happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Understanding Access Governance: Its Benefits and Challenges

Happiest People . Happiest Customers

Contents

Understanding Access Governance: Its Benefits and Challenges

Access Governance is the process of monitoring and controlling who within your organization has access to what, when and how. However, this is easier defined than done. It is easy to confuse access governance with access management, when, in fact, the former's scope extends beyond merely managing access rights to defining security processes and policies that can impact an enterprise's management of data assets.

> The monitoring of access includes not only access to business-critical applications,
> but also harware, infrastructure and the network itself.

The growing recognition of the need for access governance can be attributed to multiple factors:

- increasingly complex regulations that demand strict adherence;
- the escalating scale and frequency of cyber attacks;
- a recognition of the high risk that disgruntled employees, ex-employees, or simply, careless employees, pose;
- and the burgeoning adoption of the cloud, which, alongside the scalability and flexibility it promises, also poses a concern—how to monitor which employees access what data, using which device!

Today's intricate regulations make compliance an essential consideration as well. Being able to track, audit, and control what individual employees have access to, reduce misuse, while providing the data trail required for audits and compliance requirements.

An access governance system governs access rights in multiple ways, by

- Assigning employees specific rights to access only what they need to fulfill their job roles and responsibilities, efficiently and in a secure manner.
- Aggregating data on user accounts that have access to the different applications, databases, data centers, network devices, etc., to offer a single, unified, and easy-to-manage view into access rights and accounts on all systems.
- Implementing strong security controls, and mitigating risk by addressing:

> - Privilege creep: when an employee's job role and hence, responsibilities, change, but he continues to retain old access rights that he does not need anymore, in addition to new access rights
> - Stale accounts: accounts that stay alive even after the employee leaves the organization
> - Orphan accounts: accounts that do not seem to belong to anyone—they may be attached to ex-employees or vendors

Deploying an access governance system offers a number of benefits.

It provides a comprehensive view of roles and privileges within each department of the organization, leading to clarity within and about each function. This results in deep insight into how access is used across the organization by different users. An access governance system offers easy-to-understand dashboards that allow business managers a high-level overview, facilitating quick customer response. It enables the regulation and control of access in an efficient, systematic, and continuous manner. An access governance system also positively impacts the certification process. Certification and recertification requirements are reduced and users can be certified on an ad-hoc basis, as required, at any point in time. Furthermore, an access governance system facilitates collaborative and analytics-based decision-making, based on the data aggregated across users and departments.

When deploying an access governance system, keep the following in mind

- The ideal system should have an easy-to-use interface that provides business users a high-level overview of access rights, as well as details of how these tie into user roles and responsibilities.
- on unstructured data. Most of the data floating around in an organization today is of the unorganized and unstructured variety. These data do not necessarily exist in a single place that can be accessed in a straightforward manner through a created account (think about the distributed file systems that enterprises use, for instance). These unstructured data tend to be ignored—despite constituting an overwhelming percentage of organizational data—by solutions that focus on controlling access to applications and not the data themselves. Lack of control across these platforms exposes the organi zation to significant risk.
- View access governance as a business initiative. The moment it is seen as yet another IT initiative with no business context built in, the system is being set up for lack of accountability. For instance, an IT team can grant access based on requests from business, but without a business context as to why that particular access is needed, IT will be unable to take an informed call on the level of access appropriate for that particular role.
- Involve your compliance team when setting up access governance solutions and measures. Their collaboration and inputs are essential for to tick all the right regulatory compliance boxes.
- Setting up access governance policies and processes is only the beginning. More critical is the need to ensure that none of the policies are violated, increasing risk.
- Move the solution towards maturity in incremental steps, by implementing identity audits, access controls and certifica tions, automated provisioning, compliance reporting and self-service access requests.
- If an identity management system is already in place, ensure that the access governance system integrates seamlessly with it, and they work together to offer a robust security framework.
- The ideal access governance solution should be scalable and future-ready, supporting a wide range of platforms and technologies, and capable of integrating new technologies and tools.

Just like any other security solution, the best access governance systems are not those that are implemented rapidly and then allowed to run uninterrupted. Rather, implementation should be an iterative process that is continually tweaked as policies evolve and visibility into user roles and responsibilities improves. Continuously monitoring regulations and the compliance policies and processes the enterprise has in place minimizes exposure to risk. In this context, automation is key to managing access-related risks in accordance with regulations. Automation helps mitigate risks by remediating issues that arise around access in a timely and efficient fashion.

Many enterprises that deploy Identity Management Solutions believe that this will suffice for access governance. However, an identity management solution is only a point solution and what access governance requires is more complex—the monitoring of the dynamic access rights of multiple users to myriad applications. An identity management solution will allow IT to automate identity management and access control.
On the other hand, an access governance system provides a high-level business overview of access requests, compliance processes, and how the risk management strategy ties into user roles and responsibilities.
However, access governance cannot work without identity management, which is an important component of the former.

About the Authors

Subhash Nukala

Has Fourteen years of experience across industries in the areas of information security consulting, Identity and Access Management, Access Governance, Privileged Access management, Data Security, Consumer identity management. Actively involved in Practice Development, pre sales and sales support, new Solution offerings and GTM creation. Pursued B.Tech in Electrical and Electronics Engineering

Sandip Gupta

Experience in areas of IT security (IDAM) Consulting, Designing and Architecture. Nearly 11 + years of IT application development & implementation experience. Working as SME / Architect in the IMSS IAM security practice, HappiestMinds Technologies, Bangalore, India.

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as “Born Digital . Born Agile”, our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Email: business@happiestminds.com

Visit us: www.happiestminds.com

Follow us on