# Getting Started With Modern Authorization

Supported by The Cyber Hut

plainID

# How To Get Started

The assessment, migration and onboarding of critical business assets to a new external authorization platform is a strategic process that has significant business impact. It is important to approach the solution with the right stakeholders involved, be in a position to understand current and future requirements, and continually assess the authorization landscape and what existing and future solutions and providers can support.

## Step 1: Identify Landscape

As with many key identity and access management projects, it is vitally important to understand the landscape. That entails understanding which assets exist, what those asset types are, documenting identities, data flows and the necessary interactions between subjects, objects and the actions being performed against them.

### ASSET INVENTORY

What is an asset inventory? Well, simply a method of documenting some of the systems, applications, APIs and objects that need to be protected by some sort of access control function. The access control functions may well be embedded, homegrown, open source, commercial or legacy.

The inventory process is likely to be an ongoing concern, working across lines of business areas, application types or perhaps projects. The key aspect is to try and understand which systems exist, what type they are, and if any unusual functions or processes exist. The inventory will also likely contain things like application or data owners and operational support ownership.

| ASSET | CATEGORY | CURRENT ACCESS CONTROL FUNCTIONS |
|---|---|---|
| **Time-Recording App** | Web application | Group-based session management |
| **Time-Recording Back-End** | Java API | Hard-coded job roles |
| **Time-Recording Database** | SQL database | Hard-coded users on tables/columns |

## Step 2: Prioritize Assets

As with any inventory process, the result may well be a long list of data. Numerous systems, duplication, confusion and a lack of clarity may initially emerge. Not all assets and systems can be migrated to a new access control system on day one. Not all assets needing protection will be the same. They most certainly will exist on different underlying technologies, be running in different logical and physical locations, and all have different levels of business impact.

A first step is to look for patterns and start to categorize assets. Categorization could initially start with something quite coarse-grained — perhaps asset types like APIs, web systems or data — as well as business location or how the asset is hosted.

Prioritization should ideally be focused on identifying which assets could be migrated to an externalized authorization system first. Compelling events for migration can often be hard to articulate, as is the case with many identity and access management functions. In this case, some basic questions can be asked of each asset, such as:

- Do the right people have the right access at the right time?
- Does the asset scale effectively for the required number of users/transactions?
- Can the access control function be changed effectively and in a timely manner?
- Can the access control function handle existing security threats?
- Can the access control function handle future security threats?
- Does the access control function create business friction?

Other issues to consider when looking to identify which assets to prioritize first for migration may include the level of complexity associated with the system and its access control functions. Are they heavily customized? Do they rely on a lot of hard-coded users, groups or permissions? What is the business impact of the application not functioning correctly?

It's important to start small in the asset migration process, looking for small and simple assets to migrate first that can allow a broader business case to develop based on a successful adoption. Larger and more complex systems are best tackled once the migration process has maturity and the technology landscape is fully understood and documented.

## Step 3: Gather Requirements

Understanding the technical requirements of an asset's access control system is a huge step in designing the new integration with an external authorization platform. The technical requirements will likely be broken into several different categories, including the types of identities, the permission management life cycle, enforcement and policy data design, along with operational management, which will include things like visibility, reporting and insights.

| BUSINESS CATEGORY | REQUIREMENTS TO CONSIDER |
|---|---|
| **Identities** | Identity storage location, schema attributes, volume of identities, change in identity population, authentication details, session management or federation requirements |
| **Permissions** | Groups, roles, attributes, identity characteristics, update frequency |
| **Context** | Locations, devices, risk signals, threat intelligence |
| **Enforcement** | Inline services, decision queries, local enforcement, API integration |
| **Operational Management** | Reporting, visibility |

Each business stakeholder will have a set of requirements which relate to how the application or asset performs in a business setting — namely what would be the impact if the system or service did not work optimally or at all. Analyzing the responses to these considerations can help to define the policy design and management processes going forward.

| BUSINESS CATEGORY | REQUIREMENTS TO CONSIDER |
|---|---|
| **Ownership** | Who owns the application, asset or service? Are they accountable?<br>Do they have budgetary control? |
| **Impact** | What is the business impact if the application is unavailable?<br>Functions, users, processes, costs? |
| **Agility / Responsive** | Can changes to the access control help the business fulfill objectives faster, or more competitively? (e.g., by sharing more to different parties?) |
| **Usability** | Can usability and end user satisfaction be improved by the access control function? |

## Step 4: Future Roadmap

Identity and access management and authorization need to have a forward-looking model. Authorization can improve both the security and usability functions that experience continual change and evolution.

A key limitation of homegrown and customized embedded access control systems is the difficulty often met when changing or modernizing them as requirements evolve. Therefore, it is important to understand the existing business and technical requirements and also how they may change in a 12- to 36-month timeframe.

This could include requirements surrounding how and by whom an asset is being accessed — different user communities, federation boundaries or partnerships, for example — as well as how the known and unknown security threats against an asset may change.
For example if an API is being exposed to external users, what threat modeling techniques may need to be adopted to understand what new threats may need to be countered.

Not only should an internal roadmap of requirements be collated and "guesstimated" but an analysis of the external authorization platform supplier roadmap should be completed too. Whilst the platform roadmap will contain capabilities that are not being used today, they may allow the business assets to be shared or accessed in a way that can enable new business operations, workflows and collaboration. These new authorization functions should be seen as a business enabler, allowing the business to improve productivity, develop partnerships further or perhaps fulfill external consumer requests in a more secure and usable manner.

## Step 5: Assess Supplier Capabilities

Clearly, a major aspect of migrating to an external authorization platform is the need to assess supplier capabilities. This should include not only technical capabilities, but also non-functional requirements, such as deployment model, support levels and integration options.

The assessment process should involve a range of steps, including book analysis (reading of whitepapers, data sheets and demo videos), live workshops and interactions, as well as more formal proof of concept or proof of value projects where the platform can be integrated and understood. Independent and impartial assessment and due diligence may also be required to understand the technical requirements and migration approach.

The assessment process is likely to be iterative, as more systems and assets are migrated and the landscape changes.

## ABOUT PLAINID

PlainID is the world's leading provider of enterprise Authorization, helping enterprises address the complex challenges of Identity Security. The PlainID Platform allows you to discover, manage, and authorize access control policies for enterprise applications and data. Our solution is architected to protect against identity-centric security threats powered by Policy-Based Access Control (PBAC). **Visit PlainID.com for more information.**