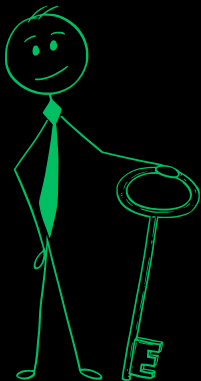


CC in a Nutshell



Access Control Concepts

By BELKHIR Selma

Key Elements of Access Control




SUBJECTS:
WHO GETS
ACCESS.

OBJECTS: WHAT
THEY HAVE
ACCESS TO.

RULES: HOW AND
WHEN ACCESS IS
ALLOWED.

Defense in Depth



A LAYERED SECURITY STRATEGY
INTEGRATING PEOPLE, TECHNOLOGY,
AND OPERATIONS TO PROVIDE MULTIPLE
BARRIERS ACROSS AN ORGANIZATION.



THIS APPROACH APPLIES TO PHYSICAL,
LOGICAL/TECHNICAL, AND
ADMINISTRATIVE ACCESS CONTROLS.

PRINCIPLE OF LEAST PRIVILEGE: USERS SHOULD
ONLY HAVE THE MINIMUM ACCESS NECESSARY
FOR THEIR ROLE.

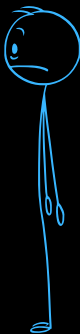
Privileged Access Management

REDUCES RISK BY RESTRICTING ADMIN PRIVILEGES TO WHEN THEY ARE NEEDED.

ENHANCES :

- **CONFIDENTIALITY:** BY LIMITING ROUTINE ADMINISTRATIVE ACCESS.
- **INTEGRITY:** BY ALLOWING ONLY AUTHORIZED ACCESS DURING APPROVED ACTIVITIES.
- **AVAILABILITY:** BY ENSURING ADMIN ACCESS IS AVAILABLE WHEN NECESSARY.

Types of Access Control



DISCRETIONARY ACCESS CONTROL (DAC): PLAN FOR INCIDENTS BEFORE THEY OCCUR.

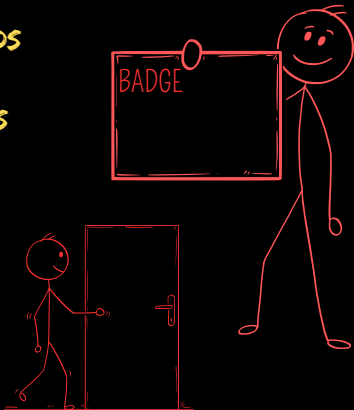
MANDATORY ACCESS CONTROL (MAC): ENFORCED UNIFORMLY ACROSS ALL USERS AND SYSTEMS.

ROLE-BASED ACCESS CONTROL (RBAC): PERMISSIONS ARE ASSIGNED BASED ON USER ROLES.

Physical Access Controls

EXAMPLES INCLUDE:

- SECURITY GUARDS
- FENCES
- LOCKED DOORS
- ALARMS
- CAMERAS
- BADGES
- MANTRAPS



Logical Access Controls

EXAMPLES INCLUDE:

- **CONFIGURATION SETTINGS** MANAGED VIA SOFTWARE (GUI) OR HARDWARE.
- **PARAMETERS** LIKE USER PRIVILEGES, ACCESS RULES, OR SYSTEM SETTINGS.

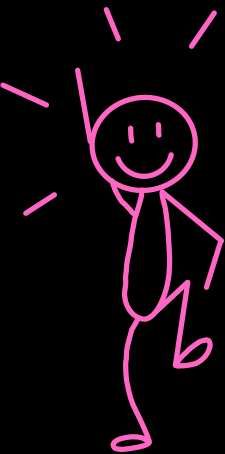


User Provisioning

ONBOARDING: CREATING ACCOUNTS FOR NEW EMPLOYEES.

OFFBOARDING: DISABLING OR DELETING ACCOUNTS FOR TERMINATED EMPLOYEES.

ACCOUNT MODIFICATIONS: ADJUSTING PRIVILEGES WHEN AN EMPLOYEE'S ROLE CHANGES.



I appreciate
you taking the
time to read,
— and I hope it
was helpful!
Feel free to
share any
feedback you
have.

By BELKHIR Selma