



Access Control Models

Every model answers one question differently: **who decides** whether you get in. Identify the decider and the model names itself.



Scan to drill
this sheet

	DAC Discretionary	MAC Mandatory	RBAC Role-based	ABAC Attribute-based	RuBAC Rule-based
Who decides	The data owner	The system , by policy	Your job function	A policy engine at request time	The admin's rule set
Granted by	Owner sets permissions per file (ACLs)	Clearance matched to a data label	Membership of a role, not the person	Attributes: user, resource, action, context	Global if-then conditions on all users
The tell	"the owner can share it"	"Top Secret", "classification", "clearance"	"all nurses", "the finance team"	"if department = HR <i>and</i> device is managed"	"no access outside business hours"
Found in	Windows NTFS, Linux file modes, Google Drive shares	Military and government, SELinux, AppArmor	Most enterprises — AD groups, AWS IAM roles	Zero trust, XACML, conditional access	Firewall ACLs, time-of-day restrictions
Trade-off	Flexible, but permissions sprawl	Strongest, but rigid and costly	Scales well, but roles multiply	Most granular, hardest to audit	Simple, but blind to identity

Principles that sit on top

Least privilege

Only the access the job needs, and no more. Applies to every model above.

Separation of duties

No one person completes a sensitive process alone — the requester cannot also approve.

Need to know

Clearance alone is not enough — the request must also be relevant to your work.

Where people lose the mark Three distinctions that decide most access-control questions.

RBAC vs RuBAC

Same abbreviation, different word. **Role**-based keys off who you are; **Rule**-based keys off conditions and applies to everyone equally.

DAC vs MAC

The tell is whether **the owner can override**. Under DAC they can share at will; under MAC no one can — not even the owner.

Authentication ≠ authorization

These models are all **authorization** — what you may do once identified. Passwords and MFA are authentication; logging is accounting.

Reading a table won't stick — turn it into instinct.

Drill scenario-to-model questions until you spot the decider in the wording. Ten minutes a day, free forever, no card.

cyberquizzier.com/go/access-sheet