cloudeagle.ai

8 Identity & Access Management Risks You Must Know

www.cloudeagle.ai

Table of Contents

Introduction

Are you constantly worried about your organization's security? What if someone gains access to your systems and steals critical data, potentially harming your ongoing operations?

If you aren't aware of all potential identity and access management risks, your priority should be identifying loopholes and implementing proactive protection measures.

In today's world, where data breaches and cyberattacks are serious risks for businesses of any size, strengthening your IAM framework isn't just a good idea—it's crucial for your organization's safety and success.

Neglecting these measures exposes your organization to exploitation by hackers who can infiltrate systems, steal sensitive data, and disrupt infrastructure. The average data breach cost has reached 4.45 million US dollars, marking a 15% increase over the past three years.

Check out this article to learn about these identity and access management risks and avoid common security mistakes. This comprehensive article covers cybersecurity, highlighting common errors and offering practical strategies for strengthening the organization’s security.

The 8 most common Identity and Access Management risks

Explore the essential aspects of the IAM framework by uncovering the top 8 identity and access management risks that organizations commonly encounter.

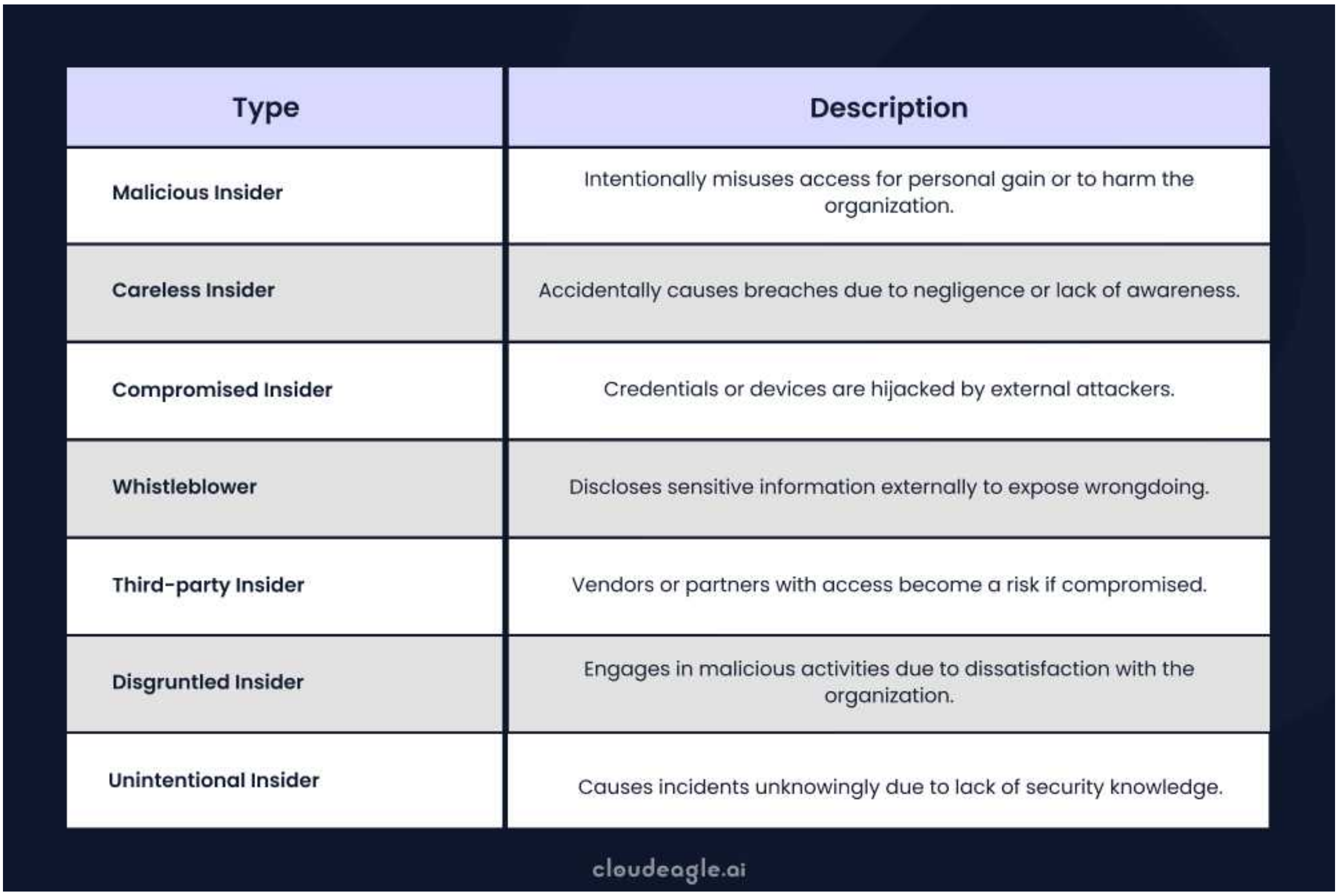
1. Insider threats and misuse of privileged access

The most common identity and access management risks include mistakes made by existing employees, known as insider threats.

For example, an unhappy employee might abuse privileged access to manipulate financial records or steal intellectual property. Similarly, a contractor with access to sensitive systems could intentionally leak confidential information to a competitor for personal gain.

These threats can be intentional or unintentional and may arise for various reasons, including disgruntlement, financial incentives, negligence, or ignorance.

This table will help you understand the different types of insider threats.



Type	Description
Malicious Insider	Intentionally misuses access for personal gain or to harm the organization.
Careless Insider	Accidentally causes breaches due to negligence or lack of awareness.
Compromised Insider	Credentials or devices are hijacked by external attackers.
Whistleblower	Discloses sensitive information externally to expose wrongdoing.
Third-party Insider	Vendors or partners with access become a risk if compromised.
Disgruntled Insider	Engages in malicious activities due to dissatisfaction with the organization.
Unintentional Insider	Causes incidents unknowingly due to lack of security knowledge.

cloudeagle.ai

These insider threats create major hurdles for IAM systems, bringing about a range of negative impacts.

- Firstly, they can lead to unauthorized access to sensitive data and systems, resulting in serious consequences like data breaches, theft of intellectual property, or financial losses.
- Secondly, these threats can disrupt business operations and critical services, causing downtime, damaging the organization's reputation, and eroding customer trust.
- Thirdly, they may result in compliance violations with regulatory requirements, leading to legal penalties, fines, and further harm to the organization's reputation.

2. Weak password and authentication practices

Many of us use weak passwords like "123456," "admin," and "password," making it easy for hackers to access our privileged accounts. Weak passwords present significant risks as they are susceptible to various cyber attacks, such as brute-force and phishing attempts.

Additionally, sharing and reusing credentials heighten the risk of compromise across multiple accounts. Surprisingly, despite the danger, 45% of remote users use the same password for both work and personal accounts.

Use strong passwords and multi-factor authentication (MFA) to keep things safe. MFA adds extra layers of security, making it harder for hackers to attack or steal identities. It also helps organizations follow security rules and makes users more responsible.

3. Lack of visibility into user access data

Organizations face big problems when they can't see who's accessing what. Not being able to see everything also means it's harder to catch someone sneaking in where they shouldn't be or spotting old accounts that shouldn't still have access.

For example, if employees have access to data they don't need anymore and no one's checking, it's easier for that data to end up where it shouldn't.

Also, undetected dormant accounts pose risks, including security breaches, data loss, compliance violations, insider threats, operational disruptions, reputation damage, and ineffective user lifecycle management.

To mitigate these risks, organizations should implement robust access controls, monitor account activity, enforce strong authentication, conduct regular audits, and provide employee training on security best practices.

Tracking and managing user access can be challenging without sufficient monitoring and auditing mechanisms. With 62% of security teams facing visibility limitations, tracking access becomes more difficult.

As organizations transform digitally and embrace cloud technologies, monitoring data access becomes more complex. IT teams struggle to track and manage user access effectively without comprehensive visibility into the entire technology stack and its access mechanisms.

So, organizations must set up secure systems to watch who's accessing what and ensure they catch any problems before they become big.

4. Unauthorized access

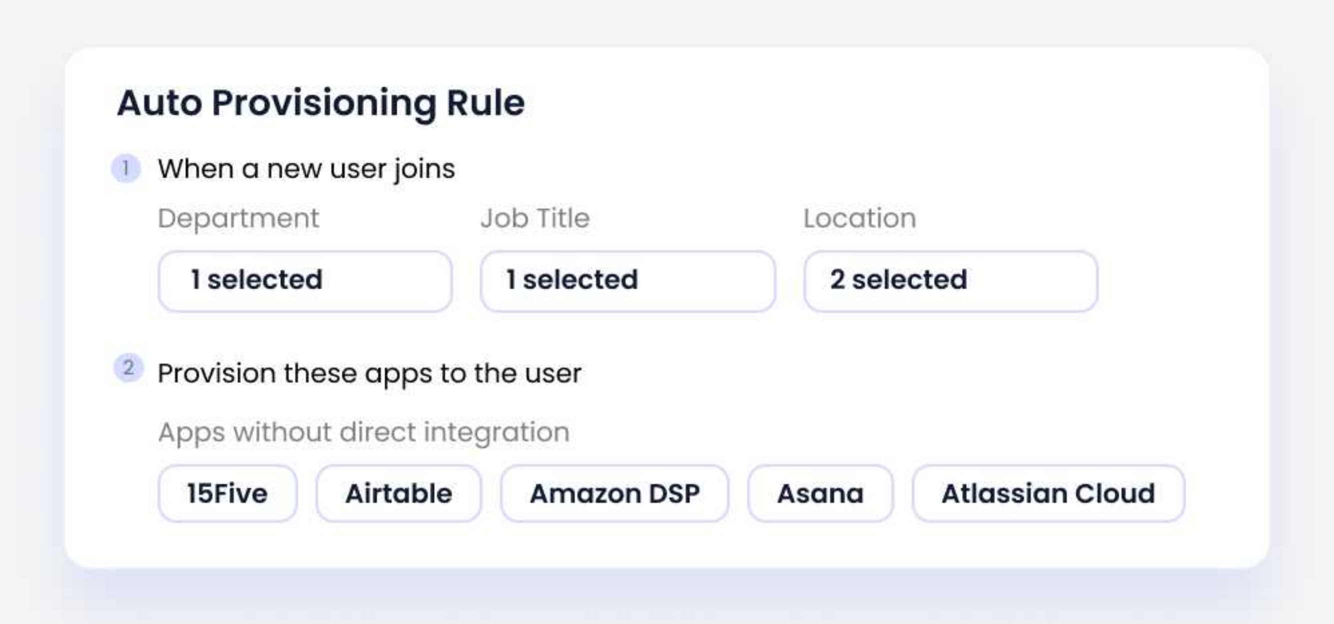
Improper user deprovisioning can lead to serious security risks, including unauthorized access by ex-employees who still retain user account privileges. Unauthorized access can lead to severe consequences for organizations, including data breaches, intellectual property theft, disruption of operations, and compromised trust.

Organizations can employ various techniques to prevent unauthorized access, including strong authentication, access control, and encryption, and provide employee training on these techniques and regular security updates.

If you want to implement advanced monitoring and prevention mechanisms to safeguard your organization, you can opt for CloudEagle. With real-time monitoring, robust authentication, and easy SSO and HR systems integration, CloudEagle ensures accuracy and efficiency across the identity and access lifecycle.

With CloudEagle, requesting access to SaaS apps and getting approval happens fast because it's automated. This also means when someone leaves the company, access can be taken away quickly, without mistakes that often happen when doing it manually.

CloudEagle makes managing all your SaaS apps simple. It helps automate employee onboarding by suggesting the apps they need. When they leave, it ensures their access is promptly removed, keeping your system secure. Everything can be done with just a click, saving time and effort.



Auto Provisioning Rule

1 When a new user joins

Department: 1 selected

Job Title: 1 selected

Location: 2 selected

2 Provision these apps to the user

Apps without direct integration

Also, hackers employ techniques such as phishing, brute force attacks, or exploiting software vulnerabilities to gain unauthorized access. Once inside, they can steal data, disrupt operations, or deploy malware. For example, exploiting outdated software vulnerabilities allows attackers to access a company's network infrastructure illegally.

Therefore, taking proactive measures will keep your systems safe and secure. With CloudEagle, you control your SaaS apps, ensuring smooth deployment and supervision. Its security features strengthen defenses, while automated processes save time.

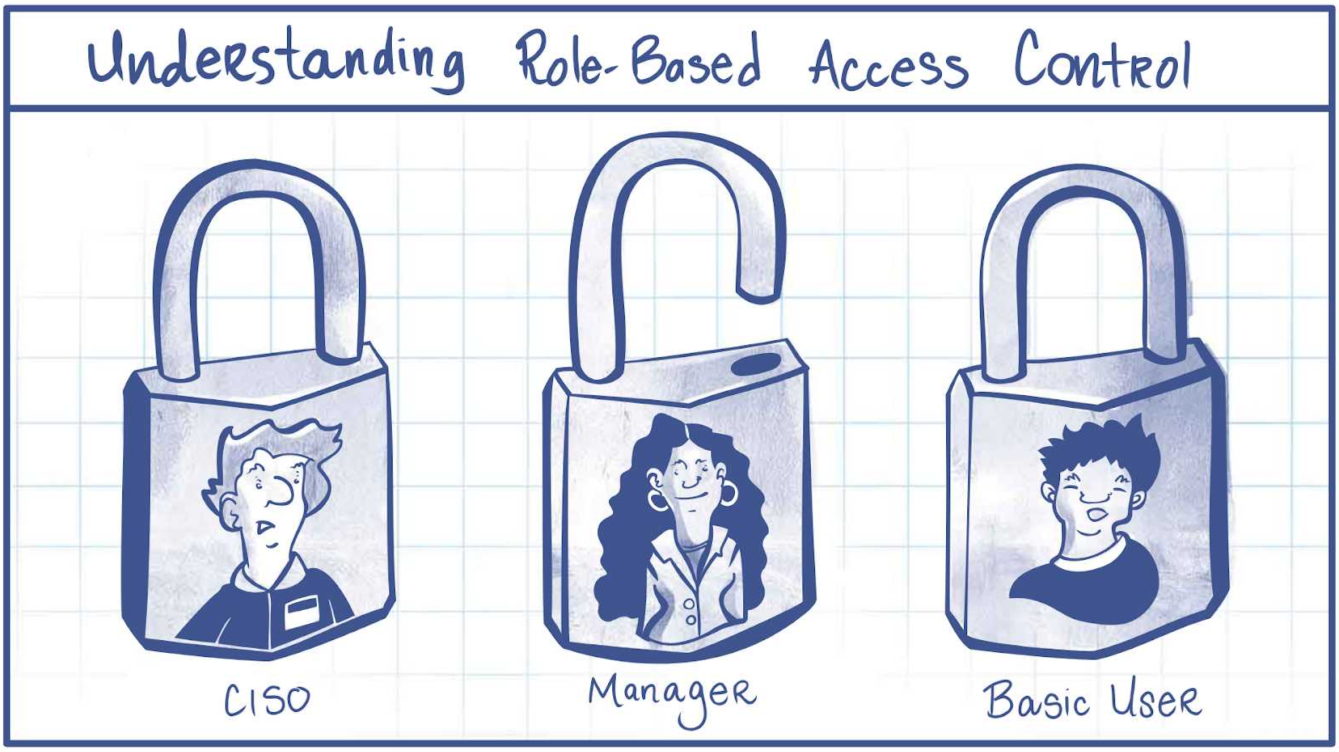
5. Inadequate access controls

Access control weaknesses are problems in how organizations manage who can access their information. Issues like weak passwords or not monitoring who's accessing what can lead to unauthorized access to sensitive data.

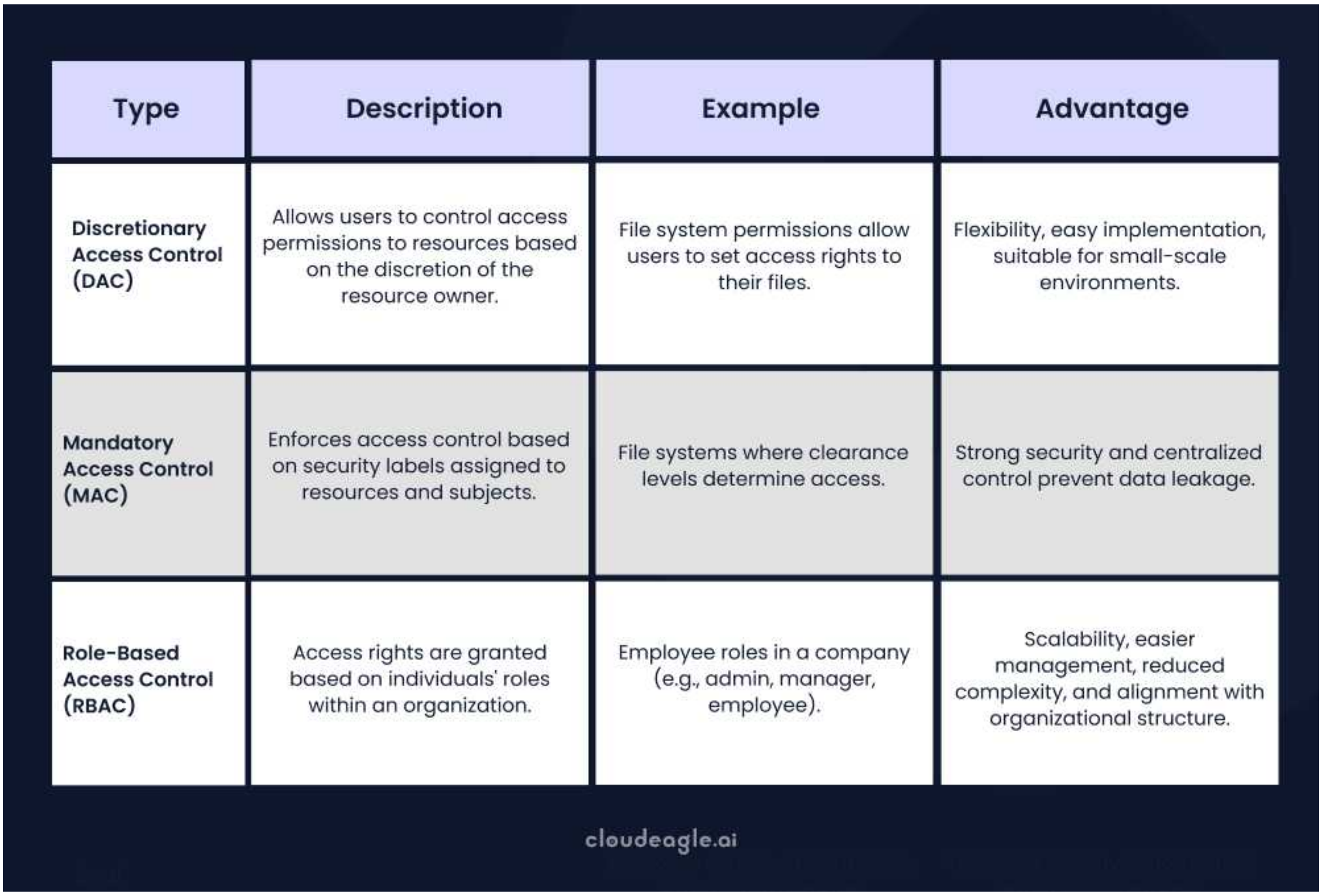
Failure to set up proper access controls can allow unauthorized people to access important information or systems. For example, having data access that doesn't match their job roles raises the chance of accidental or purposeful data leaks.

Imagine a new employee having free access to financial records. This could lead to them accidentally sharing or using sensitive data for personal gain. To prevent this, you can set up different access controls.

To prevent this, it's important to have strong ways of checking who's who, like using multi-factor authentication and ensuring people only have access to what they need for their jobs. Regularly monitoring things helps catch problems early.



This table will help you understand the various types of access controls and apply them to secure your organization's security.



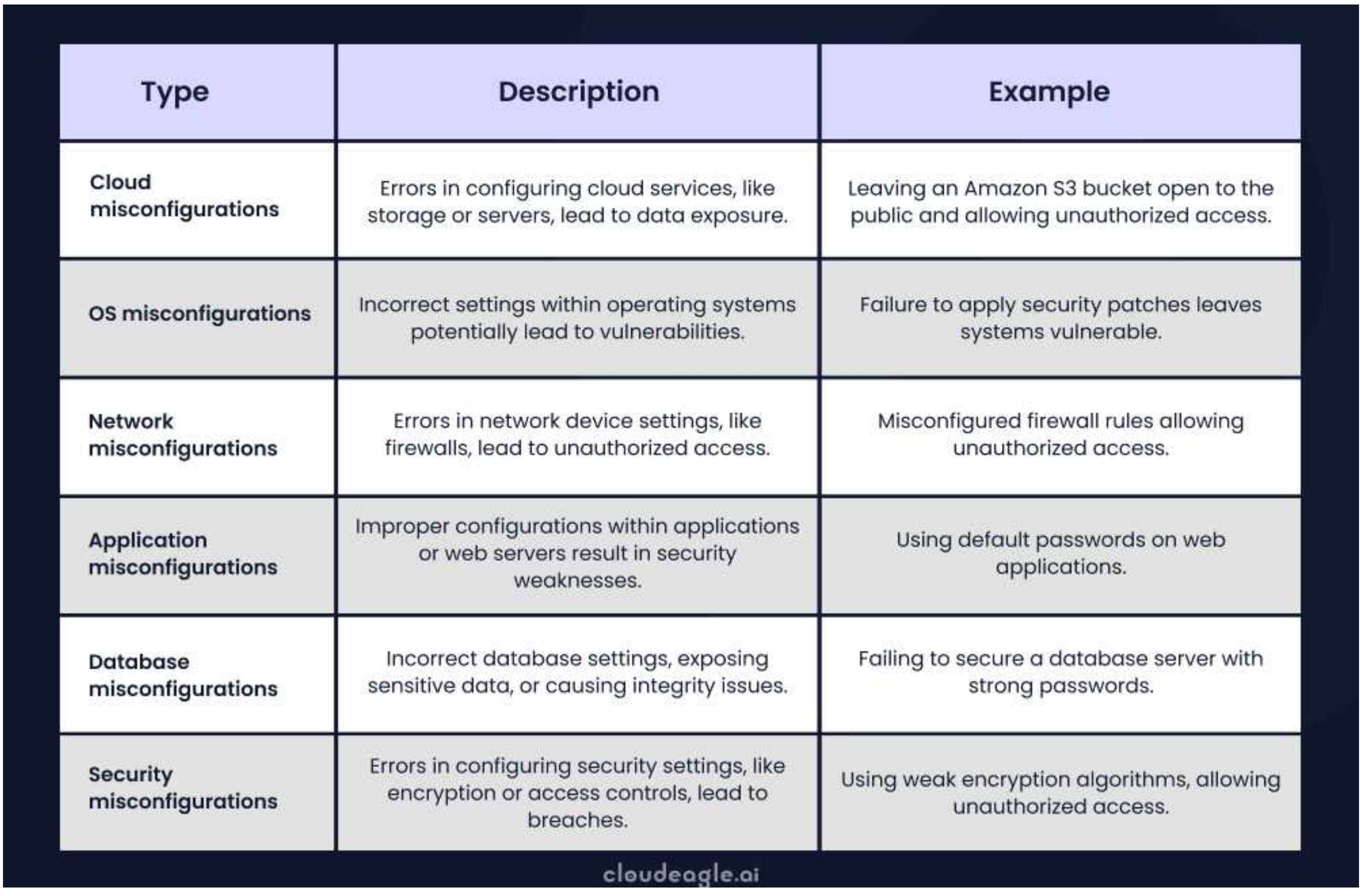
Type	Description	Example	Advantage
Discretionary Access Control (DAC)	Allows users to control access permissions to resources based on the discretion of the resource owner.	File system permissions allow users to set access rights to their files.	Flexibility, easy implementation, suitable for small-scale environments.
Mandatory Access Control (MAC)	Enforces access control based on security labels assigned to resources and subjects.	File systems where clearance levels determine access.	Strong security and centralized control prevent data leakage.
Role-Based Access Control (RBAC)	Access rights are granted based on individuals' roles within an organization.	Employee roles in a company (e.g., admin, manager, employee).	Scalability, easier management, reduced complexity, and alignment with organizational structure.

6. Misconfigurations

System or application confusion can accidentally expose sensitive data or create security risks. Nearly 23% of cloud security incidents stem from misconfigurations, while 27% of businesses have faced security breaches in their public cloud systems.

For instance, wrongly set up cloud storage could make data accessible to anyone online, resulting in breaches. Similarly, misconfigured firewall rules might permit unauthorized access to internal networks, jeopardizing the organization's security.

Review this table to grasp how various misconfigurations impact your organization's security.



Type	Description	Example
Cloud misconfigurations	Errors in configuring cloud services, like storage or servers, lead to data exposure.	Leaving an Amazon S3 bucket open to the public and allowing unauthorized access.
OS misconfigurations	Incorrect settings within operating systems potentially lead to vulnerabilities.	Failure to apply security patches leaves systems vulnerable.
Network misconfigurations	Errors in network device settings, like firewalls, lead to unauthorized access.	Misconfigured firewall rules allowing unauthorized access.
Application misconfigurations	Improper configurations within applications or web servers result in security weaknesses.	Using default passwords on web applications.
Database misconfigurations	Incorrect database settings, exposing sensitive data, or causing integrity issues.	Failing to secure a database server with strong passwords.
Security misconfigurations	Errors in configuring security settings, like encryption or access controls, lead to breaches.	Using weak encryption algorithms, allowing unauthorized access.

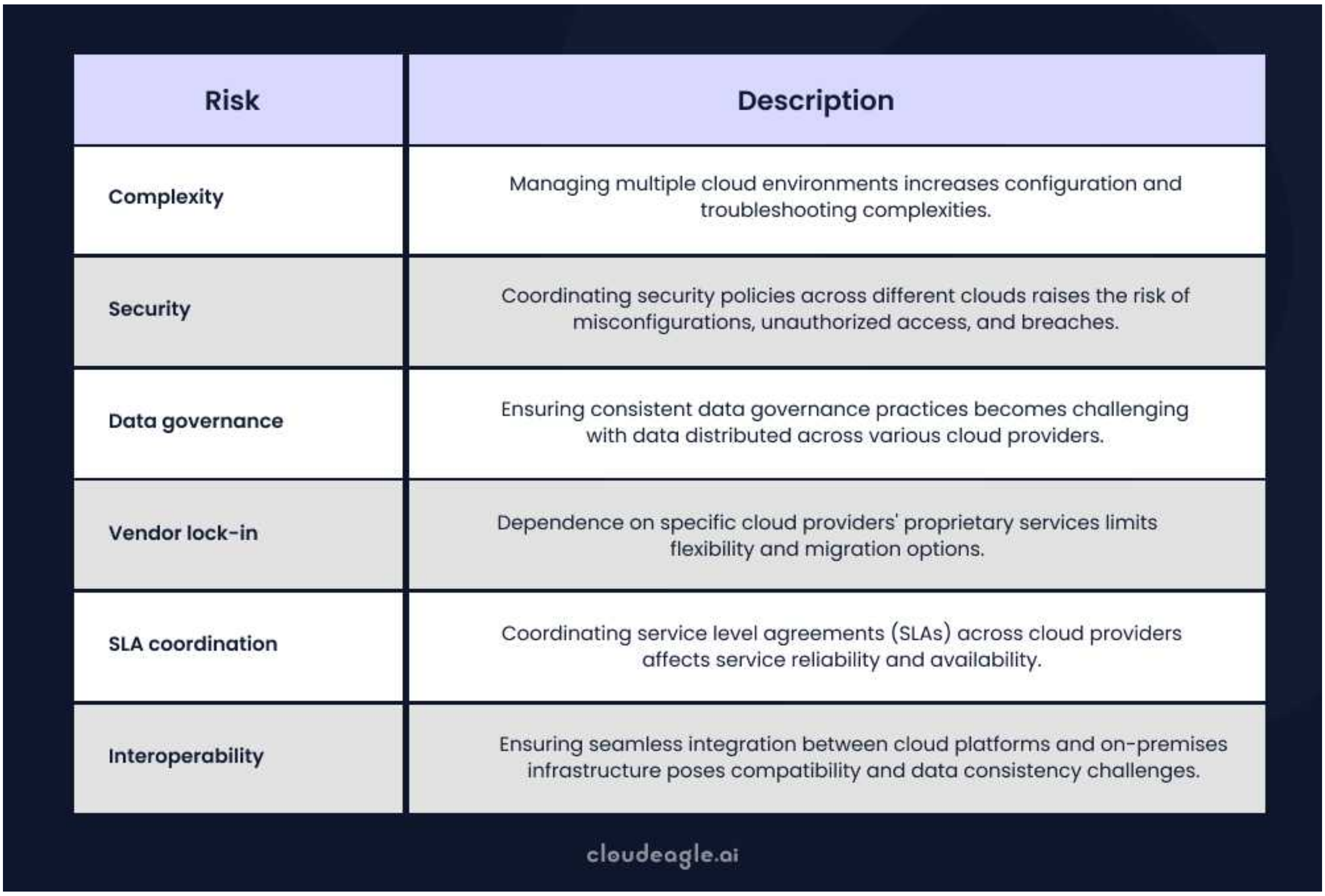
7. Risks of multi-cloud architecture

Using a multi-cloud setup has lots of benefits. It helps with disaster recovery, gives flexibility, avoids getting stuck with one provider, improves performance by using different locations, saves money, and lets organizations pick the best services from different providers.

But it's not all easy. Dealing with multiple clouds can be complicated and risky. Ensuring everyone has the right access and keeping data safe with encryption keys across different clouds needs careful planning. If not done right, there could be mistakes and security holes.

Plus, if there's a security problem in one cloud, it might spread to others if they're not kept separate. So, while using lots of clouds can be smart, it's important to focus on keeping things secure and well-managed to avoid problems.

Check this table to understand the increased risks of using multi-cloud environments.



Risk	Description
Complexity	Managing multiple cloud environments increases configuration and troubleshooting complexities.
Security	Coordinating security policies across different clouds raises the risk of misconfigurations, unauthorized access, and breaches.
Data governance	Ensuring consistent data governance practices becomes challenging with data distributed across various cloud providers.
Vendor lock-in	Dependence on specific cloud providers' proprietary services limits flexibility and migration options.
SLA coordination	Coordinating service level agreements (SLAs) across cloud providers affects service reliability and availability.
Interoperability	Ensuring seamless integration between cloud platforms and on-premises infrastructure poses compatibility and data consistency challenges.

cloudeagle.ai

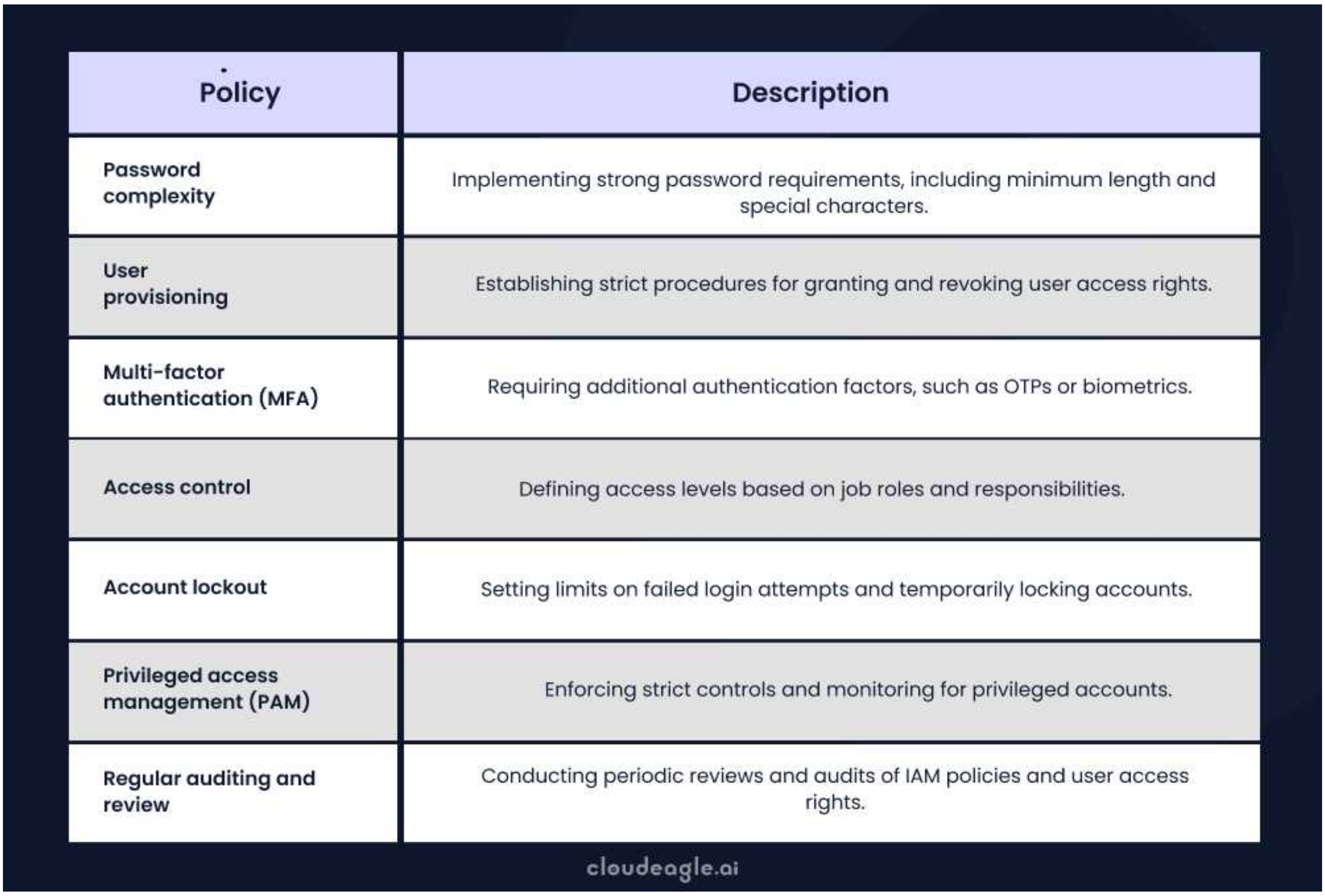
8. Weak IAM security policies

80% of cyberattacks utilize identity-based attack methods, according to CrowdStrike. Thus, organizations must establish clear and robust IAM security policies to govern user access and authentication practices.

Implementing strong password policies is vital for enhancing IAM security controls. Weak password policies can severely compromise your organization's security.

For instance, lacking strict rules for password complexity, employees might choose easily guessable passwords, inadvertently inviting attackers to exploit accounts through brute force or password-spraying attacks.

To address these risks, enforce robust password policies within your organization. You can enable the mentioned policies within your organization.



Policy	Description
Password complexity	Implementing strong password requirements, including minimum length and special characters.
User provisioning	Establishing strict procedures for granting and revoking user access rights.
Multi-factor authentication (MFA)	Requiring additional authentication factors, such as OTPs or biometrics.
Access control	Defining access levels based on job roles and responsibilities.
Account lockout	Setting limits on failed login attempts and temporarily locking accounts.
Privileged access management (PAM)	Enforcing strict controls and monitoring for privileged accounts.
Regular auditing and review	Conducting periodic reviews and audits of IAM policies and user access rights.

Mitigating IAM Risks: Proactive Measures

To mitigate the IAM risks, you must:

Select IAM solution: Evaluate existing IAM tools, access management processes, encryption policies, and logging mechanisms to identify gaps and areas for improvement.

Choose a comprehensive IAM solution that supports automation, RBAC, MFA, access reviews, encryption, and logging capabilities. Popular options include Azure Active Directory, AWS IAM, Okta, or similar platforms.

Automate role assignment and revocation: Define clear roles and responsibilities within the organization and create corresponding policies for access management, encryption, password policies, MFA, and Role Based Access Control.

Utilize IAM tools to automate the assignment and revocation of user permissions based on predefined roles or job functions. Implement scripts or workflows to adjust excessive permissions automatically as roles change.

Automate access reviews: Set up automated access review processes to periodically evaluate user access rights and identify anomalies or violations. Use IAM tools to generate reports and trigger alerts for unauthorized access.

Enforce MFA & implement strong password policies: Configure IAM solutions to enforce MFA requirements for accessing sensitive systems or data. Integrate with authentication mechanisms like OTP, biometrics, or hardware tokens for enhanced security.

Configure IAM solutions to enforce strong password policies, including complexity requirements, regular password changes, and password rotation. Automate password expiration and reset procedures.

Centralize identity management: Implement a centralized identity governance system to streamline user provisioning and deprovisioning workflows. Automate user onboarding, offboarding, and access request processes to ensure timely system access management.

Continuous monitoring and logging: Configure IAM solutions to enable continuous monitoring and logging of user activities, access attempts, and security events. Implement automated alerts for suspicious behavior or security incidents.

RBAC and privilege audits: Implement RBAC by defining roles and automating role assignments based on user attributes. Conduct regular automated privilege audits to ensure policy compliance and adjust permissions as needed.

Just-in-time access provisioning: Implement just-in-time access provisioning that grants users temporary access based on their immediate needs. Automate the process of granting and revoking access promptly to minimize security risks.

To deepen your understanding and effectively implement the above-mentioned practices within your organization, check out this blog, “7 Identity and Access Management Best Practices.”

Hear from Joshua Peskay, a 3CPO (CIO, CISO, and CPO) at RoundTable Technology, as he talks about managing Shadow IT in the era of remote work and presents an ROI score for SaaS tools to assist businesses in optimizing their technology investments.

Conclusion

When you proactively implement these identity and access management measures, you can strengthen your organization's IAM security frameworks, reduce the likelihood of security incidents, and safeguard sensitive data and systems from potential threats and vulnerabilities.

Protecting against identity and access management risks is essential for maintaining the integrity and security of digital assets within organizations. Numerous challenges exist in today's cybersecurity landscape, such as insider threats, weak authentication practices, and misconfigurations.

By prioritizing security and implementing different strategies to mitigate identity and access management risks, you can strengthen your organization’s defenses against cyber threats.

If you want to strengthen your organization's cybersecurity measures, it's wise to seek valuable insights and guidance from industry experts to build a solid plan.

Consider scheduling a meeting with CloudEagle to learn more about protecting your organization from security threats.