WHITE PAPER

Optimizing your IGA investment with Authorization

AXIOMATICS
a LEONARDO company

IGA foundation has been established

The Identity Governance and Administration (IGA) market is mature and organizations continue to look to incorporate IGA solutions to help guide them in terms of appropriate access controls. They do so because the importance of certifying only the right people to have the right access to the right information at the right time is critical to ensuring the security of their organization's data, customer information and reputation.

To achieve this goal, IGA solutions often start with a role-based access control (RBAC) approach. Through this approach, by assigning everyone a role and grouping those roles, the organization can enable access permissions based on those roles as opposed to managing access on an individual basis.

Blind spots in the IGA approach

While IGA solutions have drastically helped to control and govern access, there are gaps and challenges that present themselves when trying to scale this approach. The first is that the roles and conditions for which access can be permitted are rarely straightforward in the real world. As such, organizations are forced to create multiple roles. Imagine a company with 50,000 employees, but they have over 54,000 roles. In that case, it's even more complicated than if they had simply managed access on an individual basis and this approach certainly doesn't scale.

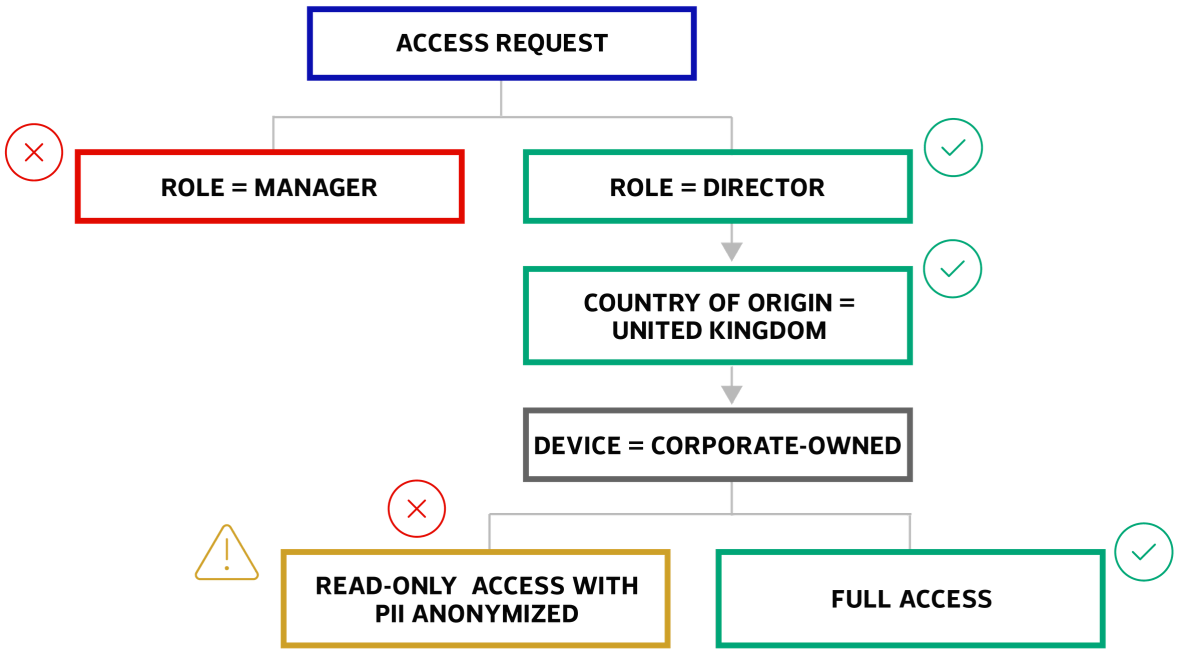
Additionally, creating policies that have conditions for approving access is quite limiting. Access can be granted if the user is in a certain role, and usually with one or two other conditions at most, such as the device they are using to access, or maybe the time of day. If the conditions do not match, then access is denied. While that may sound like a successful approach, consider that denying access to a revenue generating employee can be costly and as such, those conditions can be turned off after the first costly episode where access was denied. This is referred to as a "fail-open" state and though it may come as a surprise, in terms of security policies, it is often chosen over a "fail-closed" state simply due to the costs of a service shut down. So while the intent to govern and administer appropriate access is there, with so many unique conditions that can't be accounted for, it is often not fully possible to take advantage of IGA solutions in the way they were intended.

One of the main objectives of the crawl phase is to create baseline policies and standards that can be tested and refined with these applications. This ultimately lays the foundation for future authorization policies while enabling potential areas of concern to be managed in advance. Following a policy-driven authorization model, key contextual attributes would be identified and built into the applications. This phase also involves gaining momentum and generating anticipation for broader adoption through the measured introduction of the proven business value while conducting training as well as internal marketing.

Authorization can fill in gaps and help IGA reach its full potential

Authorization solutions can add a great deal of value to existing IGA investments. By building onto the existing RBAC approach, authorization solutions can add an attribute-based access control (ABAC) approach to address a number of scenarios and conditions. ABAC effectively adds the ability to include a real-time decision tree in the access with RBAC as one of the first decisions in the tree. With this approach, the work and investments already made with IGA solutions and the RBAC approach are not wasted, and ABAC adds additional attributes to make a more appropriate decision in real-time.

Additionally, ABAC gives security professionals the opportunity to grant access with caveats. This means that what may have been a fail-open scenario in the past can now be a limited access scenario with ABAC, perhaps offering "read only" access instead of full "write" access. This enables the user to still get the information needed to do their job, but they may be limited in their ability to alter this information, or extract it due to policy. The great thing about ABAC decision trees that can be established as policies is that there's no limit to the number of attributes a policy can account for with 'IF, THEN' scenarios. Once a policy has been created, it can be copied and modified as needed for other applications, removing much of the management burden and enables teams to quickly scale and address their most crucial applications faster..



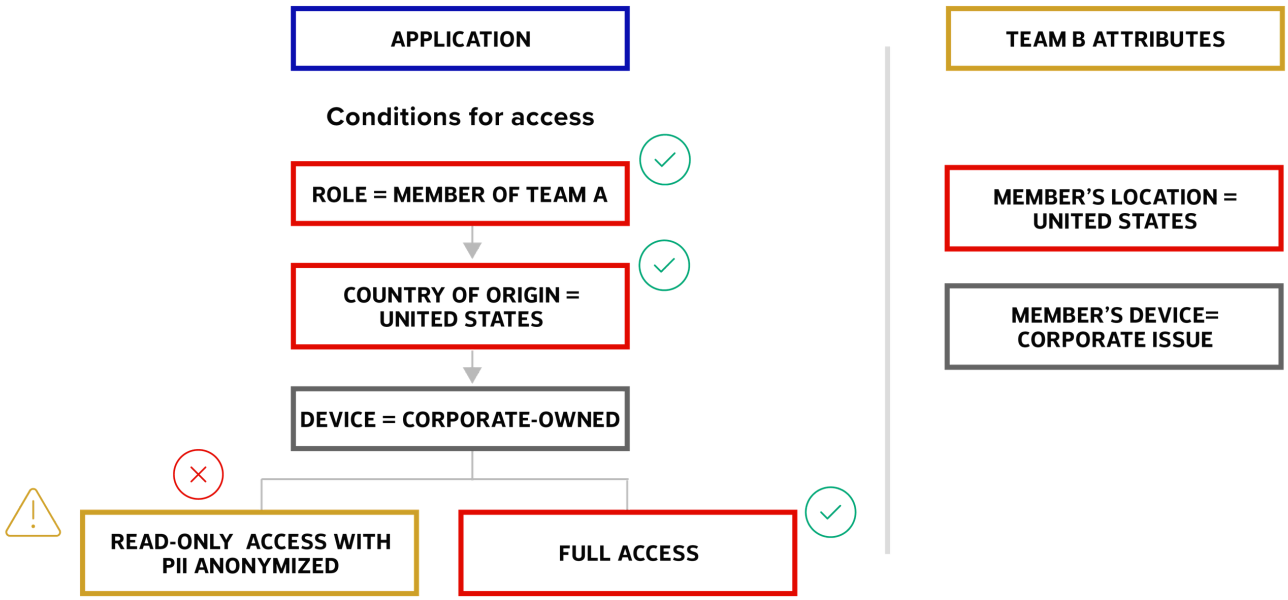
Based on the policy, in order to obtain full access to the information requested, the user must be a director, in the UK and on a corporate owned device. If the user is a director and in the UK, but not on a corporate device, the policy enables them to have read-only access and any PII is anonymized.

Contextual Authorization Query

Though it offers many benefits, ABAC is not without its challenges. While there are benefits to having policies that can account for multiple scenarios, it can be difficult to explain under what conditions information can be accessed in an application or resource to senior management or an auditor. With RBAC, it's quite simply the user's role and that can be easily explained. With ABAC, it's difficult to articulate the various levels of risk that come into play and impact the type of access permitted.

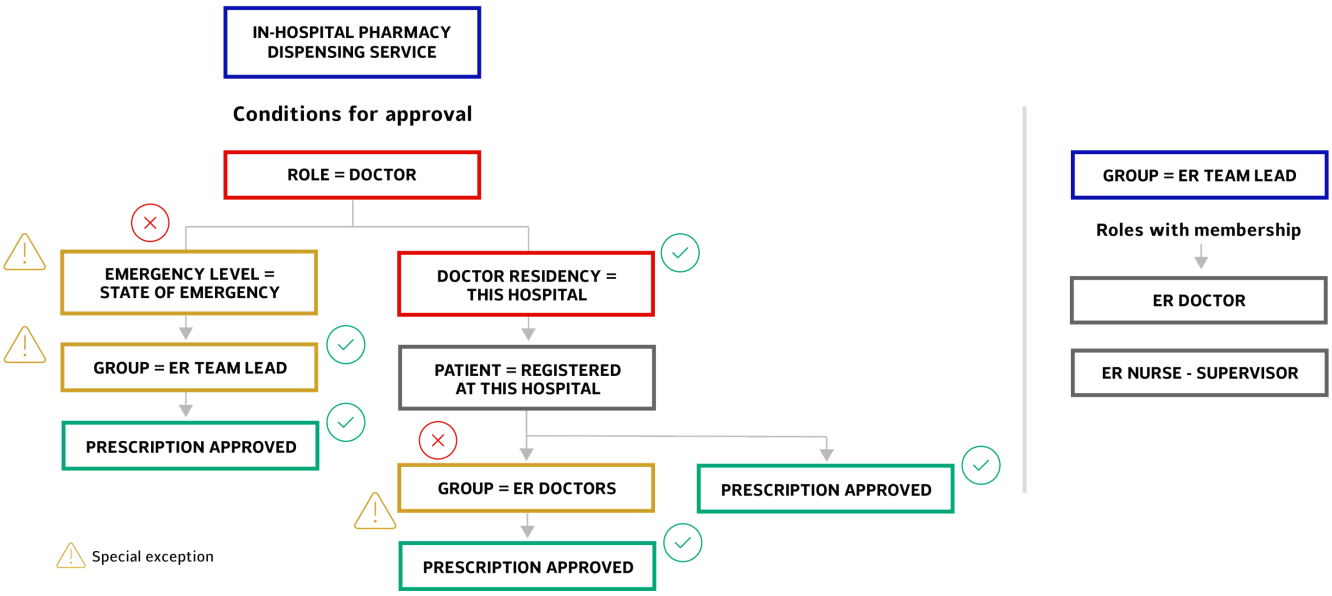
To address this need, Axiomatics leverages a functionality called **Contextual Authorization Query**. This query produces a list of conditions that describe who, what, when, where, why and how information can be accessed in an application or resource. There are two key use cases where this functionality comes into play.

The first is when evaluating access before it is given. If an organization spins up a new team, it can be convenient to review the access permissions and risk scenarios of an existing team. While RBAC provides a high-level view based on the role, the contextual authorization query goes deeper and provides context around risk and scenarios that enable, limit or prevent access. Considering the alternative is usually to manually request permission from an application owner, or security manager, by leveraging a contextual authorization query, an organization can in many cases, avoid bothering the approvers because they can see quite clearly what has been approved in the past. One organization leverages the contextual authorization query in an automated fashion for all new access requests to limit the amount of requests that must be sent for human approval. In doing so, they have drastically reduced the burden on their staff.



Based on the attributes about Team B, Assuming they will be performing a similar function, it is likely the same policy can be applied that is currently being leveraged by Team A.

The second use case is reviewing access after it is granted. Consider a situation where someone in a role that shouldn't have access to a certain application was able to perform a task in that application a month ago, and an auditor asks how that could have happened. One option would be to look through all of the event logs to try and see how the individual was able to perform the task. Did someone grant them elevated access? When and why? By running a contextual authorization query, the team can see under what scenarios that individual would ever be able to obtain access to perform such a task in that application. Even if the auditor requires proof in the form of event logs, the team will have pinpointed exactly what logs to review based on the scenario outlined in the contextual authorization query.



Based on the policy, a Nurse-Supervisor from the ER is authorized to prescribe medication under special exception when the hospital is in a state of emergency.

Another way where the contextual authorization query can come into play is during the rollout and adoption of a policy-driven authorization framework. Ultimately, the first few applications to leverage the authorization framework will likely be higher risk applications. In large organizations, there are multiple teams that manage different applications.

To speed up the likelihood of adoption among the other application owners, showing them a contextual authorization query on another application enables them to easily see the value and manner in which they can lower the risk level for their applications. Without that ability to visually see a list of conditions that describe who, what, when, where, why and how information can be accessed in an application, it can be hard to understand the value an authorization solution can bring to the existing IGA approach.

Combining authorization with IGA to lower risk

Leading analyst firms recognize the shift toward more composable IGA functions within a cybersecurity mesh architecture. This approach allows organizations to leverage data from multiple sources to gain better context and strengthen the protection of sensitive information

When it comes to what authorization can add to IGA investments, this aligns with analysts' prediction. Leveraging an orchestrated authorization approach with an existing IGA solution will enable organizations to review multiple attributes for access requests and go well beyond what RBAC reviews.

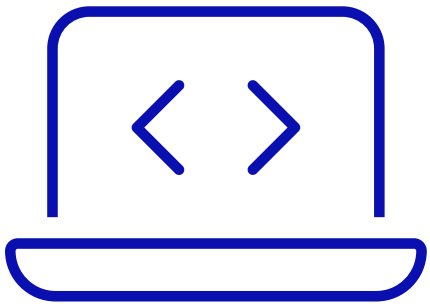
Ultimately, this ability to account for multiple attributes means enterprises can account for many scenarios and will no longer be forced to use only a "yes" or "no" response to requests. By adding authorization, they will be able to offer a "yes, BUT" response to requests that still enable end users to perform their jobs, but apply limitations, or additional protections to the sensitive information, thus preventing exposure and lowering risk.

If the goal is to increase security, lower risk and still enable the end-user to perform their jobs, then adding authorization to IGA simply makes sense.

Take the next steps

Learn how how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

Meet with our solution experts for a demo of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:

- Blog articles
- Press releases and announcements
- Resources, solution briefs, and tools
- Join us on LinkedIn
- Subscribe to our Linkedin Newsletter
- Subscribe to our YouTube channel

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: https://linkedin.com/company/axiomatics

Join us on YouTube: https://youtube.com/@axiomatics

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240