

Towards continuous monitoring of segregation of duties

30 januari 2018

Tobias Houwert

As a Global IT audit manager at Arcadis¹ I have been involved in the development of a new approach to audit our processes that are supported by a Global Oracle solution. We have implemented Oracle Sales Cloud to perform customer relationship management, eBS to manage our projects and financials and Oracle HCM to support Human Resources Management.

In the IT-Auditor, No. 2, 2017, the subject of Segregation of Duties in eBS was introduced by J. van Bruchem and R.P. de Goede. [BRUC17] These authors focused on a specific aspect of segregation of duties in Oracle eBS.

Purpose of this article

This article focuses on the wider aspect of segregation of duties (SOD) in Oracle eBS and how internal auditors can start auditing the SOD concept. I will also explore the need to work closely with the business and the Risk Management function to get their buy-in. I aim to explain the process we went through during the implementation of new processes and IT systems and the challenges our Internal Audit department faced when we started to audit the global processes in Oracle.

This article also provides some practical examples of how an organization can start to work with system-based reviews, implementing SOD models and transaction control monitoring as part of a wider control framework to cover the risks in processes.

In this article, I explain the use of one specific Oracle Product, the Governance Risk and Control tool (GRC). This application is used to connect to our Oracle eBS private cloud and will soon be replaced by a public cloud solution. Oracle is developing a public cloud solution (ERP Cloud) and we need to wait until we know how the GRC solutions will evolve. We hope that the concepts we have implemented as explained in this article, will still be valid and easy to implement in the next generation of Oracle.

Our history and Dutch heritage

Dutch people may remember the old firm Heidemij from which Arcadis originated.

Arcadis has a long and rich history, its roots tracing back to the Association for Wasteland Redevelopment in the Netherlands in 1888, whilst Hyder Consulting, which Arcadis acquired in 2014, can trace its history back to 1739. From our strong heritage, we have grown organically and through acquisition to be the leading Design & Consultancy firm for natural and built assets. See Arcadis – Our History for details.

Over the last ten years, Arcadis has grown through acquisitions and organically in many different parts of the world. These acquisitions also opened new markets through different service offerings expanding our existing portfolio of services. A need was felt to create synergies and a single common IT landscape to support our global service offerings. An additional benefit was a reduction in overhead and operational costs. Our company also embarked on a strategy of outsourcing IT to the cloud. We outsource those IT services when the market can deliver the service better than we can internally, IT not being one of our core competencies. In our recently introduced three-year strategy we identified digital as one of our pillars to build on. We provide the engineering and consultancy content and we work together with IT suppliers to provide the enabling tools and platforms.

The companies we acquired over time (see text box 'Our history and Dutch heritage') were integrated but not on one common IT platform. They were operated for long, developing / maturing their own best practices and managing their business.

In 2014, we started on a journey dubbed 'The Arcadis Way' (AW) that, by 2020, should result in the embedding of standard processes across our business with little room for deviations from this blueprint. Other goals of this single standard set of processes are to create more transparency in our financials, improving client focus and more collaboration across regions. Although this tool does not capture the product that we deliver to our clients, like designs and consultancy services, it does support our delivery to the client.

Internal audit and Arcadis Way

The change in the organization also meant that we as Internal Audit (IA) had to adjust our audit approach. We had limited experience in our Internal Audit team with Oracle and we had to learn fast and step up our effort to keep ahead of the game.

The implementation of Oracle is a significant investment for our company and IA started to follow the implementation to see if risks were identified and addressed, controls were developed and the project could deliver on its promise. We discovered that the Global Implementation team was focused on getting the application implemented as per the schedule, rather than on implementing controls. After go-live, Risk Management was tasked to revise the existing control framework to ensure alignment with the new ways of working and Oracle.

Soon the organization realized that the roll-out was more complex than anticipated. As an organization we needed to develop all our processes, a blend of best practices, that would fit all our service delivery teams across the group. It involved the configuration of an IT system that could support the processes and a change management process to facilitate the embedding and change in behaviour.

As risk management in our organization was still on its path to maturity, IA and Risk Management started to collaborate to get a good control framework in place based on a risk assessment of the new processes.

The Global team will ensure, by design, controls are implemented in the processes to enable the business to execute these controls as part of their daily operations. After implementation, IA and External Audit will be in a better position to perform their required system-based audit activities, being able to do so more effectively and efficiently.

The implementation of the AW resulted in a change in the control philosophy; from predominantly principle based to more rule based. All operations will take place in a common way, supported by one ERP. Our organization wants to be lean at the top and not strive for bureaucracy and the creation of overhead devoted to monitor controls. For that reason, we advised the business to analyse controls in the processes and IT systems so as to identify essential controls, which could then be automated where possible. Automated controls would prevent users from performing irregular activities in the application. Also, the correctness of settings can be monitored centrally throughout the year.

Taking those steps appeared to be a challenge for the organization. Our presence in different regions of the world also means that we have different levels of knowledge in using ERP-systems and the way we perform audits. In some part of our organization we relied on spreadsheet-based applications. The local business was used to having their own local IT systems, processes and key controls were described at a high level. In some parts of our organization the external auditor would use a substantive audit approach instead of a controls-based approach for efficiency reasons or because it was not effective to rely on the IT General controls.

Figure 1 describes the type of controls we expected in the new environment and the way in which assurance would be obtained.

eBS | Overview eBS environment









		Assurance obtained through:
Manual (mitigating) Controls		Execution of control by process owner . Risk Management is responsible for providing guidance on controls to be implemented. Testing of controls annually through management testing Regional Risk management.
Application Controls		Execution of control by Oracle system . Testing of controls annually by External auditor reviewing application configuration settings. Future tooling licenses have been bought by Arcadis. Pre-requirement is that IT General controls are effective (Change management).
Workflows		Execution of control by Oracle system and configured by Accenture based on the blueprint BP322 . Testing of controls annually by Internal Audit (IA) looking at workflow settings BP322. Pre-requirement is that IT General controls are effective (Change management).
Transactions		Execution of control by end users . Testing of controls annually by IA reviewing specific pre defined Transactions using ETCG tooling. Review focused users with SOD conflicts.
SOD all users		Execution: the business and GBAS are responsible that appropriate approval is obtained in the user provisioning process. IA and Regional Risk Management will perform semi-annual and quarterly reviews. The external auditor will review annually the work done by IA and Regional Risk Management .
Reports BI (IT Dep manual) controls		Execution: the BICC team is responsible to ensure the BI reports are complete and correct. Key BI reports will be tested by External auditor first in 2017 that are relevant to the financial audit.
Configuration Controls		Execution: Accenture is responsible to configure controls during the built of each Oracle environment based on the Blueprint BP322 . BPO's and BPM's are responsible to approve the configuration that is first led by the BBP team. Key configuration settings, relevant to the financial audit, will be reviewed by External auditor on an annual basis.
System settings		Execution: Accenture is responsible to configure controls during the built of each Oracle environment. BPO's and BPM's are responsible to approve the configuration that is first led by the BBP team. Key system settings, relevant to the financial audit, will be reviewed by External auditor on an annual basis.

Figure 1: Type of controls and assurance to be obtained

IA started small to identify where opportunities would arise to use a more system-based approach, adopt data analytics for our analysis and help the business through operational audits to reduce the administrative burden and create insights based on information that was at hand.

Access in Oracle

In our environment access is granted based on AW roles, which are translated into responsibilities that eventually will give users access opening menus to enter a transaction into the system (e.g. entering supplier invoice into Accounts Payable or updating supplier master data). Figure 2 visualizes the access in Oracle eBS private cloud.

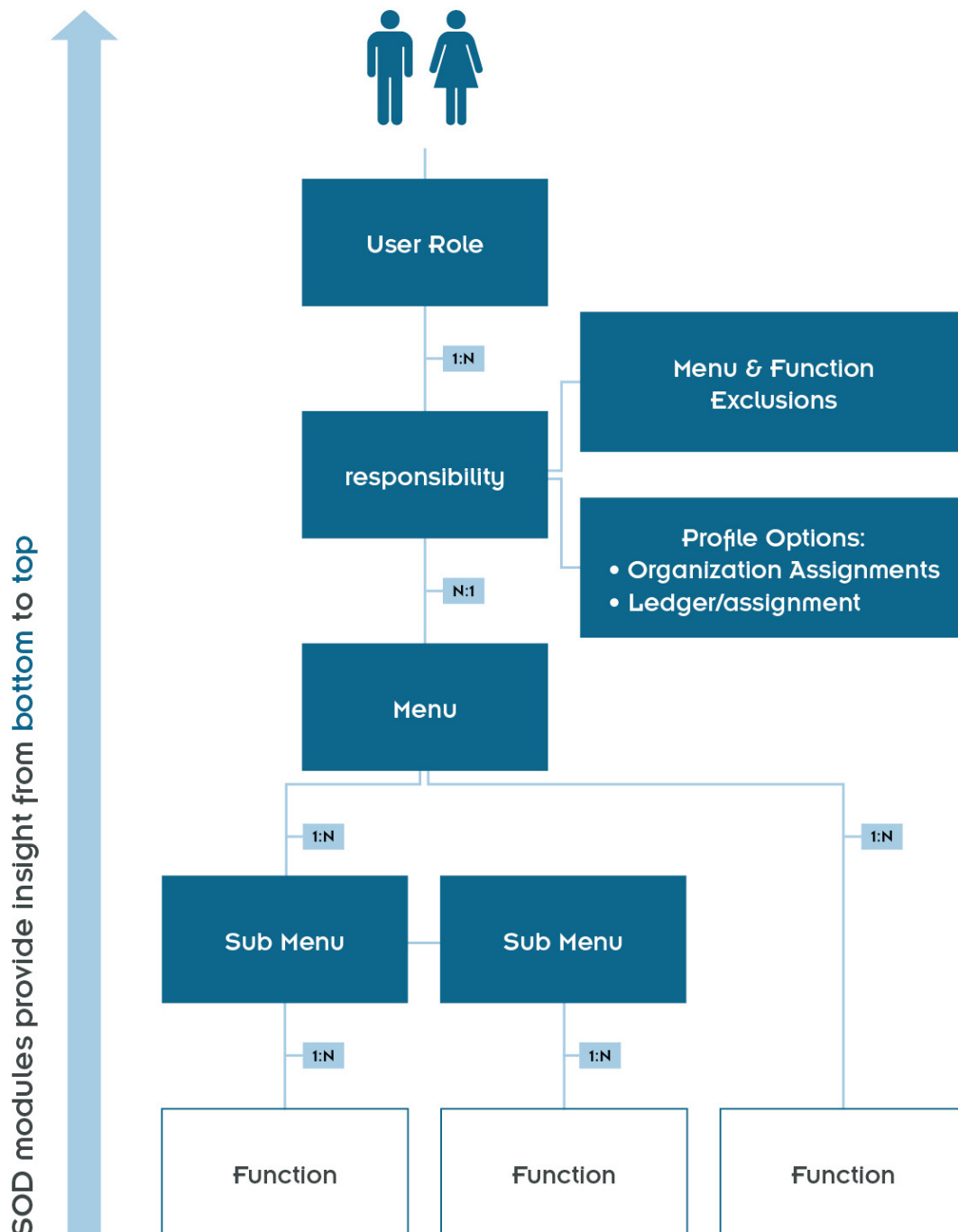


Figure 2: Access model Oracle eBS

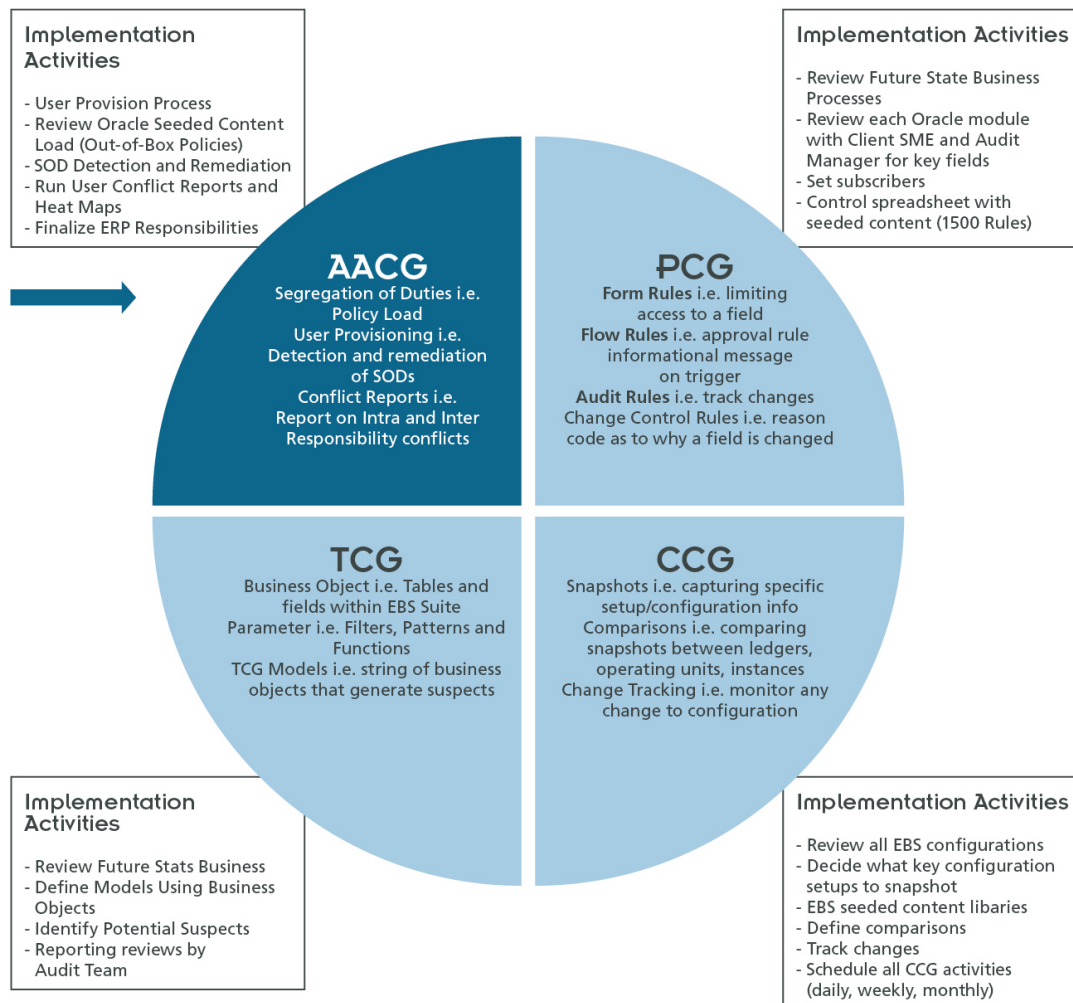
One of the first projects IA got involved in was to see how access would be granted to users and if a solid concept existed to prevent the combination of critical functions that could result in SOD conflicts. We recommended the Global Business Process managers to come up with a SOD concept, including an overview of AW Roles that should be segregated were possible.

In some parts of our organization, we have small operations and we cannot financially afford to implement the full concept of SOD. Therefore, the business had a need for a clear user provisioning process, where SOD conflicts could be identified and resolved

easily. The Global Business Process managers developed compensating (manual) controls where SOD conflicts would continue to exist. Another solution direction was to reduce SOD conflicts by transferring the responsibility for essential activities in Oracle to a new team, located in our Shared Service Centers in India and Manila. By moving tasks in Oracle to these teams we segregated duties and limited the number of people to be hired in the various countries.

For the business, it seemed like a big step, but the external auditors also needed to get an understanding of the new processes we implemented to be able to audit our financial statement.

The business bought software licenses for the Governance Risk and Controls tool (GRC) that had two key functionalities that would allow the business to monitor centrally SOD (so called 'Can Do' analysis) and to monitor transactions for known SOD conflicts (so called 'Did Do' analysis). The first is called GRC AACG, the second is called GRC TCG see figure 3.



"GRC has several modules to monitor SOD's, Transactions, Application controls and Configuration settings"

Figure 3: Oracle GRC AACG and GRC TCG models and functionality

Segregation of Duties Models

Based on the SOD model defined by the business, IA developed 158 SOD models in total that can be monitored. Models are classified in 'high', 'medium' and 'low' risk and will be implemented gradually. The business identified 42 models that should be monitored first. The models were developed with the support of an external service provider and based on our best practices developed in our SAP environment. The external auditor will review the models and the audits we perform, to see if they can rely on this work.

Currently, we provide monthly updates on existing SODs, which can be taken up by the business finance teams and regional risk management teams for follow up. On our journey, we first try to get our risk management community on board, to help them become a liaison between IA and the business to understand the concept of SOD and start the discussion with the business to resolve major SOD conflicts.

The SOD models consist of two equations, so called entitlements. These entitlements define access points in the application that should be segregated. One example is that a user should not be allowed to enter an accounts payable invoice, while also having the right to change the supplier master data. The risk would be that this employee can be tempted to create a fictitious supplier and raise invoices to be paid to the employee's own bank account in order to embezzle company funds.

It took us longer than anticipated to build these models and ensure that the roles assigned to users were conflict-free by design, and that the set of roles that were assigned to end users were stable during the first small roll outs.

Figure 4 shows how these models are built into the tool. A set of access points is bundled into an entitlement and two entitlements form one SOD model.

SOD | SOD models in AACG

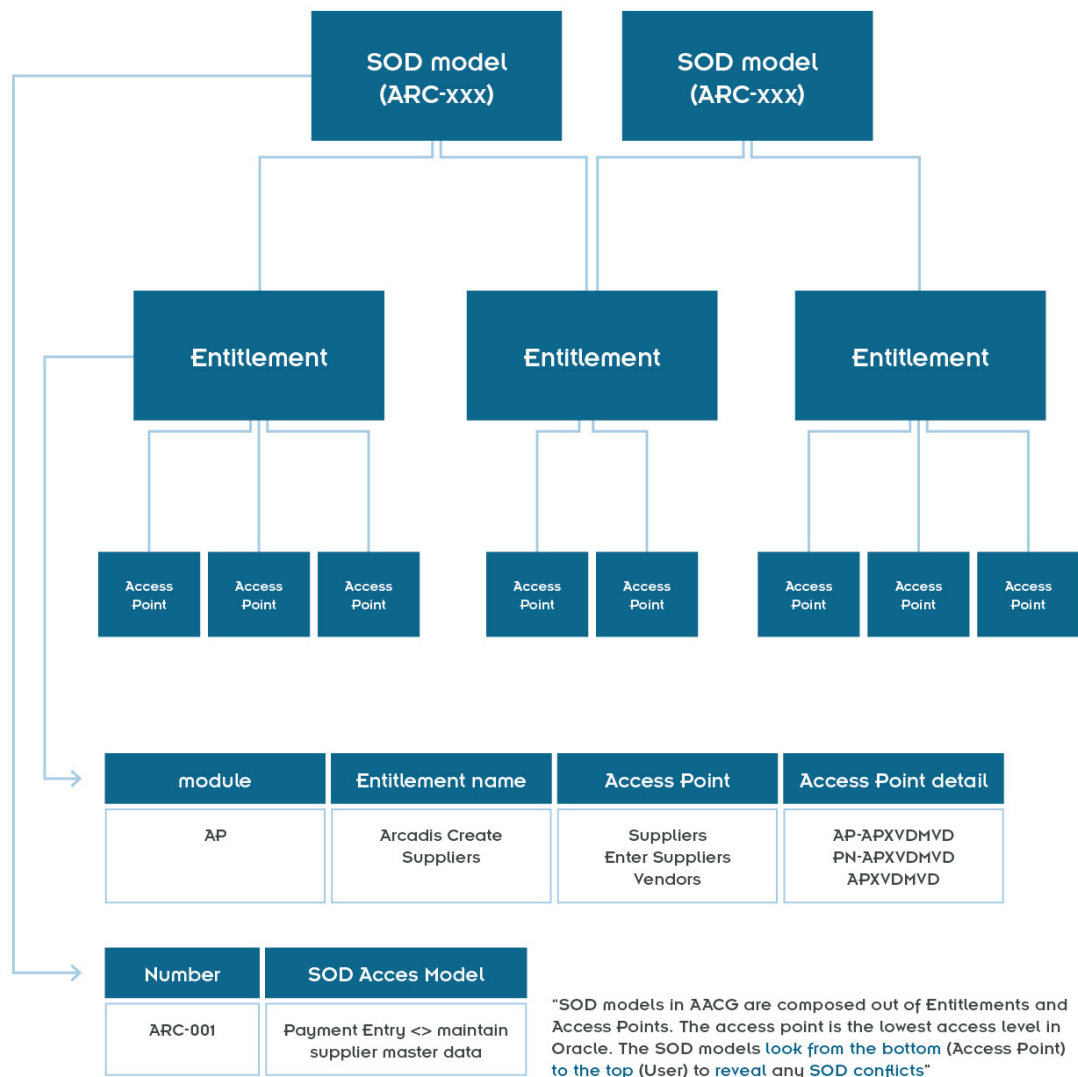


Figure 4: SOD models in Oracle GRC AACG

The output of these tools reports false positives if not well designed. These false positives needed to be investigated before we could release the outcomes of the models to a wider audience. The end result is that we are able to detect deficiencies in the control environment. The business is able to understand what we are monitoring and what they should do to prevent elevated access within their user community.

We felt privileged to have the possibility to make use of some new tools that are on the market to create and share interactive pivots to make quick and easy to read overviews in PowerBI².

In our company, we had a separate team working on a standard set of reports that could be used by management to monitor our business in a central business intelligence environment. Since there was less time to support IA with reports, IA had to be creative

and decided to make use of other tooling to distribute the outcome of the SOD models to the business. We started to use scripted system-generated lists, that show for all users created in our production system, their assigned responsibilities (see later in this text). Other information produced by these scripts included details about when an account was created, when it would end, when the responsibility was assigned to the user and when a responsibility would have been end-dated. PowerBI appeared to be the best solution to load the excel sheets outputted by our tool and create interactive and easy to (re)use pivot charts on a dashboard. We run our SOD models in the Oracle GRC AACG tool. The output is shared with the regional finance teams and with Risk Management.

The pivot charts make slicing and dicing through this information very intuitive for the users. The charts provide insights from an AW role level, responsibility level, user level, regional level, country level, user type level, et cetera. Slicing through the information, just by checking boxes, allows to quickly create overviews for Risk Management and regional finance teams to focus their remediation in the controls area under review. The overviews also allow us to perform benchmarks that can be used by the business and serve as input to our annual reviews on segregation of duties. See the example in figure 5, where benchmark results show how many users have been granted access to the General Ledger Account per country. This allows the finance team and regional risk management team to see if this role should be restricted given the size of the organization.

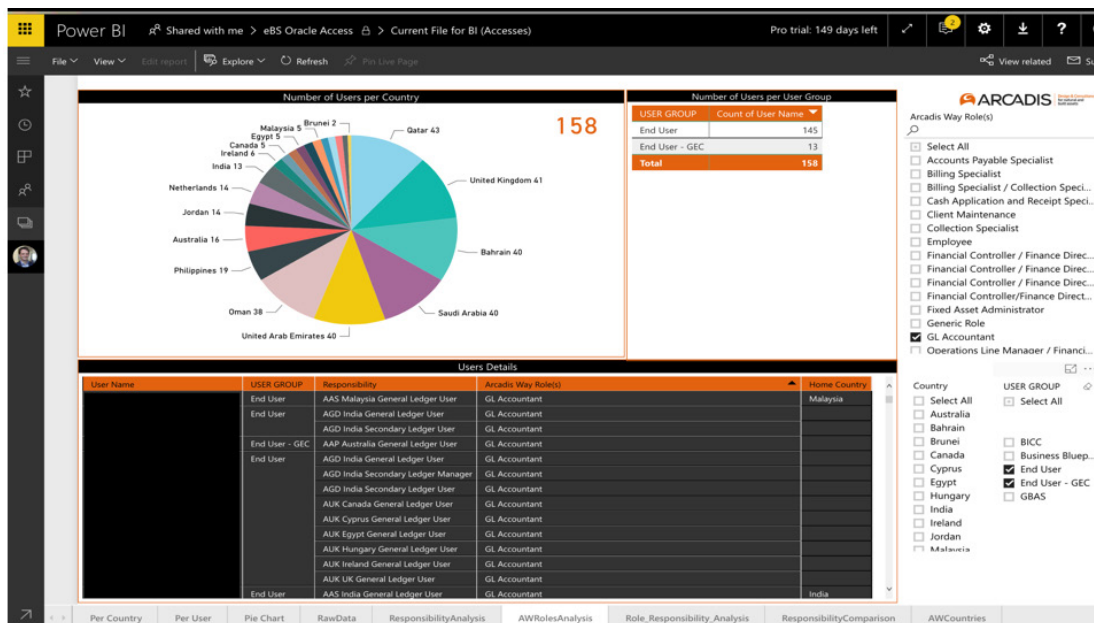


Figure 5: Benchmark results GL Accountants

Transaction monitoring

The GRC tool also provides the possibility to monitor specific transaction for identified SOD conflicts. These 'did do' analyses allow us to ensure that existing SOD conflicts have not been misused. Risk Management and the business need to develop a follow-up process for identified misuse. This part of the GRC tool allows users to select a specific table in the production system and create a query for the tool to answer a question. For instance, possible duplicate clients in our client master data can be found by running a similarity detection query. This query identifies any clients for which the name is 95% identical to other client names.

The business started to appreciate the effort that was put into developing the concept and the insights that were provided to them.

Concluding remarks

- It is important to understand how data in Oracle can be used to start continuous monitoring.
- Start by initiating a discussion with Risk Management and the business about the concepts to be applied around SOD. This model should be reflected in the solution provided by the project team.
- Apply general auditing principles when talking about the SOD concept with the business.
- IA departments should experiment and develop new audit approaches to enhance audit efficiency.
- Tooling is essential to audit the access granted in Oracle eBS, due to the vast amount of data available.
- The quality of analysis and reports improves significantly when interactive pivots are used instead of traditional Excel sheets.

Literature

[BRUC17] Jaap van Bruchem en Ronald de Goede, 'Oracle EBS, Kun je de gegeven op het scherm wel vertrouwen?', *de IT-Auditor*, Nr 2, 2017.

Notes

¹ Arcadis the leading global Design & Consultancy firm for natural and built assets.

² PowerBI is an Office 365 product that allows users to create quick and easy interactive pivots and charts.



W.T (Tobias) Houwert Msc RE | Global IT Audit manager bij *Arcadis*, *Internal Audit department*

Tobias Houwert is employed as Global IT Audit manager working for the Internal Audit department of Arcadis NV in Amsterdam. Tobias Houwert has more than 16 years of experience as an external IT auditor working for EY on various international engagements for multinationals. Tobias.Houwert@arcadis.com

Article written on personal title

Commercial offers based on this article are not appreciated.