

Access Controls Concepts for CCSM

Access Controls Concepts



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com



CCSM Certification Examination

Domains	Weights
1. Security Principles	26%
2. Business Continuity (BC), Disaster Recovery (DR), & Incident Response	10%
3. Access Control Concepts	22%
4. Network Security	24%
5. Security Operations	18%



Access Controls Concepts for the CCSM Certification

Agenda:

**Access Controls
Concepts**

**Physical Access
Controls**

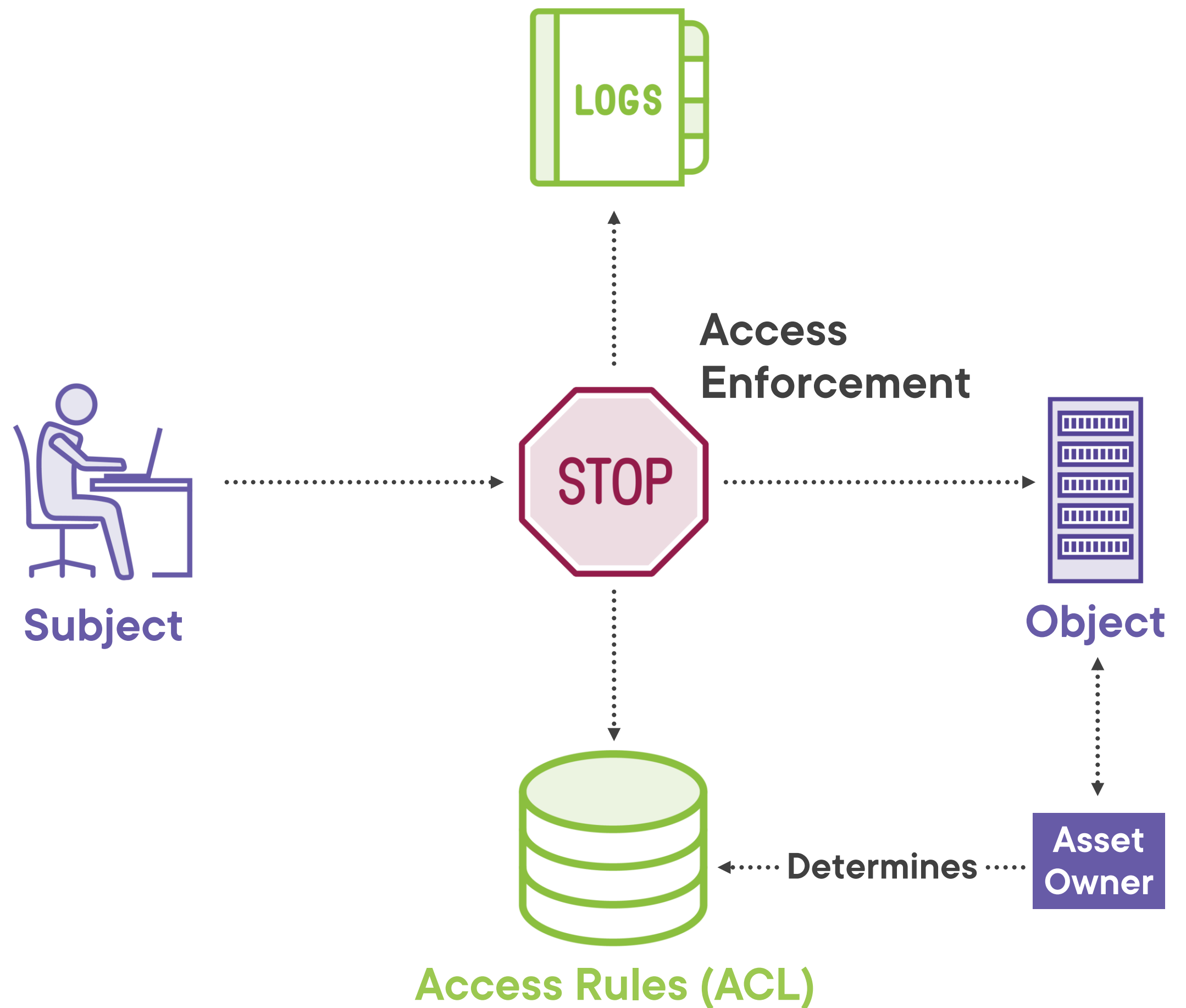
**Logical Access
Controls**



Access Controls Concepts



Access Relationships



Key Concepts

Separation of Duties

Least Privilege

Need-to-Know



Separation of Duties



AKA segregation of duties

Enforced through:

- **Mutual exclusivity**
- **Dual control**
- **Roles**

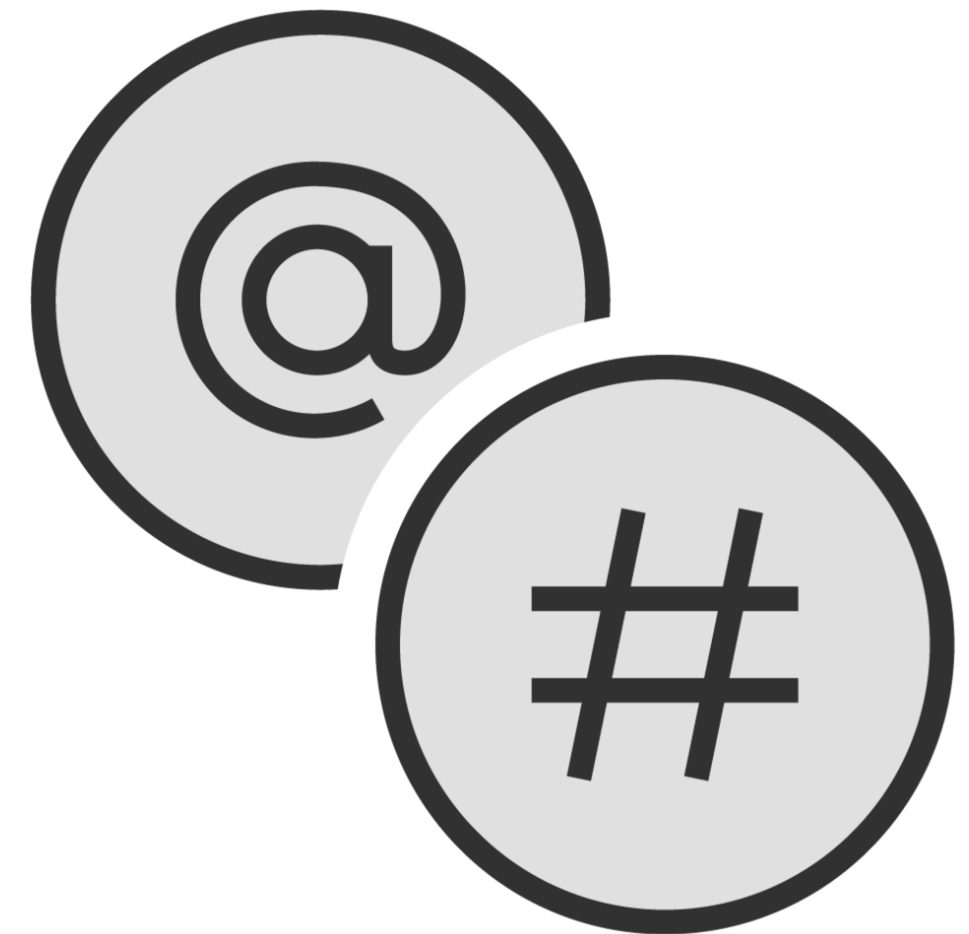
Bypassed by collusion

- **Job rotation**
- **Mandatory vacations**

Identification

Claim of unique identifier

- Account number
- Employee number
- Customer number
- Government issued identifier
- Email address
- User identifier/USER ID
- Process ID





Proofing of Identity

Establish ownership of the identity

- **Secret question**

Password resets

Modification to permissions



Identification



Unique (enables accountability)

Not shared (especially admins)

Secure registration process

- **CAPTCHA**
- **Approval**

Authentication



Authentication



Verify, validate, prove the Identity

- **Proof of possession**
- **Secret question**

What you:

- **Know**
- **Have**
- **Are**

What You Know



Password, passphrase, secret question

- Static value
- Subject to replay attack
- Should be changed on a periodic basis

What You Have



Employee ID badge

Token

Smartcard

Passport



What You Are



Biometrics

Behavioral

Physiological



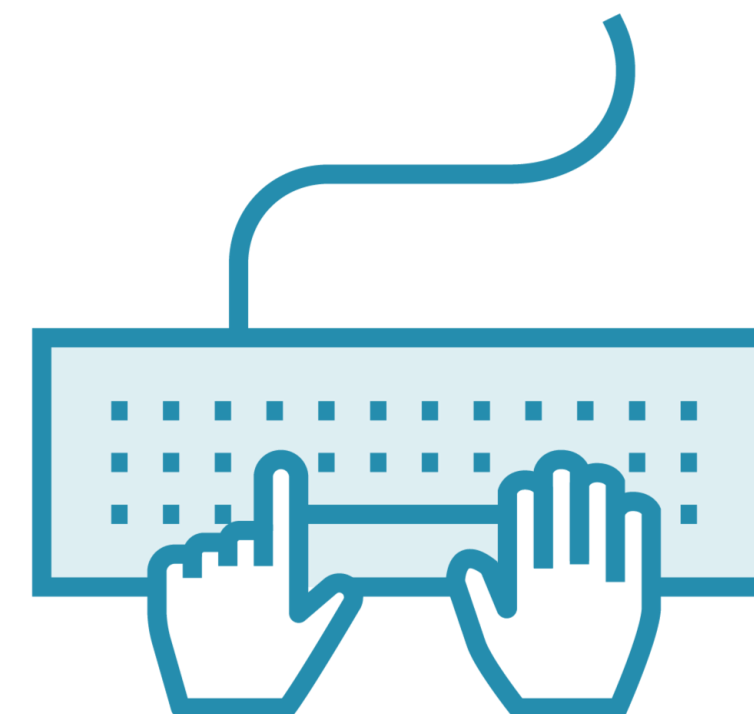
Behavioral Biometrics



Voice print



Signature dynamics



Keystroke dynamics





Physiological Biometrics

Iris scan

Retina scan

Palm print

- Venous scan

Fingerprint

Facial recognition

Biometric Acceptance

User concerns

- Privacy
- Cleanliness
- Delay in processing

Cost

Maintenance/registration



Node Authentication

Authentication based on device:



IP address



MAC address



RFID

**Radio frequency
identification**



Key Points Review

Authentication is the validation of the identity

Authentication is based on three factors:

- **What you know**
- **What you have**
- **What you are**



Authorization and Accounting



Authorization



Rights



Privileges



Permissions



**Granted to an
authenticated
entity**

Permissions



Read, write, update

Execute, create, delete

- Least privilege
- Need to know
- Separation of duties

Unauthorized users cannot make modifications

Authorized cannot make improper modifications

Accounting/Auditing

Tracking and logging all activity on a system

Associate all activity with an identified user or process

Log retention

Regulatory
Business needs



Summary



This module set out the concepts of access controls.

All authorized users should be identified, authenticated, authorized and subject to logging of all actions taken

