Unified Authorization Maturity Model

Version 1.0

Last updated May 24, 2024

Unified Authorization

All of the following are authorization questions:

- Can Sally withdraw $5,000 from account 058201?
- What actions can Javier do on an escalated ticket?
- During what hours can badge #2541 access the store room?

In legacy organizations, each of these scenarios uses a unique authorization mechanism. Trying to manage authorization across so many disparate systems hinders visibility, compliance, and the ability to adhere to security best practices.

Modern organizations are evolving towards a **unified authorization model**, where the same authorization system can be used across multiple applications, services, and technology stacks.

Unified Authorization Maturity Model

This **maturity model** describes the characteristics of organizations along their journey toward unified authorization, based on experiences working with the Fortune 100

Organizations should regularly conduct a mapping exercise against this maturity model to audit their capabilities and point them towards their next steps

Mapping Exercise Instructions

1. Gather relevant stakeholders across functions — for example, IAM, security, platform engineering, application architects
2. For each category, check the boxes next to each capability satisfied by your current authorization system
3. Pick 3 categories to improve and identify
4. Repeat the modeling process quarterly

Policies and Data

Unified Authorization Maturity Model

Area	Level 0 Novice	Level 1 Beginner	Level 2 Proficient	Level 3 Expert
Policy Location	❑ Authorization behavior is built into application code ❑ Permissions are stored in application databases	❑ Authorization behavior is tightly coupled to user management and identity management systems ❑ Authorization data is stored in an IAM system	❑ Policy is externalized ❑ Policy is stored in centralized locations ❑ Policy is version controlled	❑ Policy helpers / building blocks are centralized ❑ Application policy is decentralized according to organizational lines, e.g. HR application policy and finance application policies separated ❑ Authorization data is version controlled
Policy Complexity	❑ Authorization is user-specific	❑ Role-based access control	❑ Attribute-based access control with broad permissions ❑ Static external data ❑ Request-specific data ❑ Ands/Ors and other conjunctions of policy clauses	❑ Attribute-based access control with fine-grained permissions ❑ Relationship-based access control ❑ External service data ❑ Real-time data
Policy Enforcement	❑ Applications internally decide when and how to enforce authorization	❑ Backend applications	❑ Backend applications ❑ Service-to-service (E/W traffic) ❑ API Gateway (N/S traffic)	*All layers, zero trust* ❑ Database ❑ Frontend
Data Architecture	❑ Data is not externalized	❑ Every authorization request calls external data systems	❑ All data is duplicated in every potentially needed location	❑ Data architecture is optimized for specific needs ❑ Data gravity is considered

styra

Governance

Unified Authorization Maturity Model

Area	Level 0 Novice	Level 1 Beginner	Level 2 Proficient	Level 3 Expert
Policy Flexibility and Reuse		❑ Individual application based policies	❑ Some organizational policies defined ❑ Organizational policies are turned on/off for individual applications	❑ Mostly organizational policies with the capabilities for fine tuning in the application ❑ Organizationally mandated policies override individual application policies
Policy Content and Standardization		❑ Helper libraries are extracted for re-use across policies	❑ Idiomatic policy contents and structure are organizationally defined ❑ Enforce that certain libraries can only be used by specific applications	❑ Standard policy structure is enforced with exceptions ❑ Self-service discovery of organizationally approved policies and libraries during authoring
Policy Change	❑ Permissions can be updated in production	❑ Changes to authorization data must go through internal change management processes ❑ Non-code based change management	❑ Policies can be copied from development to staging to production ❑ Test data is separated from production data	❑ Policy artifacts are fingerprinted ❑ Policy artifacts must be directly promoted from development to staging to production
People	❑ Central IAM team is a function in HR organization	❑ Central IAM team is a function in a Security organization	❑ Authorization is a co-investment between engineering and security ❑ Central authorization team responsible for most policy authoring and management	❑ Central authorization team acts as helper, guide and coach ❑ Application development teams author and manage policies ❑ Business users able to create meaningful policy

styra

Security and Auditability

Unified Authorization Maturity Model

Area	Level 0 Novice	Level 1 Beginner	Level 2 Proficient	Level 3 Expert
Policy Testing and Assurance	❑ Application code integration testing	❑ IAM system governance ❑ Periodic reporting and auditing of roles and permissions	❑ Policies are covered by unit tests ❑ Policy unit tests are run on every check-in	❑ Policy drafts are tested against historical decisions ❑ Policy drafts are compared against live traffic ❑ Least privilege / Separation of Duties analysis ❑ Right-sized permissions analysis
Privileged Access Management and Escalation	❑ Modify permissions in production application database	❑ Assign and unassign privileged role	❑ Exceptions based policies	❑ Exceptions based policies with separation of duties enforcement
Observability	❑ Monitor application API responses for 4xx status codes		❑ Authorization decision logs integrated into an observability platform	❑ Anomaly detection, e.g. spikes in requests or errors
Auditability	❑ Applications do not generate audit trails of authorization decisions	❑ Rely on IGA tools	❑ Access log records saved to an external log management system ❑ Ad-hoc audit reporting from external management system	❑ Constant monitoring of audit-triggering behavior ❑ Changes to policies generate audit logs

styra

Additional Resources

- Knowledge Hub - Styra
- Authorization Resources
- 2023 State of Policy as Code Report

