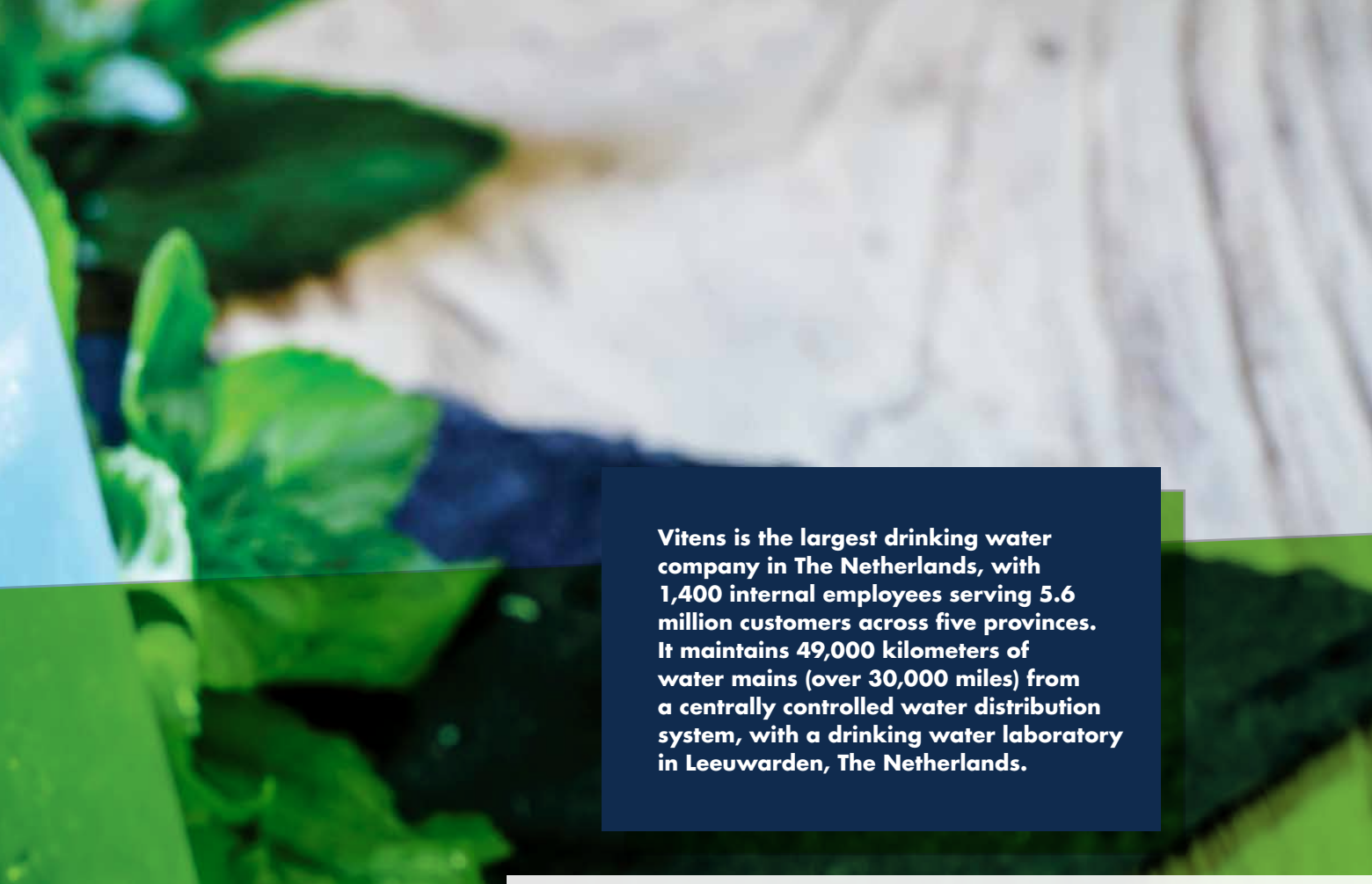
This article appears here with permission from the *SAPinsider*. Copyright © 2020 WIS Publishing. All rights reserved.



Drinking Water Company **Vitens** Connects **HR** and **GRC** Business Roles to Achieve an **80% Automated Provisioning Rate**



Vitens is the largest drinking water company in The Netherlands, with 1,400 internal employees serving 5.6 million customers across five provinces. It maintains 49,000 kilometers of water mains (over 30,000 miles) from a centrally controlled water distribution system, with a drinking water laboratory in Leeuwarden, The Netherlands.

by **Craig Himmelberger**, Contributing Writer

Among the 65+ presentations at the November 2019 SAPinsider conference in Barcelona, Spain, was a case study presentation by Tinette Beuving of Vitens and Virgil Verloop of Profilus that outlined their successful project to better automate the provisioning of application roles in both SAP and (later) in non-SAP systems. SAP customers that are eager to streamline their onboarding and provisioning processes can learn a lot from the experience and success at Vitens.

This article recaps that presentation and adds insight from a follow-up interview with Tinette and Virgil about how Vitens automated and expedited its onboarding and provisioning process — and how the company now provides its employees with an improved and streamlined experience. It contains project plan tips and lessons learned that can save readers significant time and effort in their own projects.

Customers Are Seeking Ways to Achieve Harmonized and Automated Identity and Access Management

Heterogenous system landscapes present multiple identity and access provisioning challenges. Effective risk

assessments in addition to auditing all access and prohibitions are critical responsibilities of the teams in charge of those landscapes. Without a holistic, automated approach, the effort tends to be expensive, time-consuming, and burdensome on business users for whom those systems are intended to serve — not to mention the IT staff members who support them. Worse, failure to provision and monitor correctly can have expensive consequences; the Association of Certified Fraud Examiners estimates that organizations lose 5% of their revenue to fraud, with more than 80% of that total committed by company employees in accounting, operations, sales, purchasing, and customer services roles — the typical users in a broad-line SAP solution landscape. Add additional systems from multiple vendors to the mix, and the resulting complexity becomes even more daunting.

Vitens has pushed forward with innovative technology available in SAP software to enable achievement of remarkable results — pulling together the potential in its human resources (HR), governance, risk, and compliance (GRC), and Lightweight Directory Access Protocol (LDAP) portal foundations, and automating an impressive 80% of its current access provisioning process.

Tinette Beuving cautions that this 80% achievement in SAP systems can be misleading and will likely decline slightly due to anticipated complexity to be added through supplemental non-SAP systems planned for integration into the architecture, and the need to manually review system licensing cost impacts before granting access to those systems. "These approvals will be expedited via SAP Fiori interfaces for access-request exceptions and made part of automated workflows, but the added approval steps will reduce the percentage of access provisions that can be fully automated," says Beuving. "Even so, we expect to maintain a 60% to 70% automation rate even through the addition of these new non-SAP created role definitions." Vitens' plan is to assess a prototype application to streamline the additional 20% to 30% of requests that will need to be handled manually and evaluate from there.

Vitens' System Landscape and Technology Foundation

Vitens' case study contains valuable detail on the company's system landscape and technology foundation.



Figure 1 shows the framework of Vitens landscape, and **Figure 2** shows the roadmap and project timeline, as discussed in the case study. A quick summary from the presentation material includes:

- In 2016, Vitens completed a project entitled "Implementation Authorization Policies (IAM)" that fully redesigned authorization roles and procedures. To aid in the effort, the business leveraged automation from a third-party solution for risk analysis.
- From November of 2017 to December of 2018, Vitens automated its authorization processes with SAP GRC solutions, utilizing the full integration of the suite, including risk analysis, firefighter, access request management, and business role management.
- In 2019, Vitens continued its IAM project to expand the solution to the non-SAP landscape, in addition to a complete reimplementation of its core systems to SAP S/4HANA: SAP GRC solutions connect to Microsoft Active Directory and legacy systems, update procedures, and de-provision the current Microsoft IAM system, while redesigning and cleaning up user roles; SAP S/4HANA redesign includes a complete redesign of the Vitens SAP landscape, and transfers current SAP systems to the SAP S/4HANA, SAP SuccessFactors, and SAP C/4HANA solutions.

Essential to the success of Vitens' automated provisioning project are the building-block components found in its SAP ERP Human Capital Management (SAP ERP HCM) and SAP GRC solutions, as well as the complementary solutions from Microsoft. But first, the organization had to come to a consensus on how to leverage the identity and access components of its internal Microsoft and SAP investments and make the right choices on how to best utilize each. Critical to the success of the project is the cooperation of the entire organization.

Beuving relates, "Most important is that we started with the commitment of the team manager



Figure 1 Framework of Vitens's system landscape and technology foundation

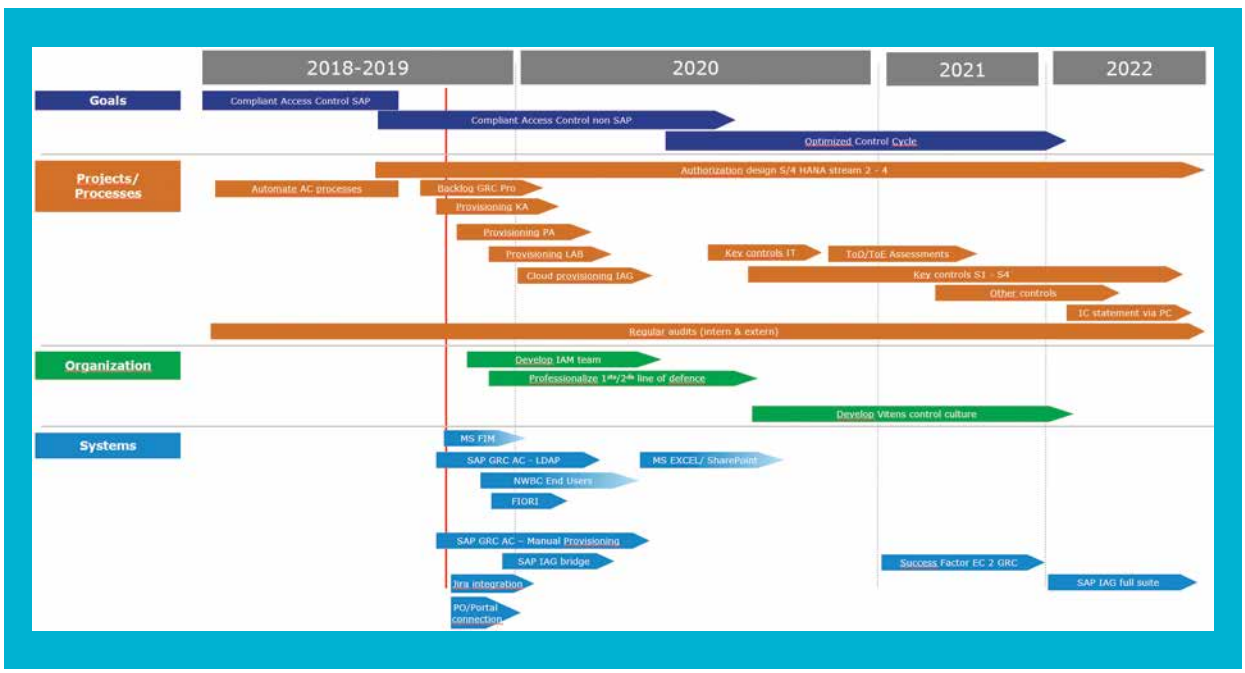
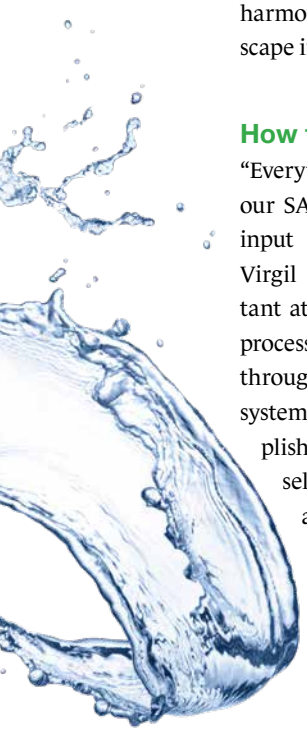


Figure 2 Vitens' GRC and identity access management roadmap and project timeline

"Everything flows from the personnel record in our SAP ERP HCM system, and from the initial input from the corresponding manager."

— **Tinette Beuving**, Senior Functional Application Consultant, Vitens

to let us do this." As many readers will recognize, and Beuving observes at Vitens, it is extremely common for team members to both recognize and trust in the specific strengths of the applications they work with, and they will not be shy to advocate for their inclusion in each new project scope — as they should! Beuving is clear that starting with a strong management commitment, and gaining the consensus of the full team, was essential to the success of a very large project that harmonized a broad and complex system landscape into a single access and control architecture.



How the Project Was Built

"Everything flows from the personnel record in our SAP ERP HCM system, and from the initial input from the corresponding manager," says Virgil Verloop, SAP Security and GRC Consultant at Profilus. "We have formal internal joiner process and leaver process flows that are initiated through an interactive PDF form built on our HR system data." Master data updates are also accomplished in a similar fashion. These flows are all self-service for the business user/managers, and easy to use; however, Verloop says, "The trick is mapping business roles to the HR function codes and using the Location attribute to carry the specific roles we will be using in the business systems." He also stresses the essential importance of consistent mapping across all systems to be automated. He says, "Data maps are never consistent across application systems, and our project to map and harmonize them in a single view was essential to the automation level we have achieved." In addition to fully automated provisioning via SAP GRC, there are still some manual steps, such as the associated license codes in the user master record. These can be further automated in the target systems using the role based classification feature in the SAP standard license management application.

The SAP GRC and Microsoft Components

Vitens' new landscape leverages Microsoft Active Directory Domain Services to bridge between the access system of record (SAP Access Control) and other non-SAP applications. The case study presentation details examples from the project, and itemizes the job role functions, and group access requirements, that are conveyed as part of the provisioning process. Also included is a handy mapping example that follows how name information needs to be mapped, translated, and carried from SAP ERP HCM, to SAP GRC, and fully through to their LDAP process. "We are planning to maintain these mappings as we upgrade the various components of our system," says Verloop. "On our roadmap timeline [refer to Figure 2], for example, you can see how we are planning to accommodate our implementation of SAP SuccessFactors solutions and take time in 2021 to update the mapping from our current SAP ERP HCM system."

Vitens' Microsoft Active Directory account creation is thus able to carry through automatically from the HR record created in the joiner, leaver, and master data update processes. The access request/update/termination process automatically maintains the corresponding user record in the GRC system. This record is then sync'd via LDAP from the GRC system, and directly provisioned in the target system. The only manual step necessary across the entire process, is the manager interaction with the PDF form (except as noted for non-SAP system license cost evaluation workflows).

Specific to the LDAP protocols being leveraged by Vitens, Verloop says the company is committed to hardening its security by enforcing the use of Secure LDAP (LDAPS), which is based on the Secure Sockets Layer (SSL) protocol. Because the LDAP connector in SAP GRC does not implement that LDAP protocol itself, but uses the LDAP client library of the operating system, Vitens is choosing a three-part architecture that sets up a dedicated Windows host between the instance host and the directory server host, so that extra LDAP software does not burden their directory server host. The case study presentation shows the other LDAP deployment options that execute



> "It's been suggested that up to 70% of SAP's current development efforts are already dedicated to cloud systems."
>
> — **Virgil Verloop**, SAP Security and GRC Consultant, Profilus

the LDAP protocol, either on the instance host or on the directory server host, and many more system details.

Building for the Future

Vitens' 80% automation of provisioning requests was recently fully enabled by the delivery of new SAP S/4HANA technology. However, new technology also renews the challenge to achieve useful mappings of user data, system parameters, and transport protocols across a company's full system landscape. Verloop cautions that additional project phases need to be anticipated, and, in fact, built into the initial plan so that future system enhancements do not break the previously achieved automation rates. "We already know that we will be moving to SAP SuccessFactors solutions from our present SAP ERP HCM platform in 2021," he says. "The HR role data and mappings in SAP GRC will need to be evaluated and managed so that the value we are achieving now can be preserved in the future."

Improved future technology also comes with benefits: "We expect SAP Cloud Identity Access Governance will be sufficiently mature in 2022 to commit to moving to it in that timeframe, though SAP Customer Identity and Access Management may still remain out of our scope until later." Verloop anticipates good functional value from the upgrade, and he says, "It's been suggested that up to 70% of SAP's current development efforts are already dedicated to cloud systems — we are looking forward to evaluating cloud-based access governance to streamline our architecture."



Advice for SAPinsiders

SAP, Microsoft, and others have promised the potential of leveraging HR job roles for automated application provisioning. In practice, this is more challenging than it sounds. Not every organization has a stable and solid HR organizational structure and can therefore leverage the position-based access control approach. Finding ways to harmonize company processes into consistent flows suitable for automation is one step. Mapping and translating various application architectures across heterogenous solution landscapes is also critically important. Managing the necessary transports, protocols, and system functions to accomplish all this without manual intervention is also an essential component of any successful project.

Vitens has created a useful example of how identity and access provisioning possibilities can be turned into practice with impressive automation rates. Below are some key elements of the case study, which are valuable learnings for other customers considering a similar undertaking:

- **Achieve commitment and clear direction from senior management**: Vitens' experience shows the importance of executive commitment to team consensus on selecting and coordinating components of a harmonized solution. It's also critical to fully leveraging the experience, technology proficiency, and business perspectives of all team members.
- **Start by building a foundation of harmonized employee role data, authorization policies, and system access procedures**: Vitens' ultimate project success was enabled by consistency across data and process components, without which its automation achievements would not have been possible.
- **Determine the specific systems of record for all data and procedures, and map required data and system attributes across the entire landscape**: Vitens found it necessary to adapt certain data records to carry attributes through landscape elements lacking those necessary control elements.
- **Include future project timeline phases to accommodate known system upgrades and additions**: Vitens' anticipates cutting over its SAP ERP HCM foundation to SAP SuccessFactors solutions, and the consequent changes to employee role tables and data, as well as planned adoption of maturing SAP technology like SAP Cloud Identity Access Governance. ■