3

DOMAIN

TOPIC THREE

Access Control Concepts

22% of the exam · 7 lessons

Who gets access to what, why it is necessary, and how it is managed

AT A GLANCE

The second-heaviest domain

22%

of the exam — second only to Domain 1

7

lessons in this topic

~90

minutes

What makes this domain different

- Domains 1 and 2 were mostly definitional
- This one asks you to SELECT a control for a scenario
- And to name an access control model from a description

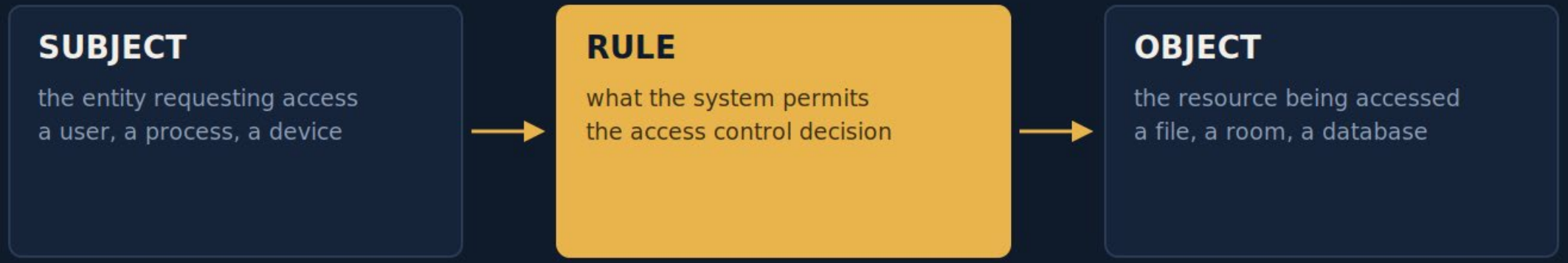
So, the practice changes

- Sorting exercises, not just recall
- Given a described system, name the model
- Given a described risk, choose the control
- Both skills are drilled repeatedly in this deck

THE FOUNDATION

Subject, rule, object

Every access control question is really about these three things.



Change who may set the rule, and you change the access control model.

Why this matters more than it looks

- The three access control models differ only in who is allowed to set the rule — that single question separates DAC, MAC and RBAC

LESSON MAP

The seven lessons

1. **Controls and assessment**
   The three control categories revisited, and how you know a control works

2. **Defence in depth**
   Layered controls, why overlap is deliberate, and what it looks like in practice

3. **Least privilege and PAM**
   Need-to-know, privileged accounts, and the extra controls they require

4. **Separation of duties**
   Splitting transactions, collusion, job rotation, authorised personnel

5. **Physical access controls**
   Deter, authenticate, detect — plus biometrics and monitoring

6. **Logical access controls**
   DAC, MAC, RBAC, ABAC and rule-based, and how to tell them apart

7. **Consolidation**
   Scenario selection practice and the memorisation set

Lesson 6 carries the single most reliably tested skill in the domain: naming the model from a description.

3.1

LESSON

Controls and Assessment

OBJECTIVE

Re-apply the three control categories to access, and explain how an organisation knows a control is actually working.

- Technical, administrative and physical — applied to access
- What a control is for: subject, rule, object
- Control assessment: testing, auditing, reviewing
- Why an unassessed control is an assumption

LESSON 3.1

Access control is the applied form of Domain 1

The three categories you learned as theory now have a specific job:
deciding who reaches what.

- TECHNICAL — access control lists, permissions, authentication systems, encryption
- ADMINISTRATIVE — access request procedures, approval workflows, periodic reviews, policy
- PHYSICAL — locks, badge readers, guards, barriers, cameras
- Same three categories, same sorting rule: classify by the mechanism doing the work

LESSON 3.1 — PURPOSE

What access controls are actually for

The three things they protect

- Confidentiality — keeping the wrong subject from reading an object
- Integrity — keeping the wrong subject from changing it
- Availability — making sure the right subject is NOT blocked
- That third one is easy to forget when designing controls

The failure modes

- Too permissive — unauthorised access succeeds
- Too restrictive — legitimate work is blocked, and users route around the control
- Users routing around a control is itself a security failure
- A control nobody can work with will be disabled, shared or bypassed

LESSON 3.1 — ASSESSMENT

How you know a control works

Assessment methods

- Testing — try the control and see if it holds
- Auditing — check records against policy
- Access reviews — confirm current access is still warranted
- Penetration testing — an adversarial attempt
- Monitoring — continuous rather than periodic

What assessment finds

- Access that was granted and never removed
- Accounts belonging to people who have left
- Permissions accumulated through role changes — "privilege creep"
- Controls that were configured once and drifted
- Controls that were never actually switched on

The principle

- An unassessed control is an assumption. This is the same argument as the untested backup in Domain 2, applied to access

3.2

LESSON

Defence in Depth

OBJECTIVE

Explain why controls are layered, identify the layers in a described environment, and say why overlap is deliberate.

- The principle, and the asymmetry it creates
- The layers, from policy down to data
- Why layers should differ in kind
- What it looks like in a real environment

LESSON 3.2

Layers, not a wall

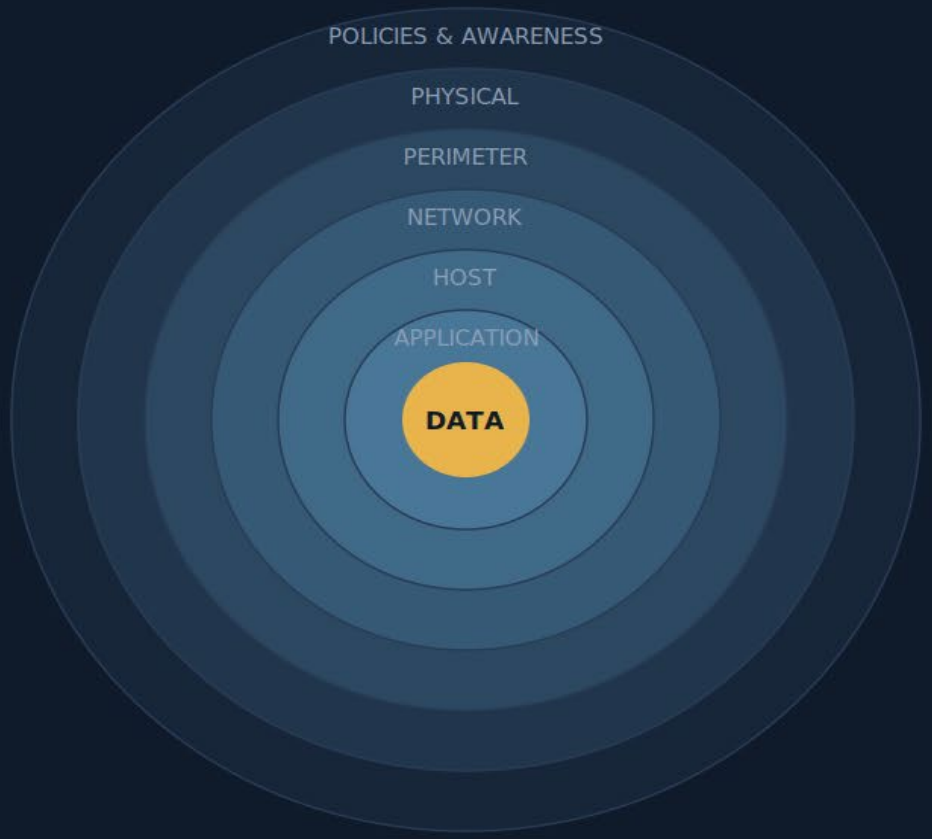
No single control is trusted to work alone.

The principle

An attacker must defeat every layer. A defender only needs one to hold. Layers should differ in kind, not just in quantity.

In practice

A locked server room AND an ACL AND encryption AND monitoring. Redundant on purpose — overlap is the point, not waste.



LESSON 3.2 — THE RULE

Layers must differ in kind

Three firewalls in a row is not defence in depth.
It is one control, three times.

- Layers should fail for DIFFERENT reasons
- A password and a second password fail to the same phishing email
- A badge reader and an encrypted disk fail to nothing in common — that is depth
- This is the same logic as multi-factor authentication from Domain 1, applied to architecture

LESSON 3.2 — IN PRACTICE

One asset, several layers

A customer database in a data centre.

Policy defines who may access it · a locked facility and server cage · network segmentation and a firewall · host hardening · application authentication · database permissions · encryption at rest · monitoring across all of it.

An attacker phishes a valid user's password.

The password layer failed. MFA, network restrictions, database permissions and monitoring are all still standing — which is exactly why they exist.

A contractor is escorted into the server room and left alone.

The physical layer was defeated by an administrative failure. Layers are only as good as the procedures around them.

A company buys an expensive next-generation firewall and skips access reviews.

Depth in one dimension, nothing in another. Spending concentrated in one layer is a common and expensive mistake.

3.3

LESSON

Least Privilege and Privileged Access

OBJECTIVE

Apply least privilege to a described situation, explain why privileged accounts need different controls, and list what PAM adds.

- Least privilege and need-to-know
- Privilege creep, and why access reviews exist
- What makes a privileged account different in kind
- The controls PAM adds on top

LESSON 3.3 — LEAST PRIVILEGE

Least privilege

Every subject gets the minimum access needed to do the job — and no more.

- Minimum RIGHTS: read where reading is enough, not write
- Minimum SCOPE: this project's files, not the whole share
- Minimum DURATION: for the length of the task, not permanently
- Need-to-know is the related idea: having clearance does not mean having a reason

LESSON 3.3 — EXAMPLES

Least privilege applied

A helpdesk technician needs to reset passwords but not read email.

Grant password-reset rights only. A broad administrator account would exceed what the job needs.

An accountant moves from payables to receivables and keeps both sets of access.

Privilege creep. The old access should have been removed with the role change — this is exactly what access reviews catch.

A developer needs production data to debug an issue this afternoon.

Time-limited, logged access to the minimum dataset — not standing production access. Better still, masked data.

An employee with top-secret clearance asks to see an unrelated classified project.

Refused on need-to-know. Clearance establishes trustworthiness; it does not establish a reason.

Privileged accounts are different in kind

Privileged accounts are not just bigger accounts. They need different controls.

A NORMAL USER ACCOUNT

Least privilege by default
Access to own work only
Standard authentication
Ordinary logging
Removed at offboarding

A PRIVILEGED ACCOUNT

Can change the system itself
Can alter or delete logs
Can create other accounts
Can bypass many controls
A single compromise is catastrophic

Privileged Access Management adds:

- Separate admin account from daily-use account
- Credential vaulting and check-out
- Just-in-time elevation, not standing access
- Multi-factor authentication, always
- Session recording and enhanced logging
- Keep the number of holders small and reviewed

LESSON 3.3 — ACCOUNT TYPES

Know these account types

By purpose

- User — a normal named individual
- Privileged / administrative — can change the system
- Service — used by an application, not a person
- Guest — limited, temporary, often anonymous
- Shared — used by several people, and best avoided

Why shared accounts keep coming up

- They destroy non-repudiation (Domain 1)
- They cannot be tied to an individual in an audit
- They are rarely changed when someone leaves
- Service accounts are the legitimate exception — they belong to a system, and need their own controls and rotation

3.4

LESSON

Separation of Duties and Authorised Personnel

OBJECTIVE

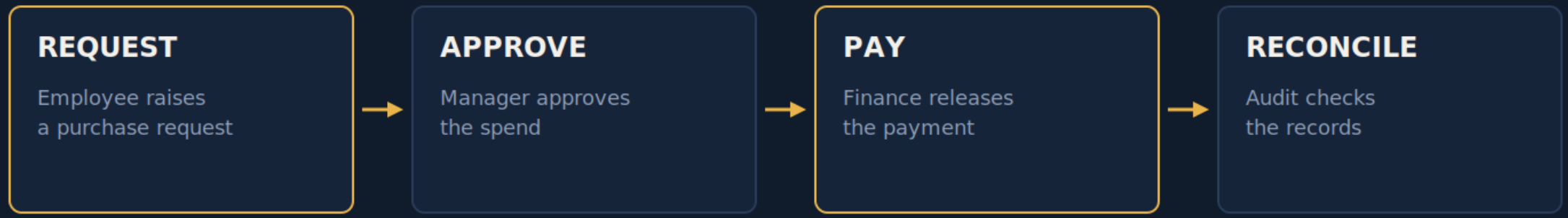
Explain how splitting a transaction reduces risk, name the related controls, and describe how authorised and unauthorised personnel are distinguished.

- Separation of duties, and collusion
- Two-person control, split knowledge, job rotation, mandatory vacation
- Authorised versus unauthorised personnel
- Visitors, escorts and tailgating

LESSON 3.4

No one person owns the whole transaction

No single person controls a whole transaction end to end.



Fraud now requires collusion

Related controls: two-person control, split knowledge, job rotation, mandatory vacation.

- The control does not make fraud impossible — it makes it require agreement between people, which is far rarer and far more detectable

LESSON 3.4 — RELATED CONTROLS

Four controls in the same family

Two-person control	A single action requires two people acting together — the classic example being two keys turned at once. Sometimes called dual control.
Split knowledge	No one person holds the whole secret. Two halves of a password or key, held separately.
Job rotation	Staff move between roles periodically. Fraud that depends on one person staying in one seat becomes hard to sustain, and it also builds cover.
Mandatory vacation	Enforced time away. Ongoing schemes that need daily maintenance tend to surface while the person is absent.

All four exist to make wrongdoing require either collusion or continuity — and to remove both.

Authorised versus unauthorised

Establishing who is authorised

- Badges and visible photo ID
- Access lists tied to specific areas
- Visitor logs — signed in, signed out
- Escort requirements for visitors and contractors
- Distinct badge colours for staff, contractors, visitors

Where it goes wrong

- Tailgating / piggybacking — following an authorised person through a door
- Propped-open doors and disabled alarms
- Contractors left unescorted after being signed in
- Badges not collected at offboarding
- Staff reluctant to challenge a stranger — which is a training problem, not a technology one

3.5

LESSON

Physical Access Controls

OBJECTIVE

Compare physical access controls, choose one appropriate to a scenario, and interpret biometric error rates.

- Three jobs: deter and delay, authenticate, detect and respond
- Locks, barriers, vestibules and turnstiles
- Biometrics and the FAR / FRR / CER relationship
- Monitoring — guards, cameras, alarms, sensors

LESSON 3.5

Physical controls do three jobs

Physical controls work in three jobs. Most real sites use all three.

DETER & DELAY

Fences, walls, bollards
Gates and turnstiles
Lighting and signage
Landscaping (CPTED)
Locks: key, combination, electronic, cipher

AUTHENTICATE

Badges and photo ID
Proximity and smart cards
PIN pads
Biometrics: fingerprint, iris, face, palm
Access control vestibule (mantrap)

DETECT & RESPOND

Security guards
CCTV cameras
Alarms and sensors
Motion and glass-break
Visitor logs and escorts
Patrols

Tailgating / piggybacking

Following an authorised person through a door. A control FAILURE, not a control — and the reason vestibules and turnstiles exist.

Most sites use all three. A question asking for the BEST control usually wants the job that matches the described problem.

LESSON 3.5 — VESTIBULES

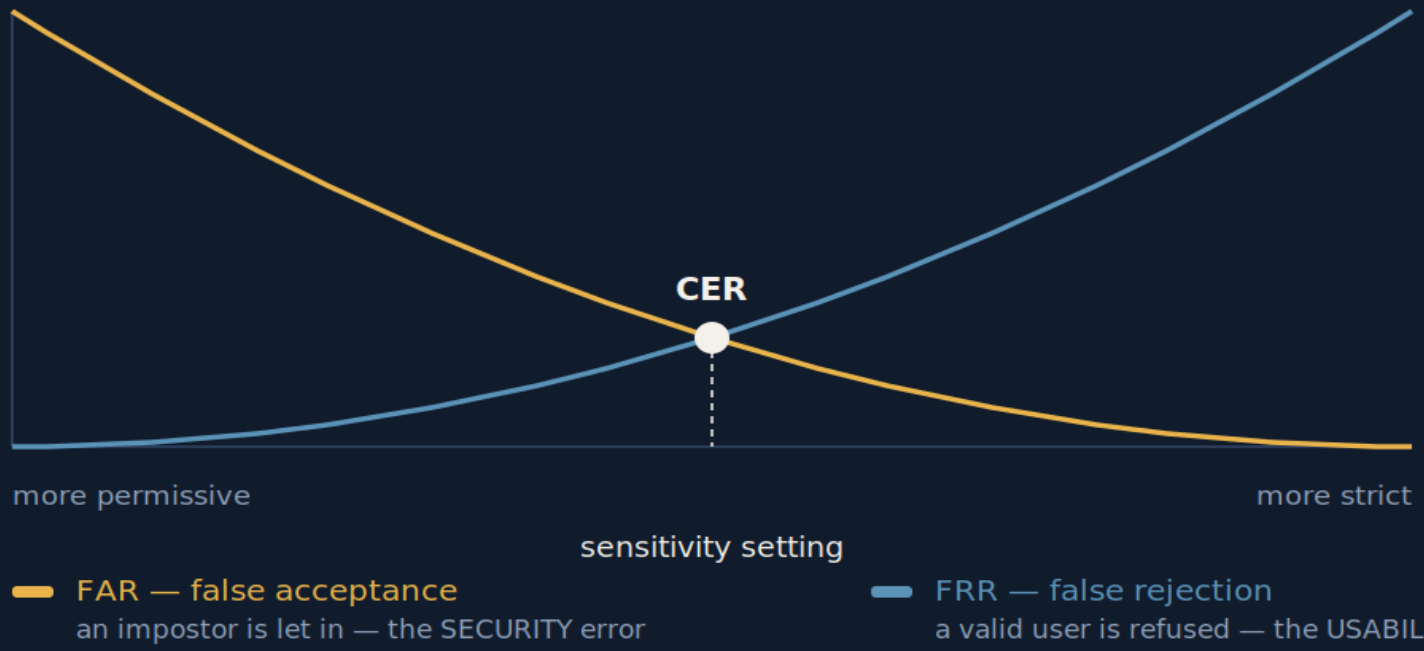
The access control vestibule

Two doors, one at a time. The second will not open until the first has closed.

- Also known as a mantrap
- Its whole purpose is defeating tailgating — one authorised entry admits exactly one person
- Often paired with a weight sensor or a guard station
- If a scenario describes people following others through a door, this is the control being tested

FAR, FRR and the crossover

Tighten a biometric system and you trade one error for the other.



CER (crossover error rate) is where FAR and FRR meet — the standard way to compare two systems.

Lower CER = better system. A high FAR is the dangerous direction.

LESSON 3.5 — BIOMETRIC TRADE-OFFS

Choosing and tuning biometrics

What biometrics are good at

- Cannot be forgotten or lent to a colleague
- Hard to duplicate compared with a badge
- Convenient at high-traffic doors

What they cost you

- Cannot be reissued after compromise (Domain 1)
- Measurable error rates in both directions
- Privacy concerns and regulatory weight
- Environmental sensitivity — wet hands, gloves, injuries, lighting
- Expensive relative to a card reader

The tuning decision

- A high-security vault tolerates a high FRR to keep FAR near zero. A busy staff entrance cannot, so it accepts a higher FAR and adds a second factor

LESSON 3.5 — MONITORING

Watching, and being seen to watch

Guards

- Can exercise judgement
- Can respond, not just record
- Deter by presence

- Expensive; inconsistent; can be socially engineered

Cameras (CCTV)

- Record for later investigation
- Deter when visible
- Cover more ground than guards

- Do not intervene; need someone to watch or review them

Alarms and sensors

- Motion, door contact, glass-break
- Detect and escalate automatically
- Cheap to cover many points

- False alarms erode response; useless without a response plan

A camera nobody reviews is a deterrent, not a detective control. The exam expects you to know the difference.

3.6

LESSON

Logical Access Controls

OBJECTIVE

Describe logical access controls and name the access control model from a description of how access decisions are made.

- What counts as a logical control
- DAC, MAC and RBAC — who sets the rule
- ABAC and rule-based as the additional two
- Provisioning and deprovisioning

LESSON 3.6

Logical controls enforce the rule in software

Same subject, same object, same rule — now enforced by code rather than a door.

- Passwords, tokens, biometrics used for system login
- Access control lists and file permissions
- Firewall rules and network segmentation
- Encryption, which denies the object even when access succeeds
- Account lockout, session timeout, screen locks

Three models, one discriminator

The exam gives you a description and asks for the model. The discriminator is WHO SETS THE RULE.

DAC
Discretionary

The OWNER of the resource decides who gets access

File sharing, NTFS permissions

Most flexible, least consistent

MAC
Mandatory

The SYSTEM enforces access using labels and clearances

Classified military and government systems

Most restrictive, least flexible

RBAC
Role-Based

Access follows the JOB FUNCTION, not the individual

Most business systems; HR-driven provisioning

Scalable; watch for role explosion

Also know: ABAC (attributes — department, time, device) and Rule-Based (conditions applied to everyone, e.g. firewall ACLs).

Ask one question: who is allowed to set the rule? The owner, the system, or the job description.

LESSON 3.6 — DAC

Discretionary Access Control

Who decides	The owner of the resource. If you create a file, you choose who else may see it.
Where you see it	Shared drives, NTFS permissions, cloud file sharing, most consumer systems.
Strength	Flexible and fast — no administrator needed for routine sharing.
Weakness	Inconsistent. Access decisions are spread across every user, so nobody has an overall picture, and a careless owner can over-share.

Cue words in a question: "the file's owner grants", "users can share their own", "at the creator's discretion".

LESSON 3.6 — MAC

Mandatory Access Control

Who decides	The system, using labels on objects and clearances on subjects. Neither the owner nor the user can override it.
Where you see it	Classified military and government systems; some high-assurance operating systems.
Strength	The most restrictive and the most consistent. Policy is enforced centrally and uniformly.
Weakness	Inflexible and administratively heavy. Sharing outside the label scheme is difficult by design.

Cue words: "classification", "clearance", "label", "the system enforces regardless of the owner".

LESSON 3.6 — RBAC

Role-Based Access Control

Who decides	The organisation, by defining roles. Access attaches to the role; people attach to roles.
Where you see it	Most business systems. Commonly driven from HR — a job title change updates access.
Strength	Scales well. Onboarding, transfers and offboarding become role changes rather than permission audits.
Weakness	Role explosion — organisations end up with hundreds of near-identical roles. And a role granted too broadly over-privileges everyone in it.

Cue words: "all nurses can", "based on job function", "when she was promoted her access changed automatically".

LESSON 3.6 — THE OTHER TWO

ABAC and rule-based

ABAC — Attribute-Based

- Decisions use attributes of the subject, object, action and context
- "A manager, in the finance department, on a corporate device, during working hours"
- The most granular and the most complex to administer
- Increasingly common in cloud environments

Rule-Based

- Conditions applied uniformly to everyone, regardless of identity or role
- A firewall ACL is the standard example: block this port, from anywhere, always
- Time-of-day restrictions on a door apply the same way
- Not to be confused with role-based — the names are close and the exam knows it

LESSON 3.6 — LIFECYCLE

Provisioning and deprovisioning

Provisioning

- A request, an approval, and a record of both
- Granted against a role or a documented need
- Approved by someone with authority — not by the requester
- The account and its access are documented at creation

Deprovisioning

- The step organisations habitually fail at
- Access removed promptly on departure or role change
- Badges, tokens and keys physically returned
- Shared credentials the person knew must be changed
- An orphaned account with valid credentials and no owner is one of the most dangerous artefacts in any environment

And in between

- Periodic access review — does this person still need this? This is where privilege creep gets caught

3.7

LESSON

Consolidation

OBJECTIVE

Name the model from any description, select an appropriate control for a scenario, and produce the memorisation set from memory.

- Model identification drill
- Control selection drill
- The memorisation set
- Common traps

LESSON 3.7 — DRILL 1

Name the model

"All ward nurses can view patient charts"

RBAC — access follows job function

"Access allowed only on managed devices, in hours"

ABAC — contextual attributes

"Documents are labelled Secret; only cleared staff open them"

MAC — labels and clearances

"Her access changed automatically on promotion"

RBAC — role change drove it

"Ravi created the folder and chose who could see it"

DAC — the owner decided

"The system refuses even though the owner approved"

MAC — the owner cannot override

"Port 23 is blocked for everyone, always"

Rule-based — a condition, not an identity

"Staff share their own files at their discretion"

DAC — discretion is the giveaway

Cover the amber answers and work down. Anything missed goes in the error log with its lesson number.

LESSON 3.7 — DRILL 2

Choose the control

People follow staff through the secure door

Access control vestibule or turnstile

Staff accumulate access as they change roles

Periodic access review

Leavers' accounts stay active for months

Deprovisioning process + access review

Contractors wander unescorted

Escort policy + visitor badges and logs

One clerk raises and approves payments

Separation of duties

A stolen laptop exposes client files

Encryption at rest — physical control failed

Admins use one shared root login

Individual privileged accounts + PAM

No record of who entered the server room

Badge logging + CCTV, reviewed

Note the pattern: several answers are administrative, not technical. The best control is often a process.

LESSON 3.7 — MEMORISE

Produce these, don't just recognise them

The models

- DAC — owner decides
- MAC — system decides, by label
- RBAC — job function decides
- ABAC — attributes and context
- Rule-based — same condition for all

- Discriminator: who sets the rule

The principles

- Least privilege — minimum rights, scope and duration
- Need-to-know — clearance is not a reason
- Separation of duties — split the transaction
- Defence in depth — layers differing in kind

- Two-person control, split knowledge, job rotation, mandatory vacation

Physical and biometric

- Three jobs: deter and delay, authenticate, detect and respond
- Vestibule / mantrap defeats tailgating

- FAR — impostor admitted (security error)
- FRR — valid user refused (usability error)
- CER — where they cross; lower is better

Also: tailgating is a control failure, not a control. And a camera nobody reviews is a deterrent, not a detective control.

COMMON TRAPS

Where marks get lost

Rule ≠ role

- Rule-based applies a condition to everyone
- Role-based attaches access to a job function
- The names are nearly identical and the exam uses that

Clearance ≠ reason

- Clearance says you are trustworthy
- Need-to-know says you have a reason
- Both are required under MAC

Tailgating

- It is the attack that vestibules exist to stop
- If an option offers it as a control, it is wrong

Technology first

- Many correct answers here are administrative
- Access reviews, escort policy, separation of duties
- Read for what the described problem actually is

And: assuming a hot answer. "Biometrics" is not automatically the strongest choice — cost, FRR and irrevocability all matter.

EXAM TECHNIQUE

How this domain is tested

1	**Name the model**	Given a description of how decisions are made, identify DAC, MAC, RBAC, ABAC or rule-based. Ask who sets the rule.
2	**Select the control**	Given a described weakness, choose the best control. Match the control's job to the problem's shape.
3	**Physical or logical**	Classify a control, or pick the physical control that addresses a described physical weakness.
4	**Biometric reasoning**	FAR versus FRR, which is security-critical, and what CER is used for.
5	**Principle application**	Apply least privilege, need-to-know or separation of duties to a scenario.
6	**Lifecycle failures**	Orphaned accounts, privilege creep, missing deprovisioning — and the review that catches them.

Six patterns. The first two carry the majority of the marks in this domain.

Next: Domain 4

Network Security

24% of the exam and the most technical domain. The OSI and TCP/IP models, ports and protocols, threats and attacks, and the infrastructure that defends against them.

Before you move on: can you name the discriminator between DAC, MAC and RBAC in one sentence, and say which biometric error rate is the dangerous one?