

NEW IDENTITY STRATEGY REFORMS COMPANY PROCESSES

how a Midwest utilities company revamped their identity and access management strategy to increase efficiency, reduce risks, and meet compliance

CASE STUDY: IDENTITY & ACCESS MANAGEMENT



OVERVIEW

A desire to truly change business processes led this Midwest utility company to reform their Identity and Access Management strategy and systems. With nearly 4,000 employees and over 1 million customers in Iowa and Wisconsin, it wouldn't be easy.

This case study will illustrate how Zirus helped this utilities company define the best project path, increase automation and efficiency, better control user access, and ensure compliance throughout their systems.

THE CHALLENGE

This utilities company was using old, inefficient systems. But, of even greater importance to them than simply bringing on a new system, was:

- Driving toward the best practice of “least privilege access”;
- Ensuring compliance with SOX and NERC regulations;
- Automating user lifecycle management, including onboarding and offboarding of employees, contractors, and vendors;
- Automating enterprise-critical business processes and application provisioning and deprovisioning;
- Reducing manual labor efforts and minimizing the likelihood for human error; and
- Automating access certifications, including following a job transfer.

In order to achieve this tall stack of goals, the company needed to replace failing, end-of-life-systems that managed user login ID generation, user access requests, and password management.

If these systems were to fail completely, the company could have faced some or all of the consequences associated with not having an Identity and Access Management program at all. Risks included time and money wasted on manual processes, failing to meet compliance regulations, greater risk for human error in user access control, and having no centralized control system to efficiently see and manage which users have access to which applications.

THE SOLUTION

In the Fall of 2013, Zirus collaborated with the utilities company to thoroughly understand current state identity governance business processes, define future state business requirements and business processes, diagnose barriers between the two, and define an implementation roadmap for their Identity and Access Management program.

Since 2014, Zirus has worked to implement automation of the company's enterprise-critical business processes and target systems, including:

- User Lifecycle Management for employees, vendors, and contractors (i.e. onboarding, off-boarding, and everything in between);
- Access Certifications, including both scheduled access certifications, to meet regulatory requirements, as well as job transfer certifications to ensure least privilege access;
- Approval Workflow;

QUICK FACTS

Company

- Midwest utilities company
- Nearly 4,000 employees
- Over 1 million customers

Technologies Involved

- Oracle Identity Manager (OIM) 11gR2 PS3
- Oracle SOA
- Oracle BI Publisher
- SOAP
- PowerShell
- PL/SQL
- Company Active Directory (AD)
- Company PeopleSoft (HR, EPM, Financials, Portal)
- Company RSA
- Company Oracle Databases
- 50+ Other Company Applications

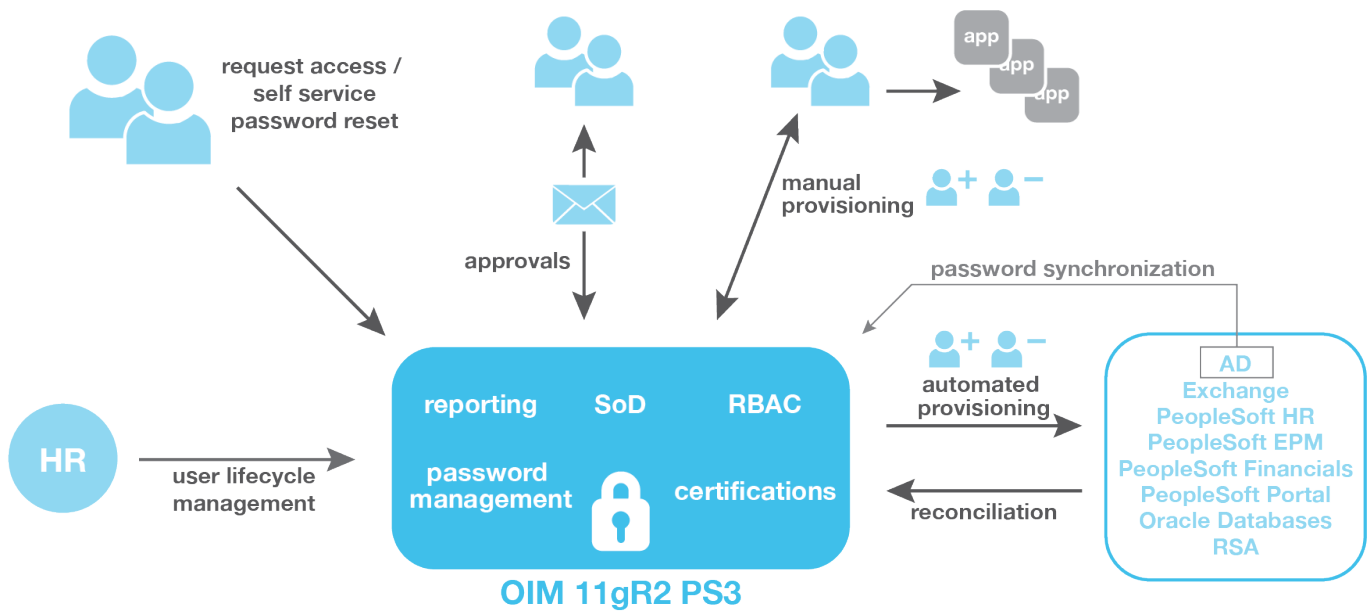
HIGHLIGHTS

- The company recognized the need to update their identity strategy to avoid system failure risks.
- They also determined they wanted to start from the ground up with a new and improved strategy.
- Zirus and this company have revamped their identity strategy throughout several stages.
- The utility company has increased efficiency, reduced risk, and can more easily follow regulatory requirements.



- Meet regulatory requirements for deprovisioning NERC access;
- Automated reconciliation from all enterprise applications, into OIM; and
- Automated provisioning and deprovisioning for:
 - Active Directory,
 - Exchange,
 - PeopleSoft (HR, Financials, EPM, Portal),
 - RSA, and
 - Oracle Databases.

Zirous continues to work with the utilities company on an ongoing basis to refine and enhance their Identity and Access Management posture.



THE IMPACT

Zirous implemented an identity governance solution that allows for the integration and centralization of security access for all enterprise applications. This results in compliance with SOX and NERC regulations, and automates the company's enterprise-critical business processes and target systems. With the full integration between OIM and several key target systems, provisioning and deprovisioning triggered from OIM automatically happens with no human intervention required.

The company has been able to retire their legacy identity governance platform and centralize all security access governance processes within a single solution. Their solution has increased efficiency, handled regulatory compliance concerns, reduced risks, saved money, and ultimately, achieved their goals of reforming their Identity and Access Management strategy, while remaining agile for future improvements.