Identity and Access Management for Local Government

intragen
SECURING YOUR IDENTITY

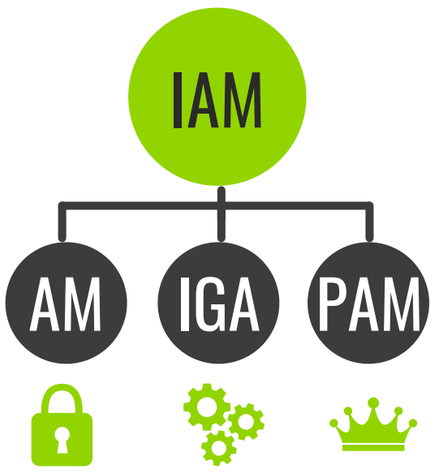
TRUSTMARQUE
Part of Capita plc

Local councils are confronted with the challenge of managing thousands of citizens and employees who expect fast, efficient delivery of public sector services. Technology plays a more important role than ever before for **optimising user experience**. However, the shift to digital access is coupled with the **risk of data breach**, particularly with sensitive public data involved. A security strategy should encompass **people, processes and technology** and **centralising this strategy around the identity** is the only way to tackle the modern obstacles associated with remote working. **Strong management of identities and access is paramount** to ensuring secure and seamless services within local government organisations in order to maximise public safety. But what does this involve?

WHAT IS IAM?

Identity and Access Management **(IAM)** is essentially the way in which you ensure that the **right people** have access to the **appropriate data** at the **right time**. It is the umbrella term for the solution and organisational processes involved with managing user identities and access. IAM covers **three key domains**:

- Identity Governance and Administration **(IGA)**
- Access Management **(AM)** or authentication and authorisation,
- Privileged Access Management **(PAM)**.



Identity Governance and Administration (IGA) centralises the control and management of identities and access.

EXAMPLE of IGA
An employee stops working for a local council. Their access to sensitive public data must be revoked immediately. Joiner, mover, leaver processes can be defined and automated with IGA.

Access management (AM) controls users' access to applications and infrastructure by authenticating their identity and authorising their access.

EXAMPLE OF AM
An employee requires a different password for every area of the council's online portal. Single sign-on (SSO) securely verifies the user's identity to provide centralised access to multiple applications.

Privileged access management (PAM) involves the implementation of additional control measures for elevated access roles such as administrative accounts.

EXAMPLE OF PAM
Someone has gained access to an elevated account in a government organisation. PAM can detect anomalous behaviour and automatically terminate a session before a breach can occur.

COMMON IAM CHALLENGES FOR LOCAL GOVERNMENT

- Huge user population
- Sensitive data
- Budget cuts combined with IT infrastructure and maintenance costs
- Availability of skillsets
- Administrative delays
- Off-boarding security gaps
- Lack of centralised operations
- Lack of access policies for applications
- Lack of awareness
- Maintaining defences against evolving external threats
- Reporting and governance

CYBER ATTACKS ON LOCAL COUNCILS

A minimum of **60 government entities** were impacted by ransomware during the first two quarters of 2020.

Ransomware attacks in February and October 2020 cost Redcar and Cleveland Borough and Hackney Borough Councils more than **£10m each**.

Aside from the financial impact, cyber attacks also disrupt essential services such as **online appointment bookings, council housing complaints and social care systems.**