Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Identity, Credential, and Access Management (ICAM)

August 2022

ITSAP.30.018

Identity, credential, and access management (ICAM) is a set of security tools, policies, and systems that helps organizations manage, monitor, and secure access to their information technology (IT) infrastructure. ICAM represents the combination of digital identities, credentials, and access controls into a single comprehensive approach. ICAM reduces the risk of cyber attacks to your organization by preventing unauthorized access to your networks, systems, and data. This document offers information on how implementing ICAM can benefit your organization's cyber security.

What does ICAM Include?

Your organization's ICAM model will impact the following three elements of your IT security processes:

Identity management: Identifies a subject and establishes that they are and who they claim to be when authorizing access to a system (i.e. physical entity, digital entity).

Credential management: Binds the identity to an authenticator, allowing the system to identify the user through login (i.e. user authentication, identification card, username and password).

Access management: Grants permissions for what users can do and see within a system (e.g. using specific groups and role for separation). Access management determines which roles or users can access different information and processes at specific times and levels of security (i.e. restrict access to a database unless the user is authenticated and is in a role that has been granted access to that resource).

What are the benefits to using ICAM?

Benefits of a well-structured ICAM program include:

- Improving your cyber security by limiting access to authorized users
- Simplifying your organization's user management
- Securing access to information
- Tracking access to sensitive information with more effective management
- Helping prevent identity fraud

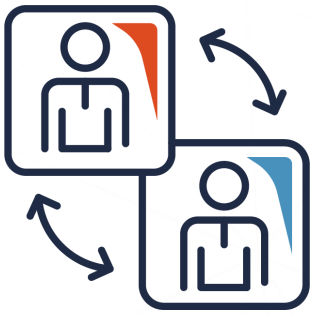
Awareness SERIES

Cat. No. D97-1/30-018-2022E-PDF
ISBN 978-0-660-44910-4

What are the risks without ICAM?

Threat actors seek to steal user identities and credentials in order to access networks, systems, and data. These types of cyber attacks pose significant risks to your organization, including:

- Compromising sensitive information
- Spreading misinformation
- Compromising proper function of processes and equipment
- Damaging system and information integrity and availability
- Losing organization reputation and credibility
- Compromising execution of emergency processes
- Risking impacts to national security



These risks usually stem from threats associated with phishing attacks and malware that have exposed credentials and access information to threat actors. Compromised access is a high risk for organizations dealing with sensitive information, critical resources, and emergency processes.

What should I consider when implementing ICAM?

There are a few considerations when implementing ICAM to ensure your organization's information is secured. Some security tools to consider when creating your ICAM framework include:

Passphrases and passwords

Enforcing best practices for passphrases and passwords is an important security measure for ICAM. Ensure all accounts and access areas are protected with complex passphrases or passwords to keep information secure.

Biometrics

Biometrics are used as a convenient form of authentication. Using your unique body characteristics as identification, biometrics can be used instead of or alongside a pin, password, or passphrase.

Multi-factor authentication (MFA)

MFA offers two or more different authentication factors to unlock a device or account. Enforcing the use of MFA on your organization's devices and accounts will add an extra layer of protection for individuals and organizational data.

Two-person integrity (TPI)

TPI requires at least two authorized individuals to access a secured area of system. This reduces the risk of sensitive information or processes being accessed by singularly stolen credentials. TPI also ensures that the sensitive area can only be accessed on a need-to-know basis.

Principle of least privilege

Create groups and roles for specific users to gain access to equipment and information only if they need to. Implementing the principle of least privilege will help ensure access is granted to only those who need it.

Cyber security training

Cyber security training to offer awareness and appropriate usage of organizational information and security tools is an important step in creating a cyber safe environment. Enhancing awareness and security practices in regards to individuals' credentials and access is important for your ICAM structure.

For further details on the security tools mentioned above, see the following publications on our website:

- *Best practices for passphrases and passwords (ITSAP.30.032)*
- *Biometrics (ITSAP.00.019)*
- *Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)*
- *Offer tailored cyber security training to your employees (ITSAP.10.093)*

What should I remember?

Your organization may not need an entire model for ICAM, depending on the sensitivity of information being handled. Implementing any security tools used in ICAM models that fit your organization's needs will help secure you and your organization from cyber threats.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**