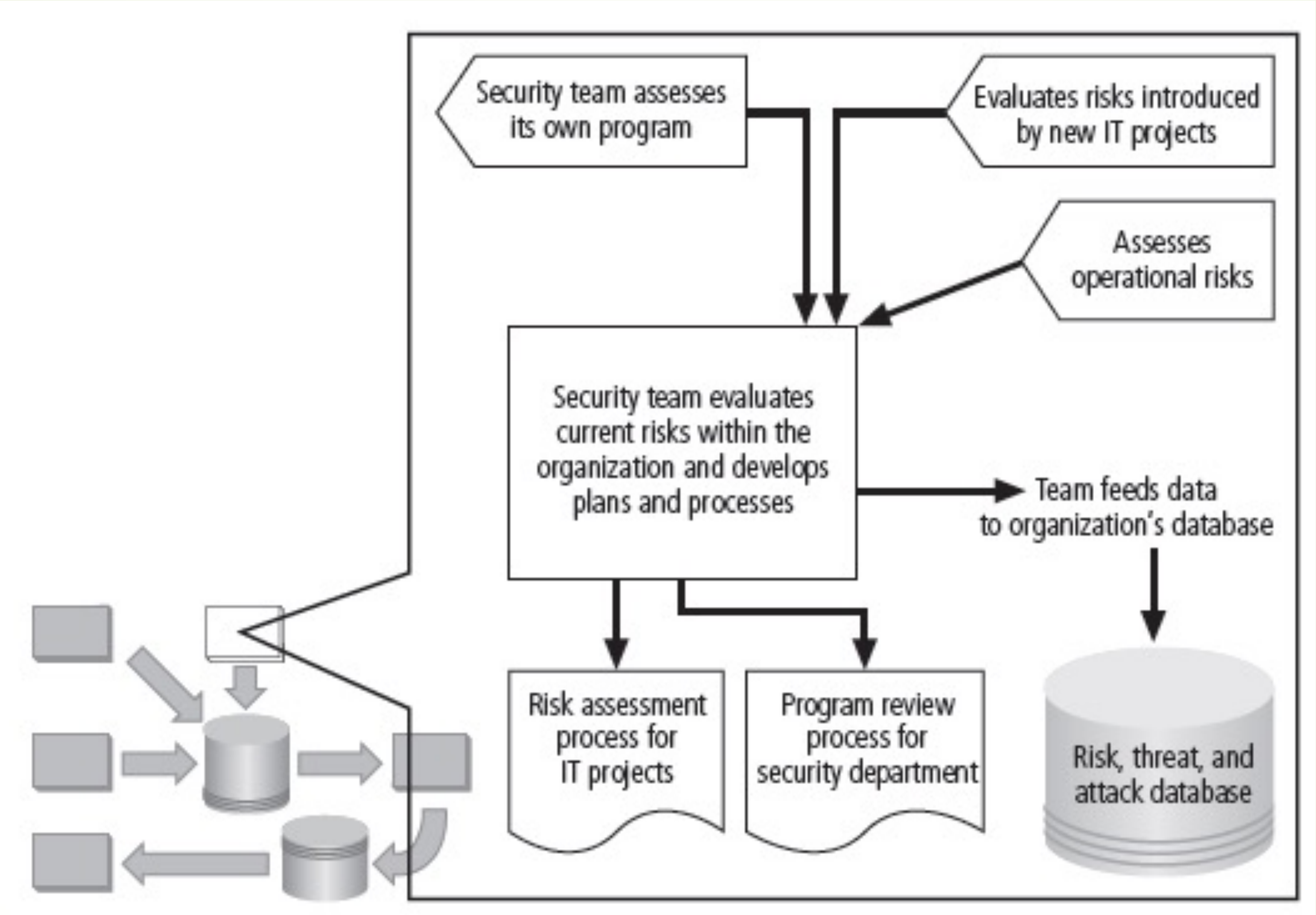

Security team assesses its own program
Evaluates risks introduced by new IT projects
Assesses operational risks
Security team evaluates current risks within the organization and develops plans and processes
Team feeds data to organization's database
Risk assessment process for IT projects
Program review process for security department
Risk, threat, and attack database

Figure 12-14 Planning and Risk Assessment

# Planning and Risk Assessment (cont'd.)

- Information security program planning and review
  - Periodic review of ongoing information security program coupled with planning for enhancements and extensions is recommended
  - Should examine IT needs of future organization and impact those needs have on information security
  - A recommended approach takes advantage of the fact most organizations have annual capital budget planning cycles and manage security projects as part of that process

# Planning and Risk Assessment (cont'd.)

- Large projects should be broken into smaller projects for several reasons
  - Smaller projects tend to have more manageable impacts on networks and users
  - Larger projects tend to complicate change control process in implementation phase
  - Shorter planning, development, and implementation schedules reduce uncertainty
  - Most large projects can easily be broken down into smaller projects, giving more opportunities to change direction and gain flexibility

# Planning and Risk Assessment (cont'd.)

- Security risk assessments
  - A key component for driving security program change is information security operational risk assessment (RA)
  - RA identifies and documents risk that project, process, or action introduces to organization and offers suggestions for controls
  - Information security group coordinates preparation of many types of RA documents

# Vulnerability Assessment and Remediation

- Primary goal: identification of specific, documented vulnerabilities and their timely remediation
- Accomplished by:
  - Using vulnerability assessment procedures
  - Documenting background information and providing tested remediation procedures for vulnerabilities
  - Tracking vulnerabilities from when they are identified
  - Communicating vulnerability information to owners of vulnerable systems
  - Reporting on the status of vulnerabilities
  - Ensuring the proper level of management is involved

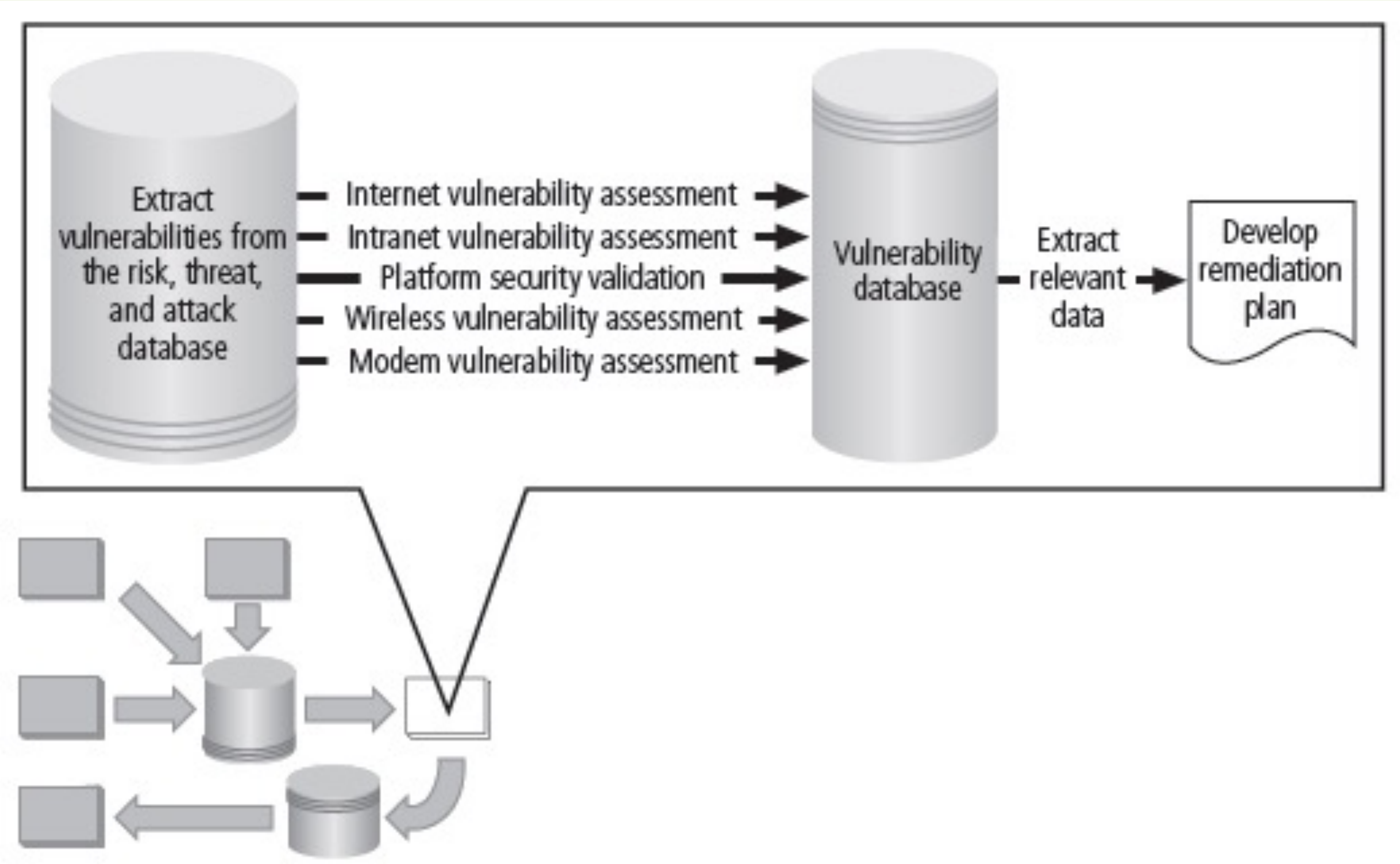

Extract vulnerabilities from the risk, threat, and attack database
Internet vulnerability assessment
Intranet vulnerability assessment
Platform security validation
Wireless vulnerability assessment
Modem vulnerability assessment
Vulnerability database
Extract relevant data
Develop remediation plan

Figure 12-15 Vulnerability Assessment and Remediation

# Vulnerability Assessment and Remediation (cont'd.)

- Process of identifying and documenting specific and provable flaws in organization's information asset environment
- Five vulnerability assessment processes that follow can serve many organizations as they attempt to balance intrusiveness of vulnerability assessment with need for stable and productive production environment

# Vulnerability Assessment and Remediation (cont’d.)

- Penetration testing
  - A level beyond vulnerability testing
  - Is a set of security tests and evaluations that simulate attacks by a malicious external source (hacker)
  - Penetration test (pen test): usually performed periodically as part of a full security audit
  - Can be conducted one of two ways: black box or white box

# Vulnerability Assessment and Remediation (cont'd.)

- Internet vulnerability assessment
  - Designed to find and document vulnerabilities present in organization's public-facing network
  - Steps in the process include:
    - Planning, scheduling, and notification
    - Target selection
    - Test selection
    - Scanning
    - Analysis
    - Record keeping

# Vulnerability Assessment and Remediation (cont'd.)

- Intranet vulnerability assessment
  - Designed to find and document selected vulnerabilities present on the internal network
  - Attackers are often internal members of organization, affiliates of business partners, or automated attack vectors (such as viruses and worms)
  - This assessment is usually performed against selected critical internal devices with a known, high value by using selective penetration testing
  - Steps in process almost identical to steps in Internet vulnerability assessment

# Vulnerability Assessment and Remediation (cont'd.)

- Platform security validation
  - Designed to find and document vulnerabilities that may be present because of misconfigured systems in use within organization
  - These misconfigured systems fail to comply with company policy or standards
  - Fortunately, automated measurement systems are available to help with the intensive process of validating compliance of platform configuration with policy

# Vulnerability Assessment and Remediation (cont'd.)

- Wireless vulnerability assessment
  - Designed to find and document vulnerabilities that may be present in wireless local area networks of organization
  - Since attackers from this direction are likely to take advantage of any loophole or flaw, assessment is usually performed against all publicly accessible areas using every possible wireless penetration testing approach

# Vulnerability Assessment and Remediation (cont'd.)

- Modem vulnerability assessment
  - Designed to find and document any vulnerability present on dial-up modems connected to organization's networks
  - Since attackers from this direction take advantage of any loophole or flaw, assessment is usually performed against all telephone numbers owned by the organization
  - One element of this process, often called war dialing, uses scripted dialing attacks against pool of phone numbers

# Vulnerability Assessment and Remediation (cont'd.)

- Documenting vulnerabilities
  - Vulnerability tracking database should provide details as well as a link to the information assets
  - Low-cost and ease of use makes relational databases a realistic choice
  - Vulnerability database is an essential part of effective remediation

# Vulnerability Assessment and Remediation (cont'd.)

- Remediating vulnerabilities
  - Objective is to repair flaw causing a vulnerability instance or remove risk associated with vulnerability
  - As last resort, informed decision makers with proper authority can accept risk
  - Important to recognize that building relationships with those who control information assets is key to success
  - Success depends on organization adopting team approach to remediation, in place of cross-organizational push and pull

# Vulnerability Assessment and Remediation (cont’d.)

- Acceptance or transference of risk
  - In some instances, risk must simply be acknowledged as part of organization’s business process
  - Management must be assured that decisions made to assume risk the organization are made by properly informed decision makers
  - Information security must make sure the right people make risk assumption decisions with complete knowledge of the impact of the decision

# Vulnerability Assessment and Remediation (cont'd.)

- Threat removal
  - In some circumstances, threats can be removed without repairing vulnerability
  - Vulnerability can no longer be exploited, and risk has been removed
  - Other vulnerabilities may be amenable to other controls that do not allow an expensive repair and still remove risk from situation

# Vulnerability Assessment and Remediation (cont'd.)

- Vulnerability repair
  - Optimum solution in most cases is to repair vulnerability
  - Applying patch software or implementing a workaround often accomplishes this
  - In some cases, simply disabling the service removes vulnerability; in other cases, simple remedies are possible
  - Most common repair is application of a software patch

# Readiness and Review

- Primary goal is to keep information security program functioning as designed and continuously improving
- Accomplished by:
  - Policy review
  - Program review
  - Rehearsals

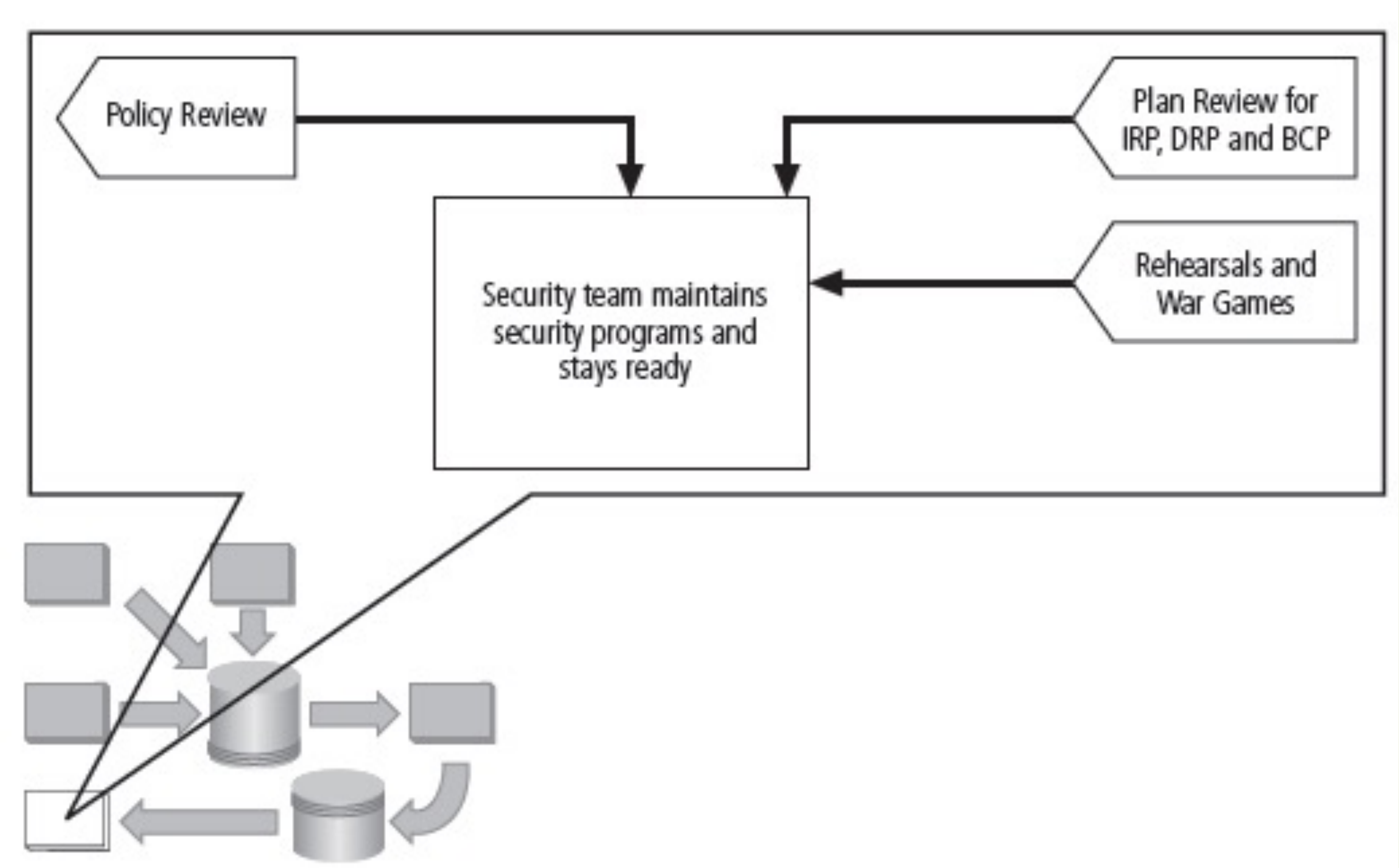

Policy Review
Plan Review for IRP, DRP and BCP
Security team maintains security programs and stays ready
Rehearsals and War Games

Figure 12-16 Readiness and Review

# Digital Forensics

- Used to investigate what happened during attack on assets and how attack occurred
- Based on the field of traditional forensics
- Involves preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
- Evidentiary material (EM): any information that could potentially support organizations legal or policy-based case against suspect

# Digital Forensics (cont’d.)

- Used for two key purposes:
  - To investigate allegations of digital malfeasance
  - To perform root cause analysis
- Organization chooses one of two approaches:
  - Protect and forget (patch and proceed): defense of data and systems that house, use, and transmit it
  - Apprehend and prosecute (pursue and prosecute): identification and apprehension of responsible individuals, with additional attention on collection and preservation of potential EM that might support administrative or criminal prosecution

# The Digital Forensics Team

- Most organizations
  - Cannot sustain a permanent digital forensics team
  - Collect data and outsource analysis
- Information security group personnel should be trained to understand and manage the forensics process to avoid contamination of potential EM
- Expertise can be obtained by training

# Affidavits and Search Warrants

- Affidavit
  - Sworn testimony that certain facts are in the possession of the investigating officer that they feel warrant the examination of specific items located at a specific place
  - The facts, the items, and the place must be specified
- When an approving authority signs the affidavit, it becomes a search warrant, giving permission to:
  - Search the EM at the specified location
  - Seize items to return to the investigator for examination

# Digital Forensics Methodology

- All investigations follow the same basic methodology
  - Identify relevant items of evidentiary value (EM)
  - Acquire (seize) the evidence without alteration or damage
  - Take steps to assure that the evidence is at every step verifiably authentic and is unchanged from the time it was seized
  - Analyze the data without risking modification or unauthorized access
  - Report the findings to the proper authority

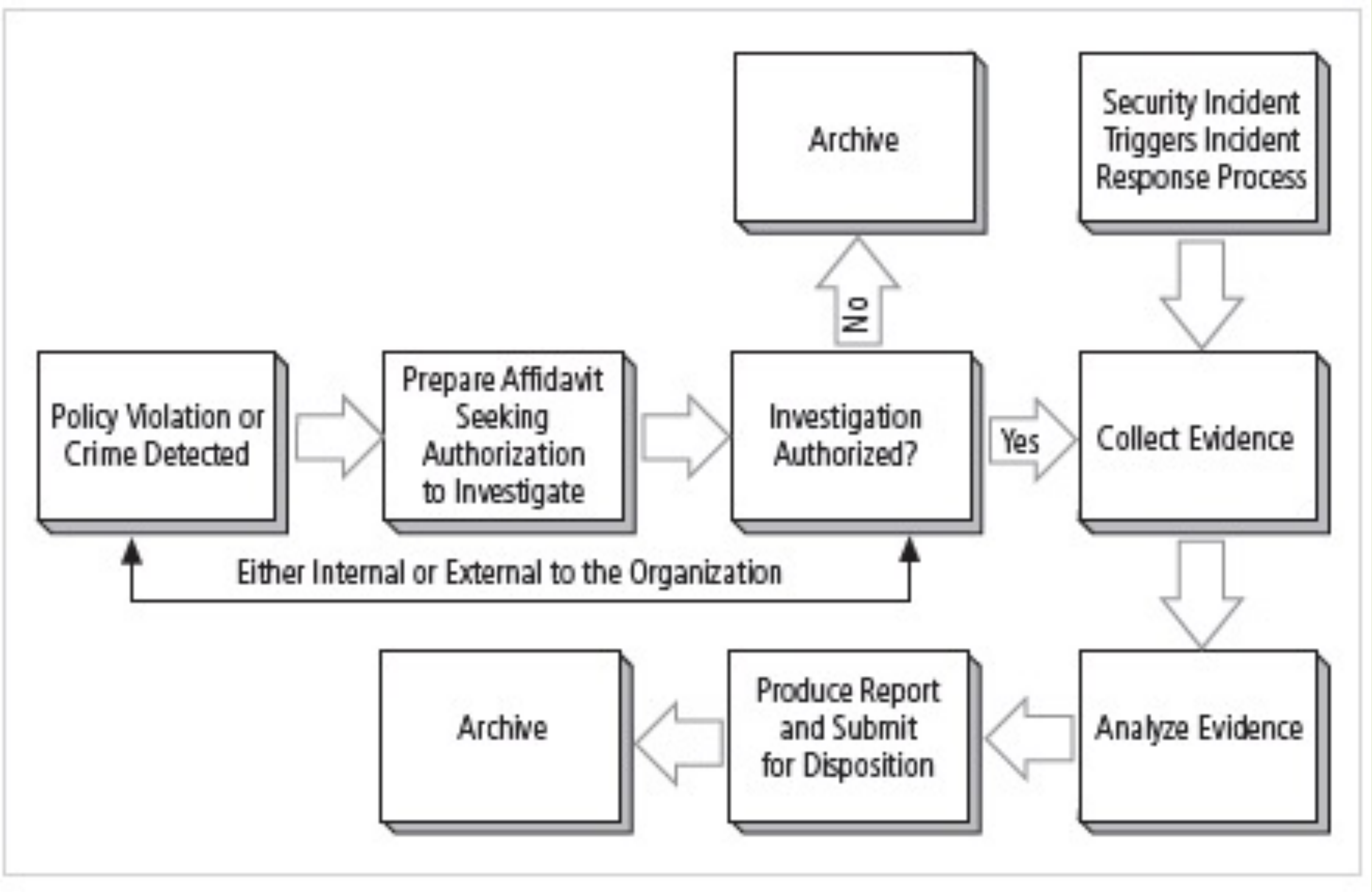

Archive
Security Incident Triggers Incident Response Process
No
Policy Violation or Crime Detected
Prepare Affidavit Seeking Authorization to Investigate
Investigation Authorized?
Yes
Collect Evidence
Either Internal or External to the Organization
Archive
Produce Report and Submit for Disposition
Analyze Evidence

Figure 12-17 The Digital Forensics Process

# Evidentiary Procedures

- Strong procedures for the handling of potential evidentiary material can minimize the probability of an organization's losing a legal challenge
- Organizations should develop specific procedures with guidance, for example:
  - Who may conduct an investigation and who is authorized in an investigation
  - What affidavit- and search warrant-related issues are required
  - The methodology to be followed
  - The final report format