WHITEPAPER

IAM: Enhancing Information Security Through Effective Access Reviews

Introduction

As businesses usher in a new year, it's an opportune time to reassess and strategize their information security programs. This is particularly crucial for small and medium-sized enterprises (SMEs), which often grapple with limited resources. While continuous improvement in information security is ideal, it may not always be feasible for these businesses. This whitepaper underscores the importance of access reviews as a vital component of an organization's information security strategy, especially for SMEs.

The Importance of Access Reviews

Access reviews, or user access reviews, are critical in determining who has access to specific resources within an organization. This process involves scrutinizing the rights and privileges of individuals or entities interacting with data, applications, systems, or other sensitive resources. The primary objectives of access reviews are:

1. **Preventing Unauthorized Access:** Ensuring that only authorized users have access to resources; access reviews play a pivotal role in preventing data breaches.
2. **Adhering to Least Privilege and Zero Trust Principles:** These reviews help in maintaining the minimum necessary access for users to perform their job duties, aligning with the principles of least privilege and Zero Trust.

Regular and relevant access reviews are not only essential for security but may also be legally or contractually mandated.

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Regulatory Requirements for Access Reviews
Access reviews are mandated or implied in various regulations and standards, including:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Service Organization Control 2 (SOC2)
- Control Objectives for Information and Related Technologies (COBIT)
- ISO 27001
- NIST 800-53 and NIST CSF
- Federal Information Security Management Act (FISMA)

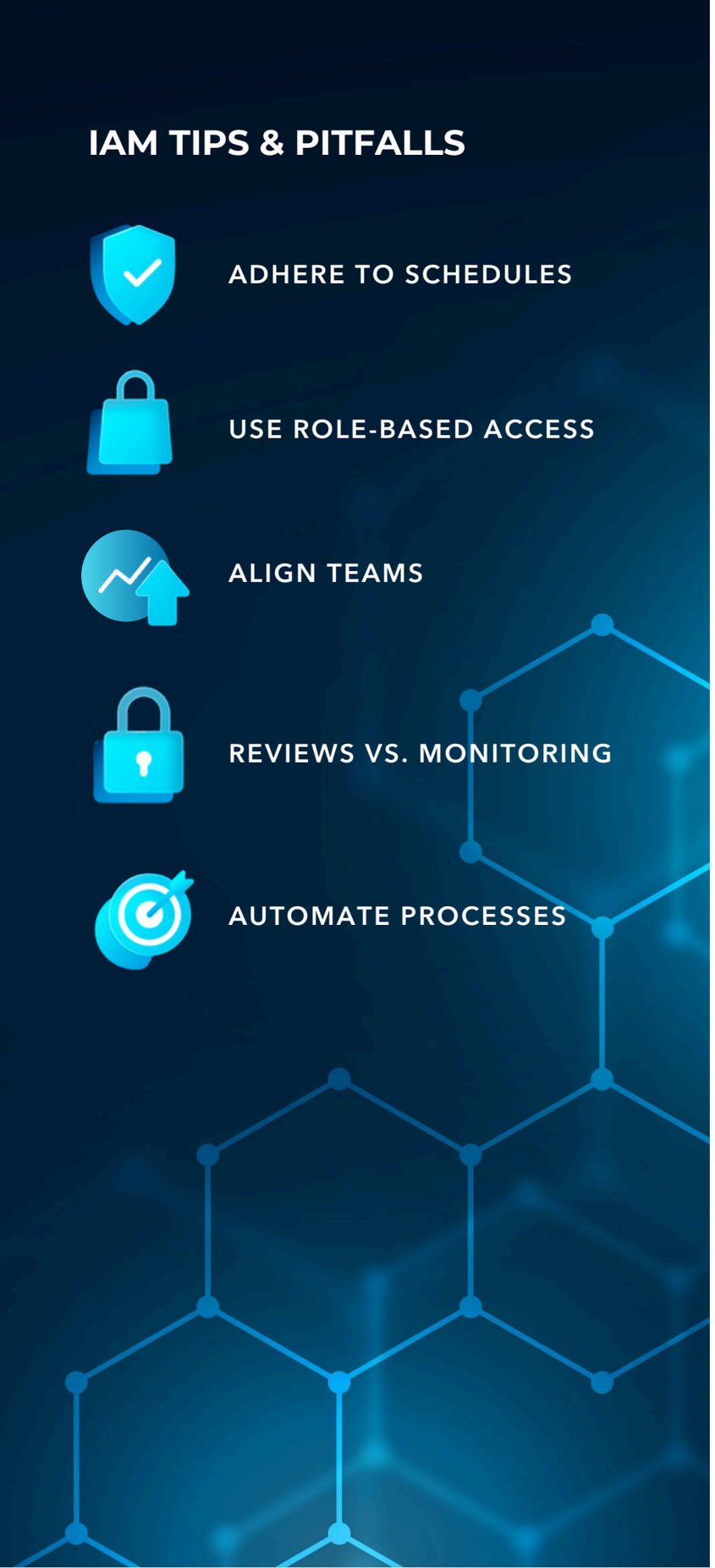
These regulations often consider access reviews as reasonable and customary controls within a comprehensive enterprise security strategy.

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Conducting an Access Review Campaign
Performing access reviews can be manual or technology-supported, with AI and Machine Learning increasingly streamlining the process. The typical steps involved are:

1. **Identify Resources:** Determine the applications, systems, data types, or repositories subject to review.
2. **Identify Users:** List all users with access, including employees, contractors, and vendors.
3. **Identify Decision Makers:** Determine who will make decisions about access, such as managers or data custodians.
4. **Create and Distribute Review Requests:** Develop communications and distribute documents to reviewers, setting a response deadline.
5. **Conduct Reviews and Make Decisions:** Reviewers should decide whether to modify, remove, or maintain existing access.
6. **Compile Results:** Follow up with non-respondents and compile responses for remediation.
7. **Remediate Access:** Methodically adjust access as indicated by the review.
8. **Archive Documentation:** Retain all documents and logs for future reference and proof of activity.

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661



Tips and Pitfalls to Avoid

- **Adhere to Schedules**: Preschedule reviews and stick to timelines.
- **Use Role-Based Access**: Define access based on job functions.
- **Include All Account Types**: Review service and local accounts, which are often high-access targets.
- **Align HR and IT Systems**: Ensure consistency between HR and IT records.
- **Distinguish Between Reviews and Monitoring**: Access reviews are moment-in-time checks, while monitoring is continuous.
- **Automate Processes**: Leverage tools to automate reviews, reducing time, labor, and errors.

Conclusion

Access reviews are a critical component of an effective security program. Regular, predictable, and methodical execution of access reviews is essential for maintaining the integrity and security of an organization's data and systems. SMEs, in particular, should prioritize these reviews as part of their annual security strategy planning, ensuring compliance with various regulatory requirements and safeguarding against unauthorized access. By integrating access reviews into their security protocols, businesses can significantly enhance their overall security posture.

RKON

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

The Value of An IT Partner

For over 25 years, RKON's human brilliance has driven our technology solutions, guiding customers to a fortified, Quiet IT environment. At RKON, we do that through a security-first approach that meets our customers where they are in their digital journey. Security is seamlessly integrated into every aspect of our work, ensuring peace of mind and proactive protection for your organization. Where others see challenge, we see opportunity.

Because of our record in providing best-in-class IT solutions and our staff of respected and knowledgeable professionals, RKON has been recognized by CIO Coverage as a top 10 leading Microsoft Partner to Watch, Crain's Fast Fifty, CRN Growth 150, Inc. 5000 and Inc. Magazine's list of 500 fastest-growing private companies.

RKON's trusted advisors deliver strategic guidance, advanced technical knowledge and realistic assessments to give your organization the competitive advantage it requires in today's environment of rapidly evolving technologies. Here at RKON, we understand that our client's success starts with our organizational cohesion.

Are you looking for a proactive approach to fortifying your digital environment? Get rid of the unknown and control, secure, and monitor your business for a better peace of mind. Talk to a cybersecurity expert today.

ABOUT RKON

Founded in 1998 in Chicago, RKON has grown to become one of the nation's leading IT advisory practices. Our comprehensive understanding of execution strategies, technology, business processes, operations analytics, risk and compliance, and planning and integration supports hundreds of organizations.

Recognizing that no two companies have the same IT challenges, RKON takes a truly customized approach. We serve as trusted advisors to our customers, providing strategic guidance, technical resources, and honest assessments to address competitive challenges and meet long-term goals.

CONTACT US

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661