IDENTITY UPGRADE SAVES TIME AND REDUCES RISK

how upgrading from an overly-customized system increased efficiency and security for an enterprise-level financial company

CASE STUDY: IDENTITY & ACCESS MANAGEMENT

zirous®

zirous®

OVERVIEW

Legacy and end-of-life systems which have been heavily customized are still in use in many IT departments. Tools are customized so much that the base functionality is hardly put to use, making maintenance difficult and expensive. What useful upgrades is your business missing out on due to these scenarios?

In this case study of an enterprise-level financial company, you'll get an inside look at how their choice to upgrade to Oracle Identity Manager (OIM) 11gR2 PS3 - leaving behind their heavily customized older version - saves them dollars, hours, and headaches.

THE CHALLENGE

With over 15,000 employees and hundreds of billions of dollars under management, this financial company has a lot at stake when it comes to keeping processes efficient and information secure. An aging, unsupported system meant that failure could lead to risks such as wasted time and money, failure to meet auditing and compliance regulations, no centralized system for understanding which users have access to which applications, and more.

The financial company had utilized an older version of OIM since 2008 as their Identity Governance solution. The previous implementation was highly customized, ran on unsupported technologies, and underutilized the capabilities of the software. The solution also had little to no automation, did not provide capabilities required by the business, and was difficult for the business to use. Since the company was on such an old version, many new and improved pieces of functionality had been released that they were missing out on. These included important functions like integration with their Human Resources applications to automatically onboard and offboard workers, automated provisioning and deprovisioning to key target systems, role management, and certification of security access which would provide a high value to such a large company.

THE SOLUTION

In the Spring of 2015, Zirous' staff began a thorough gap analysis for the company in order to understand the current processes and gather the benefits of upgrading and utilizing OIM to its fullest extent. Zirous' business analysts are experienced in showcasing the business impact of an upgrade like this. Many times, IT departments are understandably busy maintaining the use of current systems and cannot take the appropriate time to understand that a new system can save on troubleshooting and maintenance hours.

Once the current state processes were understood and requirements were collected, benefits were realized, and implementation of OIM 11gR2 PS3 began in January of 2016. With Zirous' guidance, detailed phases for implementation were planned, and future state requirements were set.

Most importantly for the financial company, in the new version of OIM they could automate all provisioning and deprovisioning of Active Directory (AD), Exchange, and Office 365 (O365) accounts and group memberships. Complete integration with these key target systems allows for a reduction in planned staff hours to enter

QUICK FACTS

Company
- Enterprise-level financial company
- Over 15,000 employees

Technologies Involved
- Oracle Identity Manager (OIM) 11gR2 PS3
- Oracle SOA
- Oracle BI Publisher
- REST
- IBM MQ
- SOAP
- Apigee
- Oauth2
- Company Active Directory (AD)
- Company Exchange Account
- Company Office 365 Account (O365)
- Company Top Secret Mainframe
- 150+ Other Company Applications

HIGHLIGHTS

- Enterprise-level financial company had outdated, over-customized identity solution.

- A high risk for human error was present in a system with very little automation.

- Implemented OIM 11gR2 PS3, which integrated human resources systems, centralized identity governance processes for over 150 applications, and provided full automation for AD, Exchange, and Office 365.

zirous®

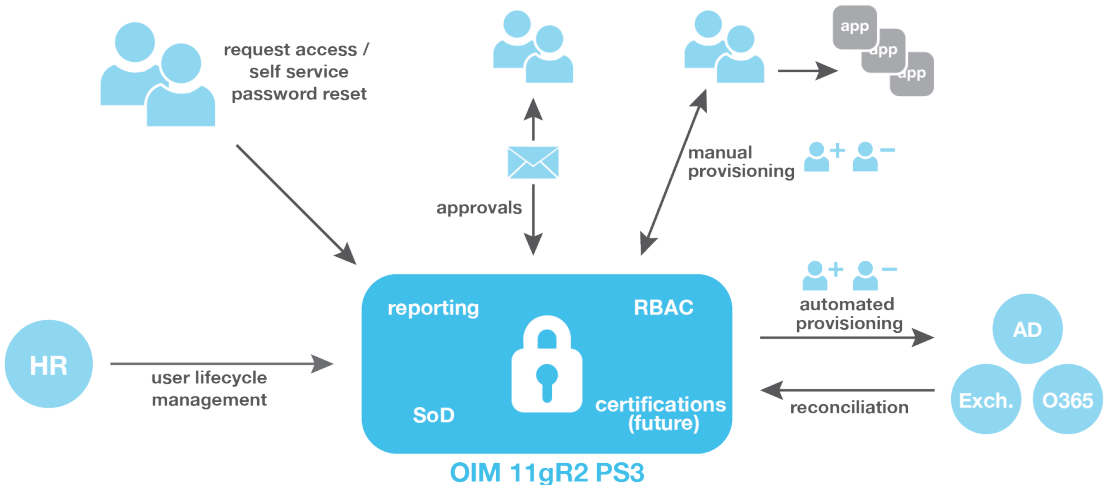
data into the system, freeing them up for other work. Additionally, this greatly increases quality of work, virtually eliminating the risk of human error.

Other important functionalities include:

User Lifecycle Management: Integration with Human Resources Systems. As employees are hired, terminated, or promoted, the HR systems talk directly with OIM, which, in turn, communicates to AD, Exchange, and O365 to automatically provision/deprovision basic access for that employee without any manual tasks. This is especially useful for employee termination; making sure that employee's access is revoked in a timely period greatly reduces the potential risk of a data breach.

Security Role Management: Role Based Access Control (RBAC). This financial company had spent many hours identifying more than a thousand roles within their company. In the future state with the new OIM system, the company will now be able to utilize the out-of-the-box functionality provided by OIM instead of having to maintain those roles with custom code. With thoughtful guidance and design from Zirous' experienced staff, the company's needs, as it relates to security role management, were met - without falling outside of the scope of the new tool.

Workflow: Approval and Fulfillment Workflow. The financial company will utilize OIM's capability to configure approval and fulfillment workflows specific to their business requirements. Approval workflow for this financial company is configured to gather Manager, Access Owner, and/or Account Owner approval under certain conditions, and will allow approvers to take action upon their tasks directly from a detailed email notification. OIM's fulfillment workflow allows this financial company to assign human workflow tasks to target system administrators where automation will not be implemented with the first release. Fulfillers will perform provisioning and/or deprovisioning in their target system and complete the human workflow task in OIM.



THE IMPACT

OIM is all about centralizing security access governance processes and has extensive capability to configure various components based on company-specific business needs. With the full integration between OIM and AD, Exchange, and O365 that the financial company now has, provisioning and deprovisioning triggered from OIM automatically happens in the key target systems.

Integration with AD will automate the tasks, previously handled manually, for hundreds of applications that use AD for their authorization mechanism. This financial company also integrated with Office 365 cloud applications. Finally, having manual fulfillment workflow for more than 150 applications that do not use AD for their authorization mechanism will allow this company to retire their heavily customized older version and centralize all security access governance processes within a single solution.