Authorization Buyer's Guide

Supported by The Cyber Hut

plainID

Table of Contents

Introduction 3

Who Is This Guide For? 3

Enterprise Pain Points and Challenges 4

Existing Solutions 5

Where We Are Today. 5

Where We Are Heading 6

Use Cases and User Stories 7

B2E Enterprise / Workforce 7

B2C Consumer / Customer 8

Understanding Business Outcomes 9

Operations Optimization 10

Improved Business Agility. 10

Improved Security Performance 11

Reduced Business Friction 11

Vendor Evaluation 12

Vendor Capabilities 12

Questions to Consider 13

How To Get Started 16

Identify Landscape. 16

Prioritize Assets 17

Gather Requirements 18

Future Roadmap 19

Assess Supplier Capabilities 19

INTRODUCTION

Who Is This Guide For?

Authorization is a complex topic. Often difficult to get right, measure and modernize.

Authorization within the modern enterprise, which is faced with numerous competitive, technological and security challenges, is seen as a key enabler — driving the business to share more assets, with more people, faster and under more threat than ever before. As such, stakeholders interested in a successful authorization solution are increasingly varied, each with different measures and metrics for success.

This guide aims to inform and enable numerous business stakeholders in their use of authorization as a means to improve a broad set of business outcomes.

STAKEHOLDER	EXAMPLE SUCCESS OUTCOME	EXAMPLE RISK OUTCOME	EXAMPLE METRIC
CISO	Fewer data breaches	Data loss	User access to sensitive data
CIO	Compliant infrastructure	Open audit findings	Automated audit analysis
Chief Digital Officer	Increased customer engagement	Customer churn and abandonment	User onboarding rates and times
Identity & Security Architect	Reusable policy components	Bespoke access control	Coverage of authorization policy
Application Owner	Responsive UX	Slow and unresponsive releases	Level of devops automation
Data Owner	Knowing who has access to what	Blind access control	Data asset visibility

Enterprise Pain Points and Challenges

How does authorization fit into the modern enterprise and how can it enable success for such a broad array of stakeholders — all with different levels of success and measurement?

AREA	PAIN POINTS
Access Control	• Inability to connect subjects (employees, customers, partners, services and sometimes devices) to objects, namely the resource they want to access • Inability to centralize and re-use access control components such as identity data, policy and enforcement processes • Excessive and stale permissions — either due to hard coding or a lack of process to remove them
Security	• Increased risk due to a lack of security control coverage — blind spots with respect to data protection, infrastructure management and application delivery • Security control that are difficult to iterate, change and adapt to new and emerging threats, either known or unknown
Time to Market	• Inability to respond to external market and competitive pressures due to slow application delivery, identity or application programming interface (API) management • Inability to share data with those who need it, in a time that is responsive to demand
Performance	• Application and infrastructure bottlenecks with respect to access control decision and processing logic
Visibility	• Lack of visibility into who has access to what, where and why

Where We Are Today

Existing Tools, Processes and Solutions

A weak authorization architecture can inhibit the business from a security and competitive perspective, but often those barriers are not well understood, and can create a larger blast radius of damage to operations and go-to market strategies. Here's an overview of typical authorization methods and solutions that organizations adopt.

SOLUTION	DESCRIPTION
Directory Services	The use of an lightweight directory access protocol (LDAP) directory service to store identities and permissions, in the form of groups. The directory can be used to authenticate the user or service, with groups and the organizational unit used as part of the permission model. Most systems that rely on this are enterprise applications.
Role-Based Access Control (RBAC)	RBAC provides access based on roles assigned to users within an organization, rather than on an individual basis. The roles are assigned according to the job responsibilities and requirements of the users.
Attribute-Based Access Control (ABAC)	ABAC provides a similar abstraction layer to RBAC, but is based on providing access related to identity and contextual attributes, such as job title, location, grade, device type or perhaps historical transactions.
Classic Access Management	An authentication and session management system (commonly seen as an identity provider [IDP]) that has extended to include web access management. Typically relies on policy agents as an enforcement point with basic policy-based access to URLs.
Standards: XACML & OAuth2	Extensible access control markup language (XACML) is seen as a legacy approach, based on extensible markup language (XML) that provides a powerful range of features and a model relying on a PDP (policy decision point), PAP (policy administration point), PIP (policy information point) and PEP (policy enforcement point). Not likely used for new projects. OAuth2 (open authorization) was originally created to solve the anti-pattern of password sharing when accessing third-party websites. None seen as the de-facto standard for protecting modern APIs. Many different profiles and extensions.
Homegrown	Embedded access control, often using homegrown solutions and open source libraries is common, mainly due to bespoke requirements, cost, and a previous lack of commercially available authorization solutions. A broad array of features, protecting portals and websites.
Declarative Authorization	A more recent addition to the authorization arsenal, where access control rules are externalized into a rules language away from the asset being protected. Several different approaches — including the popular open policy agent (OPA) — that provides generic decision processing, allowing access control to be extended to new areas such as infrastructure, data and IoT.

Where We Are Heading

The requirements for authorization are continually evolving.

The user communities encompass B2E/enterprise, B2C/consumer and partner ecosystems. And the systems and services requiring protection are broad and varied – from infrastructure to APIs and microservices to personally identifiable information stores to IoT-generated data – and more.

Specialist authorization platforms allow an organization to invest more time and resources into building and operating core business technologies, while allowing commercial off-the-shelf software to handle the security, governance and user experience of implementing policy-based access control.

SOLUTION	DESCRIPTION
Directory Services	An externalized, central management console that provides specialist authorization and access control services for a range of protected assets. It is likely that this centralized platform is delivered as a service, or at least in a cloud-native setting. Access control logic is captured in policies which can be managed via standard governance processes. The assets under protection are varied, and policy enforcement points come in a range of different guises — including inline proxies, microservice decision points, representational state transfer (REST) APIs and software development kits (SDKs). • Centralized management • Extensibility for technology patterns • Distributed enforcement • API • SDK • Policy-based access control (PBAC) • OPA support

B2E Enterprise/Workforce

Example Use Cases

1. Organizations leverage a range of applications and services to empower their workforce. These applications are located both on premises and in the cloud, and are often a mixture of homegrown and commercial systems. They all require authorization and access control functionality.

2. Organizations that have experienced a shift to a more digital-first delivery model often leverage APIs in order to share data, functionality and capabilities across multiple application owners or even business boundaries. The “API Economy” allows for more flexible and rapid collaboration and integration. How can the deployment of these APIs be streamlined and made more secure, yet still deliver business value?

3. The next evolution of the API delivery mode is to break down front-end APIs into a range of back-end microservices. These microservices allow for a more distributed work effort, a more modular and coherent delivery model, and a deployment model that leverages reusable components and a programmatic control plane.

Example User Stories

AS A...	I WANT TO...	SO I CAN...	CONTEXT
As an application owner...	I want to remove hard coded access control logic...	so I can ship my applications faster.	Static users, groups, and user and group permissions reduce security and deployment speed.
As an application owner...	I want to externalize the enforcement process from my applications...	so I can spend more developer effort on building our core features.	Authorization logic cannot necessarily drive business value for the app owner.
As an identity architect...	I want to have a consistent way of managing on-premises web access...	so I can reduce operational complexity.	Siloed access control systems and logic are expensive to maintain and support.
As a security architect...	I want to have full visibility of what items are protected...	so I can fulfill risk assessment and audit reporting functions.	A lack of visibility often results in unknown data leaks.
As a line of business manager...	I want to be able to share data with my team members directly...	so I can enable better collaboration and reduce the time it takes to start new projects.	Cumbersome access request processes reduce productivity and the ability to collaborate.
As a line of business manager...	I want to be able to manage access to my applications in a non-technical way...	so I can provide the correct level of access to my team.	A natural language way of representing access and policy data helps reduce technical fatigue and obfuscation.

B2C Consumer/Customer

Example Use Cases

1. External-facing identity systems will require the need to capture, store and process personally identifiable information, such as social security numbers, addresses, preferences and application activity. That data needs to be protected, at scale, across a range of geographies.

2. Digital consumer journeys require the integration of many different disparate systems in order to fulfill data sharing, aggregation, tracking and analytics requirements. These systems typically leverage REST-based APIs. This integration and sharing process needs to be fulfilled in a privacy-preserving and scalable way.

3. Sectors such as retail banking, healthcare and insurance are bound by numerous regulatory clauses that organizations must comply with. The move to digital online processing in these sectors amplifies the need for a consistent, highly controllable and visible security control infrastructure. The foundation for this should be policy-driven to allow for the capture of the correct access data, the ability to deliver a consistent security experience, and improve visibility with respect to knowing “who has access to what.”

Example User Stories

AS A...	I WANT TO...	SO I CAN...	CONTEXT
As an identity architect...	I want to create access control logic using a policy-based model...	so I can create reusable components for a standard approach to app security.	Migrating bespoke access to a policy model helps improve visibility but also improve standardization.
As an identity architect...	I want to integrate a range of different data sources into the access policy creation process...	so I can support a range of complex access control scenarios.	Access policies require data from persistent stores (LDAP, structured query language [SQL]) as well as more runtime systems providing transaction context.
As a security architect...	I want to create a more composable and reusable security infrastructure...	so I can reduce our compliance risk.	Finserv compliance requires complex security controls which are best implemented via policy and reusable components.
As a security architect...	I want to protect a range of different systems using the same access policies...	so I can have a consistent enforcement plane to improve security.	Having bespoke protection processes for APIs, custom apps, web apps and data reduces security effectiveness.
As a chief digital officer...	I want to reduce PII protection risk...	so I can improve end-user trust and, in turn, customer engagement.	PII collection, storage and sharing requires a strong and well-described access control foundation.

Understanding Business Outcomes

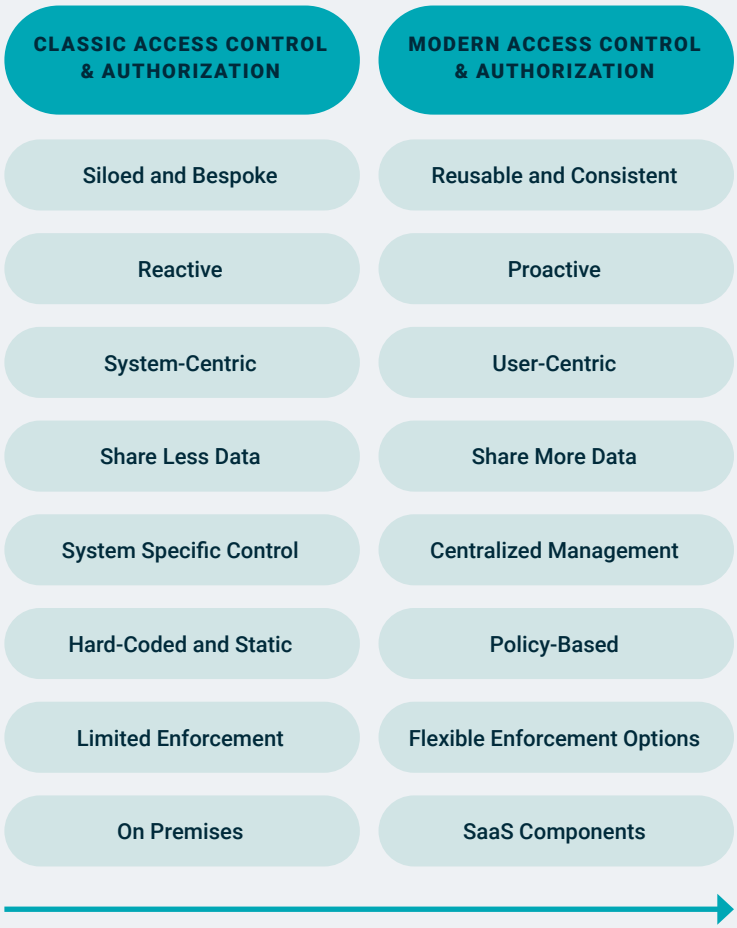
Authorization has historically — and in line with the broader identity and access management sector — been driven by operational constraints. This has often resulted in access control solutions that are reactive to technical challenges, heavily system centric and tactical in their feature evolution.

Today access control can be seen as a business enabler — allowing those not necessarily involved in the day-to-day access control life-cycle to benefit from the services it provides.

Organizations want to share more data to more organizations, within teams, across teams and to supply chain partners. Yet, they want to do this in a secure, compliant and user-friendly way.

The successful outcomes for authorization are becoming varied and distributed and benefit new and emerging stakeholders within the organizational landscape.

It is important to be able to map technical controls and performance metrics, with outcomes that not only impact the organization, but can also be communicated to a range of non-technical stakeholders. This helps to monitor the performance and productivity of a vendor and allows total cost of ownership and return on investment to be calculated and future authorization funding analyzed.



Operations Optimization

Improving the productivity and efficiency of operations is a key success criteria for historical IT investment. Employee productivity must at worst not be impacted and at best, improved inline with technology change.

BUSINESS OUTCOME	DELIVERED BY
Improved Employee Productivity	**Reduced Access Request Fulfillment Speed** — Essentially speeding up the time it takes to associate a subject (identity) to an object (piece of data, process, task) with the necessary permissions.
Improved Security Administration	**Reducing Excessive Permissions** — By aligning users and services more succinctly via policy, permission management and removal becomes less burdensome.
Improved Compliance Performance	**Knowing Who Has Access to What (and Why)** — By leveraging a more holistic, observable and policy-based approach to access control, reporting and insights can be improved.

Improved Business Agility

Whilst authorization may not immediately be linked with higher-level business functions, it is becoming increasingly clear that the secure collection, handling and sharing of important information and data can improve collaboration across both the supply chain and application management functions.

BUSINESS OUTCOME	DELIVERED BY
Faster Business Partner Integration	**Improving Data Sharing Capabilities** — By making it easier to share information, by data owners and administrators with trusted business partner identities.
Improved Supply Chain Management	**Securely Opening More APIs** — The API economy allows for improved integration options across both the upstream and downstream ecosystems.
Improved Competitive Responsiveness	**Reducing Application Release Time** — A more programmatic and external access control framework creates reusable components that can speed up application release times.

Improved Security Performance

Security metrics are becoming a critical tool in the spend profile of the CISO and senior security management team. Cyber security metrics for the coverage, performance and effectiveness of security helps to understand the return on investment and the level of support of the controls with respect to the risk management process. Authorization has a key role in improving the security control landscape.

BUSINESS OUTCOME	DELIVERED BY
Reducing PII Theft	**Securely Protecting APIs** — The security of APIs at both the north/south entry point and east/west intra-service communications layer is key in preventing data loss.
Reducing IP Theft	**Providing Secure B2E Controls** — The theft of intellectual property relies heavily on excessive permissions, a lack of visibility and hard-coded permissions. Movements to a more dynamic policy-led approach can help reduce this threat.
Improved Audit Reporting	**Knowing Who Has Access to What** — Reporting from a compliance perspective is often compulsory, but can be turned into a security productivity enhancer through the ability to visibly see, report and analyze which users have access to which systems — and why. Making audit insight and performance a direct benefit.

Reduced Business Friction

A key issue many CISOs face is knowing how to allocate finite resources — such as people, license spend and effort — and how to do so against an ever-growing list of security threats. However, this battle needs to be completed under the continuous eye of the business — where security controls that are too inhibitive or introduce and amplify friction will not only be unacceptable but often avoided by end users if they are implemented.

BUSINESS OUTCOME	DELIVERED BY
Improved Employee Onboarding	**Reusable Policy-Based Access** — By allocating users with the correct access when they join an organization, the speed at which they can start working is greatly expedited. The use of modular policies to allocate access (often incorporating RBAC, ABAC and contextual information) supports this approach.
Optimized Team Working	**Improved Line of Business Access Management** — By providing non-technical line of business managers with the ability to perform permission management (users to objects) or be part of the policy design process means the right staff members get the right access they need.
Optimized Hybrid Working	**Improved Intra-Team Data Sharing** — Data collaboration is a key component of a modern enterprise's ability to solve complex problems in an agile and timely fashion. The ability to share to other teams (even from other organizations) can be designed using dynamic policy-based access control that contains identity data, context and a broad array of data assets.

Vendor Evaluation

Identity and Access Management can be a complex topic and one area where this complexity is most evident is in access control. Evaluating an authorization provider requires a range of steps that can help remove the information barriers between the buyer and the provider.

What Capabilities Should the Vendor Provide?

CAPABILITY	DESCRIPTION
Platform Approach	A platform-wide set of capabilities that are specific to access control life cycle management — from the creation of controls, their enforcement and the governance surrounding them. This platform should be centrally managed and accessible by a range of different stakeholders interested in the protection of applications, APIs and data.
Policy Management	Authorization controls should be wrapped in a policy-based approach that results in reusable components which can be applied to a variety of different user communities, assets and stakeholders.
Policy Design	Policy design should be able to use a range of different data sources, including existing persistent identity stores, directories and databases, and more contextually aware signals such as risk, threat, device and location data. Policy creation should be both programmatic and by natural language user interfaces.
Enforcement	The enforcement of policy will be a critical component of the access control life cycle. A range of enforcement options will be needed, from inline proxies to microservice-based decision engines to APIs and SDKs to accelerate enforcement coverage.
Deployment Acceleration	Authorization is a key pain point for data, API and application access. The ability to deploy access control services and create and manage policy must be automated as much as possible, through a range of integration and management options.

Questions to Consider During Vendor Evaluation

CAPABILITY	EXAMPLE QUESTIONS
Platform Approach	1. Does the solution support a wide range of authorization capabilities? 2. Does the solution provide a centralized management console? 3. Is the management console designed to be used by a range of stakeholders, including non-technical line of business managers and application owners? 4. Can the platform be extended and customized? 5. Can the management console be delivered in a cloud environment? (either as a service or cloud-native private setting) 6. Can the authorization capabilities be made external from the application, API or data object being protected? 7. Does the platform support a range of standards-based integration options? (e.g., OIDC, OAuth2, LDAP, SCIM) 8. How does the platform help support a range of security architectures such as zero trust, identity-centric design and continual/adaptive risk? 9. Does the platform provide the ability to see who has access to what and why? 10. Does the platform support the ability to search for user permissions? 11. Does the platform support the ability to search for identity/subjects associated with a particular object/asset?
Policy Management	1. Can access control logic be encapsulated in policies? 2. Can policies be labeled, named, tagged and version-controlled? 3. Can policies be assigned to an owner? 4. Can policies be approved or tested before use against a production system? 5. Can policies be reused against a variety of user communities or target systems? 6. Can polices be duplicated or part-copied? 7. Can a policy be created programmatically? (e.g., REST API) 8. Can existing access control data be migrated into a policy framework? 9. Can policies be searched and queried?

Questions to Consider During Vendor Evaluation

CAPABILITY	EXAMPLE QUESTIONS
Policy Design	1. Can the access control policy contain data relating to roles? (e.g., role-based access control) 2. Can the access control policy contain data relating to attributes? (e.g., attribute-based access control) 3. Can the access control policy contain data relating to persistent identity? 4. Can policies integrate with data from existing directory services? (e.g., LDAP) If so, what systems are supported? Can this be extended? 5. Can policies integrate with data from existing relational databases? (e.g., SQL) If so, what systems are supported? Can this be extended? 6. Can polices be created based on authentication or assertion data? (e.g., id_token, SAML assertion, JWT) 7. Can policies be created for abstract objects? (e.g., pieces of data, physical objects, devices, IoT) 8. Can permissions (user to object associations) be edited by non-technical stakeholders? 9. Can polices leverage contextual data? (e.g., location, device, risk, threat signals) 10. Can polices be used to protect cloud or SaaS systems? 11. Can policies be stored on the file system? (e.g., YAML, JSON) 12. Can policy data be exported/imported via a version control system? 13. Do policies support the implementation of fine-grained authorization? (e.g., contextual and runtime evaluation)
Enforcement	1. What mechanisms are available to enforce the policy model? (e.g., policy enforcement point) 2. Is an inline service available to intercept access requests? 3. Is a decision service available for protected assets to query access control logic? 4. Is an API available for protected assets to query access control logic? 5. Is an enforcement capability available for APIs? 6. Is an enforcement capability available for data? 7. Is an enforcement capability available for microservices? 8. Can the enforcement point make access control decisions locally? (e.g., does not have administration point) 9. Can the enforcement point download or cache policy data from a central policy administration point? 10. Can the enforcement point be extended? 11. What performance metrics are available for the enforcement mechanisms? (e.g., transactions per second, time to respond) 12. Does the enforcement architecture support or leverage Open Policy Agent?

Questions to Consider During Vendor Evaluation

CAPABILITY	EXAMPLE QUESTIONS
Deployment Acceleration	1. Can the create, read, update, delete activities of policies be completed via an API? 2. Can policy data be queried via an API? 3. Can the enforcement points be deployed into containers? 4. Can the enforcement points be deployed programmatically? 5. Can the control plane/management interface be deployed in a cloud/cloud-native environment? 6. How does the authorization platform support secdevops-based deployment? 7. How does the authorization architecture support the likes of policy as code or no-code implementations? 8. Are processes or tools available to assist in access control discovery or policy migration? 9. Are policy updates automatically made available to enforcement points? 10. How does the authorization platform support hybrid deployment patterns? (e.g., components split in an on-prem, cloud-native, or SaaS ecosystem)

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? Do they have budgetary control?
Impact	What is the business impact if the application is unavailable? 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.