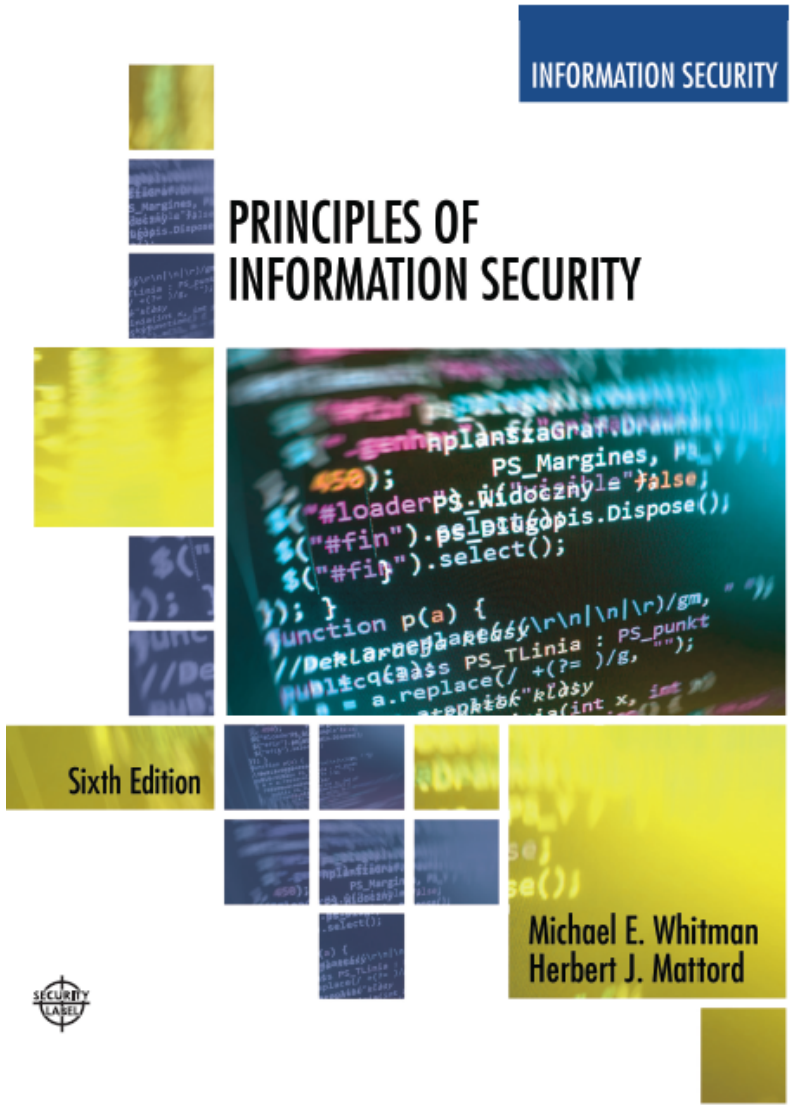


Source: Principles of Information Security

Chapter 12

Information Security Maintenance

Dr. Ibrahim Waziri Jr.

Learning Objectives

Upon completion of this material, you should be able to:

- Discuss the need for ongoing maintenance of the information security program
- List the recommended security management models
- Define a model for a full maintenance program
- Identify the key factors involved in monitoring the external and internal environment
- Describe how planning, risk assessment, vulnerability assessment, and remediation tie into information security maintenance
- Explain how to build readiness and review procedures into information security maintenance
- Discuss digital forensics and describe how to manage it
- Describe the process of acquiring, analyzing, and maintaining potential evidentiary material

Introduction

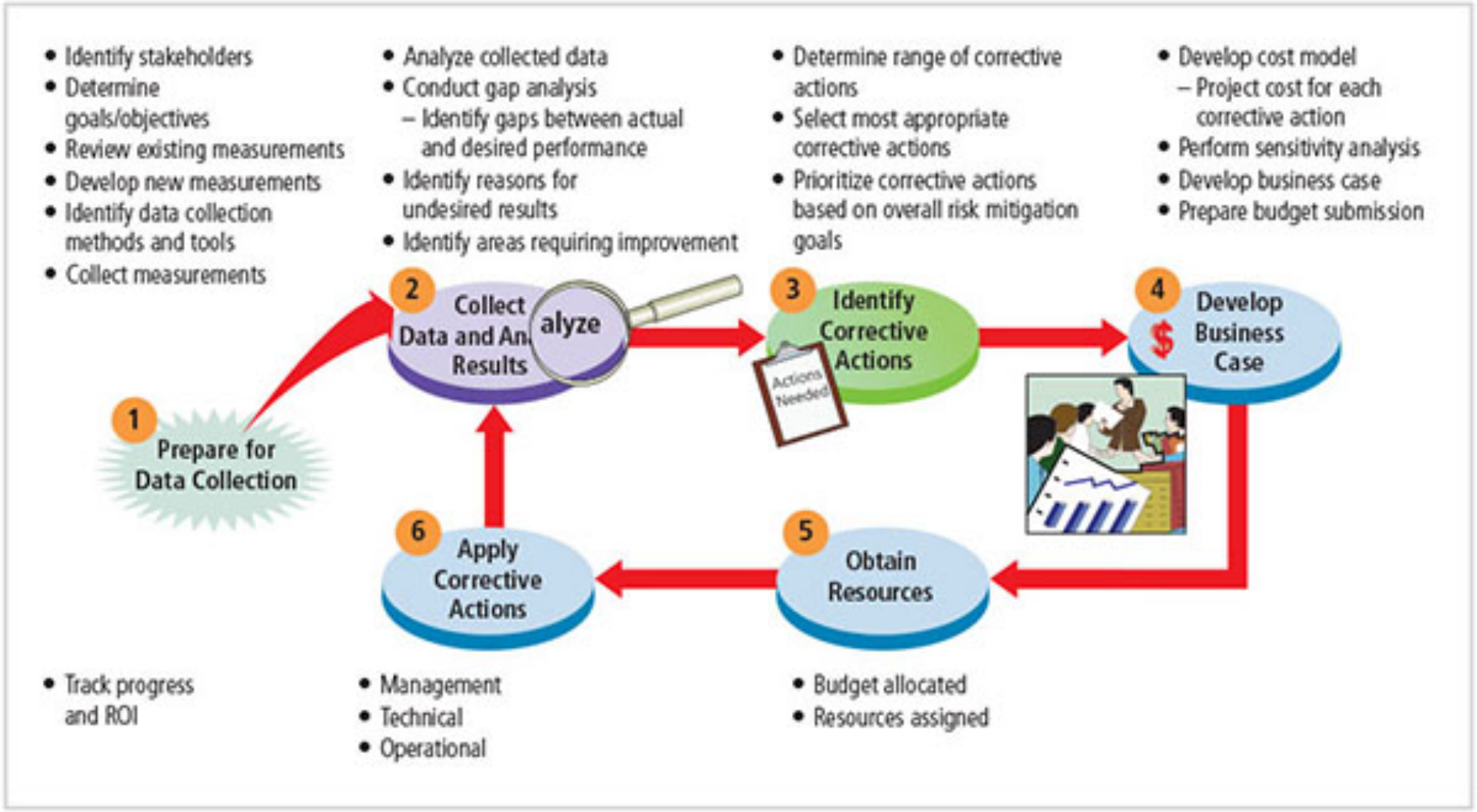
- Organizations should avoid overconfidence after improving their information security profile.
- Organizational changes that may occur include:
  - Acquisition of new assets, emergence of new vulnerabilities, shifting business priorities, partnerships form or dissolve, employee hire and turnover
- If a program is not adequately adjusting, it may be necessary to begin the cycle again.
- If an organization creates adjustable procedures and systems, the existing security improvement program can continue to work well.

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

This provides managerial guidance for establishing and implementing an information security program. There are 13 areas of information security management presented:

1. Information security governance
2. System Development Life Cycle
3. Awareness and training
4. Capital planning and investment control
5. Interconnecting systems
6. Performance measures
7. Security planning
8. Information technology contingency planning
9. Risk management
10. Certification, accreditation, and security assessments
11. Security services and products acquisition
12. Incident response: incident response life cycle
13. Configuration (or change) management

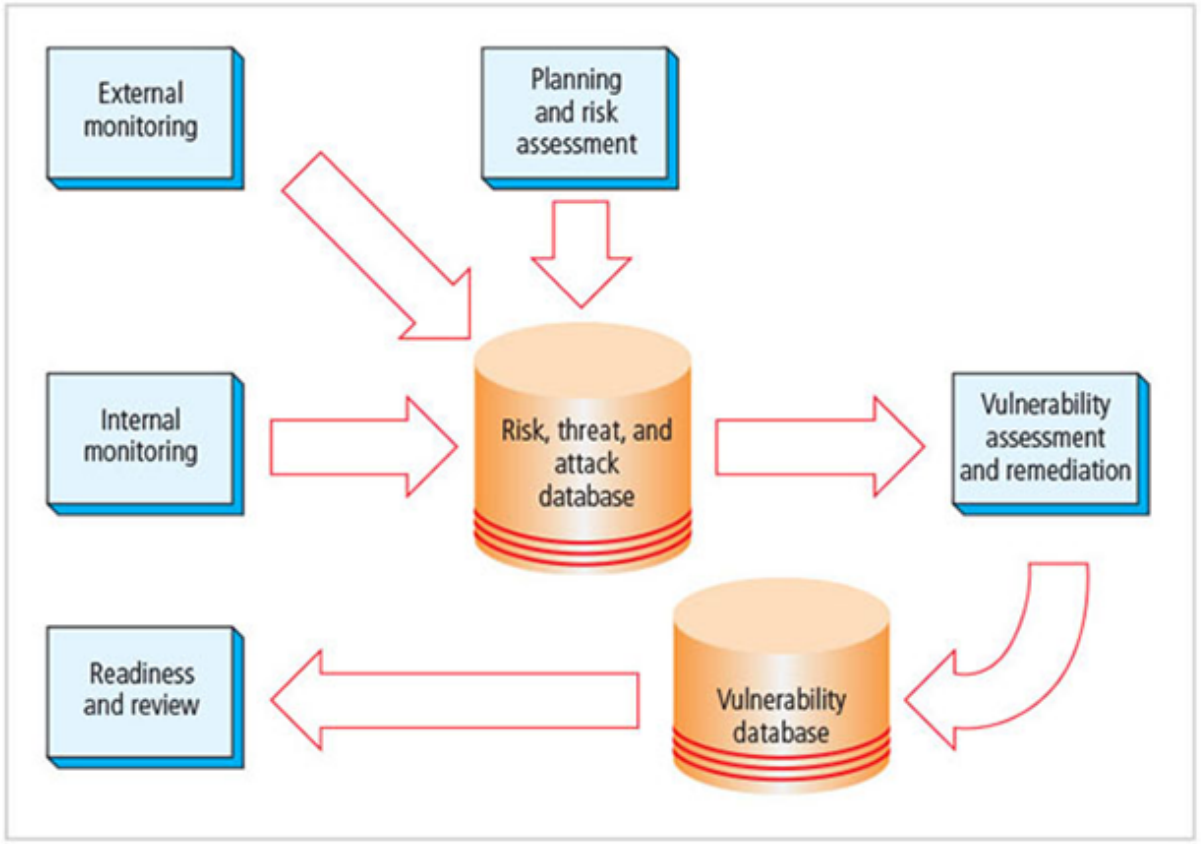
Measurement Program Implementation



Source: NIST SP 800-55 Rev. 1

Security Management Maintenance Models

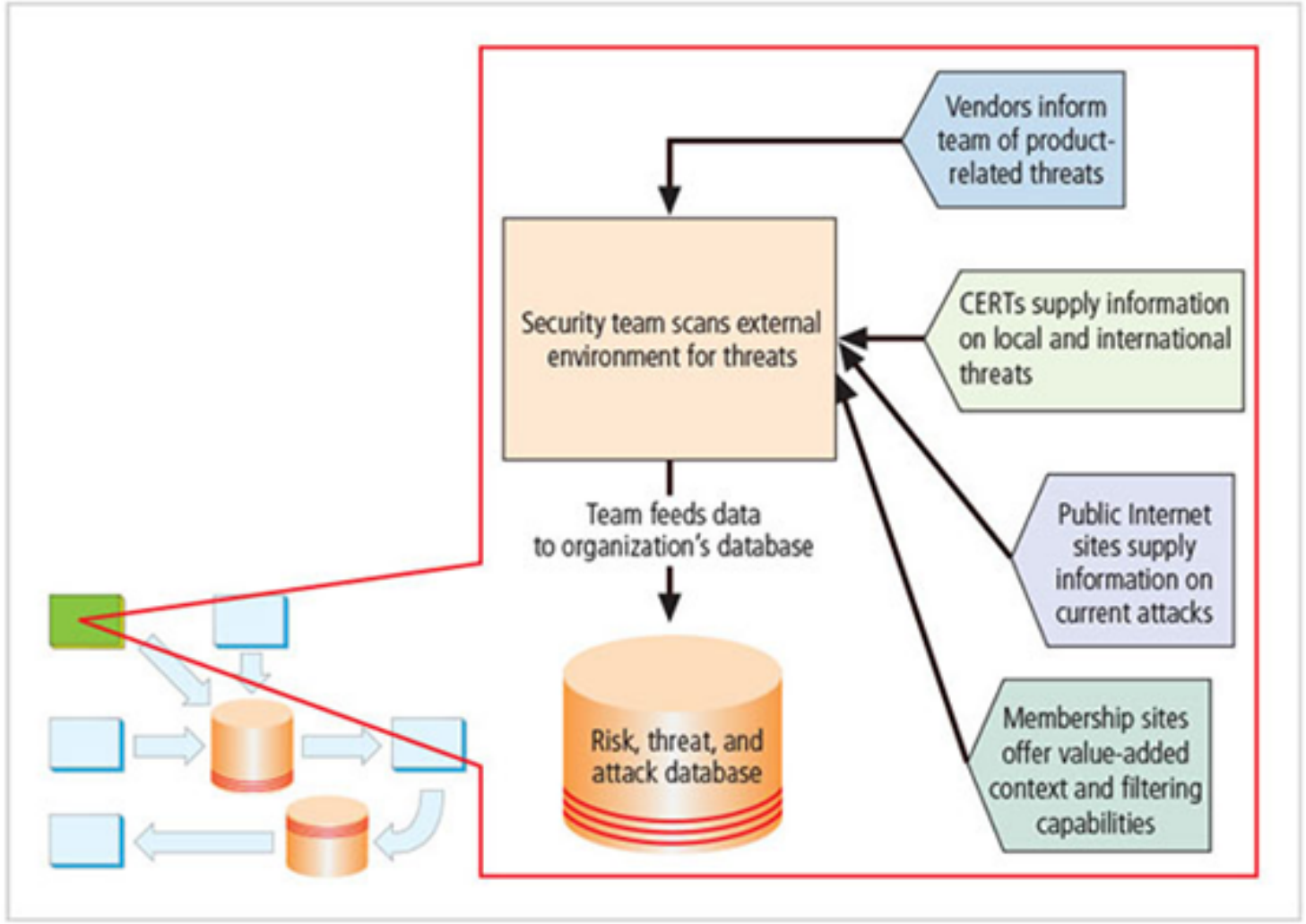
Management model must be adopted to manage and operate the ongoing security program.



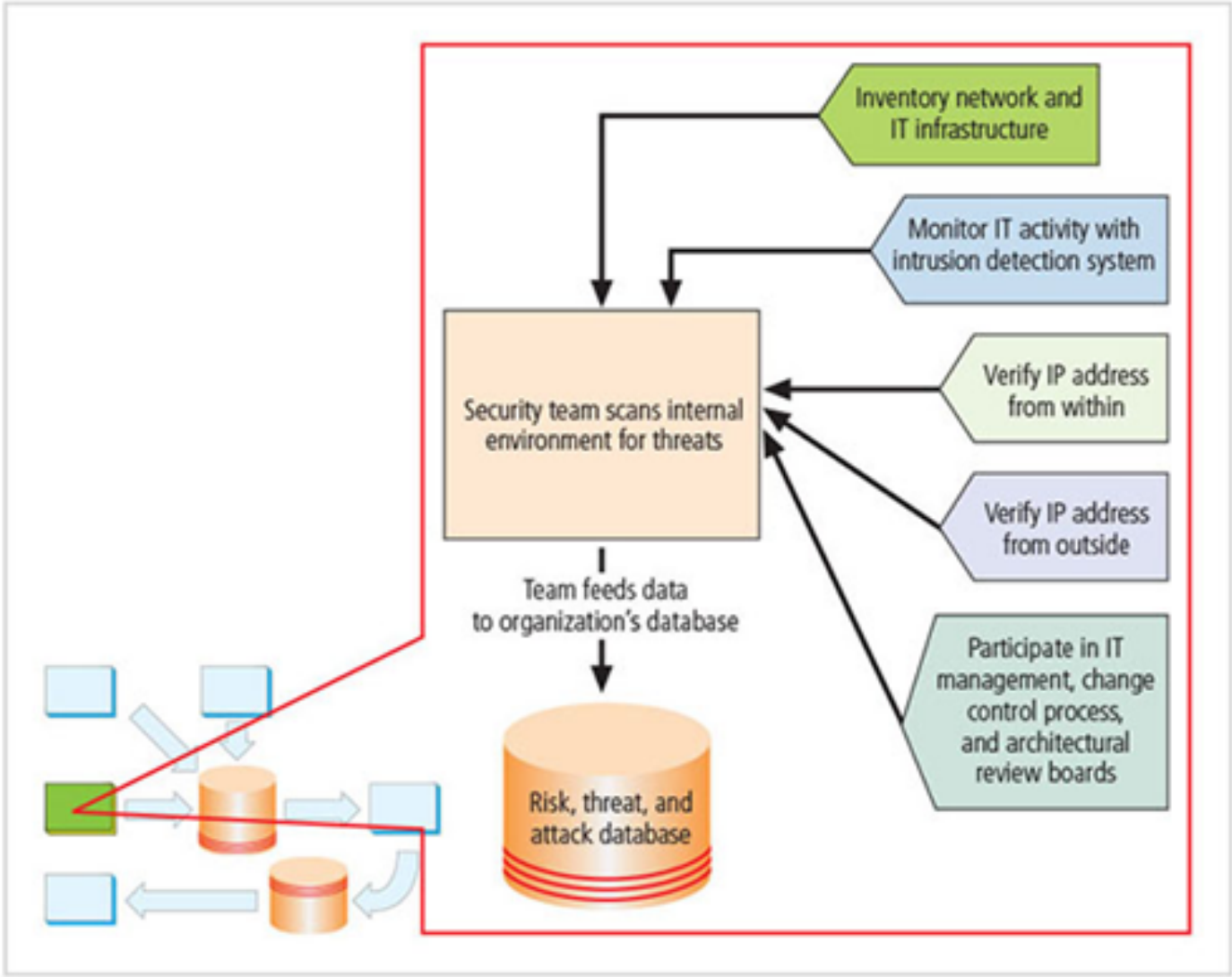
Recommended maintenance model based on five subject areas:

1. External monitoring
2. Internal monitoring
3. Planning and risk assessment
4. Vulnerability assessment and remediation
5. Readiness and review

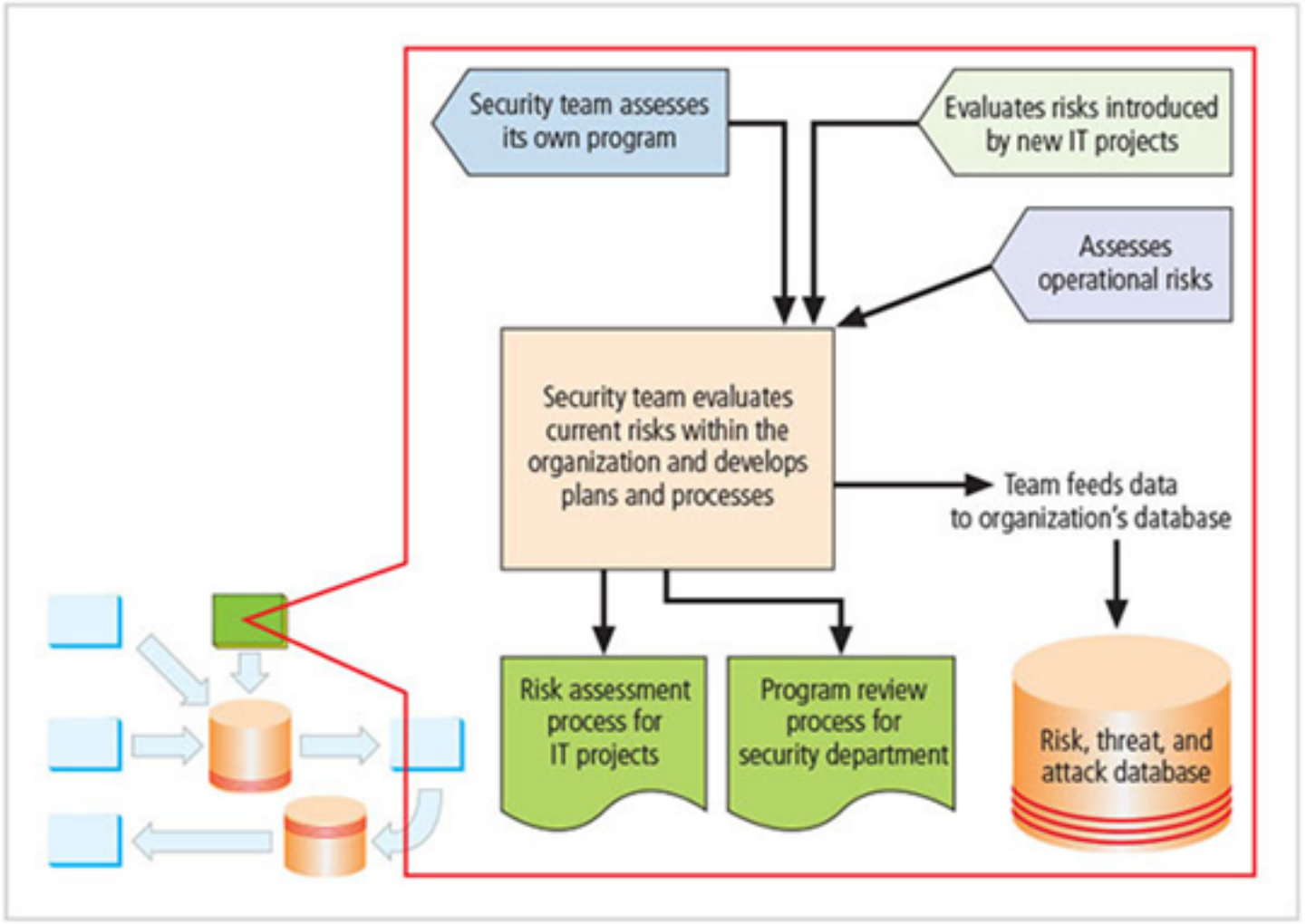
1 - External Monitoring



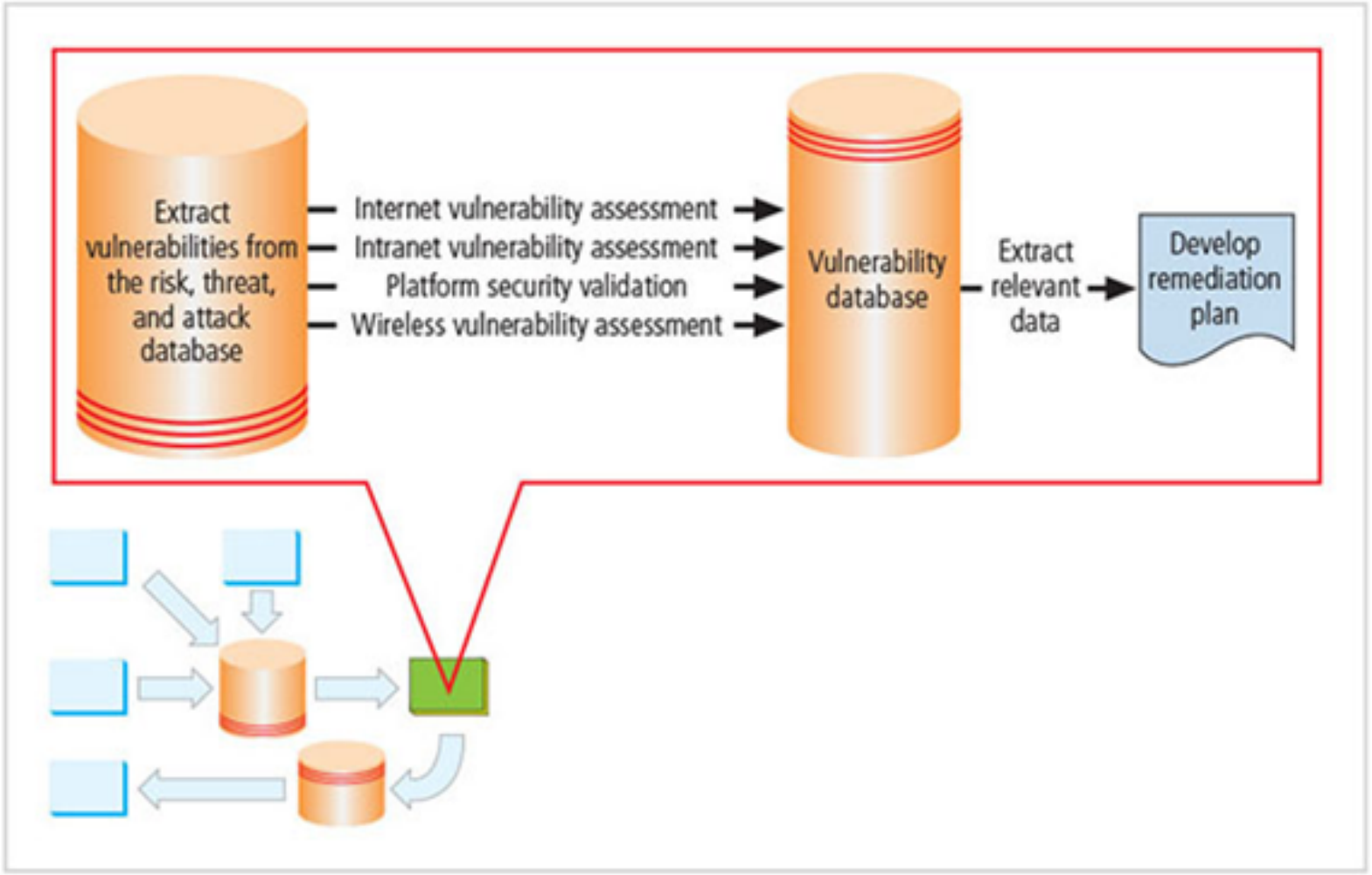
2 - Internal Monitoring



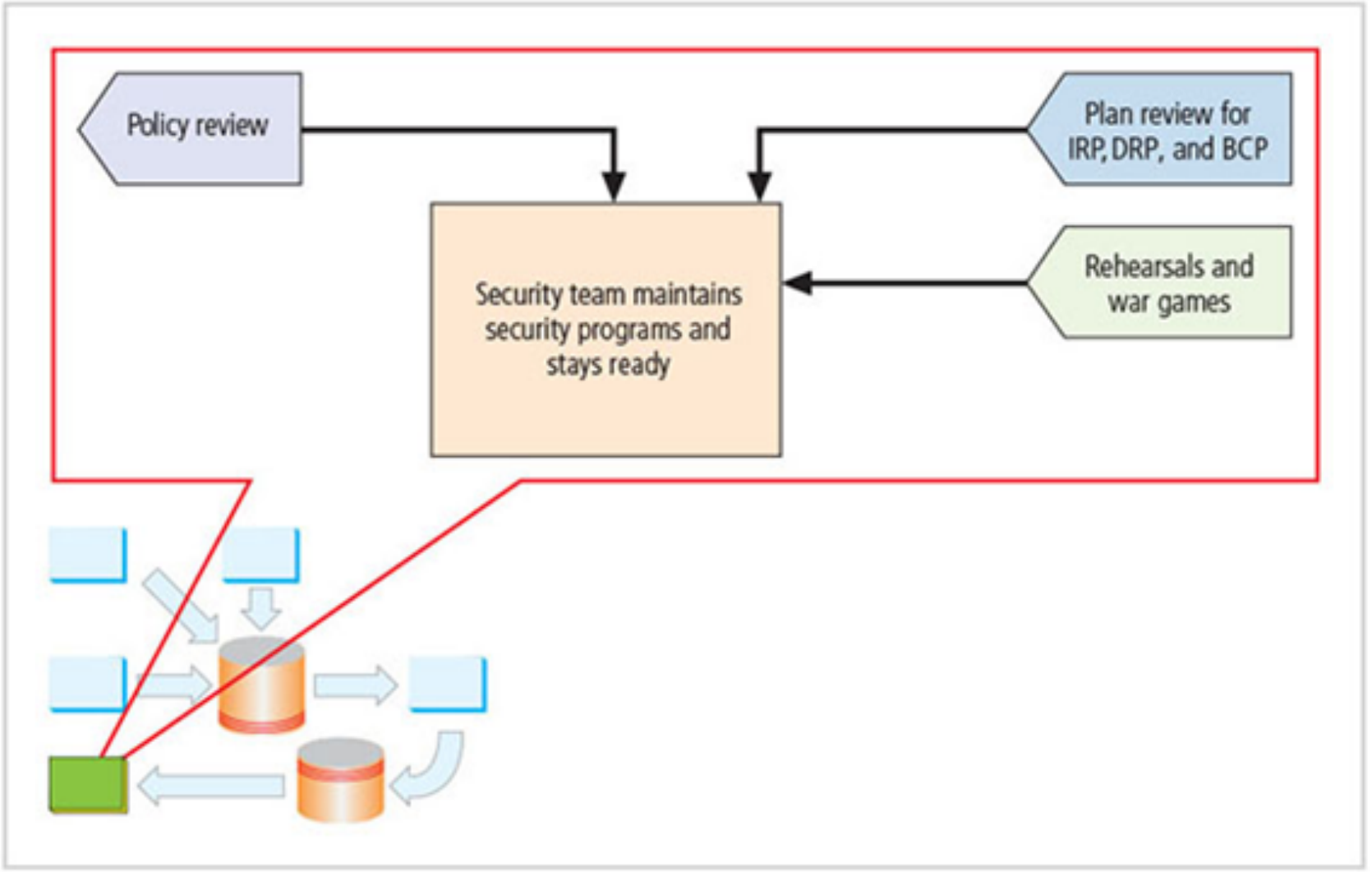
3 - Planning and Risk Assessment



4 - Vulnerability Assessment and Remediation



5 - Readiness and Review



Digital Forensics

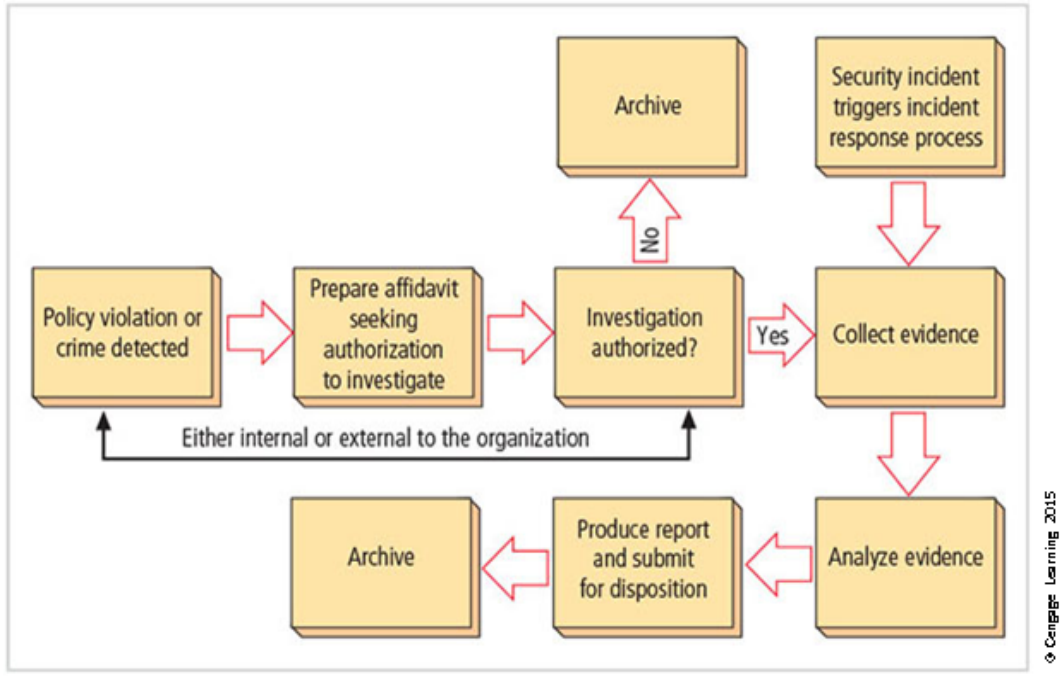
Used to document what happened during attack on assets and how attack occurred. Digital Forensics involves preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary and/or root-cause analysis

- Used for two key purposes:
  - To investigate allegations of digital malfeasance
  - To perform root-cause analysis
- The Digital Forensics Team

- Affidavits and Search Warrants

Digital Forensics Methodology

All investigations follow the same basic methodology



- Identify relevant 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

Summary

- Maintenance of the information security program is essential
- Security management models assist in planning for ongoing operations
- It is necessary to monitor the external and internal environment
- Planning and risk assessment are the essential parts of information security maintenance
- Need to understand how vulnerability assessment and remediation tie into information security maintenance
- Need to understand how to build readiness and review procedures into information security maintenance
- Digital forensics and management of digital forensics function