DirX Identity

Identity management and governance for security and success

User and access management aligned with business processes

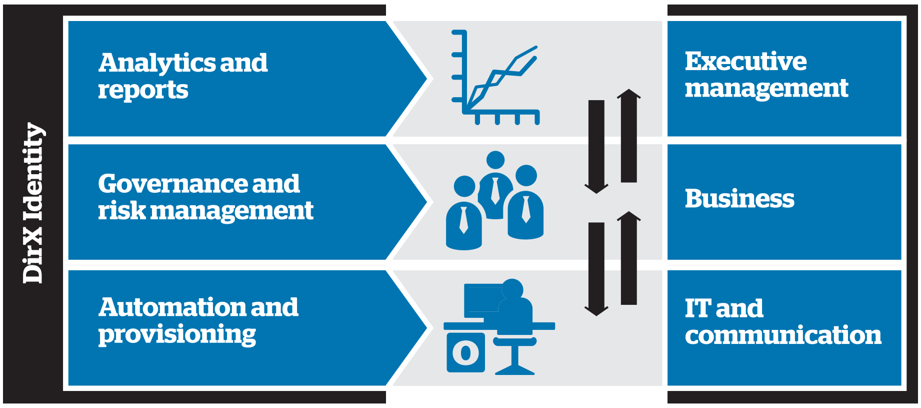
The challenge

Business relationships are growing ever more complex. More and more users have access to enterprise IT systems – and the pressure is on to enable every one of these users to maximize productivity while ensuring privacy, compliance and cost control. The cloud, which is high on the agenda of many but which creates potential security issues, complicates this already challenging security situation.

In this fast changing business environment, effective identity management and governance is imperative – for enterprise security and for business success. Traditionally, IT departments have deployed identity management to increase efficiency and reduce costs. Now, business relationships and compliance are becoming predominant. Managing and securing business processes requires the consistent administration of users, roles and entitlements across applications and in business partner networks. Giving the right people the right access to the right resources at the right time is essential for protecting corporate data, and for enabling users to be innovative, productive, responsive, compliant and cost-effective.

Our solution

DirX Identity from Atos is a comprehensive solution for today's demanding business environment. It aligns IT, business and executive management in the lifecycle management of users and their access rights. For IT, DirX Identity provides automated user provisioning; for business and general management, DirX Identity offers improved governance and risk management; and for executive management, DirX Identity provides analytics and reports essential for steering and control functions. Process-driven, customizable, cloud-ready, scalable and highly available, DirX Identity is the identity management and governance solution that organizations need for today and tomorrow.



Bull
atos technologies

The case for Governance

The security and business case for identity and access management is strong. There are also compelling factors driving the need for strong governance in this area.

Regulatory compliance

Secure user access to corporate information is a growing legal issue. Governments worldwide are passing laws to ensure security, privacy, and integrity of sensitive data such as consumer and financial records.

Financial services, healthcare, pharmaceutical and many other industries require a secure access control infrastructure. Non-compliance can result in legal action, with heavy financial penalties, and even criminal proceedings.

To prove compliance, companies must be able to show "who did what, and when, with what information". This requires a single view of a user's access rights to all IT systems, a method of tracking access continually and automatically through an identity-based audit and access certification, and a way to archive this information securely for long-term access and analysis.

Enabling eBusiness

Companies provide content and business processes via portals and online services for employees, subscribers, customers, and trading partners. eBusiness sets challenges in security governance, managing risk, demonstrating accountability, and proving regulatory compliance. Where services are delivered by cloud providers, there are new issues to consider.

Organizations need to clearly define corporate security policies, and enforce them consistently across all systems in the IT infrastructure. To do that, they need to know: "who is allowed to access what information, and how."

Fast and flexible change management

To maximize productivity, and guard against security risks, new users, and users changing job functions, must get the access rights they need to be up and running quickly. Departing users must have their access rights revoked immediately to close security holes. Governance of users and their access rights must be consistent and effective across the user landscape.

Cost control

Staying competitive demands cost control and reduction. IT is an obvious focus for cost management, particularly as user numbers grow.

Companies want to minimize the number of calls made to help desks and hotlines for forgotten passwords, for example.

They want to reduce administrative costs of user management and provisioning, and improve user costs transparency.

Unlocking the solution

One of the major obstacles to identity and access management and governance is the way that IT is commonly organized.

Often, user management, access management, password management and auditing are carried out on a per-IT system basis. IT staff administer users and their access rights on each IT system in the network or in the cloud, usually by manual administration.

Users get one account and one password for each IT system they use. Each IT system has its own audit or monitoring function to track changes to users and their access rights on that system.

This structure challenges good user and access management:

- User and access data is duplicated across IT systems and becomes inconsistent over time, making it difficult to find correct and up-to-date information and to de-provision users
- Decentralized auditing and monitoring makes it difficult to track changes to users and their access rights. There is no way to tell what a single user's total access rights are across the enterprise, making it hard to audit for regulatory purposes
- One password per IT application means that users must remember a lot of different passwords, one for each system they use. Password proliferation leads to more help desk and hotline calls, lost productivity as users wait for password reset, and increased IT administration costs
- Manual administration is expensive and error-prone and leads to delays in provisioning and de-provisioning users. This affects productivity, jeopardizes security and compliance, and introduces data inconsistencies.

The route to effective identity management and governance is an enterprise-wide, cross-platform, provisioning and access management system, with centralized and automated user management. This system will control access to IT resources securely, efficiently and cost-effectively, based on users' business roles, policies and processes.

The system will also align identity management and governance with business processes. Routine administrative functions and decisions will be offloaded from IT staff to users and their managers, so that decisions about what users really need are made by the people who know best.

DirX Identity

DirX Identity delivers overall identity and access governance functionality, seamlessly integrated with automated provisioning. It provides life-cycle management for users and roles, cross-platform and rule-based provisioning in real-time, Web-based user self-service and delegated administration, request workflows, access certification, password management, metadirectory and auditing and reporting.

DirX Identity gives
the right people
the right access to
the right resources at
the right time...

DirX Identity delivers

User management

An accurate and up-to-date directory of users, and facilitates the assignment of privileges.

Role management

A logical layer for modelling and management of privileges, supporting role hierarchies and context-based granular entitlements.

Access certification

Ability for responsible parties to verify that roles and entitlements are assigned to users in compliance.

User self-service

Freedom for users to manage own data records and passwords, request privileges, monitor request status, and delegate access rights to other users.

Delegated administration

Responsibility is passed to designated administrators to manage specified user groups.

Management of organizational data (business objects)

Entities maintained that are relevant for, and related to, identity management processes, such as organizational units, locations, cost centers, and projects.

Request workflows

Ability for requesting and approving privilege assignments and attestation, and user and role creation and modification via multi-step workflows.

Password management and synchronization

Management of central password policies and reset user passwords by administrators, and users can maintain a single password for multiple applications.

Management of shared accounts

Management and control of how users access shared privileged accounts.

Policy management

Security and administrative policies maintained, such as provisioning policies to grant and revoke privileges automatically.

Real-time provisioning

Privilege assignments resolved into target system-specific entitlements, and user accounts and their entitlements are managed in target systems.

Metadirectory

Integrated and synchronized directories, user databases and other repositories to provide consolidated and consistent data.

Domain management

High-level separation of DirX Identity data for multi-tenant support is maintained and customized.

Target system management

Integration of applications and systems as data sources and provisioning targets are maintained.

Identity Web services

Identity management functionality provided, as Web services for integration in portals and custom applications.

Compliance

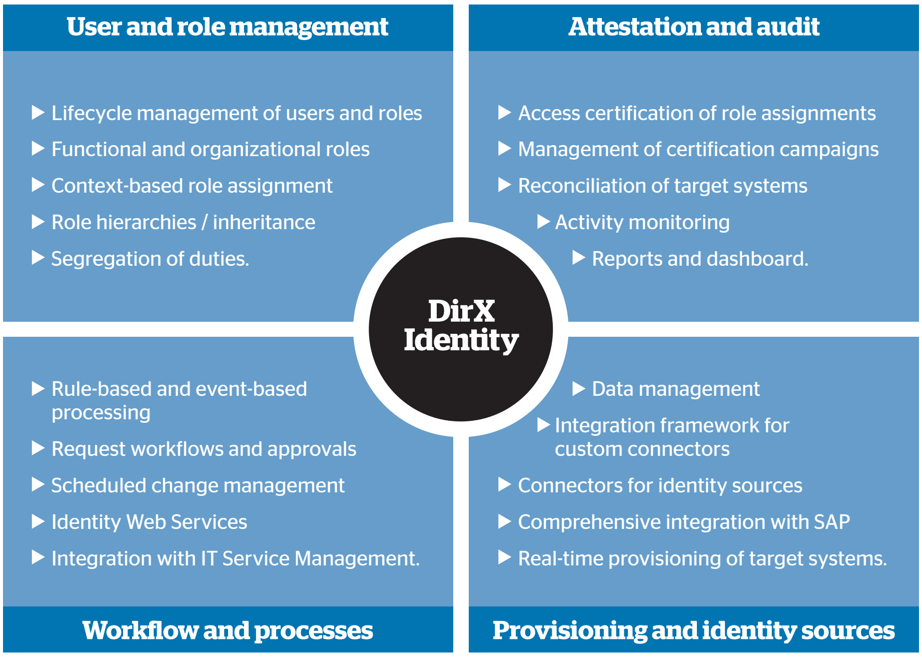
Supported risk management and mitigation to avoid or control violation of security policies, allowing for enforcing segregation of duties for entitlements across and within target systems.

Audit and monitoring

Tracking of administrative changes, and generated reports to view users and their entitlements.

Your benefits

- Provides cost-effective automated administration of users and entitlements
- Speeds up user deployments
- Reduces complexity and manages risks
- Supports ongoing processes for risk management and compliance
- Supports quick and easy adaption of identity management processes to customer requirements
- Provides for seamless integration with IT Service Management (ITSM)
- Allows management of ERP and IT systems centrally and consistently
- Helps manage heterogeneous environments, and allows for integration in horizontal and vertical solutions (PLM, healthcare, physical access, smartcards, unified comm.)
- Delivers excellent data management capabilities to cleanse, consolidate and keep identities up-to-date
- Delivers continuous and resilient services for business critical deployments with high-availability and scalability options.



User and role management

- Lifecycle management of users and roles
- Functional and organizational roles
- Context-based role assignment
- Role hierarchies / inheritance
- Segregation of duties.

Attestation and audit

- Access certification of role assignments
- Management of certification campaigns
- Reconciliation of target systems
- Activity monitoring
- Reports and dashboard.

DirX Identity

- Rule-based and event-based processing
- Request workflows and approvals
- Scheduled change management
- Identity Web Services
- Integration with IT Service Management.

Workflow and processes

- Data management
- Integration framework for custom connectors
- Connectors for identity sources
- Comprehensive integration with SAP
- Real-time provisioning of target systems.

Provisioning and identity sources

About Atos & Bull

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.
Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, and Worldline.

For more information, **visit www.atos.net**

Bull, the Atos technologies for the digital transformation

Bull is the Atos brand for its technology products and software, which are today distributed in over 50 countries worldwide. With a rich heritage of over 80 years of technological innovation, 2000 patents and a 700 strong R&D team supported by the Atos Scientific Community, it offers products and value-added software to assist clients in their digital transformation, specifically in the areas of Big Data and Cybersecurity.

Bull is the European leader in HPC and its products include bullx, the energy-efficient supercomputer; bullion, one of the most powerful x86 servers in the world developed to meet the challenges of Big Data; Evidian, the software security solutions for identity and access management; Trustway, the hardware security module and Hoox, the ultra-secure smartphone. Bull is part of Atos.

For more information, **www.atos.net/identity**

For more information: **security@atos.net**

IMPRIM'VERT®

This brochure is printed on paper combining 40% eco-certified fibers from sustainable forests management and 60% recycled fibers in line with current environment standards (ISO 14001).

Your business technologists. **Powering progress**

Atos