What Is Identity and Access Management, and Why Do You Need It?

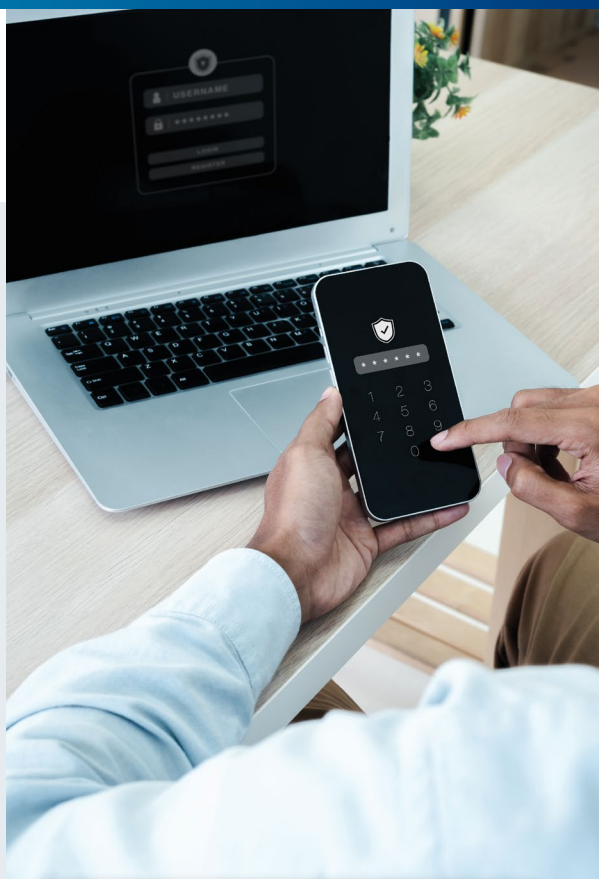
With the news full of cyberattack reports, it's no surprise that the Center for Digital Government names cybersecurity as the top IT priority. To meet cybersecurity challenges and optimize efficiency, governments must have an effective identity and access management (IAM) strategy.

A lack of an IAM strategy is a burden for overextended IT staff. We see the challenge of fragmented identity management in our personal lives, where we have multiple passwords for banks, streaming services, and subscriptions. We juggle multiple passwords, which we may unwisely keep on unsecured scraps of paper or spreadsheets.

Governments face the same issue but on a much more complex scale. Without an effective IAM strategy:

- Employees must deal with multiple passwords for different solutions and devices.
- IT staff must manage credentials for multiple solutions.
- Consistent cybersecurity practices are difficult to maintain.

This is where an IAM strategy comes in. IAM is a security and business discipline that ensures the right employees have access to the right assets – and that the process is secure. IAM is composed of many components, including processes, technology, and services like an identity provider (IdP), a core part of an IAM strategy.



IAM systems can provide a centralized and standardized way to manage identities, access controls, and authentication across different applications, networks, and devices, making it easier and safer for users to access them securely.

What is an Identity Provider (IdP)?

An IdP is a service that stores and manages digital identities for applications, devices, and networks. An organization then uses this service to manage its identity operations.

In your personal life, you likely use a single sign-on (SSO) tool all the time — such as using your Google or Facebook user account to log in to various websites rather than creating and using a unique username and password for each site.

When an IdP is in place in your organization, the experience for the end user will feel similar, but it will come with additional layers of protection and administrator management.

An IdP allows IT staff to use centralized credential management across an organization's systems rather than needing to manage identities in multiple applications. This means users can access their supported solutions via SSO even when the solutions are from different vendors. (The ability for software to connect to an IdP is described as being able to "federate with" that IdP.)

ERP-IAMWYN-II-35576-0624

Key benefits of an IdP include:

- An SSO experience, which saves users time and makes it easier for them to adhere to password guidelines.
- Centralized IT management of employee access, such as adding or removing users or privileges.

Common IdPs include:

- Google Cloud Identity
- Microsoft's Entra ID (Formerly Azure Active Directory)
- Okta Workforce Identity Cloud

How Can an IdP Enhance Cybersecurity?

An IdP is central to safeguarding sensitive information and ensuring operational continuity. Using an IdP offers the following security benefits:

- One set of login credentials is required to access all supported services, making it possible to enforce strong authentication policies.
- Assigning and managing access rights to users can be managed at scale according to roles, which reduces the risk of unauthorized access and allows consistent security policies to be applied to all users across all devices.
- Visibility into access control activity in the form of audit reports, user authentication logs, and resource access requests and usage logs, improving oversight.
- Reducing the number of different passwords a user must remember makes it less likely that the average user will feel the need to write down or otherwise create unsecure copies of passwords.

The Benefits of an Effective IAM

In short, IAM is all about security and efficiency, which is especially valuable for IT departments that are stretched thin and for organizations worried about cybersecurity.

An organization's IAM strategy enables:

- Enhanced cybersecurity, with consistent best practices, used organization-wide.
- Centralized credential management, which ensures consistent practices (such as password requirements).
- Streamlined management of an employee's identity lifecycle. Changes related to onboarding, offboarding, or responsibility must only be made once rather than in multiple applications.
- Multi-factor authentication (MFA), a secure authentication method that requires at least two verification factors. For example, users might need to enter information from a text message on their cell phone to complete a sign-on.

Choosing the right IAM system is critical for decision-makers, particularly IT managers and security professionals. When considering government IAM systems, it's recommended to keep the following factors in mind:

- **Usability and Convenience:** Select an IAM system that focuses on user-friendliness and intuitive interfaces, fostering an easy-to-use experience for staff.
- **Security and Privacy:** Prioritize security. Implement encryption, role-based access controls to safeguard against unauthorized access and data breaches, and multi-factor authentication.
- **Interoperability and SSO:** Enable seamless data exchange and integration with existing systems across multiple departments and agencies. For example, an approved staff member could use one sign-on to access ERP, asset management, and permitting and licensing software.
- **Scalability:** Select an IAM system with scalability to accommodate growing numbers of users and services over time.

To learn how Tyler applications can fit in with your IAM strategy, please contact us at **info@tylertech.com I 833.895.3783 I tylertech.com**

Source: Center for Digital Government (2023)