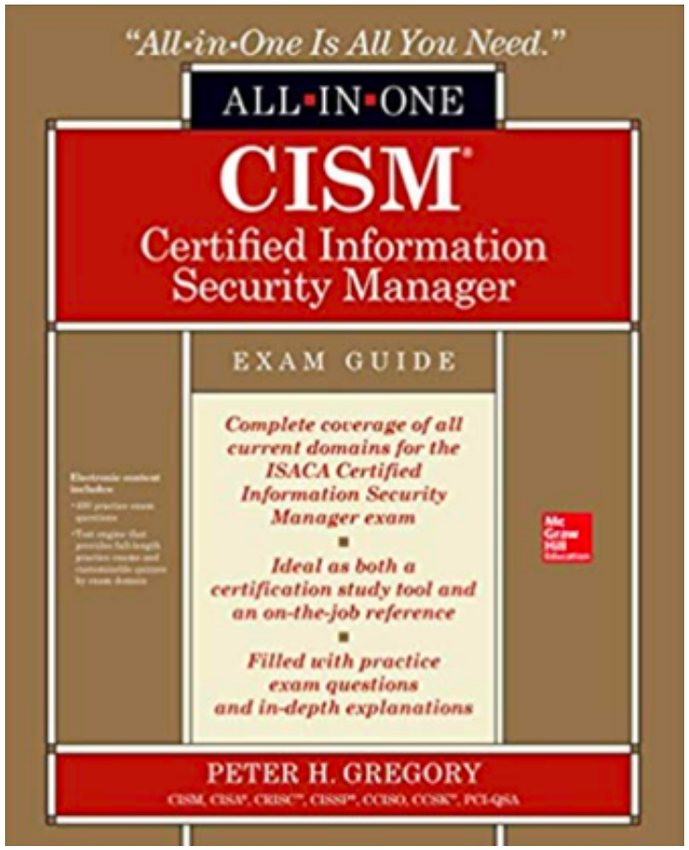
CNIT 160: Cybersecurity Responsibilities

4. Information Security Program Development Part 2



Pages 202 - 235

Updated 11-1-23

Topics in This Lecture

- **Risk Management**
- **The Risk Management Program**
- **The Risk Management Process**
- **Risk Treatment**
- **Audits and Reviews**

Topics
For Later Lectures

- **Policy Development (p. 235)**
- **Third-Party Risk Management**
- **Administrative Activities**
  - **Internal Partnerships**
- **External Partnerships**
- **Compliance Management**
- **Personnel Management**

Topics
For Later Lectures

- **Administrative Activities**
  - **External Partnerships**
  - **Compliance Management**
  - **Personnel Management**
  - **Project and Program Management**
  - **Budget**
  - **Business Case Development**
  - **Vendor Management**

Topics
For Later Lectures

- **Security Program Operations**
- **IT Service Management**
- **Controls**
- **Metrics and Monitoring**
- **Continuous Improvement**

Risk Management

Risk Management

- **Purpose of risk management**
  - **Identify risk and enact changes to bring risks to acceptable levels**
- **Risk management program supports and aligns with overall business objectives**
  - **Includes adopting a *risk appetite***
    - **Ex: banks are risk-averse**
    - **Startups accept more risk**

Four Possible Actions

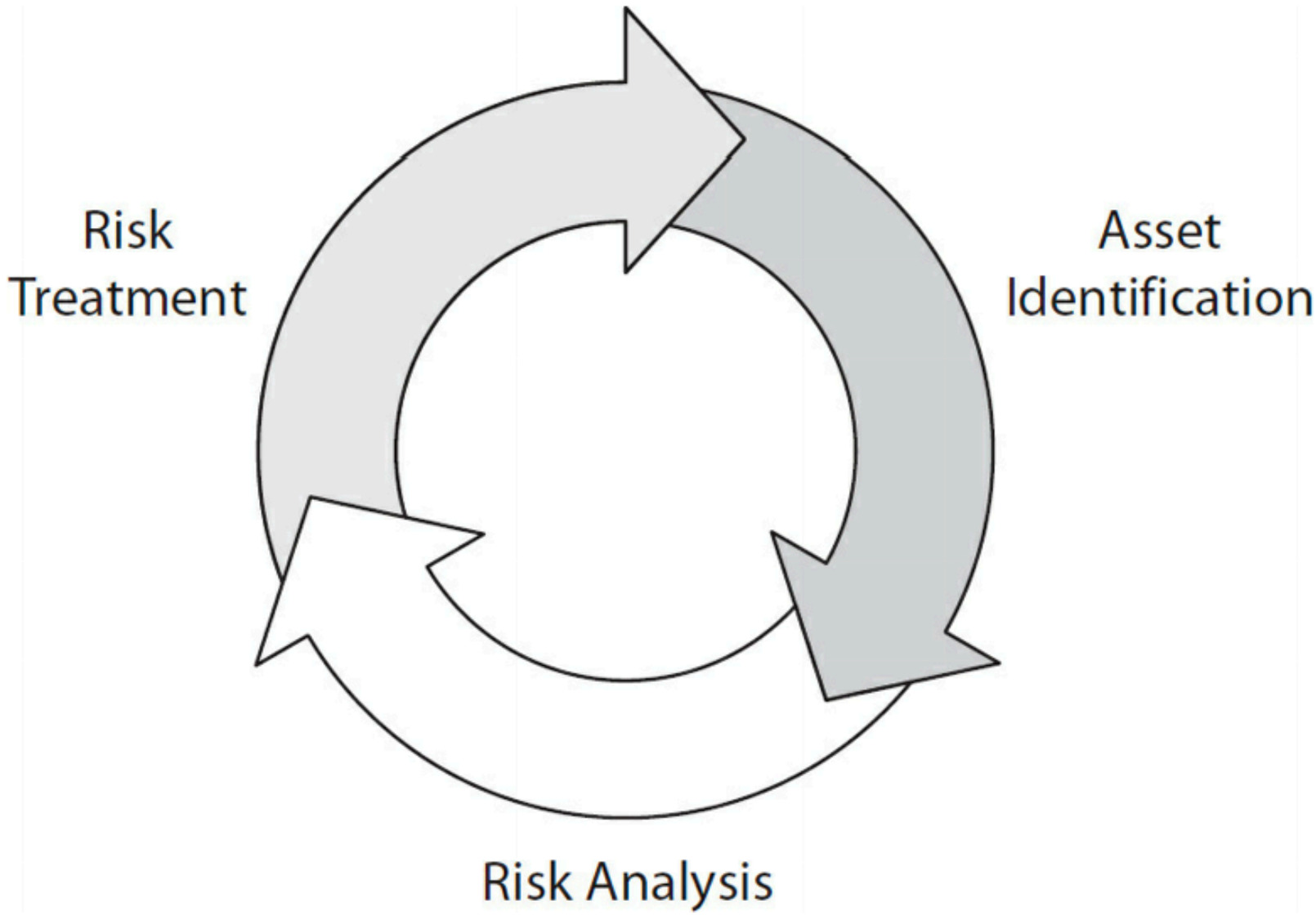
- **When a risk is identified**
- **Accept**
- **Mitigate**
- **Transfer**
- **Avoid**

The Risk Management Program

Principles

- **Objectives**
- **Scope**
- **Authority**
- **Roles and Responsibilities**
- **Resources**
- **Policies, processes, procedures, and records**

The Risk Management Lifecycle



The Risk Management Process

ISACA's Risk-IT Framework

- **Risk Governance**
  - **Integrating with Enterprise Risk Management (ERM)**
- **Risk Evaluation**
- **Risk Response**

Identifying and Grouping Assets

- **Many organizations are unaware of their assets**
  - **Especially virtual and information assets**
- **Usually it's enough to list groups of assets**
  - **Such as laptop computers, servers, etc.**
  - **Because they all have similar risks**

Risk Analysis

- **Simplest terms**
  - ***Risk = Probability x Impact***
- **But often risk is qualitative**
  - **High, medium, low**
- **Requires identifying threats and impacts**
  - **Including vulnerabilities**

Threat Analysis

- **An event that might harm an asset**
- **List all threats with a realistic chance of occurring, with probability**
  - **Storms, earthquakes, floods, power outages**
  - **Labor strikes, riots, terrorism**
  - **Malware, intrusions, crime**
  - **Hardware or software failures**
  - **Errors**

Threat Analysis Approach

- **Geographic for each location**
- **Logical for each type of asset**
- **Unique threat analysis for each highly valued asset**

Data is Sparse

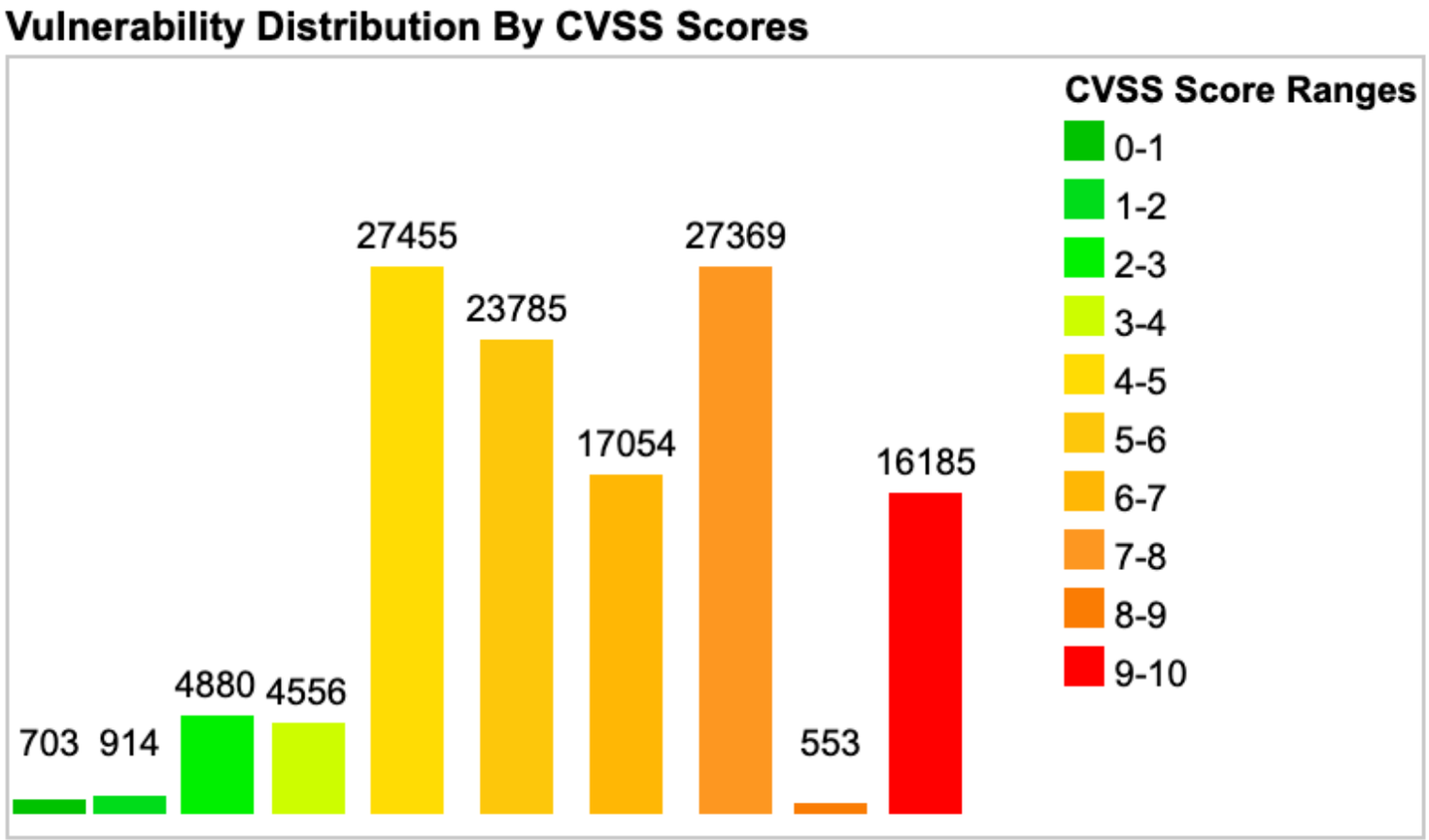
- **Lack of data on probability of many types of threats**
  - **Unlike auto and airplane accidents and human lifespan**
- **Cyber risks are educated guesses**

Vulnerability Identification

- **Missing or inoperative antivirus or anti-malware software**
- **Outdated and unsupported software in use**
- **Missing security patches**
- **Weak password settings**
- **Unnecessary services running on a server or workstation**
- **Misconfigurations in devices, operating systems, or programs**
- **Missing or incomplete audit logs**
- **Inadequate monitoring of event logs**
- **Weak or defective application session management**
- **Building entrances that permit tailgating**

Ranking Vulnerabilities

- **How serious is a vulnerability?**



- **https://www.cvedetails.com/cvss-score-distribution.php**

Probability Analysis

- **Probability that the threat will be realized**
- **Difficult to do accurately**

Impact Analysis

- **Estimate the effect on the organization, for highest-ranked threats on critical assets**
- **Consider relationship between an asset and business processes**
- **Must include statement of impact for each threat, in business terms**
  - **Ex: "inability to process customer support calls",**
  - **not "inability to authenticate users"**

Qualitative Risk Analysis

- **Used to quickly identify most critical risks**
  - **Without the burden of identifying precise financial impacts**
- **High-Medium-Low, or 1-5 scale, or 1-10 scale**
- **Often precedes a quantitative risk analysis**

Quantitative Risk Analysis

- **Uses numeric methods**
  - **Asset Value (AV)**
    - **Often replacement value**
- **Exposure Factor (EF)**
  - **Financial loss from realization of a threat**

Quantitative Risk Analysis

- **Single Loss Expectancy (SLE)**
  - **SLE = AV x EF**
- **Annualized Rate of Occurrence (ARO)**
- **Annualized Loss Expectancy (ALE)**
  - **ALE = SLE x ARO**

Business Continuity Planning

- **Uses risk analysis to plan for disasters**
- **Same as the risk analysis discussed in this chapter**

High-Impact Events

- **Threaten the viability of the organization**
  - **Require risk treatment with executive management visibility**
- **Belongs in business continuity planning and disaster recovery planning**

Risk Analysis Standards

- **NIST SP 800-30, "Guide for Conducting Risk Assessments"**
- **ISO/IEC 27005, "Information technology – Security techniques – Information security risk management"**

Ch 4a

Risk Treatment

Who Decides

- **Security Manager**
  - **Most knowledgable about risk**
  - **Should not decide alone, because others may not support the decisions**
- **Security Steering Committee**
  - **Consensus of stakeholders: best**
- **Undefined**
  - **No effective security management program**

Risk Mitigation

- **Lowers risk**
- ***Residual risk* remains**
- **Usually preceded by cost analysis**

Risk Transfer

- **To an insurance company or business partner**
- **Examine policy carefully**
  - **Check for exclusions**

Risk Avoidance

- **Organization abandons risky activity**

Dick's Sporting Goods to stop selling guns in 125 stores

BY SARAH MIN
MARCH 12, 2019 / 4:45 PM / MONEYWATCH

Risk Acceptance

- **Should be a calculated decision, not just ignoring the risk**

Residual Risk

- **Remaining risk after risk treatment**
- **May be regarded as a new risk and subjected to another risk management cycle**

Compliance Risk

- **Regulations**
  - **GLBA for financial businesses**
  - **PCI-DSS for businesses that accept payment cards**
- **Fines and other sanctions for non-compliance**

Risk Ledger

- **Records discovery of risks and decisions**
  - **Risk identification**
  - **Risk description**
  - **Affected assets**
  - **Risk score**
  - **Risk treatment analysis**
  - **Risk treatment**

Risk Ledger Form

- **Spreadsheet is OK when first starting out**
- **More mature organizations need a Governance, Risk, and Compliance (GRC) tool**

Audits and Reviews

Security Audit

- **Determines whether safeguards are in place and working properly**
- **Security Audit**
  - **Formal and rigorous**
  - **Requires presenting evidence**
- **Security Review**
  - **Less formal and rigorous**

Audits

- **Systematic and repeatable process**
- **Performed by a competent and independent person**
  - **Interviews personnel**
  - **Gathers and analyzes evidence**
  - **Delivers a written opinion on effectiveness of controls**
- **May be internal or external audit**

- **Will hopefully be taught at CCSF soon**

Audit Planning

- **Purpose**
- **Scope**
- **Risk analysis**
  - **Focus on problematic areas**
- **Audit procedures**
- **Resources**
- **Schedule**

Audit Objectives

- **Determine whether controls exist**
  - **And whether they are effective**
- **Often part of regulations, compliance, or other legal obligation**
  - **Or aftermath of an incident**

Types of Audits

- **Operational audit**
- **Financial audit**
- **Integrated audit**
- **IS audit**
- **Administrative audit**
- **Compliance audit**

Types of Audits

- **Forensic audit**
  - **Preparation for a lawsuit**
- **Service provider audit**
  - **Because organizations outsource to third parties**
  - **Those third parties undergo external audits**
  - **To increase customer confidence**

Standards for Attestation Engagements No. 18 (SSAE 18)

- **Performed on a service provider's operations**
- **Audit report transmitted to customers**
- **Closely aligned with global standard**
  - **International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organization (ISAE 3402), from the International Auditing and Assurance Standards Board (IAASB)**

Pre-Audit

- **An examination of business processes, information systems, applications, or business records**
- **In anticipation of an upcoming audit**

Audit Methodology

- **Formal methodologies ensure consistency**
  - **Even when performed by different personnel**
- **Phases**
  - **Subject, objective, type, scope, pre-audit planning**

Audit Statement of Work

- **Describes purpose, scope, duration, and costs**
- **May require written approval from client before work begins**

Audit Procedures

- **A list of people to interview**
- **Inquiries to make during each interview**
- **Documentation (policies, procedures, and other documents) to request during each interview**
- **Audit tools to use**
- **Sampling rates and methodologies**
- **How and where evidence will be archived**
- **How evidence will be evaluated**

Audit Communication Plan

- **Evidence requested**
- **Regular written status reports**
- **Regular status meetings**
- **Contact information for IS auditor and auditee**

Report Preparation

- **Format and content of report**
- **How findings will be established and documented**
- **Report must comply with applicable audit standards**
- **Identifies parties that perform internal review**

Wrap-Up

- **Deliver report to auditee**
- **Closed meeting to discuss report and collect feedback**
- **Send invoice**
- **Collect and archive work papers**

Post-Audit Follow-Up

- **Contact auditee**
  - **To determine progress on audit findings**
- **Establishes tone of concern**
- **Establishes a dialogue**
- **Helps auditor understand management's commitment**
- **Improves goodwill and prospect for repeat business**

Audit Evidence

- **Observations**
- **Written notes**
- **Correspondence**
- **Independent confirmations from other auditors**
- **Internal process and procedure documentation**
- **Business records**

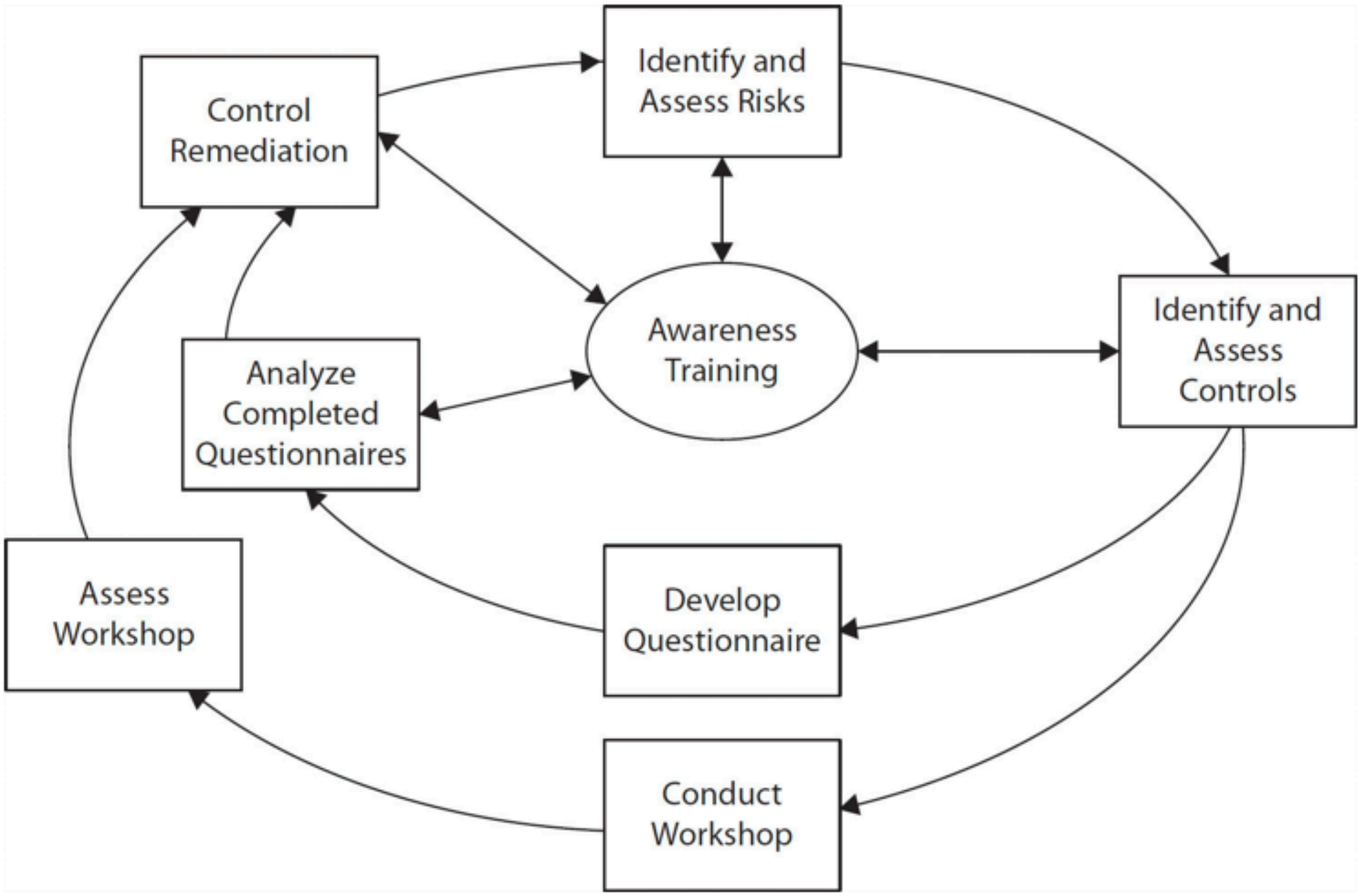
Evidence Characteristics

- **Independence of the evidence provider**
- **Qualifications of the evidence provider**
- **Objectivity**
- **Timing**

Observing Personnel

- **Real tasks**
- **Skills and experience**
- **Security awareness**
- **Segregation of duties**

Control Self-Assessment



Ch 4b