Unit - II & III

Content

1) How to select proper standard

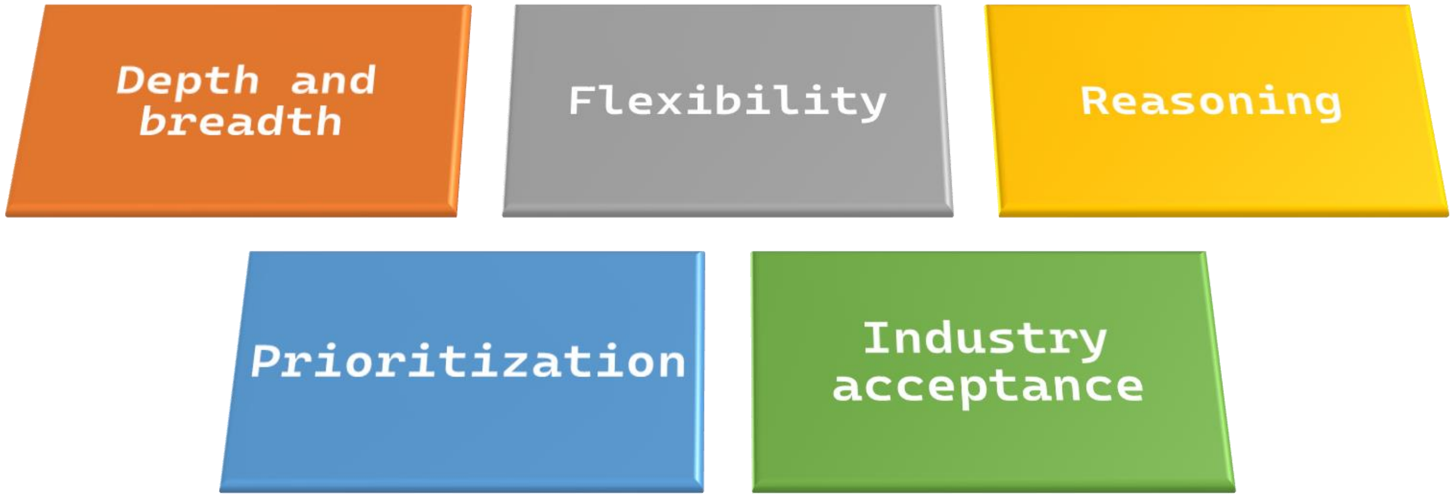
2) What are Controls and their importance

3) What is CAAT?

4) Compliance in all 7 domains (Maximizing C-I-A)

How to select proper standard?

- While trying to determine a specific standard to which to adhere, it is helpful to consider the high-level differences among them.
- The following attributes should be considered:



Depth and breadth

Flexibility

Reasoning

Prioritization

Industry acceptance

How to select proper standard?

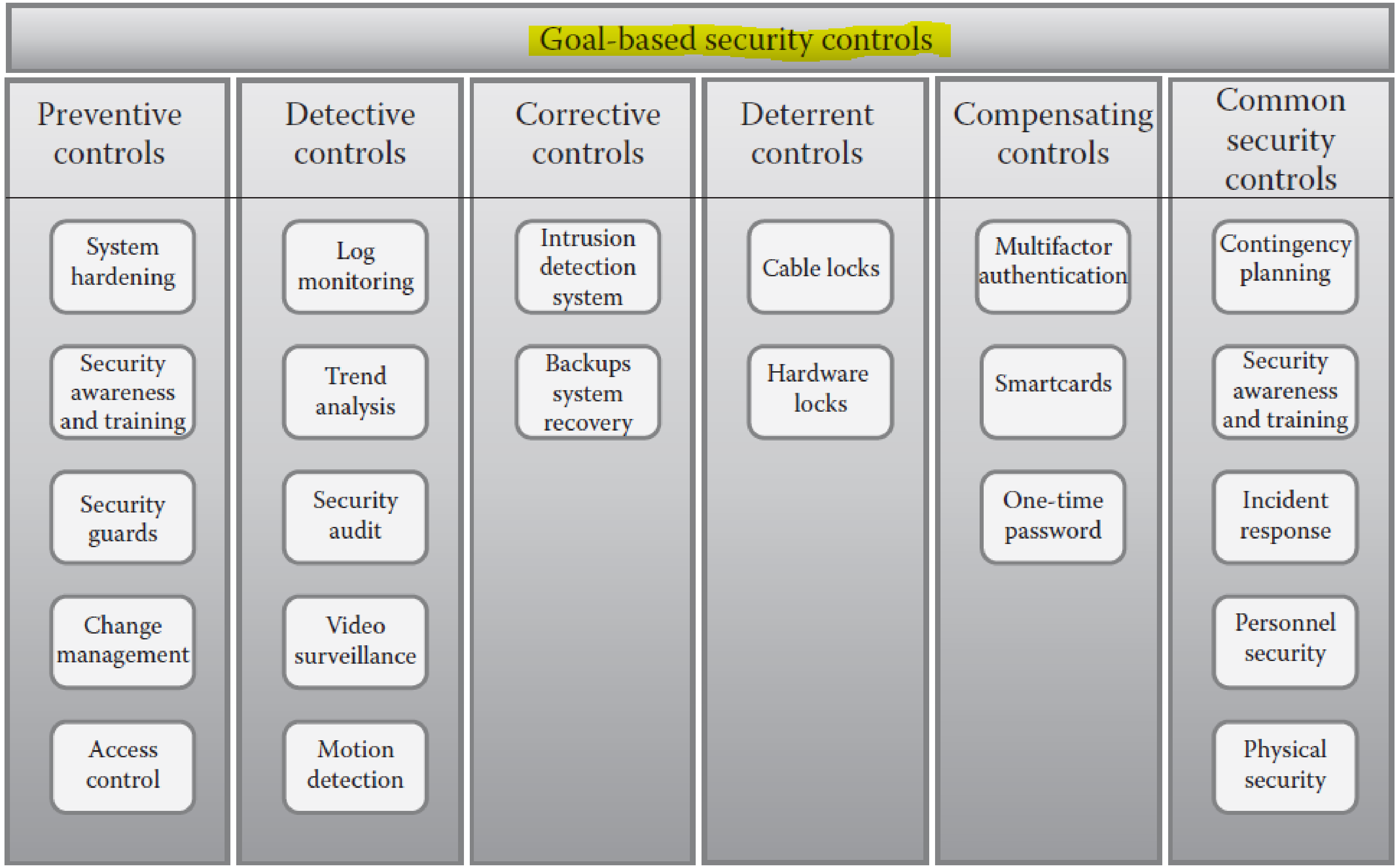
- ❑**Depth and breadth**—Some go far and wide, whereas others are narrow and deep. Guiding principles that cover a wide range might be most suitable to your organization.
- ❑**Flexibility**—One standard might apply across the entire organization, whereas another might be limited to a specific department or team.
- ❑**Reasoning**—Some standards provide stronger guidance about why they make a particular statement around controls. Sometimes, the reasoning can be important, as those putting in place and auditing controls understand how and why they apply.
- ❑**Prioritization**—Although each organization determines acceptable risk, some standards can provide guidance for focusing on certain areas over others.
- ❑**Industry acceptance**—Some standards are generally accepted more than others. Acceptance also varies by industry.

What is Control?

"Security controls refers to any type of safeguard or countermeasure used to avoid, detect, counteract or minimize security risks to physical property, information, computer systems or other assets."

- ❑Two Classifications:
  - ❑Goal-based security controls:
    - ❑ Preventive controls: attempt to prevent an incident from occurring.
    - ❑ Detective controls: attempt to detect incidents after they have occurred.
    - ❑ Corrective controls: attempt to reverse the impact of an incident.
    - ❑ Deterrent controls: attempt to discourage individuals from causing an incident.
    - ❑ Compensating controls: are alternative controls used when a primary control is not feasible.
    - ❑ Common controls: are implemented across multiple ICT systems.

What is Control?



Goal-based security controls

Preventive controls	Detective controls	Corrective controls	Deterrent controls	Compensating security controls	Common security controls
System hardening	Log monitoring	Intrusion detection system	Cable locks	Multifactor authentication	Contingency planning
Security awareness and training	Trend analysis	Backups system recovery	Hardware locks	Smartcards	Security awareness and training
Security guards	Security audit			One-time password	Incident response
Change management	Video surveillance				Personnel security
Access control	Motion detection				Physical security

Figure 4.1 Goal-based security controls.

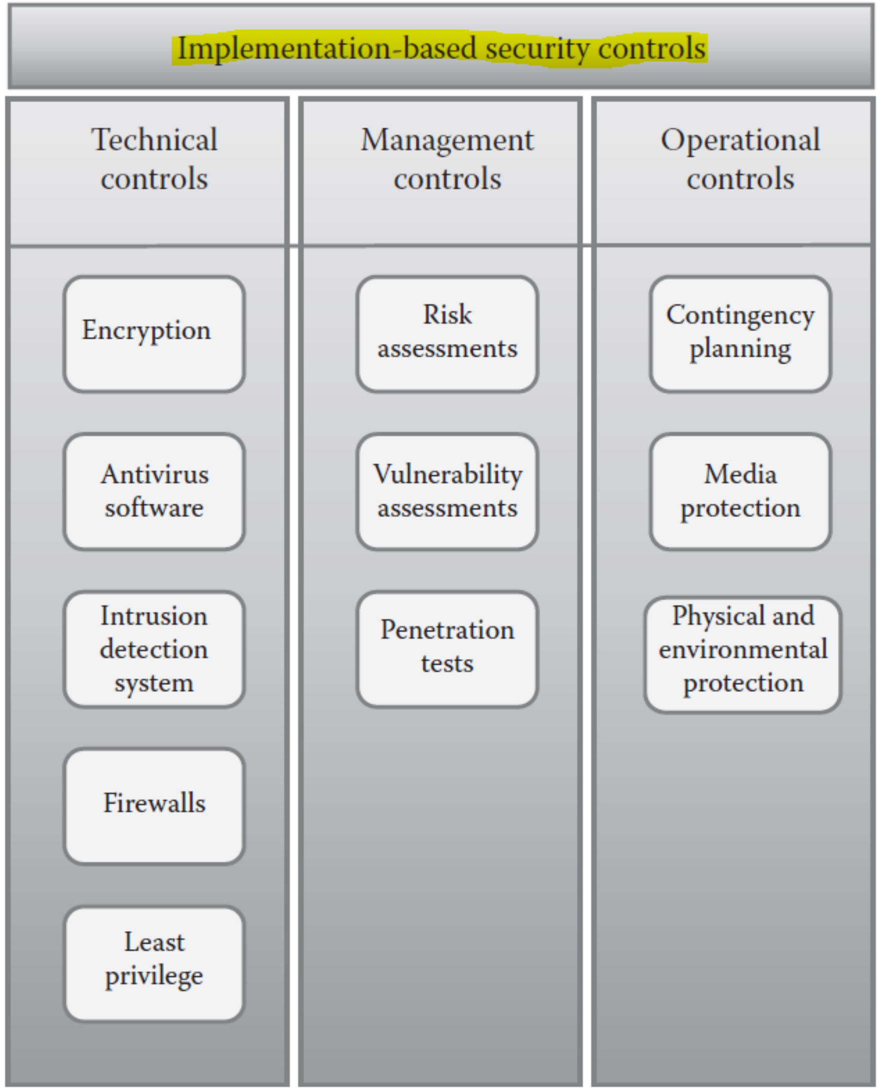
What is Control?

"Security controls refers to any type of safeguard or countermeasure used to avoid, detect, counteract or minimize security risks to physical property, information, computer systems or other assets."

❑Two Classifications:

- ❑Implementation-based security controls:
  - ❑ Technical controls use technology.
  - ❑ Management controls use administrative or management methods.
  - ❑ Operational controls are implemented by people in day-to-day operations.

What is Control?

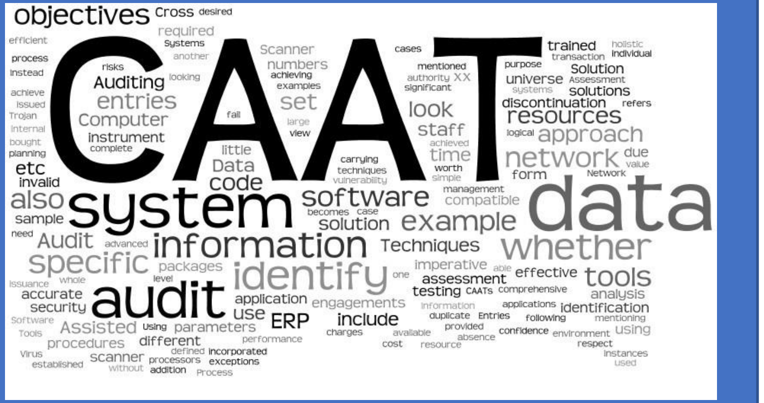


Implementation-based security controls

Technical controls	Management controls	Operational controls
Encryption	Risk assessments	Contingency planning
Antivirus software	Vulnerability assessments	Media protection
Intrusion detection system	Penetration tests	Physical and environmental protection
Firewalls		
Least privilege		

Figure 4.2 Implementation-based security goals.

What is CAAT?



“Computer-Assisted Audit Techniques (CAATs) is the software that helps auditors evaluate application controls, and select and analyze computerized data for substantive audit tests.”

❑CAATs can be used by both IT or financial auditors in a variety of ways to evaluate the integrity of an application, determine compliance with procedures, and continuously monitor processing results.

What is CAAT?

- ❑Common CAATs like **ACL (Audit Command Language)** and **Interactive Data Extraction and Analysis (IDEA)** can be used to:
  - ❑Select a sample
  - ❑Analyze the characteristics of a data file
  - ❑Identify trends in data
  - ❑Evaluate data integrity.
- ❑Other techniques used for analyzing data include, for example, **Microsoft Access** and **Microsoft Excel**. Microsoft Access can be used to analyze data, create reports, and query data files.
- ❑Microsoft Excel also analyzes data, generates samples, creates graphs, and performs regression or trend analysis.

CAAT for Sampling

- ❑Some audit techniques assist in defining sample size and selecting the sample. For example, ACL automatically calculates the sample size and selects a sample from a population. Spreadsheet Applications also generate random numbers for selecting a sample.
- ❑There are two types of sampling techniques:
- ❑**Judgmental sampling:** The sample selected is based on the auditor’s knowledge and experience. The judgment may be to select a specific block of time, geographic region, or function.
- ❑**Statistical sampling:** The sample is randomly selected and evaluated through the application of the probability theory.

Compliance in User Domain

❑**Who are part of User Domain:**

❑Employee: Most Trusted, Full Access

❑Contractors: Some Trust, Partial Access

❑Guests: Least Trust, Limited Access

❑**Controls:**

❑RACI Matrix (Responsible, Accountable, Consulted, Informed)

❑IT-Asset AUP (Acceptable Usage Policy)

❑Internet AUP

❑Email AUP

❑HR Security Controls

Compliance in Workstation Domain

- ❑**Devices of Workstation Domain:**
- ❑UPS, PC, Laptop, Tablet, Printer, Storage Media, Smartphone

- ❑**Controls:**
- ❑ACLs (Access Control Lists)
- ❑Authentication and Identity Management

- ❑**Maximizing C-I-A:**
- ❑**Availability:**
  - ❑Surviving power outages (UPS)
  - ❑Executing a solid backup and recovery strategy

Compliance in Workstation Domain

- ❑**Maximizing C-I-A:**
- ❑**Integrity:**
  - ❑Anti-malware software (up to date)
- ❑**Confidentiality:**
  - ❑Access Control
  - ❑Encryption
- ❑**Other security controls:**
  - ❑OS Patch Management
  - ❑Application Patch Management
  - ❑IT Security policy and procedures for work station

Compliance in LAN Domain

❑**Devices of LAN Domain:**

❑PC, Laptop, Printer, Storage Media, Switch, Hub, Router, Server computer (file, printer server)

❑**Controls:**

❑Access Control for protected resources

❑Communication Control to limit the malware

❑Recovery plans including backup for devices in LAN

❑Procedure to control configuration changes

❑Monitoring tools and other detective control for LAN

❑Software patch management

Compliance in LAN Domain

- ❑**Maximizing C-I-A:**
- ❑**Confidentiality:**
  - ❑Strong access control
  - ❑Encryption
  - ❑Privacy policy
- ❑**Integrity:**
  - ❑Anti malware software installation in all PC of LAN
  - ❑Audit the critical data for unauthorized changes
- ❑**Availability:**
  - ❑Comprehensive recovery plans
  - ❑Backup of computers and device configurations

Compliance in LAN-WAN Domain

SPRINGFIELD PHONE COMPANY
WE'RE APPROACHING BANDWIDTH OVERLOAD, SIR.

❑**Devices/Technology of LAN-WAN Domain:**

❑Switch, Router, Firewall, Proxy Servers, DMZ, Honeypots, ISP, IDS/IPS, DLP.

❑**Controls:**

❑Traffic monitoring and analysis in real time

❑Configuration management

❑Change management

❑Firewall rules

❑Access rights and Access Controls

❑Network Access Control (NAC)

  ❑Anti malware, Firewall status, OS Patch level, Node identity

❑VAPT

Compliance in LAN-WAN Domain

- ❑**Maximizing C-I-A:**
- ❑**Availability:**
  - ❑To minimize downtime die to device failure, ensure every mode has an alternate whenever possible.
  - ❑Dual homed ISP Connections (Diff. ISPs)
  - ❑Redundant Routers and Firewalls
  - ❑BCP & DRP
  - ❑VAPT
- ❑**Integrity:**
  - ❑Use of VPN for remote access
  - ❑Configuration Management Verification
- ❑**Confidentiality:**
  - ❑Encryption & DLP

Compliance in WAN Domain

❑**Devices/Technology of WAN Domain:**

❑WAN Service Provider, Dedicated lines/circuits. MPLS, WAN L2/L3 switches, WAN backup and redundancy links.

❑**Controls:**

❑WAN Optimizer

❑Traffic monitoring and analyzer

❑Configuration and change management

❑Access rights and access control

❑VPN

Compliance in WAN Domain

- ❑**Maximizing C-I-A:**
- ❑WAN Service Availability SLAs (Service Level Aggreement)
- ❑WAN recovery and restoration SLAs
- ❑WAN traffic Encryption/VPNs
- ❑WAN service provider SOC compliance
- ❑Redundancy
- ❑Backup & recovery

Compliance in Remote Access Domain

❑**Devices of Remote Access Domain:**

❑Remote Users, Remote workstation or laptop, Remote access control tools, Authentication server (TACACS, RADIUS), VPNs (IPSec, L2P, PPTP, L2F) & Encryption, ISP

❑**Controls:**

❑Protection of data privacy

❑Application data encryption

❑Application control encryption (HTTPS)

❑System connection encryption (VPN)

❑Remote access AUP

❑Remote access & VPN tunnel monitoring

❑Access configuration, management, rights & control

Compliance in Remote Access Domain

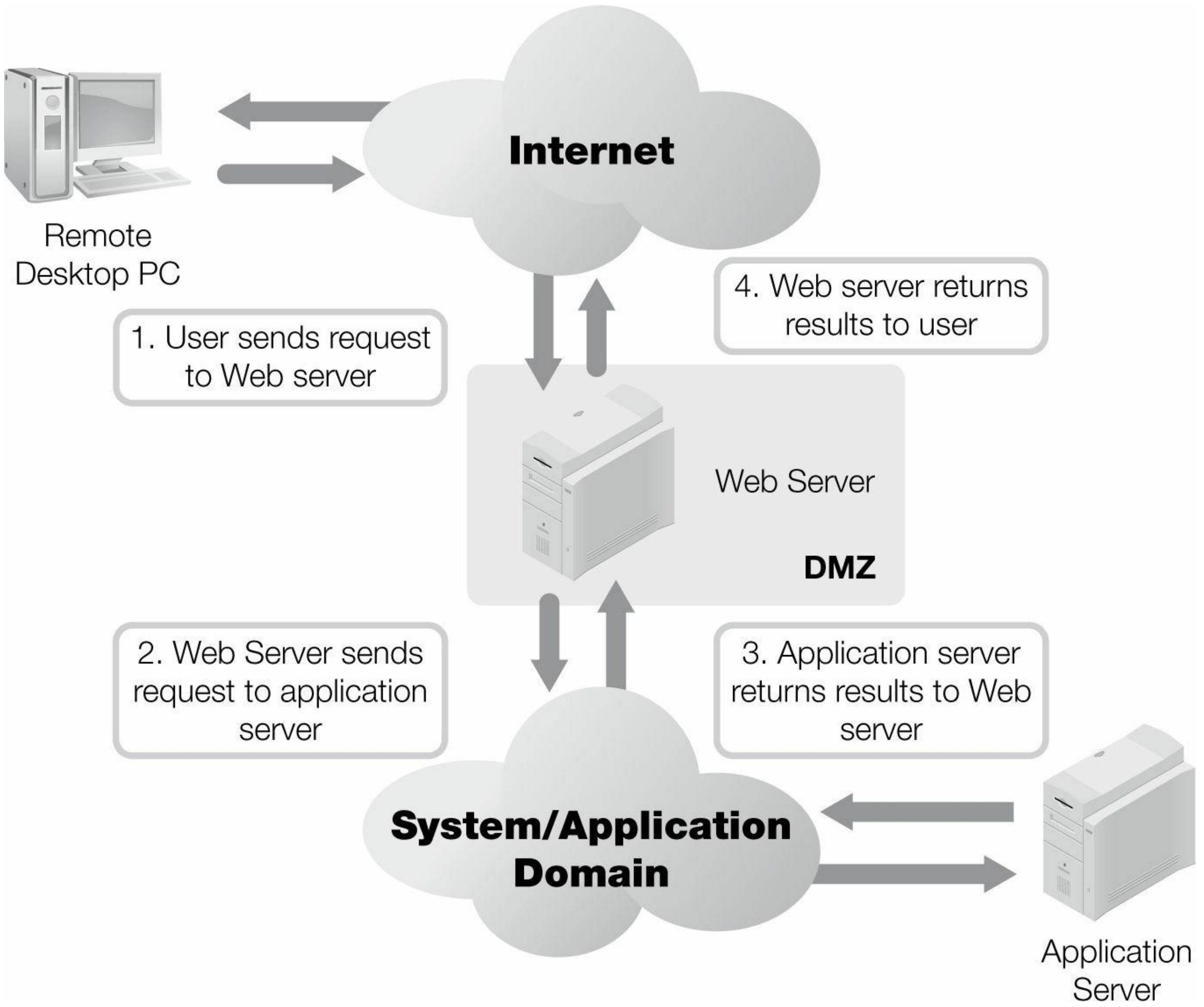
❑**Controls:**

❑VPN Client Definition and Access Controls

❑TLS VPN Remote Access Via a Web Browser

❑VPN Configuration Management Verification

Compliance in System/ Application Domain


Remote Desktop PC
Internet
1. User sends request to Web server
4. Web server returns results to user
Web Server
DMZ
2. Web Server sends request to application server
3. Application server returns results to Web server
System/Application Domain
Application Server

Compliance in System/ Application Domain

- **Devices of System/Application Domain:**
- Main frame, Minicomputer, File server, UPS, storage devices, source code, applications, DB, Data center, Backup data center

- **Controls:**
- Isolate data
- Limit access to data
- Protect data loss through redundancy
- Physical access control
- Environmental control
- Fire suppression control
- DR Sites

Compliance in System/ Application Domain

❑**Controls:**

❑Software configuration management

❑QA-QT testing

❑Access rights and access control

❑**Maximizing C-I-A:**

❑BCP & DRP

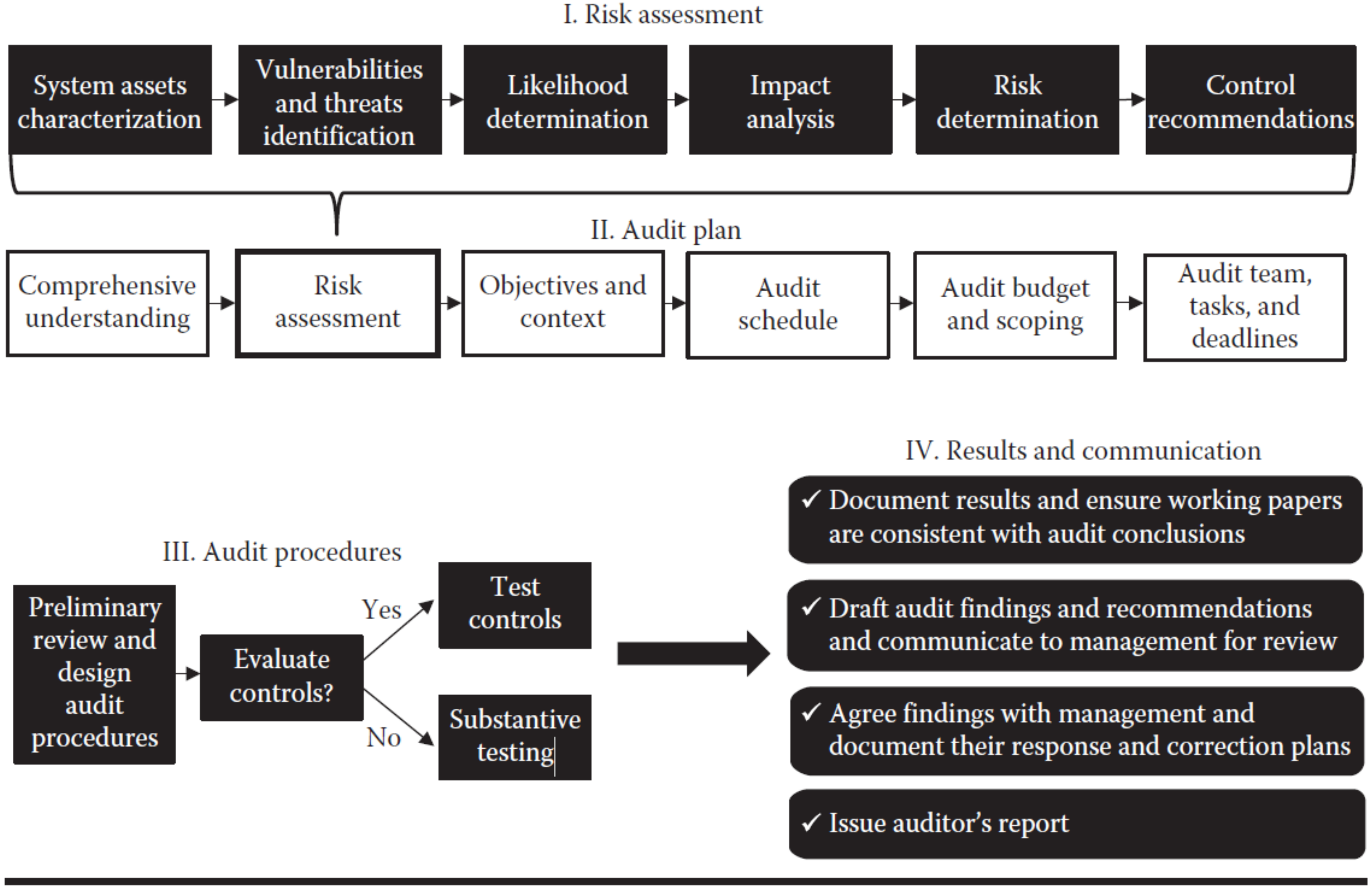
❑Access Control

❑Drive encryption

❑Vulnerability management

❑Adherence to the security policy

Summery of Auditing Process



I. Risk assessment

System assets characterization → Vulnerabilities and threats identification → Likelihood determination → Impact analysis → Risk determination → Control recommendations

II. Audit plan

Comprehensive understanding → Risk assessment → Objectives and context → Audit schedule → Audit budget and scoping → Audit team, tasks, and deadlines

III. Audit procedures

Preliminary review and design audit procedures → Evaluate controls?

Yes → Test controls

No → Substantive testing

IV. Results and communication

- ✓ Document results and ensure working papers are consistent with audit conclusions
- ✓ Draft audit findings and recommendations and communicate to management for review
- ✓ Agree findings with management and document their response and correction plans
- ✓ Issue auditor's report

Exhibit 3.10 Summary of the audit process.

References

[1] The Complete Guide to Cybersecurity Risks and Controls by Anne Kohnke, Dan Shoemaker & Ken Sigler, CRC Press.

[2] Information Technology Control and Audit (fifth edition) by Angel R. Otero, CRC Press.

[3] Weiss, M., & Solomon, M. G. (2015). Auditing IT infrastructures for compliance. Jones & Bartlett Publishers.

[4] https://www.linkedin.com/pulse/how-improve-organizational-effectiveness-using-caats-wail/

Truth, Transparency and Tactics Are the Characteristics of a good Auditor