Fact sheet

DirX Audit

efficient compliance support

Analytics and Intelligence for Identity and Access

The challenge

Cost pressure is combining with increased security needs to cause enterprises and other organizations to look for new ways of optimizing their business processes. That is especially true in the observance of compliance regulations such as those stipulated in the Sarbanes Oxley Act regarding the reliability of the financial data published by enterprises. One way of providing efficient support for these efforts is to roll out an Identity and Access Management (IAM) system with audit support.

The sheer number and types of regulations, however, pose a challenge:

- Many different regulations exist today, and new ones are mandated all the time, requiring continuous revision of IAM controls.
- The policy for what is audited depends on the particular regulation, the enterprise business model in force, and the application creating the audit trail, making it difficult to establish consistent, end-to-end audit policies.
- Different regulations require different methods of analysis and reporting.

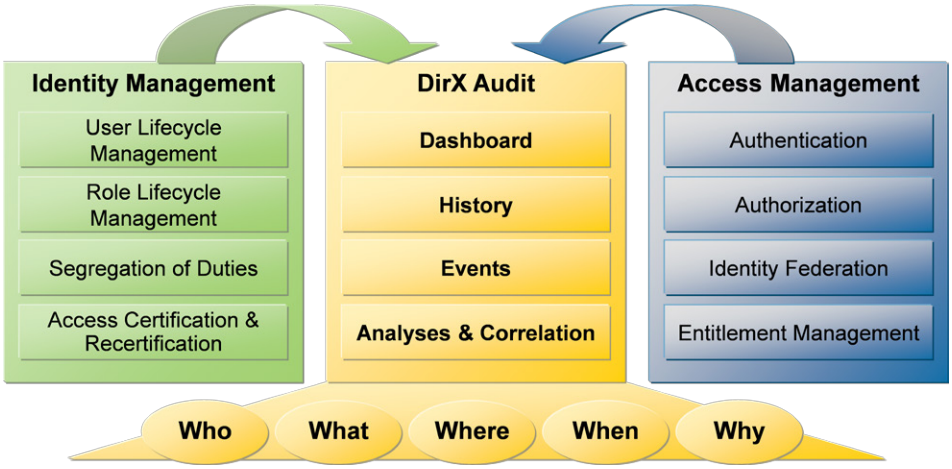
Audit data of IAM activities need to be produced that can be used to demonstrate accountability and report on the results to demonstrate control of business processes on user access and entitlements as required by applicable regulations. On a regular basis or on demand, reports must be produced on current status and history on the information in the IAM repositories - for example, the identity store in an identity management component.

The audit trails and historical data produced by IAM components can help to answer the questions that auditors ask to obtain proof of compliance. Until now, audit logs and historical data from several applications had to be analyzed to answer questions like "Who has accessed financial data in the last month?", "Who gave the users access rights for this?" and "Who approved these rights?" Different audit formats, different user identities for the same person and parallel timelines in the individual applications make such analyses very difficult and cost-intensive.

Our solution

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. DirX Audit complements the core IAM capabilities for administration, authentication and authorization by providing means to analyze and report on IAM operations and deliver the information necessary to support IAM governance and prove compliance.

Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the "what, when, where, who and why" questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, a monitor for filtering, analyzing, correlating and review of identity-related events and job management for report generation. With its analytical features, DirX Audit helps enterprises and organizations to ensure sustainable compliance and provide business intelligence for the identity and access management processes.



Sustainable compliance and transparency for Identity and Access

Bull
atos technologies

Delivering answers to auditor questions

Key Strengths

- **Activity Monitoring**

  DirX Audit collects and correlates data about administration, authentication and authorization events from different IAM audit producers and then transforms this data into intuitive and actionable intelligence with respect to compliance regulations, business security policies and corporate risk management objectives.

- **Historical Data**

  DirX Audit maintains historical data from identity repositories to reveal information about changes to identity and identity-related data over time, allowing for historical review of identities and point-in-time comparisons to demonstrate progressive compliance to governance processes, gain insight into identity and policy status or determine why an access request was permitted.

- **Key Performance Indicators**

  Employing OLAP (online analytical processing) techniques, DirX Audit generates identity audit KPIs (key performance indicators) that provide statistical information about audit events and historical data for fast, interactive analysis and insight into IAM operations.

- **Analytics and Intelligence**

  DirX Audit provides a Web-based user interface with specific views that facilitates the correlation, analysis and reporting of audit and historical data by auditors, administrators, and security compliance officers.

- **Dashboard View**

  The Dashboard view provides a personalized collection of KPI charts. Using the Dashboard, auditors can perform analyses, especially time-based trend analyses of selected KPI data and then drill down to details about audit events as necessary.

- **Event Monitor View**

  The Event Monitor view provides a convenient interface for filtering and correlating audit events. Using the Event Monitor, auditors are able to find answers to the "what, when, where, who and why" of user access and entitlements.

- **History View**

  The History view provides for browsing historical identity data. Auditors can review historical data, do point-in-time comparisons and correlate audit events with historical data.

- **Reports**

  DirX Audit provides pre-configured report templates. Auditors can set up scheduled reports that will be sent via e-mail to selected recipients at regular intervals. Jaspersoft iReport technology can be used to customize reports or to create new reports.

Your Benefits

- **Comprehensive Analyses**

  Improve the effectiveness of security controls.

- **Customizable User Interface**

  Simplifies analysis and reporting with the advantage to drill down into detail.

- **Centralized**

  Stores audit events from different sources in a single database.

- **Cost-efficient**

  Fast and convenient insight into IAM operations and historical data.

- **Expandable**

  Additional audit sources can be integrated.

- **Platform-independent**

  Support of several databases and server platforms.

For more information: Please contact security@atos.net or visit atos.net/identity

atos.net