UBL083

# Setting up client/user access and security

TLE_IACSS9-12ICCS-Ia-e-43

# Roll Call

TLE_IACSS9-12ICCS-Ia-e-43

# Recap of the Lesson

TLE_IACSS9-12ICCS-Ia-e-43

# What is client/user access?

# Client/User Access

It refers to the permissions and capabilities granted to an individual (the client or user) when interacting with a system, application, network, or service. It defines what a person can see, do, or change within that environment.

# User access management (UAM)

It is the process of controlling who has access to an organization's resources, such as systems, data, and networks. Implementing effective user access management is essential for organizations to protect their resources and sensitive information from cyber threats and meet regulatory requirements.

# User access management (UAM)

The fundamentals of user access management (UAM) involve controlling who has access to an organization's resources, such as systems, data, and networks.

# User access management (UAM)

By implementing effective user access management practices, organizations can protect their resources and sensitive information from cyber threats and meet regulatory requirements.

# User access management (UAM)

Effective user access management practices are the foundation of and can help organizations establish robust IAM (Identity and access management) and PAM (privileged access management) processes and frameworks.

# What is Identity and Access Management?

It is a set of processes, policies, and tools to ensure the right people or identities have the right access to the right resources at the right time.

# What is Identity and Access Management?

IAM helps an organization know who has access to what resources and timely grant and revoke access to resources for individual identities (users, devices, processes, etc.) based on their roles and responsibilities.

# What is User Access Management (UAM)?

It is a subset of IAM that emphasizes managing user access to various system resources and data. It helps provide users within the organization access to the tools and services they need at the correct time.

# What is User Access Management (UAM)?

The process is typically done through user accounts, roles, and permissions, which can be granted or revoked based on an individual's needs and responsibilities within the organization.

# What is User Access Management (UAM)?

The process is typically done through user accounts, roles, and permissions, which can be granted or revoked based on an individual's needs and responsibilities within the organization.

# Understanding between...

Accounts

Roles

Users

Access Levels

# Account

It represents someone or something (e.g., another server) that can access an organization's resources. Accounts are given a unique set of credentials.

# User

It is the actual or an individual that works at the organization. Users are given one or more accounts and can access resources using that account.

# Access Level

It refers to the level of access of a user (or a device, program, or process) to a particular resource. Access levels can vary depending on the resource's sensitivity and may include read-only access, read-write access, or full access to modify or delete the resource.

# Identity governance

It is a critical component of user access management and helps organizations control access to their resources and protect sensitive information by enforcing policies and processes related to user access and identity within an organization.

# Identity governance

It ensures that users have appropriate access to resources based on their roles and responsibilities and that access is granted and revoked in a timely and controlled manner.

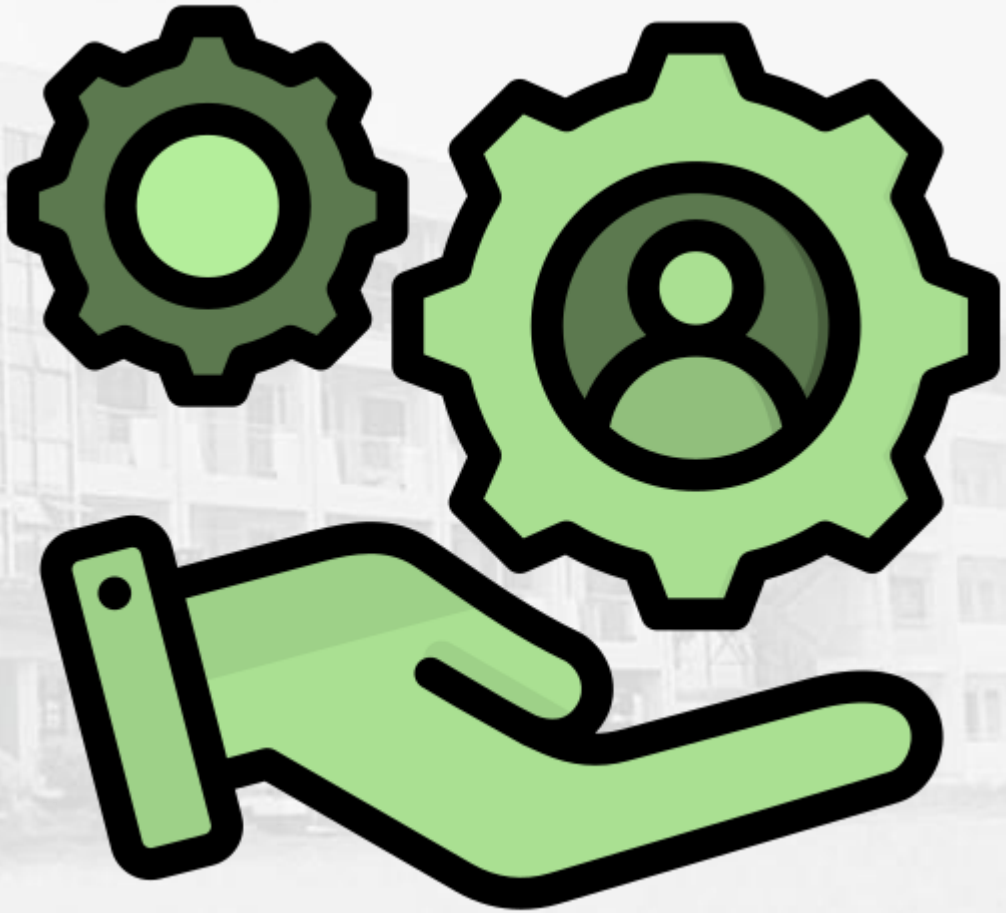
# Identity Governance

It is accomplished by monitoring roles and responsibilities, access activities, establishing and automating access management policies and procedures, and reviewing and timely updating them.

# Identity Governance

It is accomplished by monitoring roles and responsibilities, access activities, establishing and automating access management policies and procedures, and reviewing and timely updating them.

# What is the importance of User access management system?



# Importance of UAM System

## Improved Control & Data Security:

You can not safeguard information assets you have no visibility of. By controlling access to resources, organizations can have better control over data and protect sensitive information and reduce the risk of data breaches.

# Importance of UAM System

## Enhanced Compliance

A UAM system can help organizations comply with internal policies and procedures, industry frameworks, and regulatory requirements. The enhanced compliance further helps elevate stakeholder trust in the organization's capabilities to keep their data safe.

# Importance of UAM System

## Better Resource Management

By only granting access to the resources that users need, organizations can help employees work more efficiently and effectively, better manage resources, and have a comprehensive view of their information assets which in turn helps reduce the attack surface.

# Importance of UAM System

## Reduced Cost

A user access management system provides a common platform for managing user access to resources across the organization, prevents wastage of resources, and helps keep the cost in control.

# Types of UAM

- Internal User Access Management
- External User Access Management

# Types of UAM

## Internal UAM

Internal users of an organization are its employees, administrators, managers, and others. Internal user access management refers to controlling access to organizational resources for those individual identities.

# Types of UAM

## Internal UAM

It typically involves using user accounts and permissions and may include techniques such as password management policies, access control lists (ACLs), role-based access control (RBAC), etc.

# Types of UAM

## External UAM

External user access management refers to controlling access to resources for individuals outside the organization, such as customers, clients, partners, vendors or suppliers, etc.

# Types of UAM

## External UAM

It may involve using single sign-on (SSO) systems to allow external users to access multiple resources with a single set of credentials or using access control lists to specify which external users can access specific resources.