# Identity and access management IAMT

Manages identity verification and access permissions within organizational systems and environments.

|  |
| --- |
| **Guidance Notes:**  Activities may include, but are not limited to:   * implementing management (IAM) frameworks in line with organizational goals and compliance with regulations like GDPR, HIPAA, or SOX * streamlining user authentication with single sign-on solutions and enhancing security with multi-factor authentication * managing user access rights from onboarding to offboarding, including integration with cloud services, enterprise applications, and directory services like LDAP or Active Directory * using role-based and attribute-based access controls to manage user privileges and access, aligning with organizational roles and attributes * implementing privileged access management tools for secure monitoring and control of critical asset access * handling incident responses related to access issues, like unauthorized access or identity theft, and regularly auditing access to maintain security and compliance * conducting identity governance and administration to enforce policies, managing digital identities including user accounts, groups, and roles. |

## Level 1

Performs basic IAM tasks, including user account lifecycle management, under supervision.  
Maintains accurate records and follows established IAM protocols.

## Level 2

Provides assistance for IAM operations, including automated role allocation and access control management.  
Engages in user identity lifecycle management, including account creation and deletion.  
Facilitates operation of IAM tools and self-service portals.

## Level 3

Administers standard IAM services, implementing policies and resolving related issues. Manages monitoring, audits, and logging for IAM systems.  
Assists users in defining their access rights and privileges. Designs and implements simple IAM solutions, enhancing user access security.  
Investigates minor security breaches in accordance with established procedures related to IAM.  
Contributes to the enhancement and optimization of existing IAM processes and systems.

## Level 4

Designs and implements complex advanced IAM solutions, focusing on automated access control and role allocation.   
Oversees the integration of IAM services with new technologies.  
Provides specialised support for complex IAM operations and support implementation of policies and standards.  
Collaborates with stakeholders to align IAM with business objectives and emerging security trends.

## Level 5

Offers authoritative advice on IAM, ensuring services align with and support evolving business needs and security protocols.  
Manages large-scale IAM initiatives and oversees the integration of IAM services with new technologies, enhancing security and operational efficiency.  
Leads operational planning for IAM, anticipating future trends and preparing the organization for scalable growth.  
Ensures IAM systems' compliance and oversees advanced monitoring and audit processes.

## Level 6

Shapes and defines organisation-wide IAM policies, ensuring alignment with business strategies and security requirements.  
Champions IAM best practices, advocating for robust and innovative IAM solutions across the organization.  
Influences and guides organizational IAM governance, integrating emerging technologies and regulatory compliance into IAM strategies.  
Reviews and advises on IAM aspects and implications of new business initiatives.