White Paper

Exostar Identity and Access Governance A Primer

EXOSTAR®
We build trust.

Security and risk management professionals looking to strengthen control around which individuals have access to which resources face a wide set of challenges. As Identity and Access Management (IAM) solutions have evolved, so has the complexity of providing secure access for Workforce, Partner and Consumer users.

With the rapid adoption of new cloud services and accelerating needs for digital transformation, today's security professionals face a complex task when managing a growing number of digital identities and constituents. **The Access: One platform simplifies these tasks and enables organizations to quickly address security and compliance challenges including:**

- **Improving user productivity, reducing downtime and increasing user security**
- **Increasing visibility, automation and control of user access**
- **Simplifies complex security and audit tasks, making it easy to meet compliance requirements**

Many IAM solutions are focused on single pain points, including user provisioning, identity governance, web access management and/or strong authentication. With the Access: One platform, we address all of these challenges with a single SaaS based solution. We enable organizations to easily and efficiently introduce comprehensive security controls while improving user productivity and security.

Within this paper we outline how organizations can leverage the Access: One platform to provide converged services for identity governance and secure access management.

Introducing Identity and Access Governance

Identity and access governance (IAG) spans a far-reaching set of scenarios and interactions that span all identity and access management (IAM) constituencies. Done well, the right solution will address the following concerns:

- User credentials are secure and, where appropriate, leverage biometric / strong authentication methods.
- A user is always the person they claim to be.
- A user's details are correct and current.
- A user's access entitlements (privileges) are appropriate for their roles and responsibilities.
- A user is able to manage their own credentials.
- A user is able to easily request access to new services (and remove access to unnecessary services).
- Appropriate systems exist to ensure authorized employees have the ability to approve (and verify) access privileges and requests.
- The organization can easily demonstrate it has control over user access and entitlements in a timely manner.

Bringing together access management and identity governance

Access management platforms have traditionally focused on providing services for authentication, single sign-on, trust elevation and authorization. As time has progressed (and IAM solutions have matured), access management vendors have expanded their offerings to provide lightweight governance services focused on the end-user, including access request, access approvals and password management.

At Exostar, we consider governance to be an integral part of an end-to-end enterprise IAM service. Good governance is a component of the fabric that brings together users and services in a controlled way. We believe governance capabilities need to be tightly integrated and aligned with access management services to deliver platforms that are secure and easy to use.

When looking to provide governance capabilities as part of an enterprise IAM platform, we consider the following:

Ease of deployment and configuration

- The platform's deployment must be easy and quick to configure. The platform must enable organizations to configure comprehensive governance functions as an embedded part of a Software as a Service offering.
- Administration should be centralized. Users of every level must be able to complete IAM associated tasks from a single place. This includes user administration as well as end-user self-service.
- The platform must enable administrators to implement an organization hierarchy that associates users with their relevant line managers, delegates and approvers. The organization hierarchy must support flexible models, including the ability to define groups and hierarchies according to departments, locations or third-party suppliers and subsidiaries.
- The platform must bring together identity and access management use cases in one place. An integrated service means users are able to administer their preferences and privileges from the same place that they access services. The same requirements are applicable for line managers and application administrators, who need to complete all aspects of their IAM related responsibilities from a single point.

Addressing the most common access management and identity governance use cases, all of the these capabilities can be easily implemented using Exostar's Access: One.

Identity lifecycle management and governance

- The platform must provide flexible workflow and provisioning capabilities when managing fulfilment requests. These capabilities should support integration with systems of authority and control (including HR and helpdesk services).
- When reconciling HR information, the platform must support multiple feeds and types of users. Examples include different feeds and approval processes for contractors, third party providers and employees. The platform should also support end-user self-registration and manager-driven administration to ensure the right people are granted timely access to services.
- The platform must support fine-grained entitlement management. Access Management vendors have historically focused on coarse-grained provisioning use cases. The addition of governance capabilities requires finer grained provisioning and entitlements management, as well as the ability to reconcile existing identity repositories to ensure the ongoing integrity of the platform.
- When reconciling account details from integrated systems, the platform must provide the capability for automated account adoption and orphan account management.
- The platform must be capable of fulfilling access requests for both on-premise and cloud-based services. In addressing identity governance use cases, the platform must support fine-grained provisioning and reconciliation requests.

Providing Actionable Intelligence

- The platform must enrich decision making by bringing together a history of requests, approvals and usage patterns in a single authoritative service.
- The platform must make it easy to see (and understand) what privileges a user holds and also support the translation of complex access privileges into simple to understand business entitlements.
- The platform should provide the capability to model the risk and compliance impact of a user's access request at time of approval. The system should support approval or risk management workflows specific to high-risk requests or segregation of duties breaches. The platform should provide the ability to assign risk scores based on the entitlements a user holds.
- The platform should implement a flexible access certification model. Certification campaigns (including risk and time-based certification) allow organizations to group risk management actions by audience or application types. By using entitlements, access request, approval and certification tasks become straightforward, allowing end-users and line managers to more easily understand and complete everyday governance tasks.
- The platform should implement a comprehensive and flexible reporting service. This should include the ability to create user and role-specific dashboards, as well as mining and exporting data based on a user's administrative rights.

Access from a secure, single point

- The platform must provide a flexible to configure launchpad that can be tailored by the end-user to create different workspaces and groups of applications to maximize productivity.
- The launchpad must provide a central point for accessing every identity function, from single sign-on to preference management and self-service.
- Users should experience frictionless, secure access to services. The platform should provide both single sign-on and strong, passwordless authentication.

Increasing Productivity through delegated administration and self-service

- The platform must provide an easy to configure set of services that enable users to manage their passwords and preferences. These services should include configuring their strong authentication choices, recovering forgotten credentials and updating contact details and preferences.
- The platform must provide easy to consume services for access request and approval, encouraging self-service and delegated administration wherever possible. The platform should enable users to manage their access to applications and groups through an easy-to-use interface.
- The platform should provide an intuitive interface for line managers to administer access requests on behalf of their subordinates. By providing the ability to review a user's access rights, manage approvals (both access and certification requests), the platform should reduce the amount of time and effort needed to administer access across a distributed workforce.
- Employee productivity rises by enabling decisions and approvals to take place as close to the user as possible. Empowering line managers and local administrators to make decisions means that day-to-day management occurs locally, in a timely manner. Good identity governance keeps people productive.

Exostar Access: One – Securing your enterprise with a comprehensive SaaS solution for Identity and Access Governance

Delivering a comprehensive set of capabilities from a single platform, **Access: One** enables organizations to quickly improve security and productivity while enhancing their capabilities for:

- Secure access management, including single sign-on and strong passwordless authentication.
- Identity governance, delivering easy administration for line managers and application owners while providing valuable, audit-ready insights that demonstrate you're making the right kind of access decisions.

Rather than managing multiple solutions and integrations to provide the end-to-end capability outlined above, customers can leverage **Exostar Access: One** to quickly realize the benefits of a market leading service for access management, identity governance, user lifecycle management and strong authentication.

Consider how **Access: One** could help to drive compliance and user productivity through an easy to implement and configure cloud services for identity and access governance.

BENEFITS OF EXOSTAR ACCESS: ONE

- SaaS services for identity and access governance focused on serving highly regulated industry and use cases.
- Increase user productivity through easy to configure, intuitive services for single sign-on, strong authentication and self-service.
- Simplify access governance with a unified access management and governance solution that provides industry leading capabilities.
- Improve productivity and efficiency with delegated administration, automated provisioning and compliance remediation.
- Support compliance through automated policy enforcement, risk modelling and comprehensive reporting.
- Quick and easy deployment, enabling you to secure your enterprise through improved visibility and control within weeks.

ACT NOW: TAKE THE FIRST STEP TOWARDS MORE EFFICIENT IAM TODAY.

Why Exostar?

The Exostar Platform represents the culmination of **20 years of successfully and exclusively delivering secure B2B collaboration solutions** for a growing community in highly-regulated industries. It supports the **governance, risk, and compliance** requirements for collaboration between **enterprises and their partners.**

www.exostar.com/product/pirean-access-one

exostar.com/contact.