



# **SUN IdM: Migrate with Confidence**

**SDG IAG Practice: Global Technology Solutions**



[ technology + passion ] - risk

## Overview

There are many reasons why organizations are migrating away from their current Oracle Waveset (OW) identity management solution to a newer next gen Identity and Access Governance (IAG) platform. Perhaps their vendors were acquired, changing the roadmap. Or maybe the current solution is no longer a perfect fit. Some companies realize that a lot of money has been spent for little value. Others find that their solution does not suit the new requirements of managing risk and security related to identity and access governance.

## WHY? Reasons to Migrate

### Four end-of-life pressures:

- **Vendor** — Product and support is reaching end of life for Identity and Access Management (IAM) products
- **Natural** — Project has completed its life cycle
- **Technical Architecture** — Supporting middleware (databases and application servers) in need of upgrades
- **Service** — Currently offered services insufficient to meet business needs

### End of life considerations

- Your current vendor may not be your future vendor
- Any future supplier may not be a vendor at all, but instead a service/system integrator.
- End of life of current Identity Management (IDM) deployment is an opportunity to reconsider the deployment order of future IAM components.

## Challenges

Migration of existing IDM solutions is not as easy as some vendors claim. That's because identity management implementations usually are not "plain vanilla" out-of-the-box solutions. There is no such thing as a "miracle migration toolset."

More importantly, moving from one identity manager to another is not necessarily the best choice. The IAM landscape has evolved over the last few years resulting in blurred differences between user administration, provisioning and IAG solutions. Vendors have matured their offerings in view of practical business issues, regulatory compliance, risk and security and the challenges of having both identity and access governance (IAG) as a single solution. Other factors include:

- *Changing technology and business requirements since the early provisioning-focused solution.*
- *Historically, identity and access management implementations are built by, and for, IT. So, they are typically IT-oriented. And because they are more suited for technical IT users, they are not so user-friendly. This challenge is typically compounded by lack of full integration of identity management and access governance management functions under a single, unified, business-oriented console.*
- *Enterprises today are looking at operational efficiency, cost reduction and enhanced security. But the truth is that in today's scenario, failure to address provisioning as both a business and technology issue is profoundly limiting.*



## Key Considerations

No matter what solution you choose, replacing legacy OW requires effort and investment. Pick the right solution and you can achieve results that move your organization forward to a next gen IAG platform for the future.

For most organizations, making the decision to migrate from Sun Identity Manager (Oracle Waveset) to the next gen IAG platform comes about after a long process of evaluating a multitude of options for identity and access management (IAM). Yet while the decision marks the end of the selection process, it's just the first step in the actual migration. Organizations must consider the following:

- **Deployment/migration strategy**

- Business continuity
- Zero impact on “business as usual” tasks
- Maintaining the pace/synergy with adopted migration plan/strategy

- **Unified user interfaces: improved user experience**

- Access requests
- Approvals
- Password change/reset/synchronization

- **Identity Synchronization**

- Real-time (with no lag or minimal lag time)
- Synchronization of identities across the managed targets

- **Provisioning/de-provisioning**

- Seamless integration of target systems

- **Identity administration**

- Unambiguous on-boarding, off-boarding, job change/transfer

- **Identity analytics and intelligence**

- Event driven access reviews and certification
- Near real-time closed loop remediation



## Migration Approach

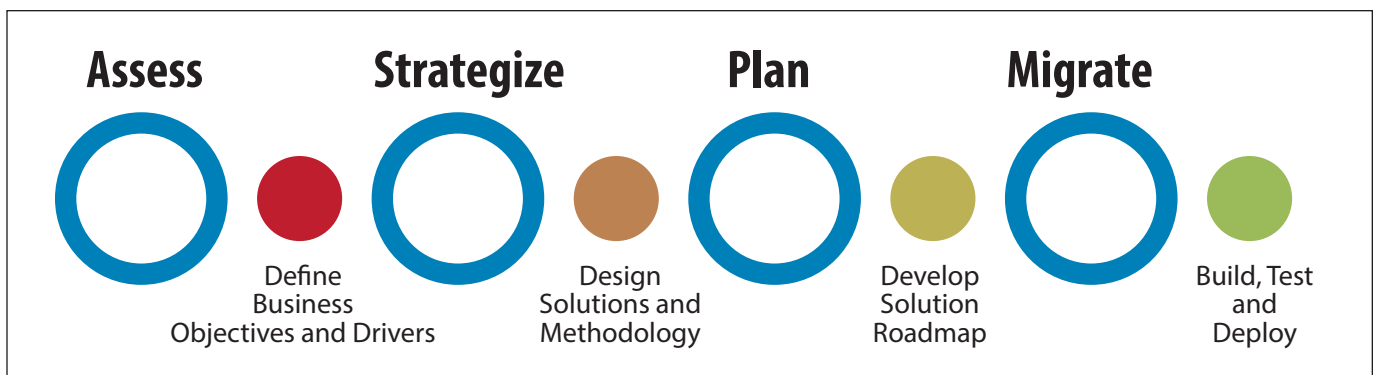
### Choosing your approach: migration by objects or business use cases

In an ideal world, migrating from OW to next gen IAG would be a simple matter. You would identify objects and processes (users, resources, policies, and so forth) directly from the former to the latter. This bottom-up approach would

*Replicating the legacy solution as-it-is may not be the ideal and real objectives of the migration.*

be fine if all objects were mapped perfectly to each other from one solution to the other. But they are not, for obvious reasons. Replicating the legacy solution as-it-is may not be the ideal and real objectives of the migration.

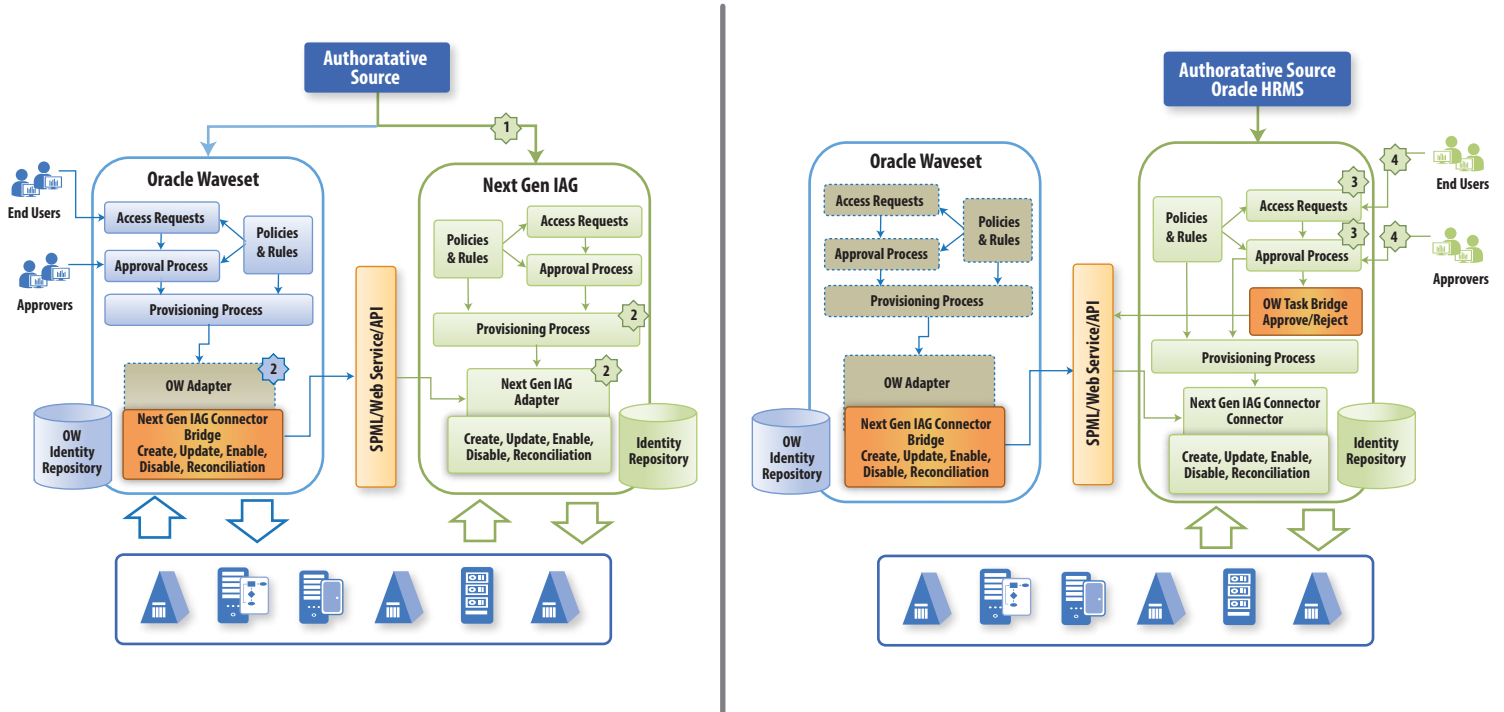
So if migration by objects isn't the answer, what is? One possible solution is migration by business use cases. This is a top-down approach in which the next gen IAG objects are defined based on current and anticipated business requirements rather than on legacy objects. However, there is always the risk of overlooking some functional detail or existing object in OW that would be useful or critical to have in next gen IAG.



### Determining the methodology: big bang vs. incremental

In any implementation or migration of an infrastructure application, the basic question is whether to move everything over to the new implementation in one “big bang,” or take a more gradual approach in which the new solution is brought up in phases. In most cases, the “big bang” approach is generally not appropriate for an OW to next gen IAG migration. This approach is more suitable for simple, first-time IAG implementations, where there are few or no major issues associated with changing from one system to another. There are risks to consider in complex implementations. For example, if next gen IAG is not tested and released in a phased manner, there is a greater chance of disrupting operations when the cutover takes place.

## Co-existence: An Incremental Approach



The best approach may be integrated deployment in which OW and next gen IAG coexist, with OW continuing to handle user-facing front-end workflows (such as access requests and approvals) while you gradually move back office workflows (such as provisioning and de-provisioning) to next gen IAG. After all the back office operations are migrated to next gen IAG, you can move forward with migrating front end workflows to next gen IAG. This self-paced migration methodology will enable you to gradually phase out the OW infrastructure and minimize any business risk associated with the change.

## Maximizing efficiency: do you need acceleration tools?

If you choose a phased approach to migration, it can be helpful to employ “accelerators”—tools designed to support a gradual transition. These tools facilitate the process of using both the legacy OW and the new next gen IAG capabilities at the same time.

There are a number of tools available for this purpose including those which enable OW provisioning workflows to use next gen IAG connectors to provision accounts on next gen IAG managed target systems. Others make it possible to work on legacy OW tasks from the next gen IAG user interface.

Fact is, there is no “one-size-fits-all” solution. Standardized tools such as those described here can be used to help decrease overall migration effort and investment.

## About SDG

SDG is a leading provider of technology, consulting and risk management solutions to strengthen enterprise businesses while managing IT risk. We focus on six practices: Risk and Security; Identity and Access Governance; Digital Collaboration; Quality Assurance; Mobility; Cloud and CRM.

*“SDG helps enterprises realize their dreams by helping them develop, manage and deploy solutions with acceptable risk.”*

For over two decades, SDG has enabled enterprises to realize their dreams by helping them develop, manage and deploy solutions with acceptable risk. We combine technology, thought leadership and a relentless passion for customer success. SDG partners with enterprise brands, but we specifically focus on mitigating client IT risk. Our ultimate goal is to help enterprises realize the opportunity of technology, increase innovation, improve speed-to-market and maximize returns on investment.

