Trends & recommendations

For Identity and Access Management in 2022

As much of the world has moved to hybrid or remote work, Identity and Access Management (IAM) has moved up the priority list for many IT leaders. KPMG offers a look at the top trends and key recommendations in IAM for 2022.

5 Trends in IAM

1 **Automating onboarding and offboarding hybrid employees**

2 **Implementing IAM across the cloud**

3 **Added protection with password managers**

4 **Adopting a zero trust mindset**

5 **Least privilege principle extends to end-point devices**

IAM is a framework of policies and technologies that allow organizations to make intelligent, risk-based decisions about who is allowed to access which information and operational assets, when, and in what context. With a growing number of employees working "anytime, anywhere and from any device," it's critical for businesses to keep up with the proliferation of identities and systems. Here are 5 trends and priorities to consider:

1 Automating onboarding and offboarding hybrid employees

Onboarding and offboarding employees traditionally involves time-consuming, manual processes. As workforces have pivoted to remote or hybrid models, a fast and seamless onboarding experience is critical, as it often sets the tone of the organization's culture.

The right IAM tools can perform onboarding and offboarding functions at the push of a button. For example, automated provisioning grants employees the right access based on their roles and permission levels – instantly and securely. Automatic deprovisioning, meanwhile, ensures those exiting the organization don't leave behind orphaned accounts, or accounts without an associated user.

2 Implementing IAM across the cloud

No business leader could have foreseen 100% of their workforce suddenly being remote because of a pandemic. The shift put huge pressure on on-premise IT infrastructure and led to slow systems and lower productivity. Businesses are now accelerating their adoption of cloud applications and services. Besides the benefits of cloud nimbleness, these types of tools allow for quick and easy implementation. Moreover, in comparison with older technologies, it will no longer be necessary to go through regular (and often tedious) update cycles.

As more organizations expand into the cloud, a chief concern is how to give employees direct access to cloud and SaaS resources in a safe and secure manner. One way they can do this is by extending the security capabilities already in place for their private infrastructure into a simple but secure approach for the cloud. Many of your existing security technologies have expanded their capabilities to meet this demand, and it is important to understand what you might be able to leverage from your existing toolset with which your teams are already familiar.

3 Added protection with password managers

Along with organizations' expansion into the cloud comes the issue of employees having dozens of accounts to manage, with each needing a unique and secure password. While it's a challenge to remember numerous passwords, using the same password in multiple places opens the door to security risks. IBM research found that compromised credentials were responsible for 20% of cyber breaches in 2021, at an average breach cost of US$4.37 million. Other password-related issues, such as authentication processes or being locked out, can slow performance and productivity.

This is why another IAM tool is becoming more important: password managers. A password manager or password keeper is essentially an encrypted digital vault that creates strong and unique passwords for each application and account, and securely stores the information. This helps make employees' credentials difficult to breach, in addition to eliminating the need to memorize multiple passwords. Many employees are already using these tools, but it is better to review and standardize on a trusted platform at the organizational level.

4 Adopting a zero trust mindset

With the motto "Never trust, always verify," zero trust is a trending architectural principle in security. Essentially, zero trust means continuous verification of user access rights, as well as their devices. This will be increasingly important in securing a remote or hybrid workforce, where users access resources in new ways and often with untrusted devices.

Zero trust is more of a mindset or strategy than a tool or technology. Businesses that adopt zero trust set up a capability architecture that assumes there is no existing trust inside or outside network perimeters; allows for continuous verification of applications, data, devices and users; and is reviewed on an ongoing basis. This approach helps to segment resources, provide just-in-time access, secure code, and protect data.

5 Least privilege principle extends to end-point devices

The principle of least privilege is the practice of restricting access rights for individuals to only those resources they need to perform a specific job or task. For example, a marketing manager doesn't need access to the company's financial statements. While many organizations already practice this principle, least privilege also applies to networks, accounts, devices, and more.

In today's changing workplace environment, organizations will have to extend least privilege across the enterprise. Greater protection must be given to high-value assets including end-point devices like laptops and services, which will help block attacks such as ransomware and insider malicious behaviour. Organizations can enact the just-in-time provisioning principle, giving access to users only at the time required.

IAM as a business enabler

When organizations deploy IAM more widely, they can realize key benefits, including:

- Quickly onboard employees and have them ready to go on day one, creating a positive experience and ensuring productivity
- Decrease IT help-desk requests and employee wait times through self-serve tools
- Provide the right people the correct level of access at the precise time they need it to protect data and guard against potential risks

Privacy matters

With the changing privacy legislation area, such as Bill 64 in Quebec and reforms taking place in other provinces, the protection of personal information has never been more vital. To that end, companies will have to adjust and focus on certain IAM functionalities, such as:

- **Allocation of duties:** Ensure that tasks related to personal data are done by more than one person.
- **Need to know:** Limit sensitive data access only to those individuals who truly require it to perform tasks.
- **Access certification:** Regularly revalidate employee access to systems containing personal information.
- **Threshold for authentication:** Establish a high level of authentication to gain access to sensitive information.
- **Unstructured data:** Carefully monitor access to unstructured data management containing personal information.
- **Automate the lifecycle:** Put in place automatic processes to revoke access when it is no longer required.

On the horizon: A passwordless world

The rise of biometrics (such as fingerprints and facial recognition) has allowed organizations to diversify authentication factors. Initially, organizations expanded their authentication processes from a single unique knowledge factor to adding several other factors (or multi-factor authentication). Despite this, the exponential increase in computing power has allowed malicious actors to rapidly crack passwords, forcing companies to revise their password selection guidelines.

From this trend emerged single sign-on (SSO), which streamlined the user experience, but often at the expense of security. This put additional pressure on organizations, requiring operations teams to constantly reset passwords – a task further complicated by their increased complexity and length.

Consequently, many companies have welcomed the shift to self-service password resetting tools. These leverage several authentication factors, allowing users to set their passwords via a secure system in case of loss.

4 Common Authentication Factors

Knowledge
Something the user knows, such as a password, PIN, or answers to secret questions

Possession
Having a specific device, such as a smartphone, USB key, or VPN key, identified using digital certificates

Inherence
Biometrics such as facial recognition, fingerprint, retina or voice

Location
Geo-location security checks are used to verify user's location

It is vital to find the right balance between security, operational efficiency and user experience. That's why, in the not-too-distant future, these factors will lead to the full disappearance of passwords – what's been dubbed a passwordless world. This shift will be made possible by progress in cryptography, the exchange of public and private keys, and the emergence of new authentication standards.

Passwordless solutions offer many benefits to organizations, including:

- Reduction in operating costs of IT centres dedicated to password resetting
- Increased protection from phishing attacks
- Increase in productivity, as users lose less time submitting requests and waiting for their passwords to reset
- Compliance with National Institute of Standards and Technology (NIST) standards (Authenticator Assurance Levels 2 and 3)

On the horizon: Predictive analytics

IAM's use in risk management processes has encouraged more businesses to take interest in predictive analytics technologies related to their identity and access management procedures. These predictive tools are responsible for the analysis of the data stored by IAM tools, automating the decision-making processes.

This is reflected in areas such as:

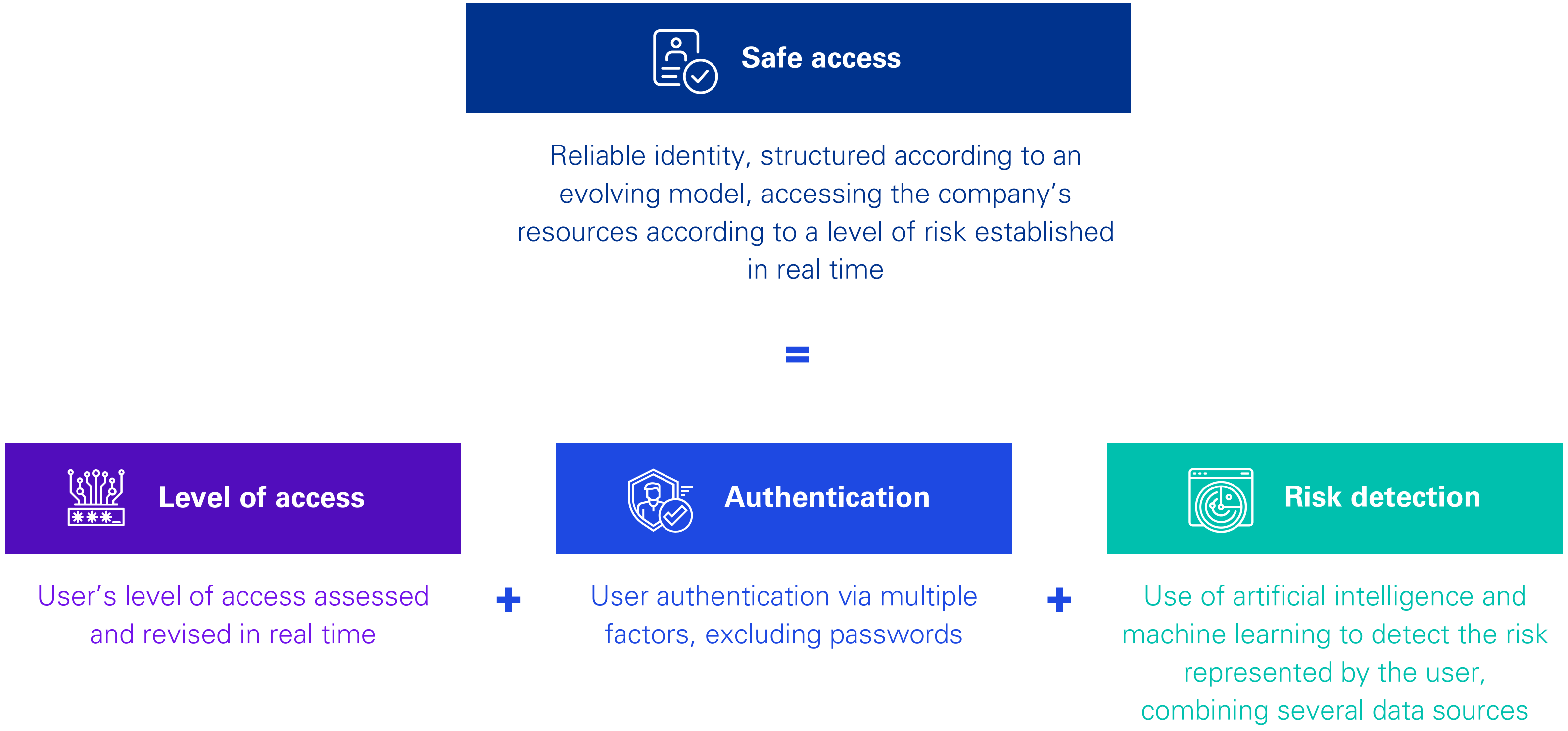
Access approval: Based on the sharing (or not) of certain attributes, the engines will facilitate and even automate certain access approvals or, on the contrary, alert the approver of risks.

Access certification: Using the same principle as the access approval, predictive tools will be able to identify which access requests require the most attention, ensuring priority revalidation.

Task segregation (SoD): Thanks to access verbatim analysis, the engines will be able to detect certain incompatibilities. This is enabled by many IAM solutions having access to libraries of incompatibility rules thanks to their strategic partnerships, for example, SAP.

Safeguarding access in the future

Artificial intelligence engines will detect threats in real time and assess the user’s level of risk when requesting access with a high degree of accuracy. From this analysis, the levels of required authentication and permission will be determined. For example, a user logging in from another country could be required to provide an additional authentication factor, and their privileges could be diminished.



Safe access

Reliable identity, structured according to an evolving model, accessing the company’s resources according to a level of risk established in real time

=

Level of access

User’s level of access assessed and revised in real time

+

Authentication

User authentication via multiple factors, excluding passwords

+

Risk detection

Use of artificial intelligence and machine learning to detect the risk represented by the user, combining several data sources

Our 6 recommendations for IAM

#01 The IAM skilled talent landscape is changing dramatically**. Look to access new talent from broader backgrounds**, such as those from the neurodivergent community, **and complementary fields**, such as Risk and Human Resources, in addition to external specialists to make up your team. Also remember that talent retention is equally as important as recruitment, if not more.

#02 Avoid the "ready, shoot, aim" approach to IAM. **Spend time with your stakeholders to build out the user stories, the processes, and the data flows** for your program. This will save you considerable time in the deployment of your solution and improve its success rate.

#03 Many organizations are **reviewing SaaS based solutions for IAM** to allow for auto-upgrading and reduced workload for infrastructure teams. Know your options and how they might fit into your organizational culture.

#04 Every day we gain greater access to technology that allows for improved capabilities, but without the measurable outcomes the tech is doomed to fail. **A well-defined outcome will help drive process and automation**. These can then be reviewed as key program metrics on an ongoing basis.

#05 **Understand all of the technology's features**. Many organizations purchase technology but only deploy a small portion of the solution. Ask for training and guidance on these other features and see if they can be leveraged for your program; in many cases these are already included in your licensing.

#06 Dedicate time to training. **Make the development of your team a priority** at your organization, set dedicated time aside, and build it into employees' annual review cycle. Individuals are more likely to stay if they feel they are supported, but it is often difficult to prioritize professional development in an operational environment without the support of senior leadership.

Contact us

Thomas Davies
Partner, National Transformation Leader
KPMG in Canada
416-468-7339
thomasdavies@kpmg.ca

Jamie Whynacht
Director, Toronto Lead
KPMG in Canada
416-468-7170
jwhynacht@kpmg.ca

Marc Chaput
Partner, Quebec Lead
KPMG in Canada
514-840-5674
mchaput@kpmg.ca

Erik Berg
Partner, Vancouver Lead
KPMG in Canada
604-691-3245
erikberg@kpmg.ca

Imraan Bashir
Partner, Eastern Canada Lead
KPMG in Canada
613 212 2852
ibashir@kpmg.ca

Robin Tong
Partner, Western Canada Lead
KPMG in Canada
780-429-7335
robintong@kpmg.ca

home.kpmg/ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.