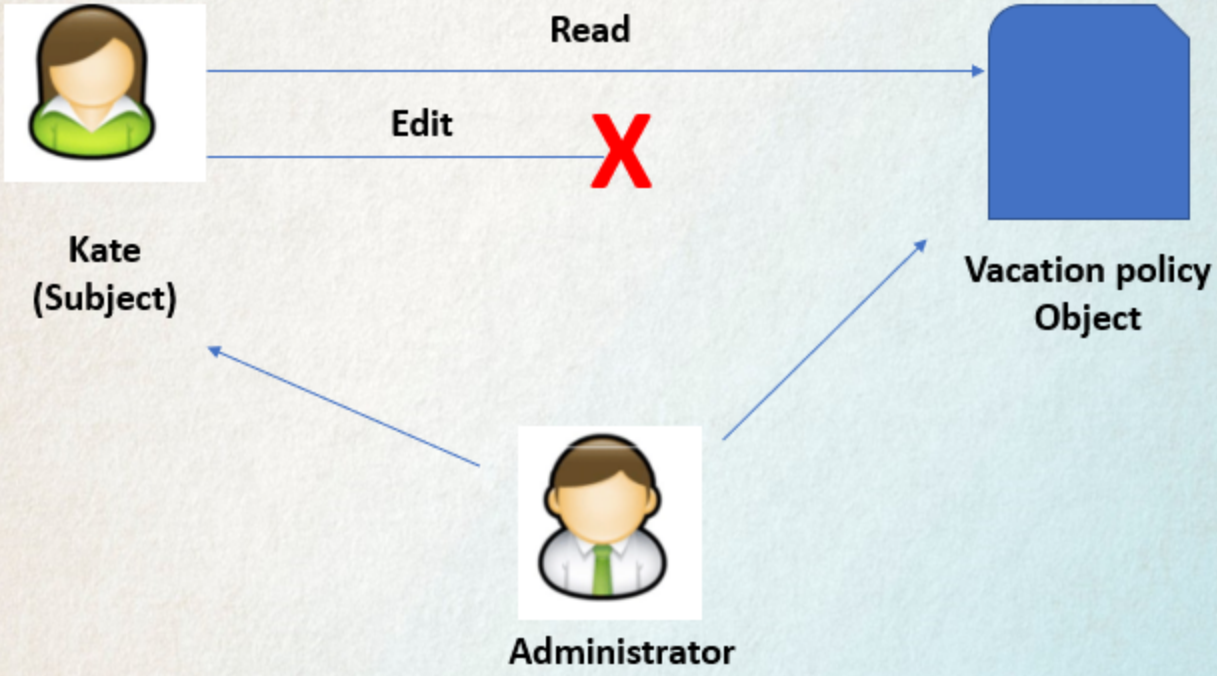
Basic of Access Control

- Access control is the basis for all security disciplines, not just IT security.
- **The purpose of access control** is to allow authorized users access to appropriate data/resource and deny access to unauthorized users.
- **Access Control : Access + Control**
  - ✓ Access: is the flow of information between a subject (e.g., user, program, process, or device, etc.) and an object (e.g., file, database, program, process, or device, etc). **Ability the subject to interact or do something** (discovering, reading, creating, editing, deleting, and executing objects)
  - ✓ Controls: mechanisms you put into place to allow or disallow object access (any potential barrier that protects your information from unauthorized access)
- **Access controls** are **a collection of mechanisms** that work together to protect the information assets/resources of the enterprise from unauthorized access.

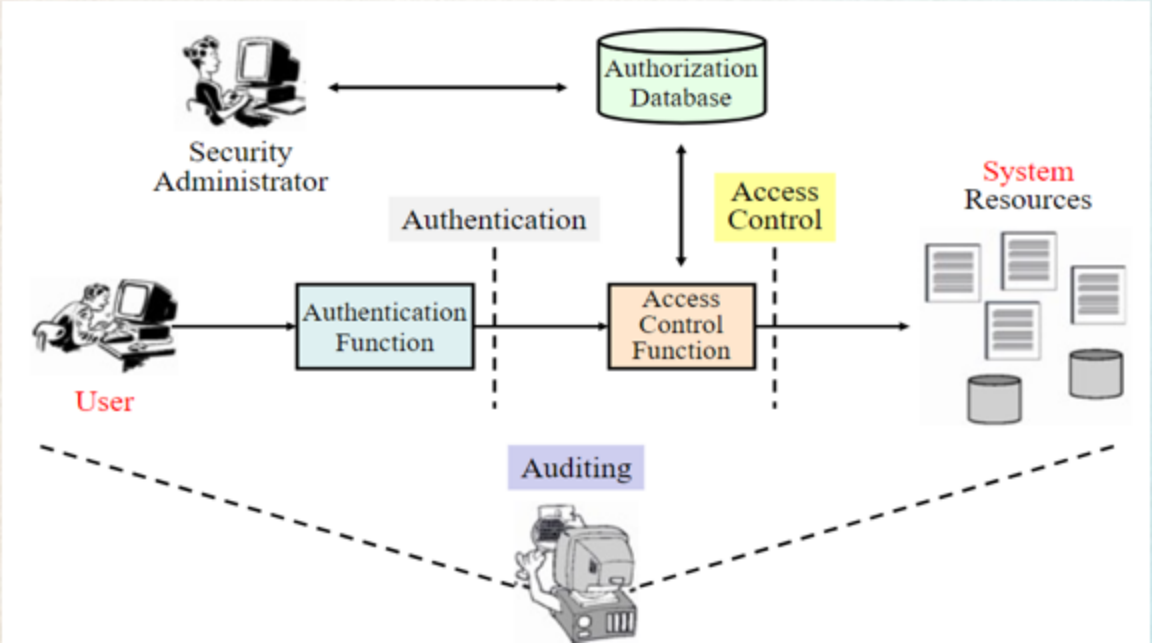
Basic of Access Control



Basic of Access Control

Access controls enable management to:

- Specify **which user** can access the resources contained within the information system (**Authentication**)
- Specify **what resources** they can access (**Authorization**)
- Specify **what operations** they can perform (**Authorization**)
- Provide **individual accountability** (**Accountability**)



Categories of Security Control

- **Management (Administrative) Controls**
  - ✓ Policies, Standards, Processes, Procedures, & Guidelines
    - ✓ Administrative Entities: Executive-Level, Mid.-Level Management
- **Operational (and Physical) Controls**
  - ✓ Operational Security (Execution of Policies, Standards & Process, Education & Awareness)
    - ✓ Service Providers: IA, Program Security, Personnel Security, Document Controls (or CM), HR, Finance, etc
  - ✓ Physical Security (Facility or Infrastructure Protection)
    - ✓ Locks, Doors, Walls, Fence, Curtain, etc.
    - ✓ Service Providers: Facility security officer (FSO), Guards, Dogs
- **Technical (Logical) Controls**
  - ✓ Access Controls , Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.
    - ✓ Service Providers: Enterprise Architect, Security Engineer, Helpdesk.

Types of Security Controls

- **Directive Controls:** Policy and standard that advise employees of the expected behavior for protecting an organization's information asset from unauthorized access.
- **Preventive Controls:** Physical, administrative, and technical measures intended to prevent unauthorized access to organization's information asset.
- **Detective Controls:** Practices, processes, and tools that identify and possibly react to unauthorized access to information asset.
- **Corrective Controls:** Physical, administrative, and technical countermeasures designed to react to security incident(s) in order to reduce or eliminate the opportunity for the unwanted event to recur.
- **Recovery Controls:** The act to restore access controls to protect organization's information asset.

Example Implementations of Access Controls

	Directive	Preventive	Detective	Corrective	Recovery
Management (Administrative)	• Policy • Guidelines	• User registration • User agreement • NdA • Separation of duties • Warning banner	• Review access logs • Job rotation • Investigation • Security awareness training	• Penalty • Administrative leave • Controlled termination processes	• Business continuity planning (BCP) • Disaster recovery planning (DRP)
Physical/ Operational	• Procedure	• Physical barriers • Locks • Badge system • Security Guard • Mantrap doors • Effective hiring practice • Awareness training,	• Monitor access • Motion detectors • CCTV	• User behavioral modification • Modify and update physical barriers	• Reconstruction • Offsite facility

Example Implementations of Access Controls

	Directive	Preventive	Detective	Corrective	Recovery
Technical	• Standards,	• User authentication • Multi-factor authentication • ACLs • Firewalls • IPS • Encryption	• Log access and transactions • Store access logs • SNMP • IDS	• Isolate, terminate connections • Modify and update access privileges	• Backups • Recover system functions, • Rebuild,

How to Design Access Control

Before you can implement a sound access control policy, you must first develop a plan or design for the access control. Some questions you need to answer:

- ✓ Which assets are to be secured?
- ✓ How do I separate restricted information from unrestricted information?
- ✓ What methods should I use to identify users who request access to restricted information?
- ✓ What forms of Authentication? Something you know, something you have, something you are.
- ✓ How many access location points in the system and how will they be used?
- ✓ What is the best way to permit only users I authorize to access restricted information?
- ✓ Does every door or gate require access control?
- ✓ What type of lock technology will be required?

Access Control Administration

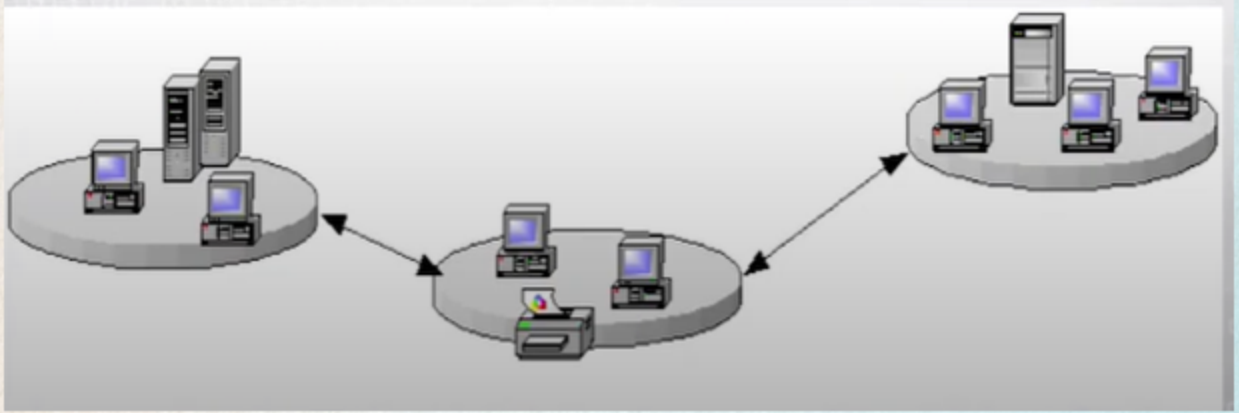
- Once an organization chooses an access control design, the next step is to decide on the method of access control administration.
- Access control administration can be implemented in both centralized and decentralized modes. It is not uncommon to find hybrid environments where both approaches are used.
- The best choice of administration style depends on the needs of the organization and the sensitivity of information stored on the affected computer systems.

Centralized Access Control

- **Centralized access control administration** requires that all access requests go through a central authority that grants or denies the request. This approach simplifies administration because objects must be maintained only in a single location.
- One **drawback** is that the central access control unit is a single point of failure. If the centralized access control unit fails, no access can be granted to objects, so all objects are effectively unavailable.
- The central point of access control can have a **negative effect on performance** if the system is unable to keep up with all access requests.
- Businesses and enterprises with large workforces or remote locations may need to wait hours or days for its security team to issue new credentials when an employee's security level changes, when the team onboards a new hire

Decentralized Access Control

- **Decentralized access control** places the responsibility of access control administration closer to the object in question. This approach requires more administration than centralized access control because an object may need to be secured at several locations. It can, however, be more stable and flexible because no single point of failure or single point of access exists.
- It is most often implemented through the use of **security domains**. **A security domain** is a sphere of trust, or a collection of subjects and objects, with defined access rules or permissions. A subject must be included in the domain to be trusted. This approach makes it fairly easy to exclude an untrusted subject, but makes general administration more difficult due to the fine granularity of security rules.



Hybrid Access Control

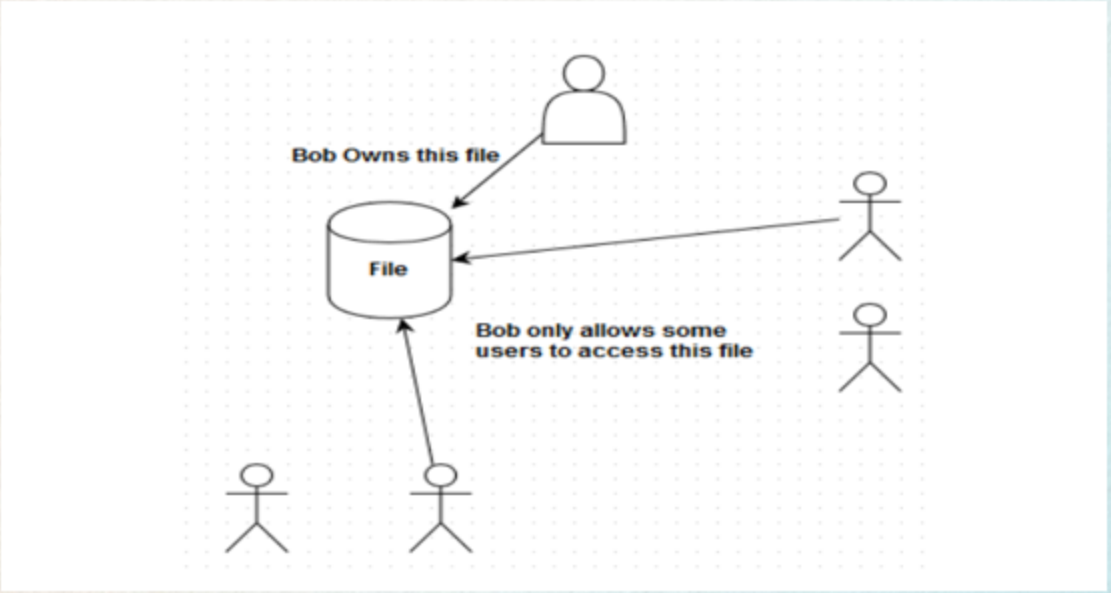
- Combine centralised and decentralised administration control methods
- One entity (network administrator) may control what users access. For example, restricting access to important network resources
- Individuals users may be allowed to decide who accesses some local resources. For instance, files, local printers.

Discretionary Access Control(DAC)

- **DAC** gives subjects full control of objects they have been given access to, including sharing the objects with other subjects.
- According to TCSEC (Trusted Computer System Evaluation Criteria)–"A mean of **restricting access to objects based on the identity and need-to-know of users and/or groups to which they belong**. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject."
- **Need to Know:** refers to answering the question: does the user "need to know" the specific data they may attempt to access.
- Subjects are empowered and control their data.
- Standard UNIX and Windows operating systems use DAC for filesystems

Discretionary Access Control(DAC)

- If a subject makes a mistake, such as attaching the wrong file to an email sent to a public mailing list, loss of confidentiality can result. Mistakes and malicious acts can also lead to a loss of integrity or availability of data.
- **Less secure** but it is **easier to implement and more flexible** for environments that do not require high level of centralized security.



Role-Based Access Control (RBAC)

- **Role-Based Access Control (RBAC)** defines how information/object is accessed on a system based on the role of the subject which are assigned in view of task functions.
  - ✓ Subjects are grouped into roles and each defined role has access permissions based upon the role, not the individual.
  - ✓ Users only are assigned a single role for their job
  - ✓ A role could be a nurse, a backup administrator, a help desk technician, etc.

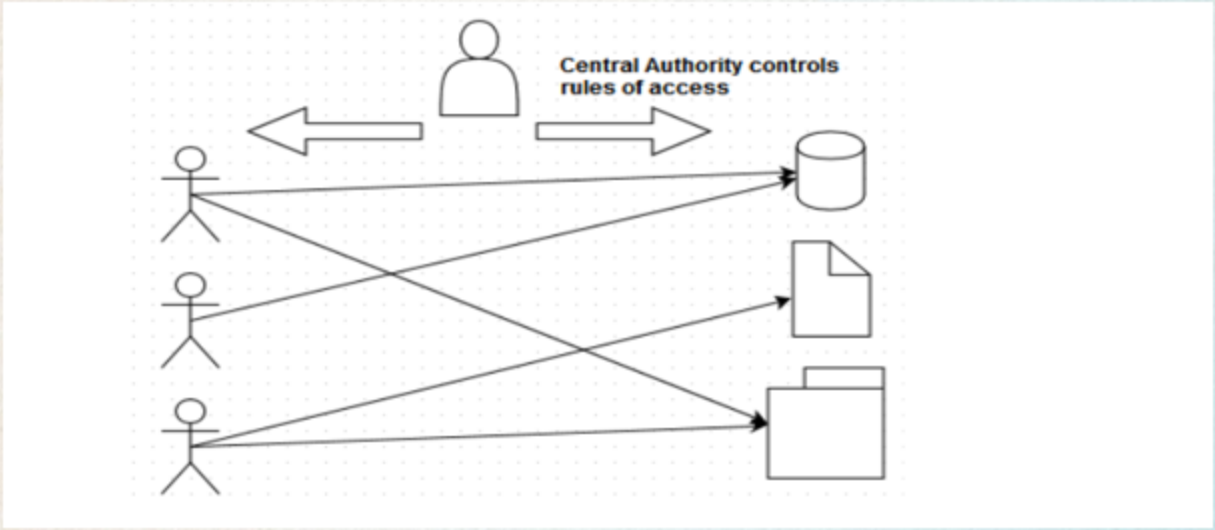
- Suitable for dynamic, turnover or reassignments environments with frequent personnel changes because administrators can easily grant multiple permissions simply by adding a new user into the appropriate role.

- It is more scalable than the DAC and MAC models

Rule-Based Access Controls

Rule-Based Access Controls: uses a set of rules, restrictions, or filters to determine what can and cannot occur on a system.

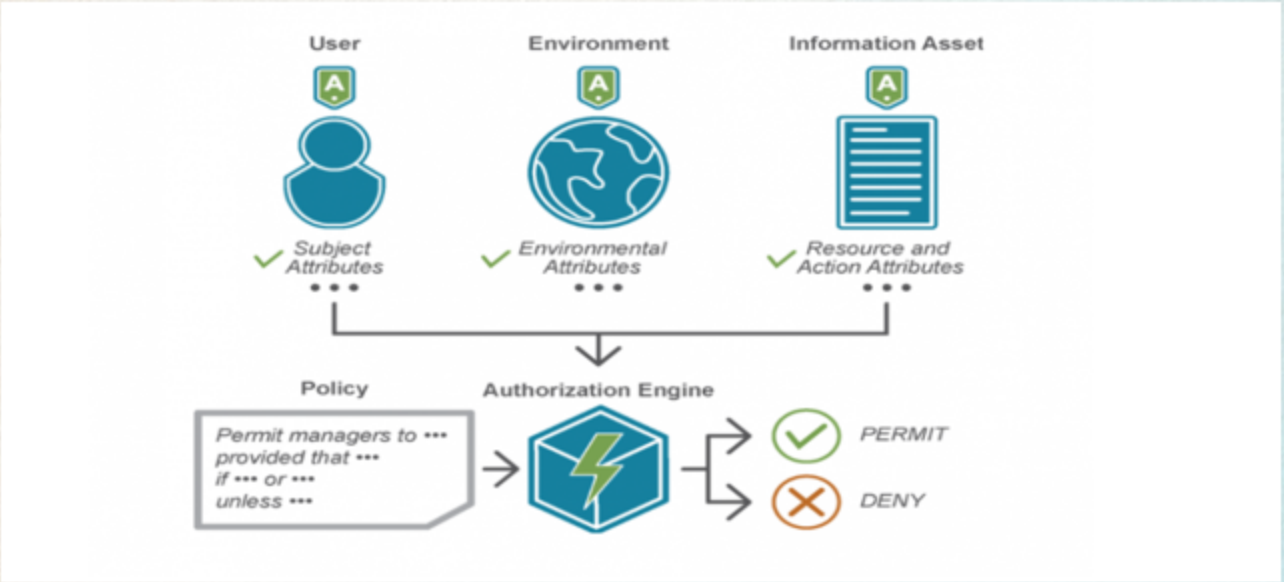
- ✓ It includes granting a subject access to an object, or
- ✓ granting the subject the ability to perform an action.
- ✓ uses a set of rules provisioned to subjects defined by a central authority.
- ✓ Rule-based Access Control is commonly used as an add-on to the other types of access control



Attribute Based Access Controls (ABAC)

ABAC: grant or deny user requests based on arbitrary attributes of the user and selected attributes of the object, and environment conditions that could be globally recognized and more relevant to the policies at hand. ABAC models use policies that include multiple attributes for rules.

- Access rights are granted to users through the use of policies which combine attributes.



Attribute Based Access Controls

- Attributes are sets of properties that can be used to describe all the entities that must be considered for authorization purposes. **Subject attributes** like identity, roles; **object attributes** like device name, file, record, table, applications, programs, and network; **environment conditions** like location, time.

Example: **A subject** is assigned a set of **subject attributes** upon employment, such as Kate William is a Nurse Practitioner in the Cardiology Department. An **object** is assigned its **object attributes** upon creation, such as a folder with Medical Records of Heart Patients. The administrator or owner of an object **creates an rule using attributes of subjects and objects** to govern the set of allowable capabilities—for example, Nurse Practitioners in the Cardiology Department can View the Medical Records of Heart Patients.

- More flexible as it enables creation of access rules without specifying individual relationships between each subject and each object.

- Ideal for many distributed or rapidly changing environments.

Integrated or combination methods

- Although one method identified above can be used as an access control solution, this is not typically the case. Most organizations choose to use a combination of these methods as they are needed based on the requirement of the organization. Using an integrated approach allows companies to base access control on their own standards and needs.

- **Example:** a company might use **role based access** control for anyone with the title of database administrator, but may also use **rule based access control** to grant exception access beyond what is granted through the role.

Type of access control attacks

- Network sniffing
- Impersonation (spoofing / masquerading)
- Rogue infrastructure (rogue mean an unauthorized resource)
- Replay attack
- Automated attacks on password (such as dictionary and brute force attack)
- Authentication attacks –losing control such as steal hashes to authenticate
- Theft

Access Controls assessment or testing methods

- **Vulnerability assessment**
  - ✓ Using various tools and methodologies to identify weak or vulnerable area and risks that need to be addressed.
  - ✓ Do we have issues? How many ? How bad are they?
  - ✓ Reduce threats to an acceptable level
- **Penetration testing**
  - ✓ Authorised attacks on your network and system using exploitive techniques similar to those used by attackers
  - ✓ They find and exploit network and system vulnerabilities
  - ✓ Its goal is to measure an organization's level of resistance to an attack and assess potential damage
  - ✓ Need written approval (contract) is required first, as pen testing often causes breakdowns