



Identity & Access Governance Analyst

About the Team and the Role

Digital, Data & Technology (DDaT) enables Mencap to deliver safe, reliable and effective services for people with a learning disability. Colleagues across the organisation rely on secure access to digital systems, applications and data in order to support operational services and work effectively.

The Identity & Access Governance Analyst plays a key role in protecting Mencap's digital environment by ensuring that access to systems and data is governed, controlled and managed appropriately across the organisation.

The role is responsible for the operational governance of identity and access controls across Mencap's technology estate. This includes ensuring that colleagues have appropriate access to systems and information while reducing security risk through effective identity governance, role-based access control and least privilege principles.

Working closely with the Help Desk, Digital Platforms Squad and Enterprise Governance function, the role ensures that identity and access management practices operate consistently, securely and in line with organisational policy and regulatory requirements.

The role is responsible for governing and assuring identity lifecycle processes including joiners, movers and leavers, privileged access management, access reviews and authentication controls across cloud and SaaS platforms.

The Identity & Access Governance Analyst supports the organisation's transition toward modern identity security and Zero Trust principles through the implementation and operation of policy-based and automated identity governance controls.

The role works extensively with Microsoft Entra ID, Microsoft 365 identity controls, conditional access policies and identity governance tooling to ensure that access management processes remain effective, auditable and aligned with organisational security requirements.

The role has authority to challenge, reject or escalate access requests that do not align with organisational policy, segregation of duties controls or least privilege principles.

The role also supports audit and compliance activities relating to identity governance controls and is responsible for maintaining accurate records and evidence relating to identity and access management processes.

The Identity & Access Governance Analyst contributes to the continuous improvement of identity governance capability across Mencap by identifying opportunities to improve automation, strengthen controls and reduce operational risk associated with identity and access management.

This is a hybrid role requiring a minimum of two days per week onsite at either the London or Peterborough office. Onsite presence is expected to support collaboration with service and governance teams and to ensure effective management of access requests and controls. The role may also require ad-hoc travel to other Mencap locations where necessary.

What you will bring to the role (Essentials)

Experience working in identity and access management, identity governance, cyber security operations or enterprise technology support within a complex organisation.

Strong understanding of identity and access management principles including:

- Role-Based Access Control (RBAC)
- Least privilege access
- Segregation of duties
- Joiner, mover and leaver processes
- Authentication and authorisation
- Privileged access management
- Identity governance and access reviews

Experience working with identity and access management platforms including:

- Microsoft Entra ID



We are **passionate**
about making the
world a better place



We are **positive**
in our work and
with each other



We are **brave**
we challenge and
try new things



We are **kind**
to everyone



We are **inclusive**
of everyone

- Microsoft 365 identity and access controls
- Conditional Access
- Multi-Factor Authentication (MFA)
- Privileged Identity Management (PIM)
- Identity governance and lifecycle management tooling

Experience governing access across multiple enterprise systems and SaaS platforms.

Operate and maintain identity governance controls to ensure access remains appropriate, secure and compliant with organisational policy.

Govern joiner, mover and leaver processes to ensure access is provisioned, modified and removed accurately and in a timely manner.

Conduct and coordinate access reviews and certification activities across enterprise systems and platforms.

Review and challenge access requests where access does not align with policy, least privilege principles or segregation of duties requirements.

Support the governance and operational assurance of privileged access across critical systems and platforms.

Work closely with the Enterprise Governance function to ensure identity and access controls align with organisational security standards and compliance requirements.

Support the implementation and operation of policy-based identity governance controls including conditional access and automated lifecycle management.

Investigate identity and access-related issues, anomalies or control failures and ensure appropriate remediation activities are completed.

Maintain accurate records, audit evidence and operational documentation relating to identity governance activities.

Identify opportunities to improve automation, strengthen access controls and reduce manual operational processes.

Strong analytical and problem-solving skills with the ability to assess access risk and apply professional judgement.

Strong attention to detail and ability to manage sensitive access controls accurately and consistently.

Experience working with service management and ticketing systems within structured operational environments.

Strong communication skills with the ability to work effectively with both technical and non-technical stakeholders.

Experience supporting audit, compliance or governance activities relating to identity and access controls.



We are **passionate**
about making the
world a better place



We are **positive**
in our work and
with each other



We are **brave**
we challenge and
try new things



We are **kind**
to everyone



We are **inclusive**
of everyone

Understanding of cyber security principles relating to identity, authentication and access management.

Experience working within structured service management environments such as ITIL.

A commitment to delivering secure, reliable and well-governed digital services.

A commitment to Mencap's values and a desire to support the organisation's mission to improve the lives of people with a learning disability.

Please note: This job description is not intended to be exhaustive. Duties and responsibilities may evolve over time to reflect the needs of the organisation and the role.



“This isn’t just a job - it’s a chance to help change the lives of people with a learning disability and their families. If you’re passionate about making a difference, join Mencap in building a more inclusive future.”

Mencap and our Commitment to Safeguarding

Mencap is committed to safeguarding and promoting the welfare of children, young people and vulnerable adults, and expects all staff and volunteers to share this commitment.

Successful applicants will be subject to appropriate pre-employment checks, including references and, where applicable, an enhanced Disclosure and Barring Service (DBS) check.



We are **passionate**
about making the
world a better place



We are **positive**
in our work and
with each other



We are **brave**
we challenge and
try new things



We are **kind**
to everyone



We are **inclusive**
of everyone