WHITEPAPER

PBAC, ABAC, and RBAC

A Guide to Navigating and Modernizing Authorization for the Enterprise

plainID

Connecting identities to digital assets is a central challenge in modern business. Especially in technological environments where digital assets are often decentralized and broadly distributed, identity-first security is an indispensable strategy to enterprises looking to ensure secure, consistent access to those assets.

Now more than ever, authorization is a powerful component of access control. As the "last mile" digital access, authorization plays the crucial role of determining who has access to what, when, and how based on policies aligned to an organization's business needs and security requirements.

The growing risk of data breaches and other cyber threats—in addition to digital advances like cloud computing, microservices, API gateways, and SaaS applications—has added an extra layer of complexity to an already complicated issue. New technologies have enabled organizations to store and access digital assets from multiple devices and platforms and, as Gartner has pointed out, this has eroded the value of legacy security controls that function at the perimeter of the corporate network.[1] **Enterprises need an identity-first strategy that can support zero trust initiatives in more complex, distributed environments.**

This poses a unique challenge to organizations. As IT environments become more intricate and distributed, and as the number of human and non-human identities grows, traditional authorization strategies such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are facing challenges in terms of scalability, adaptability, and flexibility. These methods lack the centralized and dynamic approach needed to meet the ever-changing business requirements of a modern enterprise with a diverse and distributed technological stack. In today's competitive environment, organizations that can be collaborative and digitally agile while maintaining a strong security posture will have a significant advantage.

To achieve this balance, organizations need to adopt a more advanced and flexible authorization strategy that can address the unique challenges of managing access control in complex and distributed IT environments.

Enter Policy-Based Access Control (PBAC). PBAC offers a business-oriented, comprehensive framework for **centralized authorization management.** This more flexible approach to authorization empowers application owners to create clear, adaptable policies that make sense within the specific needs of their organization. The increased adoption of this approach boils down to its business-friendly nature: Far from slowing organizations down with difficult-to-understand restrictions and stumbling blocks, PBAC positions cybersecurity as a key business enabler that makes everyday tasks both seamless and secure.

[1] Gartner, "Identity-First Security Maximizes Cybersecurity Effectiveness," 2022

The Evolution of Authorization

Authorization has had quite a journey over the last several decades, largely driven by the requirement for ever-more granularity in access decision-making.

Today, the adoption of APIs and microservices architecture has led to the need for a more granular approach to authorization, allowing access to individual services to be controlled and managed independently. A look back at the evolution of this technology provides insight into the building blocks of modern authorization architecture.

ACCESS CONTROL LISTS (ACL) were one of the first methods used for implementing authorization to resources. They used locally maintained lists of users or groups of users and their level of access for decision-making (e.g., "Janet can access resources A and B within an application, while Steve can access resources C and D"). Depending on an organization's size and risk tolerance, ACLs may still be part of their authorization framework. However, their manageability becomes an issue as the need to scale up increases.

ROLE-BASED ACCESS CONTROL (RBAC) later became the primary method for authorization, used by a broader set of emerging solutions such as Identity Providers (IdP) and Identity Governance and Administration (IGA). RBAC involves creating roles, assigning them permission sets, and then assigning roles to the users. Although a more centrally managed method than ACLs, RBAC also faces challenges with scalability, flexibility, and manageability, specifically when it comes to "role explosion" and exposure risks.

Attempts to implement fine-grained access control using RBAC can exacerbate the issue by requiring the creation of many similar roles that differ by only a few permissions. On top of this, RBAC can pose an exposure risk, either by granting a role that is too wide in scope (because it was the closest thing to what the user needed) or by granting a user access to a resource at any given moment, rather than under specific conditions that would provide more protection for sensitive data.

ATTRIBUTE-BASED ACCESS CONTROL (ABAC) emerged to address the shortcomings of RBAC. It offers more fine-grained authorization and externalized decision-making that enables the access decision to be made outside of the application—and only provide the application with that decision. ABAC uses multiple characteristics such as user attributes, location, security clearance and time of day while formulating access decisions. Attributes of the asset (access object) may include its related project, the personally identifying information (PII) it contains, and the sensitivity of that PII. Viewed holistically, these attributes can now be used to set more "right-sized" rules that enable access to data and resources. However, management issues have persisted, as ABAC is a highly technical solution and does not take non-technical stakeholders such as business managers or application owners into account.

These shortcomings of traditional authorization methods have since been amplified by organizations' modernization and digital transformation, which have been pivotal in meeting business goals. The following are some of the primary factors that have driven the necessity for a more flexible and dynamic approach to authorization:

- **Implementation of zero trust initiatives:** The premise of zero trust assumes that all devices, users, and networks are untrusted and require continuous verification of user identity and authorization status before allowing access to resources. Authorization needs to be dynamic and flexible to changes in user identity and attributes to ensure continuous verification at every stage of the digital interaction.
- **The move to cloud computing:** The widespread adoption of cloud computing has changed the way organizations think about authorization. In a cloud environment, authorization needs to be managed across multiple devices and platforms, making it more complex and challenging.
- **Complex customer portals and ERP systems:** Inherently, these systems are complex and often involve a large number of users, each with different roles and access requirements, making it challenging to set and enforce appropriate authorization rules and policies.
- **Adoption of microservices architecture:** The rise of microservices architecture has led to a more granular approach to authorization, where access to individual services can be controlled and managed independently.
- **Greater emphasis on user experience:** As organizations become more focused on user experience, authorization has needed to become more streamlined and user-friendly without impacting security.

Despite all factors pointing to the need for a more flexible approach to authorization, organizations that have adopted RBAC and ABAC have found value in these approaches—and have made them an established part of their enterprise infrastructure. So, why would enterprises want to throw them away?

Moving Forward with PBAC

While PBAC, RBAC, and ABAC are different approaches, it is more accurate to say that predecessor approaches are components of the more comprehensive and modern PBAC framework.

Though similar in name, **Policy-Based Access Control (PBAC)** is not an alternative to RBAC or ABAC. Rather, it's the answer to a universal challenge: *centralized policy management.* PBAC is a comprehensive authorization management framework that orchestrates the full capabilities of the modern authorization toolkit: RBAC, ABAC, and run-time decisions, along with fine-grained and coarse-grained decision-making.

PBAC overcomes the **management and scalability** challenges of RBAC and ABAC through its deployment flexibility. An *Authorization-as-a-Service* model addresses the management and scalability challenges; the model can run in the cloud, on-premises or as a hybrid. PlainID Authorizers™, an industry innovation, provides technology-specific, out-of-the-box integrations to authorization infrastructure to enable run-time enforcement at a highly granular level to support data security.

Importantly, the PBAC framework provides a **business-oriented approach** for authorization. It has a management user interface (UI) where policies can reflect complex business logic using graphical representation and natural language. Business managers and application owners can create and enforce policies without relying on programmer or developer intervention. PBAC works across the modern technology stack: data lakes and warehouses, APIs, microservices, cloud infrastructure, third-party and homegrown applications.

Because PBAC **fully externalizes authorization,** it allows enterprises to achieve central policy management with distributed enforcement while maintaining consistent standards and extending them to where they are needed. This gives security and administration teams full control and visibility of how people and machines access digital assets.

The PBAC Authorization Toolkit

Central Management and Distributed Enforcement

The shift toward centralized policy management has emerged as a result of the traditional approach of integrating authorization into application code. With businesses breaking down monolithic applications into smaller APIs and microservices for greater agility, it has become necessary to externalize authorization and centralize its management. This approach enables businesses to implement PBAC consistently, contextually, and at scale across their infrastructure. By managing policies centrally, businesses can gain complete visibility of how users and machines access digital assets and fine-tune access controls at every digital interaction.

PBAC provides more interoperability than many native authorization solutions, allowing businesses to pull risk signals and context from multiple sources of information. This results in more intelligent and secure access decision-making. The combination of centralized policy management and distributed enforcement enables security and business teams to align on access policies and apply dynamic authorization in real time, thus improving security posture and ease of access for users.

What sets PBAC apart from previous solutions is its emphasis on policy visibility. Business and security managers can investigate, test, and approve authorization policies without technical knowledge, thanks to PBAC's full visibility of access to digital assets. PBAC central management involves defining policies and rules for access control, which are centrally managed and enforced for a standardized and consistent approach to access control. It also provides workflow and policy lifecycle management capabilities to support security best practices and auditability. This approach is often used with dynamic authorization to support a zero trust model and an identity-first security strategy.

Dynamic Authorization

If PBAC is the chassis for modern authorization, **dynamic authorization** is the engine. Combining PBAC and centralized management with distributed enforcement, dynamic authorization calculates access decisions in real time for continuous and contextual security. This is especially important in the context of the zero trust security framework, as dynamic authorization provides the necessary security to recognize risk and enforce appropriate access decisions.

Gartner recently emphasized the importance of this flexible, distributed enforcement. Noting the failure of traditional identity and access management (IAM) to address security risk in real time, a December 2022 report on identity-first security priorities underscored the necessity of supplementing centralized policy administration with dynamic controls that can leverage contextual data to provide continuous risk assessment and authorization.[2]

[2] Gartner, 2022

The stakes are high. Gartner estimates that by 2026, 70% of identity-first security strategies will fail unless organizations adopt "context-based access policies that are continuous and consistent."

Moreover, "IAM leaders must combine centralized IAM controls, policies, data and programs with decentralized and context-sensitive enforcement" to rescue their identity-first strategies from failure.

PBAC and dynamic authorization are the one-two punch necessary to make this mandate a reality. Whether it's a change of role, organizational structure, or assignment to new projects, PBAC adapts immediately to what documents, servers, and data the user can access. No additional action is required to enable access to the new project data, the new user in the department, or a freshly re-assigned accountant.

Dynamic authorization grants users access based on their identity, the resources they are attempting to access, and external factors such as risk signals, all in real time. This makes dynamic authorization a fundamental capability in implementing the principle of least privilege.

TENETS OF ZERO TRUST

While there's more than one approach to delineating the principles of zero trust, most rely on the seven tenets presented by the U.S. National Institute of Standards and Technology (NIST) in its Zero Trust Architecture report (NIST Special Publication 800-207).

In fact, NIST explicitly specifies:

- Access to individual enterprise resources is granted on a per-session basis. Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task—meaning authentication and authorization to one resource will not automatically grant access to a different resource.
- Access to resources is **determined by dynamic policy**—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
- **All resource authentication and authorization are dynamic and strictly enforced** before access is allowed.

Zero trust is even more critical in our digital, distributed, and mobile work-from-anywhere reality. With the perimeter everywhere and the attack surface growing, no one should be completely trusted. The zero trust framework helps limit data access on a need-to-know basis, reducing the risk of data breaches and protecting critical assets.

Solving the Granularity Problem

Coarse-grained and fine-grained refer to the level of specificity addressed in access decisions: from the name and title of the person (coarse-grained) to the full set of attributes about the identity and the object or asset (fine-grained). Many organizations today use a mix of both methods based on risk, which usually requires multiple systems.

PBAC subsumes those systems under its business-oriented approach, enabling the right method to be automatically deployed at the right time.

Viewed holistically, these attributes can now be used to set the rules that enable access to data and resources. The two methods work together to deliver the appropriate authorization to the access point at hand. By integrating them into its comprehensive management framework and processes, PBAC empowers them from a business-policy perspective to deliver modern authorization.

PBAC's business-calibrated method means that authorization isn't reliant on any specific technical implementation (like XACML) and policies can be set in natural language. For example, a team lead can grant access to a project only to team members on weekdays between 9 and 5, making it much simpler to manage large numbers of users and large amounts of data.

Moreover, PBAC supports environmental controls. If there are sensitive files that should be viewed only on certain corporate computers, a policy can easily be set to limit access to on-premises systems.

PBAC also makes complying with regulations such as General Data Protection Regulation (GDPR) easier by having tighter control of data access, controlling access creep, and even preventing authorized users from accessing data in a risky manner.

COARSE-GRAINED

Coarse-grained **RBAC** authorization tools involve creating a role for every organizational or business functionality, giving that role permission to access certain records or resources and assigning a user to the role. Traditionally, these RBAC solutions have been too granular, inflexible, and limited to apply at large scale. Coarse-grained solutions are difficult to apply in the context of cloud computing, and they often don't work in changing business models such as B2B that may involve granting non-employees access to organization assets.

FINE-GRAINED

With fine-grained **ABAC** authorization tools, access to a particular record or resource is moderated based on certain traits—attributes—of the person accessing the file (e.g., their title, certifications, or training), the resource itself (e.g., its related project, the personally identifying information it contains, or the sensitivity of that information), and the time and place where the object is being accessed.

Authorization Modernization: If Not Now, When?

PBAC is built for the data and identity architecture of today's enterprises. Far from legacy identity-first strategies unfit for today's distributed technological environments, PBAC gives business leaders modernized, unprecedented control over their Identity and Access Management.

PBAC can be used to enable access and prevent access based on what happens in real time, who the user is, and where they are accessing from. It lets you make smart decisions on how data and resources will be available—and at any scale.

By leveraging the benefits of both coarse-grained and fine-grained authorization schemas, PBAC offers a supremely flexible and powerful authorization solution to businesses looking to push innovation, increase collaboration, and maintain their edge over the competition.

PlainID offers the first commercial authorization solution that deploys PBAC. To learn how PlainID can help you bring your Authorization strategy into the future, contact us for a demo.

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.**

plainID