SafePaaS Cential

How to address the risks and compliance requirements associated with securing and monitoring access to critical systems and data sets.

Current trends, challenges and solutions

Table of Contents

The aim of this ebook is to present an overview of the current challenges organizations face as they seek to address the risks and compliance requirements associated with securing and monitoring access to critical systems and data sets. It reviews the current trends and issues faced by organizations, discusses the implications of using ineffective and inefficient processes, and explores solutions for leveraging solutions such as SafePaaS in conjunction with broader GRC solutions to provide a solution to the problem.

What are some of the current trends?

Newer, more hazardous risks are arising due to advancements and improvements in technology. The increase in the sophistication of technology has provided malicious actors with better tools at their disposal. Bad actors are always on the cutting edge of technology, which can be a frightening proposition for many companies. Data breaches have become all too common, with trends like insider threats, social engineering, and lack of security awareness compounding the issue.

Trend 1: The rate at which risk can occur is also accelerating, shifting, and changing. The many disparate systems people use to perform their daily tasks change risk.

Organizations have numerous applications and databases creating a considerable challenge and threat. Effective user access and provisioning is a daunting task

Trend 2: The great resignation ups the access and provisioning game, creating significant issues when employees or contractors depart the organization:

1. Knowing what employees and contractors have access to.
2. Knowing how access is revoked.
3. Determining what organization proprietary information has not been returned/retained.

Organizations need to protect themselves when people are leaving the organization.

Trend 3: Protecting sensitive data has become more critical than ever. Organizations face a wide array of evolving requirements from regulators and industry organizations to demonstrate adequate and proper protection and security of data. This applies to virtually all data they manage – customer, employee, intellectual property, proprietary financial information, etc. As such, the scope and breadth of what they must address are vast.

It is common to have numerous applications, policies, and individuals who require access to different environments in the modern, digital organization. But the challenge is, how do you grant access and not increase risk into the organization? Many organizations perform access certification and provisioning manually, which does not provide adequate visibility over the process. Organizations need to be able to see at a granular level what each role encompasses, and managers need an easy way to analyze the access privileges before they are granted.

Organizations, therefore, need to have visibility and be able to certify at any point in time:

- Who has access to what?
- Who has access to the database?
- Who has access to the network? and
- Is there a conflict or risk with any combination of their privileges?

Without an automated solution in place, this is a difficult, error-prone, time-consuming task.

How can organizations address these new regulatory requirements to demonstrate both data protection and data security?

One of the largest threats is bad actors using sophisticated technologies and capabilities. If organizations don't invest in protection at the same rate as the bad actors, these organizations will be at a stark disadvantage. Technology can help stem the tide of threats but it requires the commitment of organizations to keep up with the cutting edge of technology.

Organizations can safeguard their data with an effective provisioning and certification process. As technology expands and applications improve, organizations will face more significant compliance requirements that will require continual monitoring and remediation when necessary.

One of the most susceptible areas in any organization is HR data with different legislation and compliance elements regulating it. However, if organizations implement effective processes to control access to that sensitive data up front, they can proactively mitigate the risk.

Organizations can't take a chance on inadvertently giving access to sensitive employee data. This starts with the provisioning process and ensuring that access reviews and approvals have been adequately vetted to prevent unintended access.

Access certification is critical for organizations to ensure that the right people have the right access to the right data at the right time. Organizations make hundreds of changes every day, and many organizations manage these changes with spreadsheets and emails. Automation is necessary to effectively get down to the granular level to understand what information people have access to.

The amount of data and what is considered sensitive data is evolving.

How can businesses keep up?

What is or is not considered sensitive data must be well defined within each organization. An obvious example is HR data. Organizations want to have a list of the employees, of course; however, these organizations don't want their pay grade or health-related information tracked within its applications. Knowing what data is considered sensitive beyond data sets as simple as within HR gets more complex. Each organization needs to understand the scope of its data and what data should be handled through a sensitive access review. For example, the ability to update formulas. Organizations should ensure the right individuals have access and continuously monitor their access.

Coupled with a provisioning challenge, people make mistakes, especially if the organization uses a manual provisioning approach. Automating these processes is vital when you have huge volumes of data and transactions to manage. Automation makes an immense difference and can allow organizations to be very definitive in what's being done, how it's being done and put controls around the process.

Standards are constantly shifting in regards to what's considered sensitive or in what combination data is deemed to be sensitive; one idea is to place metadata around the data. Fundamentally, what it comes down to is knowledge and understanding.

An organization's responsibility is to have an active understanding and knowledge of the data they hold and where it lives. Likewise, a higher-level reconciliation or evaluation of those data sets also needs to be performed on a routine basis. This will enable organizations to know that because the data is living in this combination, it's incumbent upon us to be more secure or more diligent about guarding this particular system.

Organizations can only put so much time, energy, and resources into a process or activity. Having a mechanism to help prioritize it ties into the fact that organizations need to understand and know what information they hold, where it is, and who has access to it. Correspondingly, having metadata around data is critical and something many organizations strive for but may be lacking in their ongoing processes.

How can organizations tackle a data breach?

When it comes to data breaches, it's not a matter of if; it's a matter of when. Many organizations are focused solely on prevention but they also need to think about what happens when a breach occurs and treat it as an inevitability. Organizations should have a crisis management plan in place in the event a breach happens. This plan should evaluate what they will do in the event of a data breach. What will their response be? What response procedures do they currently have in place? A disaster plan often gets overlooked in the zealousness to implement preventive controls. However, the more effective controls you can put into place, the less you'll have to worry about using that crisis plan; however, it's crucial that this step isn't forgotten.

Reputational risk is an authentic risk. Breaches impact the organization's valuation, the customer, the investor, and the community's faith in the organization to protect sensitive data. The organization also runs the risk of losing good employees that don't want to work for an organization that hasn't adequately addressed or managed data security appropriately.

To help avoid a breach, user provisioning and access certification should be reviewed periodically. These can easily be done on a reasonably consistent basis with the right solution. The provisioning process is preventative by nature. A workflow approval process that checks access against your policies and goes through various levels of approval is an excellent way to prevent risk.

It also alerts the organization in real-time to potential risks introduced into the system. Role-based solutions are no longer effective when it comes to mitigating risk.

And then, on the back end, a regular granular certification process should be performed to review access privileges. The user provisioning and access certification processes are auditable if you have an automated solution. An automated solution allows organizations to have an audit trail of who approved user access and when they granted it.

The certification will ensure that access has been approved and will enable the business process owners to request certain access for individuals. A common example is consulting. Consultants come in and are given temporary access through the standard provisioning process. On the other side, when they leave the organization, how do you ensure they no longer have access—especially in the cloud?

People no longer walk into the building and plug in. In the past, plug-in access was a preventative control in and of itself. It becomes a lot more challenging to make sure you understand where all that access exists with cloud computing and hybrid work models. It is incumbent on the organization to be hypersensitive about who has access and when it is appropriate. f employees or contractors walk out of the building and still have access to a cloud solution, organizations are not secure.

What solutions on the market today can address the challenges of fragmented access?

SafePaaS Enterprise Access Certification Manager™ (EACM) is designed to explicitly to address the challenge of fragmented access. EACM™ is an access governance hub for any application, database, operating system, and cloud infrastructure. It can be used with or without other IDM solutions and can gather data from any source, analyze it, and discover if any access conflicts exist that need to be eliminated.

To address fragmented access, organizations need to understand:

- What systems they are using
- What data resides in them
- How do these systems talk to each other

Answering these questions will help identify points of concern or areas organizations need to focus on. It is also paramount to have a central capability for understanding the implications of granting access in disparate systems.

Risk management functions need to understand where risks exist, understand the potential impact, manage it, and have a process to help reduce that risk. Organizations need to ensure that the process is auditable so they can validate that risk is being handled appropriately. This audit reporting can also be used to show investors and the board that risk is being mitigated.

Having a central view of access is highly critical. and from a risk and compliance perspective, the ability to tie that into the landscape of what you're dealing with is also crucial.

One of the most important things is understanding the impact, importance, or sensitivity of the information. Organizations tend to be bureaucratic and slower to invest so providing context and demonstrating the risk and the value of managing access and certifying access across disparate systems will help drive that investment. Again, it is essential to understand the implications of mismanaging data, knowing where it lives, who is accessing it, what they're doing, and what businesses need.

The whole risk management solution industry is still in its infancy. There are a lot of different products being promoted in the marketplace, with many capabilities. A proof of concept (POC) is worth investing time in to help understand how a solution can address your problems. A POC will allow you to define your requirements which vendors can evaluate and show you how their solution addresses them. That should give you a good idea of the fit and capabilities and if it can address the organization's requirements.

Contact Us

From a solution perspective, know what you need, understand those needs and work with your teams to identify critical requirements. Lean on vendors because they deal with requirements' challenges every day. Vendors can help guide you in terms of how they help address specific needs.

Cential assists organizations on their journey from siloed governance and compliance to fully integrated risk management technology-enabled programs. We help organizations design streamlined GRC processes, empowering businesses to reduce uncertainty and identify actionable insights in order to make better decisions that protect and grow the bottom line.

SafePaaS is a SOC-certified cloud platform for enterprise risk management solutions, recognized by leading IT analysts and recommended by major audit firms. SafePaaS delivers a single source of truth for all Audit, Risk, and Compliance needs. It is the single most utilized policy-based access control platform for detecting and controlling risk in enterprise applications with over 5.7 million ERP users on a single most reliable, secure, scalable platform. The platform offers control applications, API services, and content to detect, remediate, mitigate and prevent risks to the digital enterprise. Application suites on SafePaaS include AccessPaaS™ for audit-ready reporting, access request management, privileged access monitoring, automated fulfillment, identity analytics, and workflow orchestration; MonitorPaaS™for Configuration controls, Master Data tracking, and Transaction monitoring in ERP systems; ProcessPaaS™ to embed preventive controls in business processes; and, ARCPaaS™ to automate Audit, Risks, and Compliance Management.

Cential

www.safepaas.com
www.centialconsulting.com

SafePaaS™