Co-funded by
the European Union

Course: Security Analysis and Risk Management

Project: Cyber Security 4 ALL

CS4ALL
CYBERSECURITY FOR ALL

Chapter 6

Managing Risks to Records and Information

Overview

- Telecommunications and Network Technologies: Risks and management strategies
- Application Technologies and the Application Development Life Cycle: Risks and management strategies
- Access Control and its importance in information security

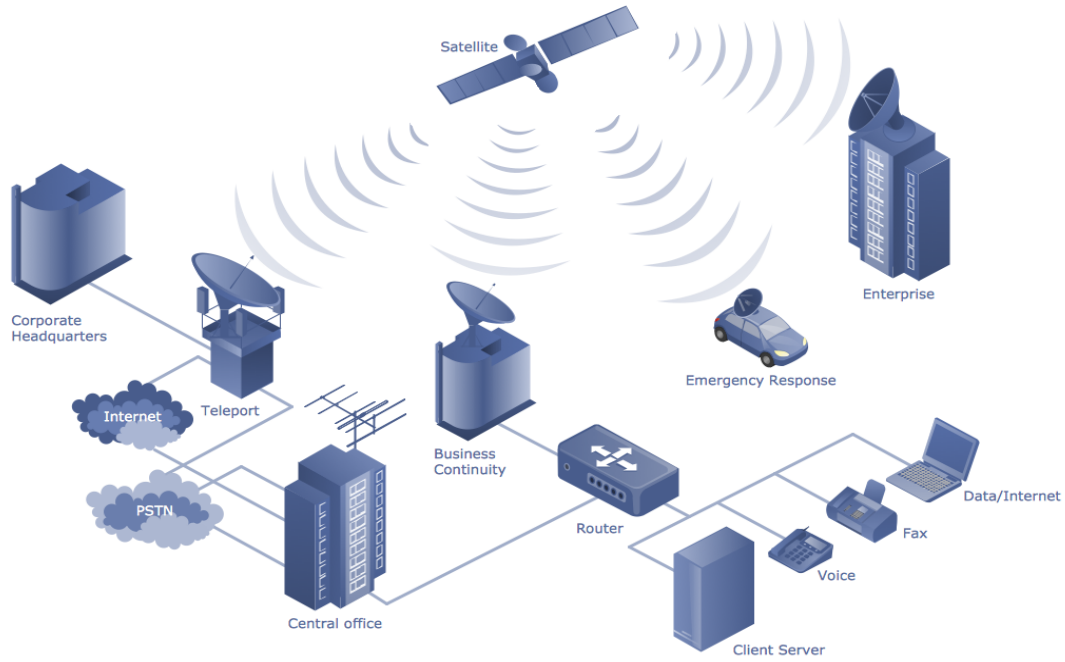
Introduction

- In today's digital age, organizations increasingly rely on information systems to manage, store, and transmit sensitive data.
- These advancements heightened risks that can threaten the integrity, confidentiality, and availability of critical records and information.
- Effective risk management strategies is essential to protect against unauthorized access, data breaches, and potential loss of information due to cyberattacks or technical failures.
- Main areas that should be considered includes:
  - Telecommunications and network technologies
  - Application technologies along with the application development life cycle
  - Access control

Co-funded by the European Union

Telecommunications and Network Technologies

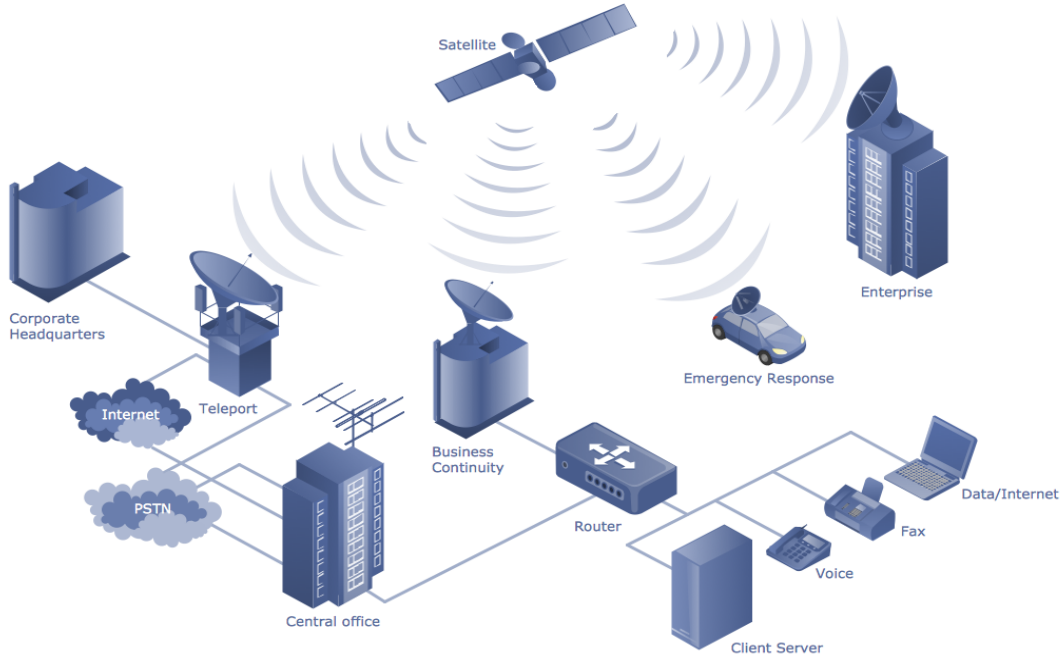
- They have important role in the flow of information within and between organizations.
- Interconnected nature of networks exposes them to various risks:
  - **Data Interception:** Data transmitted across networks can be intercepted by malicious actors, leading to unauthorized access to sensitive information.
  - **Network Vulnerabilities**: Networks are prone to attacks such as phishing, malware, and ransomware, which can compromise both data and systems.
  - **Distributed Denial of Service (DDoS)**: High traffic attacks can overwhelm networks, causing downtime and disrupting access to vital information



Co-funded by the European Union

Telecommunications and Network Technologies

- Management Strategies:
  - **Encryption:** Encrypting data both in transit and at rest can protect against interception and unauthorized access.
  - **Firewalls and Intrusion Detection Systems (IDS)**: Implementing firewalls and IDS helps monitor and block malicious activity on the network
  - **Regular Audits and Updates**: Regular vulnerability assessments, software updates, and patches can protect networks from known vulnerabilities and emerging threats.



Co-funded by the European Union

Application Technologies and Development Life Cycle Risks

- Applications are essential for daily operations for data processing, storage, and retrieval.
- Development and Deployment of applications introduce risks that can compromise data integrity, availability, and security.
- Risks are present at every phase of the application development life cycle (ADLC), from planning and design to implementation and maintenance

Co-funded by
the European Union

Application Technologies and Development Life Cycle Risks

- Applications are essential for daily operations for data processing, storage, and retrieval.
- Development and Deployment of applications introduce risks that can compromise data integrity, availability, and security.
- Risks are present at every phase of the application development life cycle (ADLC), from planning and design to implementation and maintenance:
  - **Code Vulnerabilities:** Insecure code can lead to application vulnerabilities, which hackers may exploit to gain unauthorized access.

Co-funded by the European Union

Application Technologies and Development Life Cycle Risks

- **Improper Testing**: Lack of rigorous testing before deployment can result in undetected security flaws.
- **Weak Access Controls**: Insufficient access control mechanisms within applications can expose sensitive data to unauthorized users.

- Management Strategies:
  - **Secure Development Life Cycle (SDLC)**: Adopting secure coding practices in every stages of development, such as input validation and regular code reviews, reduces vulnerabilities.

Co-funded by
the European Union

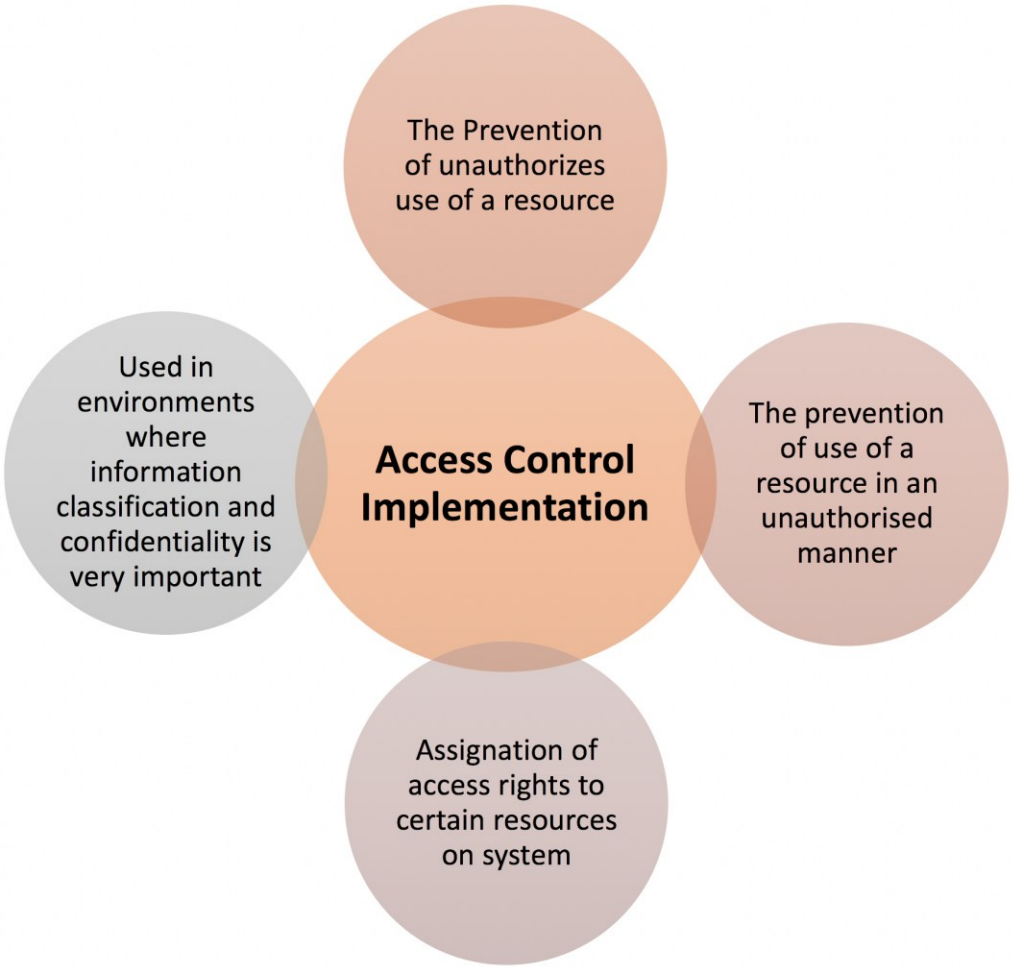
Application Technologies and Development Life Cycle Risks

- Management Strategies:
  - **Rigorous Testing**: Conducting comprehensive testing (e.g., penetration testing, code scanning, Vulnerability Scanning Tools) helps identify and resolve potential security issues before deployment.
  - **Access Controls**: Implementing role-based access controls(RBAC) ensures that only authorized users can access sensitive functions or data within applications.
  - **Regular Updates and Patches:** Ensure applications are up-to-date with the latest security fixes.

Co-funded by
the European Union

Access Control and Its Importance in Information Security

- Access control is a fundamental component of information security, dictating who can access certain resources and under what conditions.
- Ensures data integrity, confidentiality, and minimizes unauthorized access risks, thereby reducing the risk of data breaches and unauthorized data manipulation.
- Types
  1. Discretionary Access Control (DAC)
  2. Mandatory Access Control (MAC)
  3. Role-Based Access Control (RBAC)

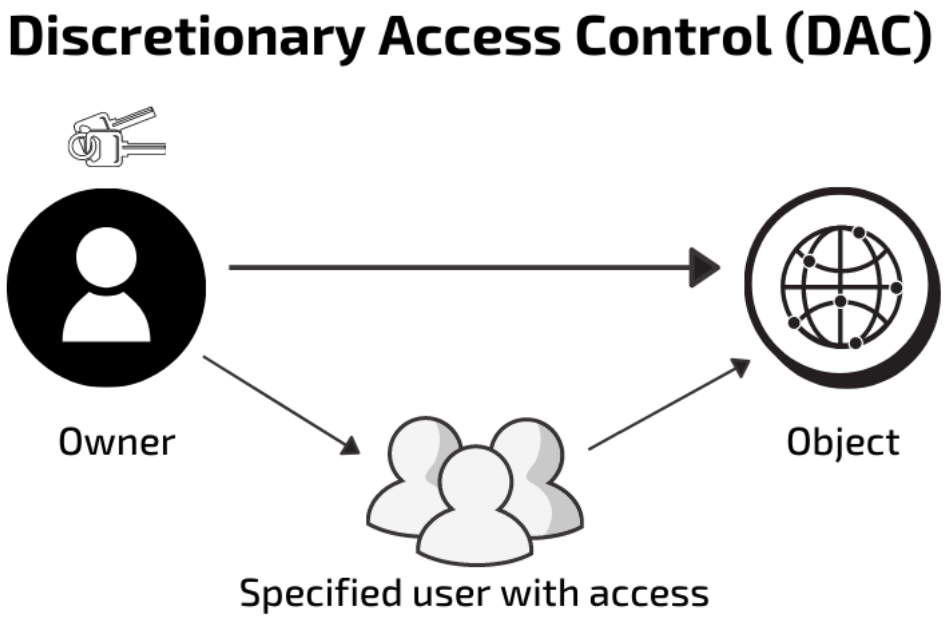


CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Discretionary Access Control (DAC) Access

- DAC models allow the data owner to decide access control by assigning access rights to rules that users specify.
- When a user is granted access to a system, they can then set access permissions for other users.
- Example:

In a file-sharing system, a document's owner can decide who can read, write, or execute the document. For instance, in Windows, a file owner can assign read-only access to a specific user while giving others full control over the file.

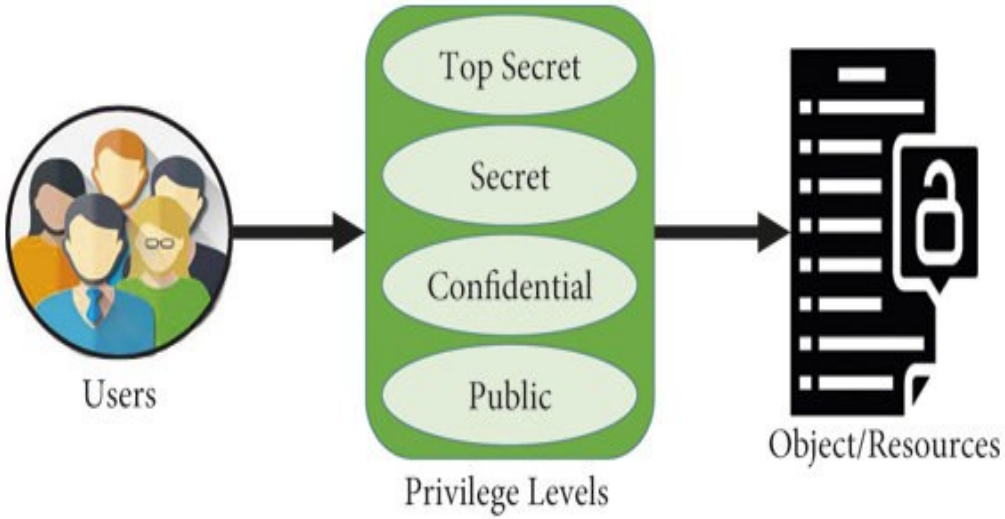


Co-funded by the European Union

Mandatory Access Control (MAC) Access

- MAC places rigid and strict access control policies on individual users and the data, resources, and systems they want to access.
- The policies are managed by central authority or an organization's administrator.
- Users are not able to alter, revoke, or set permissions.
- Example:

In a government system handling classified information, files are labeled as "Confidential," "Secret," or "Top Secret." A user with "Confidential" clearance cannot access "Top Secret" files unless they have the appropriate clearance level.

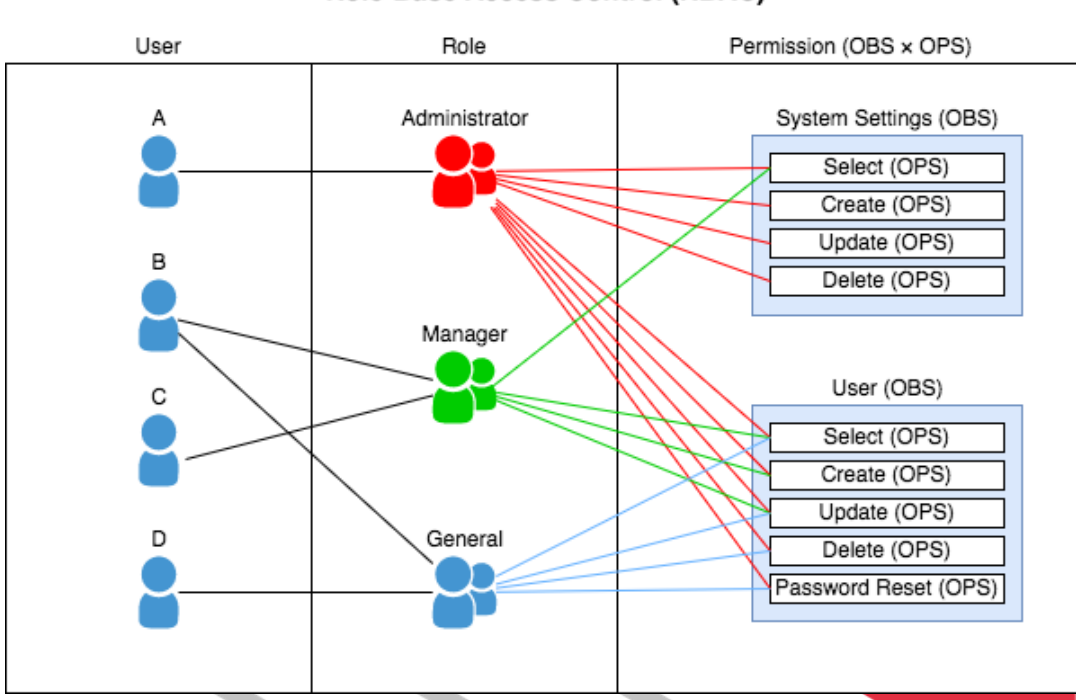


Co-funded by the European Union

Role-Based Access Control (RBAC) Access

- RBAC creates permissions based on groups of users, roles that users hold, and actions that users take.
- Users are able to perform any action enabled to their role and cannot change the access control level they are assigned.
- Similar to MAC, functions on access controls set by an authority, rather than by the owner of the resource.
- The difference between RBAC and MAC is that access control in RBAC is based on the role of the individual accessing the resource.
- Example:

In a hospital, doctors can access medical records, while administrative staff access billing information. Roles like "Doctor" and "Administrator" define access based on job functions, simplifying security management.



Co-funded by the European Union

DAC VS MAC VS RBAC

Feature	Discretionary Access Control (DAC)	Mandatory Access Control (MAC)	Role-Based Access Control (RBAC)
Definition	Access is controlled by the resource owner	Access is controlled by a central authority	Access is granted based on a user's role within an organization
Flexibility	Highly flexible; users can change permissions	Very rigid; users cannot change permissions	Moderate; admins assign access to roles, not individual users
Use Case	Common in personal or less secure environments	Common in high-security environments (e.g., government)	Common in business environments with structured roles
Permission Control	Managed by the resource owner	Managed by a centralized security policy	Managed through assigned roles and permissions
Granularity	Permissions assigned at the user or group level	Access based on strict labels and levels	Access defined by role, not individual user
Example	File owner assigns read/write access in a file-sharing system	Military systems restrict classified information based on security clearance	Doctors can access medical records; administrators access billing records
Risk of Unauthorized Access	Higher, as users control permissions	Lower, as access is tightly controlled by policies	Moderate, as access depends on role setup and assignment

Co-funded by the European Union

Conclusion

- Telecommunications and network risks can be mitigated through strong encryption and secure protocols.
- Application development requires a secure SDLC approach for effective risk management
- Access control is essential for protecting information and should be continuously monitored and updated.

.

Questions & answers

Invite questions from the audience.

Co-funded by
the European Union

References

- https://csrc.nist.gov/pubs/sp/800/218/final [Accessed on : 2024/11/6]
- https://www.conceptdraw.com/How-To-Guide/telecommunications-networks [Accessed on : 2024/11/6]
- http://www.xorlogics.com/2018/10/01/6-tips-for-implementing-access-control-authentication-system-with-security/[Accessed on : 2024/11/7]
- https://www.fortinet.com/resources/cyberglossary/access-control[Accessed on : 2024/11/7]
- https://identitymanagementinstitute.org/access-control-types-and-models/[Accessed on : 2024/11/9]
- https://dsonoda.medium.com/role-based-access-control-overview-257de64534c[Accessed on : 2024/11/9]

Co-funded by the European Union