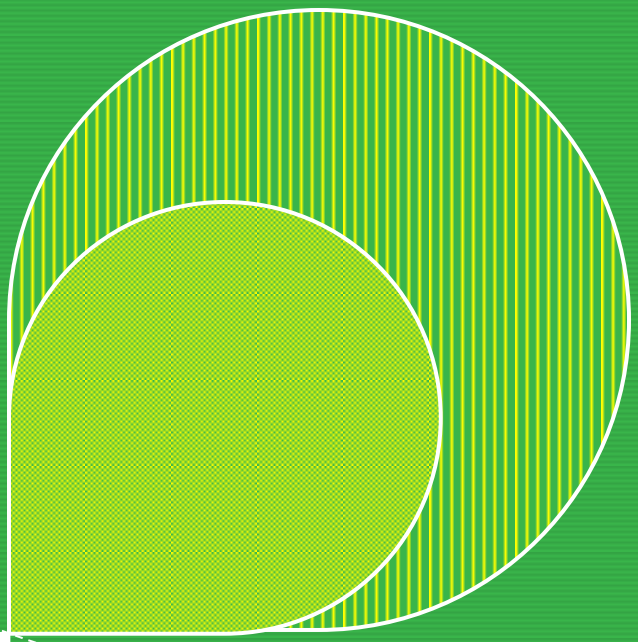
Streamlining Identity and Access Management through Unified Identity and Access Governance Solutions

By Iranna Hurakadli and Achutha Sridhar
Happiest Minds, IMSS Practice



happiest minds
The Mindful IT Company
Born Digital . Born Agile

Executive Summary

"Many enterprises that have implemented IAM technologies remain dissatisfied with the performance of these technologies and the results of their IAM programs. This dissatisfaction is driving them to consider alternative IAM vendors or alternative IAM approaches.
By 2014, discontent with program results will drive half of large enterprises considering major upgrade decisions to switch IAM vendors"

Gartner Report: Predicts 2012: A Maturing Competitive Landscape Brings New IAM Opportunities (Nov 2011)

Enterprises around the world have implemented identity and access management (IAM) solutions to address a variety of business problems. The goal of each of these implementations is to derive common business benefits like secure environment, operational efficiency and compliance and so on. It is often observed that though IAM practices have matured over the years, many enterprises fail to reap benefits despite making substantial investments.

The purpose of this paper is to highlight some of the challenges in IAM implementation, evaluate approaches to address the problems and suggest a roadmap for the successful adoption of an IAM program.

Today's IAM Challenges

Effective identity and access management enables private and public enterprises to manage identities and access in and out of the business boundaries to meet various business objectives. The benefits of IAM are more or less the same for organizations irrespective of the nature of business. Similarly, the challenges and issues associated with IAM are similar to all industry segments.

Some of the key challenges related to IAM implementations are highlighted here.

IAM is IT centric

Today, IAM is a business problem rather than a technology issue. With new security threats to the intellectual property (IP) of companies and increasing compliance demands across various industry sectors, business houses have recognized IAM to be a business problem. This shift in thinking has made it absolutely necessary for organizations to bring information technology (IT) and business stakeholders together to address IAM needs. Though ensuring business user participation in IAM efforts is challenging, there are clear advantages to be gained by making this effort. Business user participation helps in addressing security and compliance requirements from the business point of view which is an essential element to appropriately weigh the benefits and risks for the business.

Risks not accounted

"Software-as-a-service (SaaS) providers often fail to adequately address enterprise identity and access management (IAM) integration requirements, and customers face increased identity administrative burdens, reduced user convenience, and reduced audit and compliance insight."

Gregg Kreizmann, Gartner Article: "Options for Coping With New Identity Islands in the Cloud," January 19, 2011

It is observed that, many IAM implementations take a flat approach to user access management without considering the business value of the applications. By doing so, risks associated with access to critical applications are often ignored leading to poor access governance and in turn putting the organization at risk.
Further, today the organizations must be wary of threats from the outside world as well as from their own employees. It is a challenge to make information available to the employees and at the same time protect it from any kind of theft.

Compliance burden

Today, irrespective of the industry segment, businesses have to abide by many government and industry specific regulations. To audit any of the regulatory procedures, businesses often opt for manual or semi-automated approaches. These approaches are prone to manual errors and may expose the organization to the risk of a failed audit. Even if the approach addresses the aspect of regulatory compliance, the burden of periodic auditing and repeated efforts in preparation for the same will still be a challenge.

Inadequate identity assurance for Cloud Applications

The extended enterprise is here, but current security architectures are ill-suited for the task of securing the extended ecosystem. Security and risk professionals must adopt a new mindset for security.

Forrester Research

Adoption of cloud applications is becoming more of a necessity than an option for enterprises. As more end users are granted access to cloud-based applications, the efficiency of requesting and provisioning access becomes critical. With the advent of cloud services, there is a definite impact on the requirements that an IAM solution has to address. With Software-as-a-Service (SaaS) and other cloud offerings, access to data and security revolve around strong robust and trusted IAM solutions. Key concerns for both consumers and providers of cloud services with regard to IAM implementation are:

- How do I manage users' SaaS accounts and access?
- How do I collect and analyze SaaS security logs?
- How do I define and enforce access policies in Platform-as-a-Service (PaaS) applications without creating more security silos?
- How do I control privileged users in Infrastructure-as-a-Service (IaaS) — both providers and my organization's?
- How do I convince the auditors that the applications and data are secure?

How do we start?

Effective management of access-related risks demands a solution that fosters engagement between key stakeholders. Business managers are accountable for verifying access to information resources but the IT staff as well as the risk and compliance teams need help to provide visibility and context for the business managers to conduct the verification.

An identity and access management solution is required to address the current IT governance-related challenges by simplifying how access to information resources is requested, reviewed, certified and remediated thereby helping to strike a balance between business agility and control.

The growing need for identity and access management (IAM) governance will cause identity and access governance (IAG) solutions to become the lead focus of two out of three IAM projects by 2013.

Source: Gartner Magic Quadrant for Identity and Access Governance (Dec 2011)

The solution should enable access procedures to be more agile and responsive to business objectives. Compliance is a burden and the solution deployed should simplify the process of managing access rights including determining appropriate access and how to respond to anomalies. This means that business managers need simple, automated processes for reviewing and certifying users' access rights, as well as modeling, defining and certifying business roles. The access request processes need to follow established business policies and help achieve security, risk and compliance objectives.

Let us look at some of the options to address the above challenges:

Engaging business managers in identity and access governance (IAG) initiatives

Organizations must align business with IT to bring effective governance to identity and access. For better harmony and effectiveness clarity on the responsibilities is crucial. Business managers understand business risks better and can provide valuable insights as to which applications and data are more important to business. Business managers can assess the asset value and provide information on critical assets and risks associated with them.

IAG program can benefit by making business managers accountable for application classification based on risk value and approval of access to riskier applications. . Apart from this, by making business managers responsible for policies that dictate "who gets access to what and why", user access risks can be evaluated better. Business managers should also make decisions on policy violations and how to mitigate risks associated with them.

Assess Identity Risks

Organizations that are able to identify and assess identity related risks are said to be in a better position to protect their intellectual property (IP). User access to applications should have a clear process for granting access with emphasis on associated business risks. . Some of the risks arising from orphan accounts, shared accounts, test accounts and accounts of temporary workers are often not handled effectively. One of the options to handle risk is to first assign scores to the risks associated with each of the applications and their entitlements. Once the risk scoring is in place, collecting this data and combining it with the identity data will help in identification of high risk profiles. Additionally, effective Joiner-Mover-Leaver (JML) processes and monitoring of policy violations across applications help in reducing risks and maintaining control.

Businesses are focusing on SaaS services to obtain quicker wins, and CIOs are finding these services attractive for cutting costs as well. Identity provisioning will look quite different in the era of cloud services.

Forrester Research

By utilizing the identity intelligence gathered as part of the IAG program, threats from insiders can be addressed by initiating proactive measures. For example, if an employee with high risk value is expected to be terminated from service, then steps can be taken to curtail his access before his actual termination date.

Address Compliance

Compliance is an ongoing challenge for every company. Automation is the key to effectively address compliance requirements. Automation of audit and compliance requirements increases effectiveness of audit and reduces associated costs. The most important benefit of automation is the repeatable audit process which is reliable and free of manual errors and thereby reduces the chances of an audit failure.

Identity Assurance to Cloud Applications

Managing identity and access to cloud applications is one of the major challenges for companies adopting the cloud environment. From the identity management perspective, requirements related to administrative and governance functions are the same for a cloud application as any other enterprise application. But there are certain unique requirements of cloud applications. For example, timely de-provisioning from SaaS application might be important as some of the SaaS applications are charged based on user accounts. Also, dedicated cloud connectors have to be utilized for effective cloud integration in an IAG program and to achieve effective governance.

The Right Approach

As more end users are granted access to applications, the efficiency of the process of requesting and provisioning access becomes a sizeable cost consideration. Identity provisioning and access governance plays a critical role in addressing security related compliance issues and can no longer be regarded as a segregated solution. Managing access to any enterprise application requires a centralized and holistic approach.

While building an identity and access governance solution, technology alone will not solve the problem as technology is only an enabler in the process. Business processes, organizational needs, compliance requirements and risk strategy must be considered while deploying the technology solution for better results.

Figure 1 represents the essential building blocks of an identity and access governance solution.

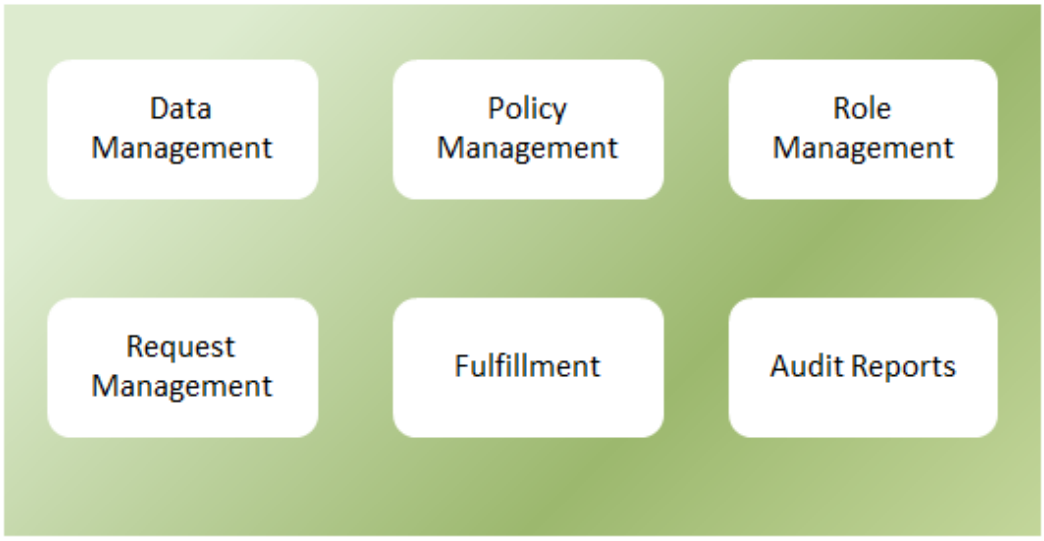


Figure 1. Essential building blocks of an Identity and Access governance solution

Each of the building blocks is important for a successful IAG program.

Data management emphasizes the data related to users, accounts and entitlements associated with accounts. It is essential to gather such data from all the applications to get a centralized view of the identity. This helps in analyzing the data from different perspectives.

Policy management deals with access policies, policy violations and rules that govern different lifecycle events within the company.

Role management deals with discovering roles from existing applications, defining new roles, managing roles and role hierarchies and role mapping. Role management, if implemented, will help the company in access management. However, the company must be willing to make efforts to implement enterprise-wide roles.

Request management will enable end users to request for access to applications and systems within the company.

Fulfillment makes the integration work by executing the requested identity and access changes.

Audit reports are essential records on identities, user accounts and their access. Any analysis done on identity and its associations will generate a report, if desired.

A Roadmap to better Identity and Access Governance

For achieving identity and access governance, a roadmap is given in Figure 2. This is a high level plan and will need to be customized based on the customer's needs.

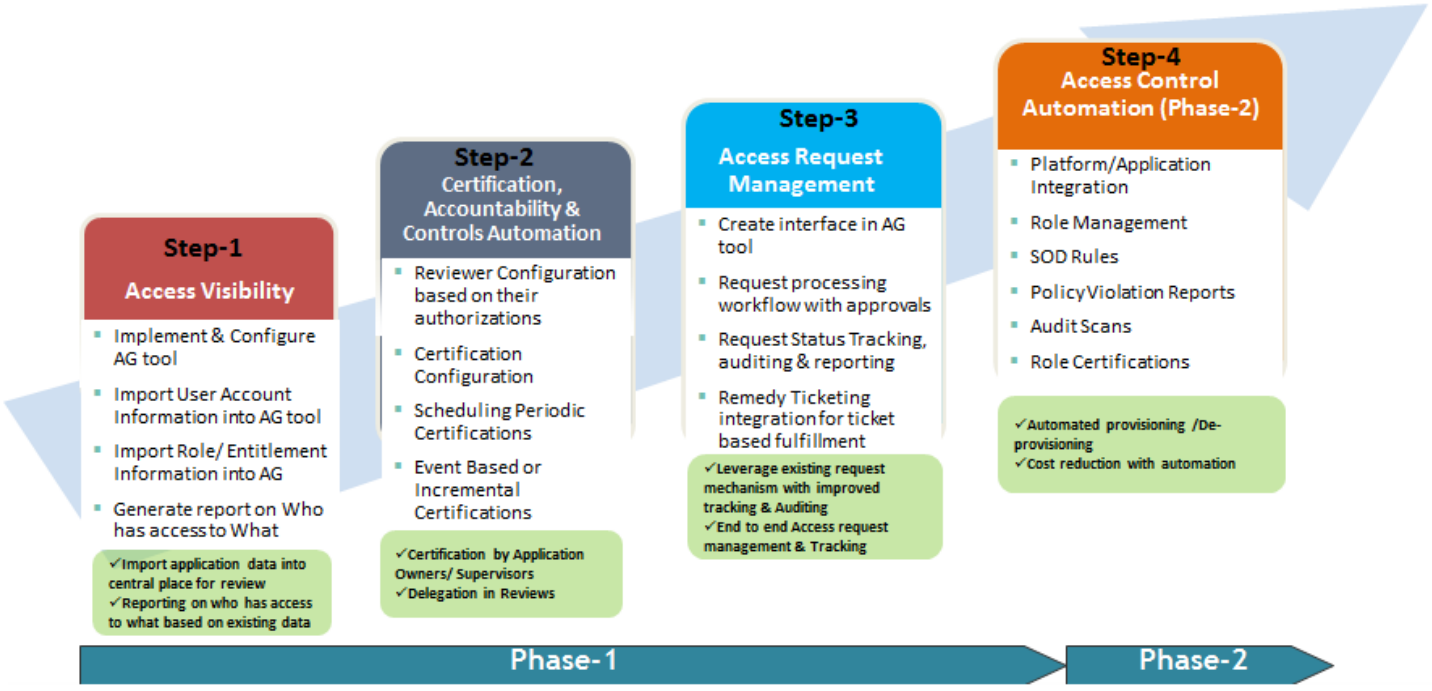


Figure 2. IAM Roadmap

We recommend a 4-step approach for total identity and access governance. Each of these steps yields a definitive business outcome and is equally important. With this staged approach, business benefits can be realized which only increases over the different steps.

Step 1 focuses on confirming customer requirements and creating a foundation for the IAG solution. Here, the focus is limited to access visibility, wherein the enterprise-wide information on "Who has access to what" is understood.

Step 2 focuses on utilizing the foundation platform for carrying out certification activities by a manager to validate the different accesses the users have.

Step 3 focuses on integrating applications for access request management with the option of manual fulfillment.

Step 4 focuses on integration with the Identity Management (IDM) application to facilitate auto fulfillment of requests related to identities and access information. Also, other features like role management, role certifications and policy violations are addressed in this step.

This step-by-step approach counters the complaint that the realization of return on investment (ROI) from IAM projects takes longer or that investment in such projects is not justifiable. This theory enables the organization to realize the Return on Investment (ROI) and make use of the savings as well. By following the step based approach described above, business benefits can be assessed at every step and a tangible operational saving can be realized. Such savings can be invested in further automation to reduce costs further and realize the overall ROI. A case explaining the model is depicted in Figure 3.

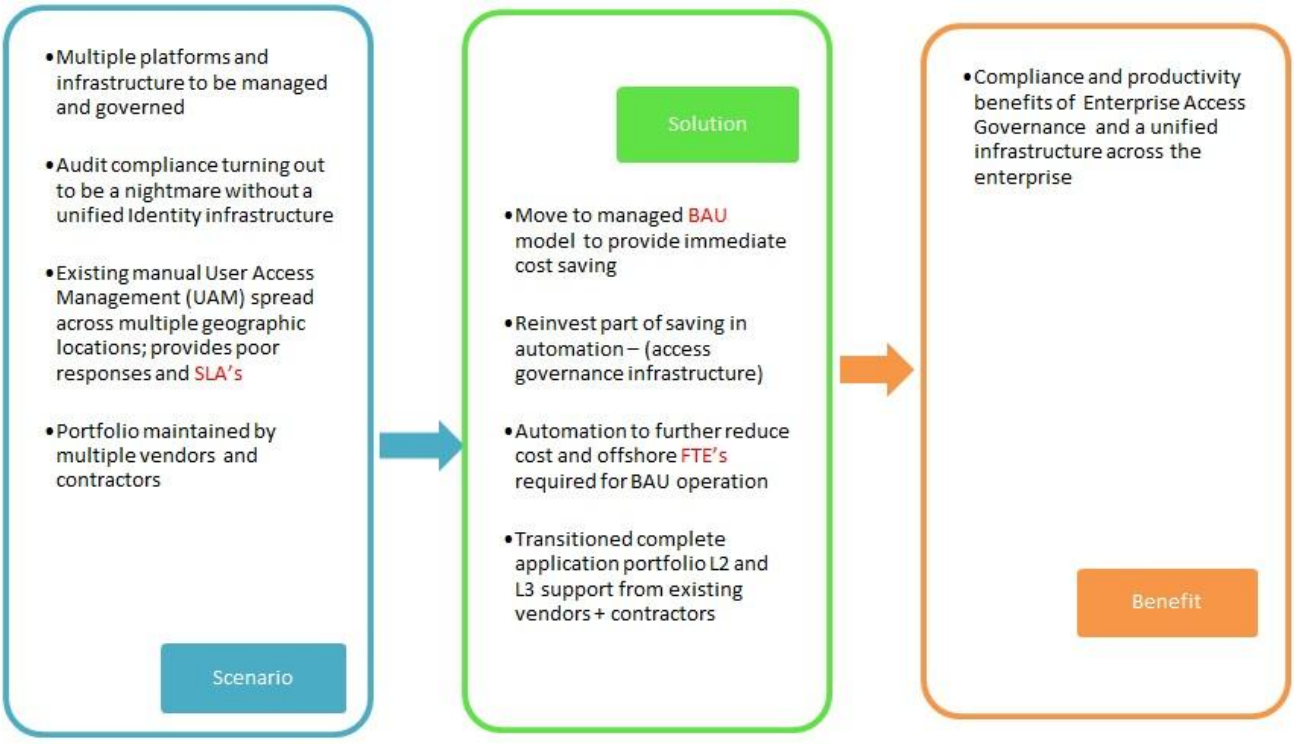


Figure 3. ROI and business benefits

Conclusion

Enterprises need *a clear, enterprise-wide view of IT resource access rights to* ***proactively prevent abuse****. At the same time, a solution that* ***simplifies the access request*** *process to* ***reduce costs and streamline operations is needed.*** *And finally,* ***auditors should be convinced*** *that the organization has* ***sufficient access controls*** *in place to prevent* ***regulatory violations. A combined Identity and Access Governance Solution*** plays a critical role in addressing these concerns and can no longer be regarded as a segregated solution.

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.

To know more about our offerings. Please write to us at **business@happiestminds.com**

About the authors

Iranna Hurakadli (iranna.hurakadli@happiestminds.com) is the General Manager and Practice Head of the IAM division of the IMSS Practice at Happiest Minds. He brings in-depth experience in leading cross functional teams for conceptualization, implementation and rollout of security solutions.

Achutha Sridhar (achutha.s@happiestminds.com) is a Principal Architect in the Happiest Minds IMSS Practice. He has more than 10 years of industry experience in IAM and application security. He has overseen implementations of identity and access management frameworks at several organizations across America, Europe and Australia.

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