CISSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 5

Identity and Access Management

INSIDE CLOUD AND SECURITY

INTRODUCTION: CISSP EXAM DOMAINS

DOMAINS	WEIGHT
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	14%
5. Identity and Access Management	**13%**
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	10%

Exam Outline

5.1 Control physical and logical access to assets

5.2 Manage identification and authentication of people, devices, and services

5.3 Federate identity with a third-party service

5.4 Implement and manage authorization mechanisms

5.5 Manage the identity and access provisioning lifecycle

5.6 Implement authentication systems

WHAT'S NEW IN DOMAIN 5?

5.6 Implement authentication systems

- OpenID Connect (OIDC) / Open Authorization (OAuth)
- Security Assertion Markup Language (SAML)
- Kerberos
- Remote Authentication Dial-In User Service (RADIUS) / Terminal Access Controller Access Control System Plus (TACACS+)
- Certificate Authentication

new sub-domain, existing topics = greater focus

DOMAIN 5: CERTIFICATE-BASEDAUTHENTICATION

Digital certificates may be used as an authentication technique for user, service, and device identities

certificates used in this process are similar to those that you use to secure websites

certificates have both a public and private key

certificates usually issued by a certification authority in a public key infrastructure (PKI)

See key exchange example “asymmetric cryptography” in the **Domain 3: Security Architecture and Engineering** session.

AAA PROTOCOLS

Several protocols provide centralized **authentication**, **authorization**, and **accounting** services.

Network Access Server
is a client to a RADIUS server, and the RADIUS server provides AAA services.

RADIUS (remote access)
uses UDP and encrypts the password only.

TACACS+ (admin access to network devices)
uses TCP and encrypts the entire session.

Diameter (4G)
is based on RADIUS and improves many of the weaknesses of RADIUS, but Diameter is not compatible with RADIUS.

Network access (or remote access) systems use AAA protocols.

ACTIVE DIRECTORY

Pass-the-hash = NTLM

Pass-the-ticket = Kerberos

Kerberos

primary purpose is authentication, as it allows users to prove their identity.

also provides a measure of confidentiality and integrity using symmetric key encryption, but these are not its primary purpose.

does not include logging capabilities so it does not provide accountability.

Common Kerberos attacks include replay, pass-the-ticket, golden ticket, and kerberoasting

AUTHORIZATION MECHANISMS

Need to Know

This principle ensures that subjects are granted access only to what they *need to know* for their work tasks and job functions. Subjects with clearance to access is only granted if they actually need it to perform a job.

Least Privilege

ensures that subjects are granted only the privileges they need to perform their work tasks and job functions. Sometimes lumped together with need to know. The only difference is that least privilege will also include rights to take action on a system.

Separation of Duties and Responsibilities

ensures that sensitive functions are split into tasks performed by two or more employees. Helps prevent fraud and errors by creating a system of checks and balances.

Know these 3 principles for the exam

MODERN APPROACHES TO LEAST PRIVILEGE

more granular approach to **least privilege**

Just-in-time (JIT) (PIM, PAM)

Allows temporary elevation of privilege (usually time-limited) as it's needed, revoking privilege at the end of the allowed window.

Sometimes implemented through **ephemeral accounts** or a **broker and remove access** strategy

IDENTIFICATION AND AUTHENTICATION

Identification

Subjects claim an identity, and identification can be as simple as a username for a user.

Authentication

Subjects prove their identity by providing authentication credentials such as the matching password for a username.

AUTHORIZATION AND ACCOUNTABILITY

Authorization

after authentication

After authenticating subjects, systems authorize access to objects based on their proven identity.

Accountability

provides proof

Auditing logs and audit trails record events including the identity of the subject that performed an action.

identification + authentication + auditing = ACCOUNTABILITY

PRIMARY AUTHENTICATION FACTORS

MFA

Something you **know** (pin or password)

Something you **have** (trusted device)

Something you **are** (biometric)

PRIMARY AUTHENTICATION FACTORS

Multifactor Authentication

includes two or more authentication factors

more secure than using a single authentication factor.

passwords are the weakest form of authentication,

password policies help increase their security by enforcing complexity and history requirements.

Smartcards include microprocessors and cryptographic certificates

tokens create onetime passwords

Biometric methods identify users based on characteristics such as fingerprints.

know "crossover error rate"

BIOMETRICS

a method of authentication using an individual's physical characteristics, which are unique to the individual.

Fingerprint Scanner
Fingerprint scanners are now very common, and used not only in MFA, but various travel, financial, and legal situations.

Retina Scanner
With appropriate lighting, the retina can be accurately identified as the blood vessels of the retina absorb light more readily than the surrounding tissue.

BIOMETRICS

a method of authentication using an individual's physical characteristics, which are unique to the individual.

Iris Scanner
Confirms the identity of the user by scanning of their iris.

Both retina and iris scanners are physical devices.

Voice Recognition
The voice patterns can be stored in a database and used for authentication.

BIOMETRICS

a method of authentication using an individual's physical characteristics, which are unique to the individual.

Facial Recognition

Looks at the shape of the face and characteristics such as mouth, jaw, cheekbone, and nose.

Light and angle/direction can be a factor, especially in software.

Microsoft facial recognition, called **Windows Hello**, was released with Windows 10.

It uses a special USB infrared camera and, as such, is better than other facial recognition programs that can have problems with light.

BIOMETRICS

a method of authentication using an individual's physical characteristics, which are unique to the individual.

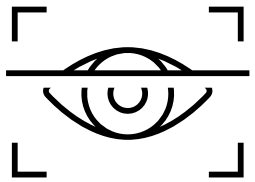
Vein

Using blood vessels in the palm can be used as a biometric factor of authentication.

Gait Analysis

gait is the way an individual walks. Identification and/or authentication using gait is possible even with lower resolution video

BIOMETRIC AUTHENTICATION FAILURES



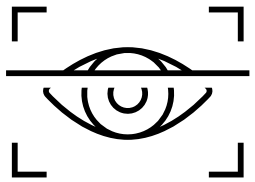
Crossover Error Rate

Biometric methods identify users based on characteristics such as fingerprints.

The **crossover error rate** identifies the accuracy of a biometric method.

It shows where the false rejection rate is equal to the false acceptance rate.

BIOMETRICS



Crossover Error Rate

A **false acceptance** occurs when an invalid subject is authenticated. Type 2 error

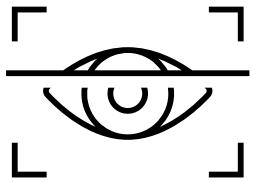
Sometimes called a false positive authentication.

A **false rejection** occurs when a valid subject is rejected. Type 1 error

Sometimes called a false negative authentication.

False rejection is undesirable, but false acceptance is worse

BIOMETRICS



Crossover Error Rate

A **false acceptance** occurs when an invalid subject is authenticated. Type 2 error

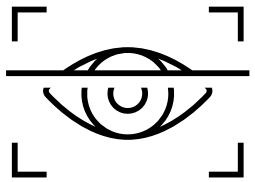
Sometimes called a false positive authentication.

A **false rejection** occurs when a valid subject is rejected. Type 1 error

Sometimes called a false negative authentication.

For the exam, remember **FAR=false acceptance rate** and **FRR=false rejection rate**.

BIOMETRICS



Crossover Error Rate

Biometric methods identify users based on characteristics such as fingerprints.

The **crossover error rate (CER)** identifies the accuracy of a biometric method.

It shows where the false rejection rate is equal to the false acceptance rate.

to move the CER higher or lower, you can increase or decrease the sensitivity of the biometric device.

SINGLE SIGN-ON

is a mechanism that allows subjects to authenticate once and access multiple objects without authenticating again.

Common SSO methods/standards include:

- SAML
- SESAME
- KryptoKnight
- OAuth
- OpenID

Know the high-level scenario where each of these fit!

The three to know for the exam are **SAML**, **Oauth 2.0**, and **OpenID**.

SAML, OAUTH, AND OPENID

Security Assertion Markup Language (SAML)

is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. common in federation scenarios

OAuth 2.0 developed by IETF updated thru RFC

is an open standard for authorization, commonly used as a way for Internet users to log into third party websites using their Microsoft, Google, Facebook, Twitter, One Network etc. accounts without exposing their password.

OpenID managed through OpenID foundation

is an open standard, It provides decentralized authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a third-party service referred to as an OpenID provider.

AAA PROTOCOLS

Several protocols provide centralized **authentication**, **authorization**, and **accounting** services.

Network Access Server
is a client to a RADIUS server, and the RADIUS server provides AAA services.

RADIUS
uses UDP and encrypts the password only.

TACACS+
uses TCP and encrypts the entire session.

Diameter
is based on RADIUS and improves many of the weaknesses of RADIUS, but Diameter is not compatible with RADIUS.

Network access (or remote access) systems use AAA protocols.

IDENTITY AND ACCESS PROVISIONING LIFECYCLE

The ***identity and access provisioning lifecycle*** refers to the creation, management, and deletion of accounts.

accounts should be deprovisioned promptly on separation

AUTHORIZATION MECHANISMS

Access control models use many different types of **authorization mechanisms**, or methods to control who can access specific objects

Implicit Deny

A basic principle of access control is *implicit deny* and most authorization mechanisms use it. The implicit deny principle ensures that access to an object is denied unless access has been explicitly granted to a subject.

Access Control Matrix

a table that includes subjects, objects, and assigned privileges. When a subject attempts an action, the system checks the access control matrix to determine if the subject has the appropriate privileges to perform the action.

Remember subjects and objects? (domain 3)

AUTHORIZATION MECHANISMS

Access control models use many different types of **authorization mechanisms**, or methods to control who can access specific objects

Capability Tables

are another way to identify privileges assigned to subjects. They are different from ACLs in that a capability table is focused on subjects (such as users, groups, or roles).

Constrained Interface

use constrained interfaces or restricted interfaces to restrict what users can do or see based on their privileges. Users with full privileges have access. Applications constrain the interface using different methods.

Content-Dependent Control

restrict access to data based on the content within an object. A database view is a content-dependent control.

AUTHORIZATION MECHANISMS

Access control models use many different types of **authorization mechanisms**, or methods to control who can access specific objects

Context-Dependent Control

require specific activity before granting users access.

example: data flow for a transaction selling digital products

AUTHORIZATION MECHANISMS

Need to Know

This principle ensures that subjects are granted access only to what they *need to know* for their work tasks and job functions. Subjects with clearance to access is only granted if they actually need it to perform a job.

Least Privilege

ensures that subjects are granted only the privileges they need to perform their work tasks and job functions. Sometimes lumped together with need to know. The only difference is that least privilege will also include rights to take action on a system.

Separation of Duties and Responsibilities

ensures that sensitive functions are split into tasks performed by two or more employees. Helps prevent fraud and errors by creating a system of checks and balances.

Know these 3 principles for the exam

ACCESS CONTROL MODELS

Discretionary Access Control

A key characteristic of the Discretionary Access Control (DAC) model is that every object has an owner, and the owner can grant or deny access to any other subjects.

Example: New Technology File System (NTFS),

Role Based Access Control

A key characteristic is the use of roles or groups. Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles. Typically mapped to job roles.

Rule-based access control

A key characteristic is that it applies global rules that apply to all subjects. Rules within this model are sometimes referred to as **restrictions** or **filters**.

example: a firewall uses rules that allow or block traffic to all users equally.

ACCESS CONTROL MODELS

Attribute Based Access Control

A key characteristic of this model is its use of rules that can include multiple attributes. This allows it to be much more flexible than a rule-based access control model that applies the rules to all subjects equally.

often used by software-defined networks (SDNs)

Mandatory Access Control

A key characteristic this model is the use of labels applied to both subjects and objects. For example, if a user has a label of top secret, the user can be granted access to a top-secret document. In this example, both the subject and the object have matching labels.

referred to as a lattice-based model.

SECURITY CONTROLS

Security controls, countermeasures, and safeguards can be implemented administratively, logically/technically, or physically.

Types of security controls include

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

Categories of controls include

- Logical/Technical
- Physical
- Administrative

The three primary control types are **preventative**, **detective**, and **corrective**.

CATEGORIES OF SECURITY CONTROLS

Logical / Technical

the hardware or software mechanisms used to manage access to resources and systems and provide protection for those resources and systems.

EXAMPLES: encryption, smart cards, passwords, biometrics, constrained interfaces, access control lists (ACLs), protocols, firewalls, routers, intrusion detection systems, and clipping levels.

Physical

security mechanisms focused on providing protection to the facility and real-world objects.

EXAMPLES: guards, fences, motion detectors, locked doors, sealed windows, lights, cable protections, laptop locks, swipe cards, guard dogs, video cameras, mantraps, and alarms.

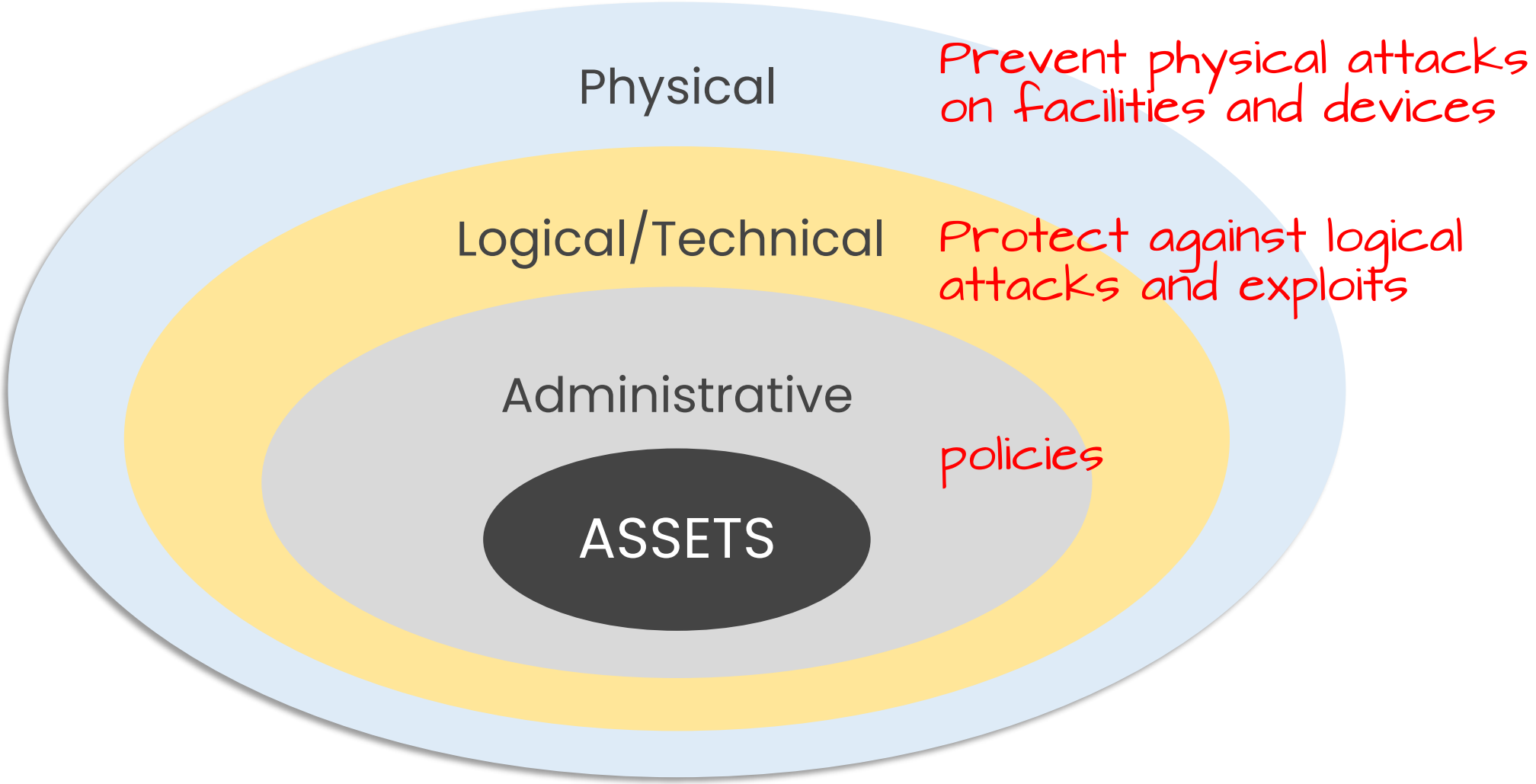
CATEGORIES OF SECURITY CONTROLS

Administrative

policies and procedures defined by an organizations security policy to implement and enforce overall access control. Focus on two areas: personnel and business practices.

EXAMPLES: policies, procedures, hiring practices, background checks, data classification, security training, vacation history, reviews, work supervision, personnel controls, and testing.

SECURITY CONTROLS



TYPES OF SECURITY CONTROLS

Security controls, countermeasures, and safeguards can be implemented administratively, logically/technically, or physically.

Types of security controls include

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

Categories of controls include

- Logical/Technical
- Physical
- Administrative

The three primary control types are **preventative**, **detective**, and **corrective**.

TYPES OF SECURITY CONTROLS

Preventative

deployed to stop unwanted or unauthorized activity from occurring.

EXAMPLES: fences, locks, biometrics, mantraps, alarm systems, job rotation, data classification, penetration testing, access control methods,

Detective

deployed to discover unwanted or unauthorized activity. Often are after-the-fact controls rather than real-time controls.

EXAMPLES: security guards, guard dogs, motion detectors, job rotation, mandatory vacations, audit trails, intrusion detection systems, violation reports, honey pots, and incident investigations,

TYPES OF SECURITY CONTROLS

Corrective

deployed to restore systems to normal after an unwanted or unauthorized activity has occurred, such as a security incident.

EXAMPLES: intrusion detection systems, antivirus solutions, alarms, mantraps, business continuity planning, and security policies,

Compensating

deployed to provide options to other existing controls to aid in the enforcement and support of a security policy.

EXAMPLES: a disaster recovery plan with an alternate office location in the event fire suppression fails and building is damaged

TYPES OF SECURITY CONTROLS

Directive

deployed to direct, confine, or control the actions of subject to force or encourage compliance with security policies.

EXAMPLES: security guards, guard dogs, security policy, posted notifications, escape route exit signs, monitoring, supervising, work task procedures, and awareness training.

Recovery

deployed to repair or restore resources, functions, and capabilities after a violation of security policies. more advanced or complex capability to respond to access violations than a corrective access control.

EXAMPLES: backups and restores, fault tolerant drive systems, server clustering, antivirus software, and database shadowing.

TYPES OF SECURITY CONTROLS

Deterrent

deployed to discourage the violation of security policies. A deterrent control picks up where prevention leaves off.

EXAMPLES: locks, fences, security badges, security guards, mantraps, security cameras, trespass or intrusion alarms, separation of duties, awareness training, encryption, auditing, and firewalls.

RISK ELEMENTS

Basic elements of risk

Risk

is the possibility or likelihood that a threat can exploit a vulnerability and cause damage to assets.

Asset valuation

identifies value of assets, threat modeling identifies threats against these assets.

Vulnerability analysis

identifies weaknesses in an organization's valuable assets.

ACCESS CONTROL ATTACKS

Dictionary attacks

These are programs with built in dictionaries. They would use all dictionary words to attempt and find the correct password, in the hope that a user would have used a standard dictionary word.

Brute force

This type of attack is attempting to break the password by trying all possible words.

Password complexity and attacker tools/compute determine efficacy

Spoofed logon screens

The last access control attack is to implement a fake logon screen, and when a user attempts to login, the logon screen will send the username and password to the hacker.

ACCESS CONTROL ATTACKS

Sniffer Attacks

In a sniffer attack (or snooping attack) an attacker uses a packet-capturing tool (such as a sniffer or protocol analyzer) to capture, analyze, and read data sent over a network.

Attackers can easily read data sent over a network in cleartext.

Encrypting data in transit stops this type of attack.

Spoofing Attacks

Spoofing is pretending to be something or someone else, and it is used in many types of attacks, including access control attacks. Attackers often try to obtain the credentials of users so that they can spoof the user's identity.

Spoofing attacks include email spoofing, phone number spoofing, and IP spoofing.

Many phishing attacks use spoofing methods.

ACCESS CONTROL ATTACKS

Social Engineering

an attempt by an attacker to convince someone to provide info (like a password) or perform an action they wouldn't normally perform (such as clicking on a malicious link)

Social engineers often try to gain access to the IT infrastructure or the physical facility.

Best defense is security awareness training (user education)

Phishing

commonly used to try to trick users into giving up personal information (such as user accounts and passwords), click a malicious link, or open a malicious attachment.

Spear phishing targets specific groups of users.

Whaling targets high-level executives.

Vishing uses VoIP technologies.

phishing is #1 cyber attack!

Know these three variants!

ACCESS CONTROL ATTACKS

Access aggregation

is a type of attack that combines, or aggregates, non-sensitive information to learn sensitive information and is used in reconnaissance attacks.

Know the common access control attacks and how to prevent them!

PREVENTING ACCESS CONTROL ATTACKS

To prevent these type of attacks:

Passwords should be long, complex and changed periodically

There should be a strong password policy in place to enforce.

Also enforcing other measures such as account lockout after X logon attempts, etc.

For spoofed logon screens

The Best prevention is to have secure endpoints, where these fake logon screens cannot be implemented.

OTHER ATTACKS

TEMPEST

allows the electronic emanations that every monitor produces to be read from a distance (effective on CRT monitors).

Shoulder surfing for monitor displays

White Noise

broadcasting false traffic at all times to mask and hide the presence of real emanations.

RFID, Barcoding and Inventory

Can help to prevent and identify device theft, which reduces risk.

ACTIVE DIRECTORY

Kerberos

primary purpose is authentication, as it allows users to prove their identity.

also provides a measure of confidentiality and integrity using symmetric key encryption, but these are not its primary purpose.

does not include logging capabilities so it does not provide accountability.

Replay attacks are a common attack against Kerberos