WHITE PAPER

A Practical Guide to Implementing Policy-driven Authorization in Three Phases of Growth

AXIOMATICS
a LEONARDO company

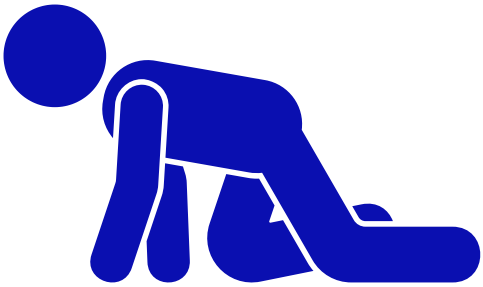
Background

Enterprises that are looking to adopt a policy-driven authorization strategy are not trying to serve just one app at a time, but are looking to adopt a vision that could seemingly support every application and resource in their purview. To successfully execute this vision, they must be methodical and thoughtful in the approach, while not resorting to 'boiling the ocean'.

Growth models are phased approaches to managing change. In the authorization market, this involves solidifying key milestones at each stage of the implementation process, which can vary depending on an organization's history with authorization. Executing a policy-driven authorization strategy lends itself well to the crawl, walk, run approach, as it enables organizations to align with the strategy in phases while addressing early challenges. Following a targeted growth model enables identity teams to deliver against specific outcomes prior to wider implementation, rather than rushing against a timeline. As with any growth model, each phase has a set of steps that reflect how the strategy is scaled across the organization.

Phase 1: Crawl - Aligning to the Why

The crawl stage is focused on creating visibility for the value of policy-driven authorization and how it will support a broader cybersecurity and/or identity vision. This starts with targeting new applications that are in the process of development, instead of trying to transition policies from legacy applications. The recommendation is to target one or two enterprise applications (typically cloud-native) that contain crown jewel information. In most instances, as the cloud becomes the modern environment for application development, these applications are ideally cloud-native and possibly even supporting a service mesh infrastructure.



Integrations could be complete across the front-end web UI through to microservices, all the way down to the data layer, as needed. This enables the program to target authorization policy deployment as part of their continuous integration/continuous deployment (CI/CD) pipeline.

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.

Ahead of the next stage, the baseline policies and standards should be established with early barriers to adoption addressed. In addition, the impact on securing these applications and data should be proven when put into practice for the target applications. In turn, the target application owners should function as champions for the authorization strategy, equipped with the tools to educate others on the program and advocate for its implementation.

Phase 2: Walk - Securing Adoption

The walk stage is centered on securing the broader adoption of the policy-driven authorization strategy for additional applications. In this phase, we may see instances of transitioning applications with existing authorization policies into this new strategy. Since it is about scaling within enterprise organizations, these applications can be either cloud-based or legacy platforms that contain more sensitive info and require timely attention. Ideally, the walk phase targets application owners or business teams that have a growth mindset and are eager to adopt a more secure way to access critical information.

As a set of common policies is adopted across more application owners, this is where identity teams can build on the existing policies and standards. In this phase, more advanced, risk-based attributes are introduced within the policy based on the framework set in place to define authorization outcomes. The application owners from the previous phase play a significant role as champions, becoming internal references who support the identity teams on broader training and internal marketing initiatives for other application owners by demonstrating how it improves their applications using the initial implementation results as a case study. This is where application owners are introduced to opportunities to author their own policies, laying the groundwork for a decentralized policy authoring strategy.

Prior to the next stage, best practices for policy authoring and application onboarding are established for ease of execution across the organization. At this point, there should be multiple application owners who have recognized the return on investment for adopting a policy-driven model, with a clear understanding of how it is operationalized for the business. In addition, the application owners in this stage can become champions for the authorization strategy, or at the very least share case studies for other application owners who have yet to transition their applications.

Phase 3: Run - Authorization by Design

The run stage is where the policy-driven model is integrated into all facets of the organization, providing a dynamic landscape for constant evaluation and improvement on how to deliver against the strategy. In this stage, the strategy is fine-tuned to continue to address new authorization requirements that may be internal, or externally-driven by compliance regulations.

The run phase will also account for the development of ongoing policies for all layers of the application stack including front-end web, data, APIs and data platforms. At this growth stage, application owners have a command of the policy language and can build their own policies based on the standardized framework within an attribute-based access control (ABAC) environment.

Though identity teams will continue with strategic oversight and some policy development, they will lean on application owners for policy definition and authoring. Additionally, any new homegrown or licensed applications will be onboarded and incorporated based on the new authorization strategy.

It is important to note that the run phase is not the final step - rather, it indicates the organization has adopted an authorization-by-design strategy that is constantly evolving based on a mission to protect its critical information.

Considerations for each growth phase

Every project management toolkit or guide has its best practices to successfully deliver on any initiative. Below are seven elements we recommend you consider defining within the context of the organization's authorization strategy for each stage of growth.

The **outcome** stays focused on the why and becomes the "North Star" for the phase. In theory, the authorization strategy does not proceed to the next phase until the outcome is achieved.

The **target scope** outlines the quantity of resources that are in scope for the phase (e.g. two to three applications).

The **resource type** provides parameters for the authorization policies (e.g. front-end UI for an application, microservices, APIs, or databases).

The **target environment** describes the location of the application(s) (e.g. cloud-native versus private data center).

The **policy authoring strategy** explains the approach for policy building (e.g. centralized to IAM or decentralized to application owners).

Integration considers both contextual inputs for ABAC policies (e.g. roles from IGA, authentication tokens from IDPs) as well as integrations for the IT ecosystem (e.g. API gateways, service mesh infrastructures).

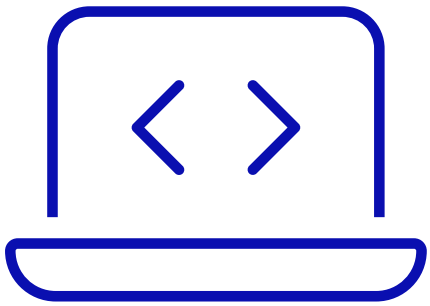
The **exit criteria** provides specific deliverables on when a particular stage is complete.

It is important to break each phase into steps based on the aforementioned elements and map out the desired results. Early adopters of dynamic authorization might find themselves moving quickly through the crawl stage, while organizations contemplating an authorization strategy for the first time may take more time getting to the first stage. This process can differ based on where an organization is in their authorization maturity, and they must take this into account in their journey. A template for mapping out each stage based on the crawl, walk, run maturity can be accessed here.

Key takeways

- Maturity models illustrate a method of deploying dynamic authorization initiatives in phases.
- The crawl, walk, run approach leads to a successful implementation of an policy-driven authorization strategy.
- The goal of the crawl stage is to demonstrate the value of the policy-driven authorization strategy and establish baseline policies and standards.
- The goal of the walk stage is to widen the adoption of the policy-driven model by educating the organization and determining best practices for policy authoring.
- The goal of the run stage is to ensure decentralized policy authoring is normalized and all resources can easily be onboarded based on the policy-driven model.
- The seven key elements of each stage in a maturity model that outline how an authorization initiative is implemented are the outcome, the target scope, the resource type, the target environment, the policy authoring strategy, integration considerations, and exit criteria.

Implementing a policy-driven authorization strategy in an enterprise organization works best when aligned with a maturity model that illustrates a clear path to success. With over 20 years of experience working with Fortune 500 organizations, Axiomatics' approach to authorization reflects the evolving needs of the business landscape.



We welcome the opportunity to connect and support you on introducing new authorization initiatives across your organization based on a maturity model. Reach out to us for a consultation on Axiomatics' Authorization Management Platform and what this might look like at your organization.

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