

Evidian
Identity and
Access Management

www.evidian.com

From process automation to reconciled, role-based IAM policy

ABSTRACT

This white paper explains how IAM is moving beyond simple process automation, enabling you to reconcile your role-based security policy with actual IT usage.

Today, identity management is mainly used to automate account administration. But how can technical tools serve the business policies that security officers define at the corporate level? How can IAM projects shift from process automation to policy enforcement, and, thus, ensure compliance and effectiveness?

Reconciliation is an effective way to unite IAM projects and ensure security is enforced throughout your organization.

Making IAM work for you

All successful IAM projects have rational, practical business goals. These objectives drive business sponsors to accept a project, fund it and drive it through to completion.

› **Compliance goals:** many laws and regulations now require businesses to run within specific rules. Some of them are cross-industry laws, such as laws on the integrity of financial reporting (e.g. Sarbanes-Oxley). Others are activity-specific, such as pharmaceutical industry norms or healthcare privacy regulations (e.g. HIPAA). But most of them require controls to be put in place, and implementing an integrity, confidentiality or availability policy.

› **Cost reduction goals:** organizations streamline procedures due to a constant demand for cost reduction drives organizations to streamline procedures. IAM can be of great help in lowering the manpower required for recurring processes. In turn, the reduced overhead for common tasks makes more sophisticated strategies possible.

› **Business flexibility goals:** making employees productive wherever they are, and implementing business decisions rapidly. Nowadays IT is an enabler of business objectives since it allows you to deploy in a few hours a new business tool, accessible to users both inside and outside the organization.

The starting point: process automation

The main challenge to IAM today is not so much one of features as it is one of project goals, execution and integration.

Most individual IAM projects involve **process automation** in one form or another . Maintaining a security policy with policy tools, automating account administration with provisioning, managing passwords with single sign-on... All these projects focus on automating manual tasks.

IAM project domain	Typical IAM project	Main business driver	Main project sponsors
Roles	Policy definition tool Role mining	Compliance	Management Internal control
Identities	User provisioning Directory consolidation	IT simplification and cost reduction	IT department
Access	Pure single sign-on Strong authentication	Business flexibility and cost reduction	Users Security officer

Process automation is a vital necessity for most organizations. As information systems become more complex, the cost of manual habilitation grows exponentially.

› **Heterogeneity:** updating accounts manually in tens of different systems types requires planning and time. Often, administrators with the right skill set are not available to perform such relatively menial tasks. This is particularly critical for legacy systems.

› **Organization and process:**

when an employee changes jobs in an organization, how do you determine the systems in which he or she must have accounts? Manual processes are often based on word of mouth, and are badly documented. Moreover, when users leave years later accounts are not removed as nobody had documented their creation.

› **Historical policy evolution:**

many enterprises have grown through acquisition and have been reorganized... The IT department is expected to keep track of habilitation requests. "Archeological" work is needed to reconstitute coherent user profiles.

As a result, IAM projects that replace manual tasks with process automation usually have an excellent return on investment. But are they enough?

From process automation to strategic IAM policy

Individual "process automation" IAM projects are useful, but the real payback lies in making them work together. The reason is simple: many guidelines for building an effective IT security policy are similar to the guidelines for other types of policies. Auditors will verify the following three areas:

- › A set of controls must exist – for IT security, this is mainly the domain of *policy management*: who has access to what, and under what circumstances ?
- › These controls must be implemented, and one good way of doing so is to automate IT security policies through provisioning or workflow, thus lessening the impact of human error.
- › When implemented, these controls must be effective. Here, access management ensures that the right persons actually access the resources as defined in the previous phases. And this can be verified centrally at all times

However, getting all IAM elements to work together smoothly is often not simple:

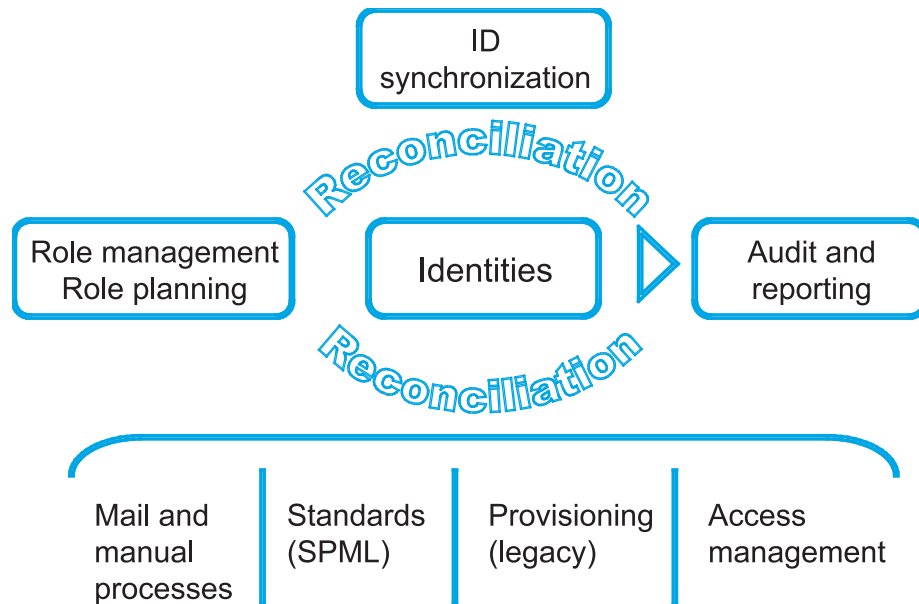
- › **Planning challenges:** projects can be kept waiting if features are not sufficiently modular. For instance, most SSO projects should not be delayed by provisioning projects.
- › **Technical challenges:** some modules are simply not meant to work together; sometimes heavy integration work is required.
- › **Human challenges:** different organizations sponsor – and manage – the different pieces of the IAM puzzle. When procedures have been formalized and audited, they should not change unnecessarily.

How then do you build an efficient IAM system, step by step, without losing sight of the overall goal? To meet these challenges, Evidian has successfully integrated the various elements of IAM using **reconciliation** processes.

Reconciliation: making sense of the IAM puzzle

To make a complete IAM system run smoothly, Evidian has found **reconciliation** to be the most efficient unifying concept. With incremental reconciliation, the whole IAM infrastructure remains manageable on a human scale. This also facilitates audit, as each step can be documented.

With reconciliation, each domain is managed by the best-skilled persons - for instance, identity directories by the HR department and application accounts by the IT department. Each organization agrees in advance on the range and boundaries of reconciliation, and how it affects its data.



Reconciling your identity sources

In many organizations, identity information is heterogeneous and partial: local directories, HR databases, phone systems, etc. How can you have a single, reliable identity repository? Evidian ID Synchronization reconciles the various identity sources, taking the most reliable elements in each. It builds and maintains a reliable user identity source - a prerequisite for most IAM projects.

Reconciling your policy with IT accounts

How do you ensure that the access rights for your resources reflect your security policy? Most applications are full of default accounts, shared accounts and otherwise ill-defined accesses. By reconciling your policy with your accounts, you will be able to document, explain or eliminate the discrepancies. Accounts are then modified either with Evidian User Provisioning, manually or otherwise.

Reconciling your policy with actual IT usage

Account reconciliation is only one side of the issue. How do you ensure that there are no orphaned accounts, or that employees actually use accounts created for them? Users accessing their colleagues' accounts can seriously damage an organization. Evidian **Access Management** monitors and controls access to critical resources. It helps you reconcile your policy with actual IT usage.

Evidian's reconciliation-based Role Management

Define and enforce your security policy easily

How can you design an effective application access policy and control its implementation? Evidian Role Management unifies the administration of your access rights while automating the authorization circuit.

How do you simply comply with new legal constraints?

You must formalize and, above all, enforce your access-right assignment procedures while monitoring their efficiency. Evidian Role Management is the control tower for your security policy.

› **A clear policy:** An employee's rights depend on his or her role, organization, location, etc. Thus, his or her access policy is brought into line with real tasks.

› **Easy maintenance:** All the components of a security policy are defined with a single tool. This simplifies procedure documentation and update.

› **Easy audits:** Audits are faster since they are performed from a single location. Your quality indicators are reliable and published regularly.

Your policy is written... but is it applied?

With Evidian Role Management, your policy is truly implemented. A workflow automates decision-making, from rights approval to account creation. Administrators can confirm whether or not an action has been performed.

The reconciliation function of Evidian's policy manager regularly and automatically checks your policy against field reality. This way, users and decision-makers naturally comply with your security policy.

How do you take existing rights into account?

Over the past years you have deployed different security policies. These policies cannot be disregarded, yet how do you know which rights still exist?

The policy manager module uses the Evidian's Access Management to design the security policy based on what users really access.

Reconciliation aligns IT usage with your IT policy

Evidian Role Management makes sure that your policy is enforced. It uses reconciliation to regularly compare your policy with application accounts and actual usage data.

› Reconcile your policy with existing user accounts

Evidian Role Management compares the accounts deduced from your policy with existing accounts. It can do this through Evidian User Provisioning or other provisioning solutions. Then, you may decide to update either your target application or your security policy in order to be as close to field reality as possible.

› Reconcile your policy with the enterprise SSO access repository

Administrators use actual access data to design and validate your model. You can detect which persons are using specific accounts. Your policy can be refined by analyzing the discrepancies.

Added values of Evidian Role Management



1. **Manage the full access-rights life cycle**

From the moment a worker arrives at a department until he or she leaves the company, Evidian Role Management manages his or her rights and the authorization circuits. Your users are immediately productive while respecting the security policy.

2. **Use reconciliation to base your policy design on field reality**

Evidian Role Management compares the status of the required rights with the reality of accesses made, and with the existing application accounts. This way, your policy is in line with the company's day-to-day activities

3. **Use reconciliation to enforce your security policy**

Decision-makers officially validate their actions and decisions with a few mouse clicks. The reconciliation function enables you to continuously enforce your policy. Audit is simple because it is centralized.



Evidian's IAM Suite 8 is a modular, integrated identity and access management solution. Its components help enterprises worldwide to manage identities, roles and accesses, including enterprise single sign-on. Modules can be deployed independently and provide full IAM functionality through comprehensive reconciliation processes.

Evidian, a subsidiary of Bull, is the European leader and one of the world's major players in Identity and Access Management (IAM). Its offering includes Identity and Role Management, Enterprise SSO, Mobile E-SSO and security for SOA and web environments.

Evidian products help organizations in the United States, Europe and Asia to improve their flexibility, enhance their security, achieve regulatory compliance and reduce costs.

Evidian has more than 1,500,000 users and 80 partners worldwide.

www.evidian.com

Evidian UK

5300 Lakeside
Cheadle Royal Business Park Cheadle
Cheshire SK8 3GP - United Kingdom
Tel: +44 (0)161 246 6909
Fax: +44 (0)161 246 6100

Evidian Iberia

Torre Agbar
Diagonal 211, planta 23
08018 Barcelona - Espana
Tel : +34 93 227 27 27
Fax : +34 93 227 27 28

Evidian SA: Headquarters

Rue Jean Jaurès BP 68
78340 Les Clayes-sous-Bois - France
Tel : +33 (0) 1 30 80 37 77
Fax : +33 (0) 1 30 80 37 10

Evidian GmbH

Theodor-Heuss-Str. 60-66
51149 Köln - Deutschland
Tel: +49(0)2203/305 1325

Evidian Systems Inc.

82 Wall Street, Suite #600
New York, NY 10005
United-States
Tel: +1 (646) 233-1239

Contact Evidian: info@evidian.com

© 2008 Evidian

The information contained in this document represents the view of Evidian on the issues discussed at the date of publication. Because Evidian must respond to changing market conditions, it should not be interpreted as a commitment on the part of Evidian, and Evidian cannot guarantee the accuracy of any information presented after the date of publication. This is for informational purposes only.

EVIDIAN MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. We acknowledge the rights of the proprietors of trademarks mentioned in this book.

EVIDIAN
A Groupe Bull Company