

ei Ecom Infotech Inc

Governance
Risk Compliance Solutions

Data Assurance
Governance Risk Compliance
COBIT , ISO 27001 , ITIL
IBM Tivoli
Identity and Access MGMNT
IT Infrastructure Managemant
Business Continuity and Resilience
Enterprise Security Managemant

Information Security
**Governance Risk
Compliance Solutions**

[Click here for more details >>](#)

[Corporate Training](#)

Holistic Approach to Your Security

Identity and Access Management for Compliance

The Sarbanes-Oxley Act of 2002 (SOX), mandates that organizations certify the accuracy of financial disclosure and accounting, is but one of a number of state and federal statutes that govern the uses of identity data. In addition the Health Insurance Portability and Accountability Act (HIPAA) sets parameters to protect the privacy of personal data in healthcare, and the Family Educational Right to Privacy Act (FERPA) does so in education. PCI DSS too mandates controlled access to credit card data . As a result of these regulations, more companies are developing strategies to link financial reporting functions with other processes and operations throughout their businesses. Identity Management solutions help ensure, monitor and audit compliance. Rather than functioning solely as a preventative measure, such as enterprise security tools including firewalls and anti-spamming software have traditionally functioned, They takes a more proactive approach, by and speeds up processes and makes them more efficient by acting as enablers to promote and facilitate secure access, inside and outside of organizations.

An end-to-end identity management solution is particularly applicable in the case of Sarbanes-Oxley (SOX), whose Section 404 calls for companies to set and enforce effective internal controls over business operations. The challenge of compliance is compounded by the vast array of external partners, customers and participants in the supply chain that are connected to the organization internally.

Further exacerbating the situation, SOX does not simply regulate the design and deployment of internal controls—it also calls for companies to show how the controls work. Specific to SOX, Identity Management Solutions have important features that are required by customers dealing with compliance initiatives: strong policy enforcement, automatic group management and centralized reporting. Identity management solutions addresses these issues and more by automating the enforcement of internal controls. In addition, it gathers data to audit transactions and show that the controls are indeed working. Identity Management solutions are use useful in other IT compliance areas like ITIL, ISO 27001/20000, COBIT and other frameworks.

Role Based Identity and Access Management (RBAC)

Business Roles in HR database, IT roles in Domain controllers and Application roles in Applications have been defined in isolation. Governance requirements or regulatory reporting needs require organization to build a comprehensive link across business, IT and application roles.

Building a Role Matrix

Role matrix gives a comprehensive view of entitlements across various applications, domain controllers and file systems for the roles defined in the HR database. Once the Role matrix is built, governance and can use this data to correlate with regulatory needs. Remediation process can be initiated as needed

Building Identity Matrix

Identity matrix has a comprehensive reporting of each user by HR data base name, application access with detail description of entitlements in each application at that point of time. Identity matrix reports the group association.

Our Solution

Our Solution has the ability to connect to different classes of network devices using its Framework. This framework allows to provide a unified web interface to the security and compliance administrators by connecting to different network devices in the back end. It can gather user names, entitlements across applications, HR database, File systems, domain controllers and reconcile users to build Role and Identity Matrix

Periodic Reports

The solution provides multiple modes of generating role and can be used for one time reporting, this process is quick with little or no installation time. To generate periodic reports Solution Framework can be enabled to interface with applications to automatically generate periodic reports.

Governance evaluation and remediation

Role matrix can be used to check against the corporate governance and compliance policies. Ground up Role matrix enables organizations to get a snap shot of current roles and respective entitlements in Once these roles are reviewed and certified, Solution Framework can be used to remediate or report violation based on user or groups.

Identity & Access Management-Components

In recent history—particularly within the past few years as companies have expanded their use of Internet-based distribution channels—the need for precise control over information access has increasingly been met by identity management solutions. Broadly defined as a set of technologies including password management, user management, access control, and user provisioning, identity management is not new. Security has been a concern for years in many enterprise applications. Many companies today are realizing significant benefits from identity management systems.

Identity and Access Management include:

- **Access control:** Authorization, the ability to manage access on different applications and platforms.
- **Authentication:** The process by which someone proves they are actually who they claim to be. Analysts recommend two-factor authentication with smart cards, biometrics or digital signatures.
- **Single sign-on :** The ability to sign on to a system once and then move through the company's networks without having to repeatedly re-authenticate. Also includes the ability to reset passwords without the assistance of the IT help desk. A typical user has on average five to ten different logins that they use on a regular basis. The single sign-on(SSO) product remembers and store those login details so that it can present these to the required application.
- **Identity Mananger** helps reduce security risk by governing how digital identities, groups and organizations are created, maintained and leveraged

throughout an organization. It does so by providing a simple, controlled means to change user, role, group and organization information that dynamically affects access privileges

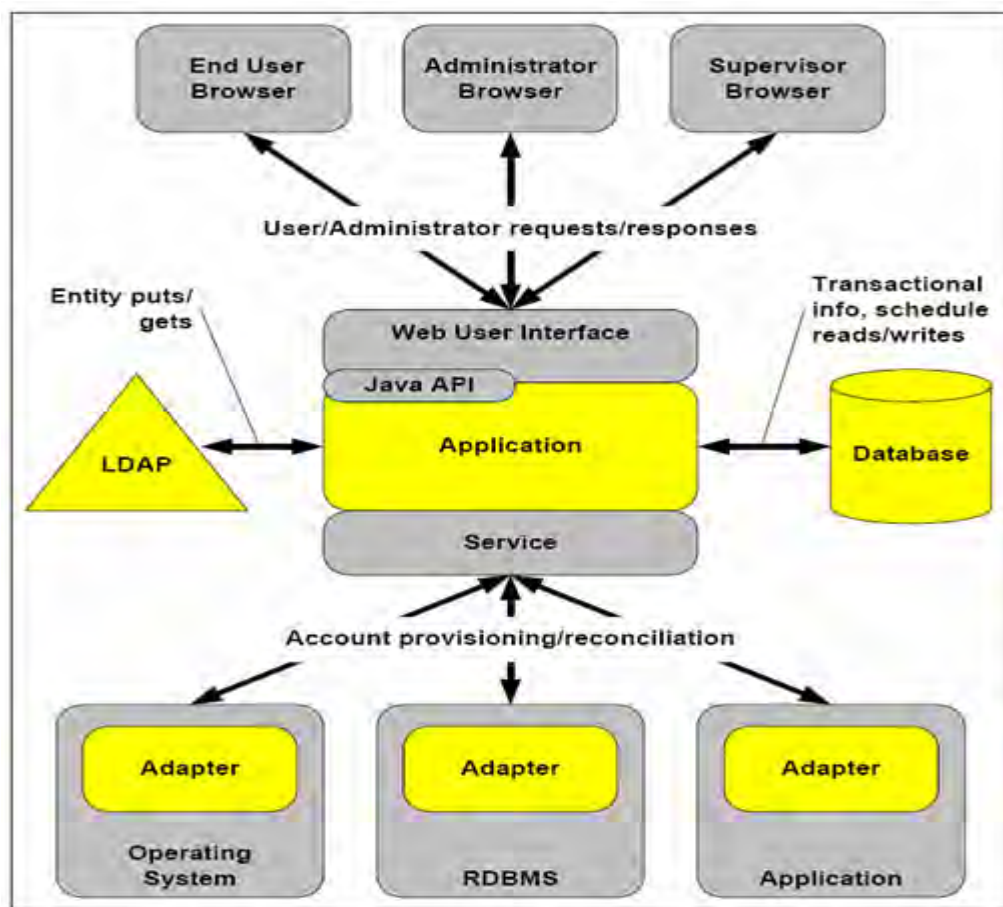
- **User Provisioning:** Granting access of specific applications and systems to employees. Includes creating user IDs and passwords and can include provisioning physical items such as cell phones, computers and key cards. User provisioning automates the tedious process of adding, updating and deleting users from multiple applications and directories. As roles, rules and policies evolve, the rights and attributes of users can change—and a workflow-controlled, automated provisioning process can significantly improve the efficiency of managing those changes.

- **Directory Services:** The storage area for user IDs and passwords. It offers one place for a company to view system access across the company. Directory Services provides a single centralized repository for user management, along with more advanced productivity-enhancing features such as dynamic groups, user self-registration and multi directory integration. Directories are implemented on the Databases. In addition Directories provides a consolidated LDAP view of directory information from multiple sources via a direct data link, whether the sources be other LDAP directories, databases, or Web services.

- **Federated identity management:** The ability to grant system access to parties outside the company's firewall, such as suppliers and outsourcing partners. Federated identity management provides a means to link internal employees to external portals, or external constituents to internal portals, without the burden of managing their identity and credential information in both places. This drastically reduces the costs and complexity of managing partners' users, and accelerates adoption of networked business portals.

- **Web access control and single sign-on.** Web access control improves security by managing who has access to what information and when. Single sign-on delivers dramatic cost savings by reducing time spent with thousands of users addressing password reset and update issues.

• **Web services management.** In an SOA, Web services expose business applications and information to the Internet for use by customers, business partners and employees. A robust, secure framework is critical for managing access control, monitoring and auditing of these services. Security in an SOA world can be complex, but it is also critical. Unfortunately, it's not realistic to expect the typical Web services developer to understand and implement all of the security functionality needed for a sound SOA implementation. Instead, SOA security needs to be part of a centralized, integrated offering that can be woven into Web services and applications by developers and easily reused. Achieving this goal requires that identity management functions be delivered as a set of standard Web services. These functions include: • **Authentication** , • **Authorization** • **Identity administration** • **Account provisioning** • **Auditing and reporting**



Contact us for more details

Ecom Infotech Inc

Call India +91 9869436685 US 1-312-224-1657

www.ecominfotech.biz <mailto:ac@ecominfotech.biz>