

Case Study: How Vitens maximizes SAP GRC 12.0 in a SAP and non-SAP landscape

Tinette Beuving
and Virgil Verloop
Vitens

Produced by Wellesley Information Services, LLC, publisher of SAPinsider. © 2019 Wellesley Information Services. All rights reserved.

In This Session

- See how Vitens combined HR triggers with GRC business roles using the standard role functionality in combination with HR job key codes
- Gain insight into how Vitens uses SAP GRC as an IAM system
- Gain insight into how Vitens utilizes SAP Lumira to visualize the status quo
- See how Vitens is expanding Access Control to Active Directory using the standard LDAP connector
- Hear how Business Role Management is being used in the role management process
- See how Vitens developed a new an improved Access Request app in FIORI

What We'll Cover

- Introduction Vitens
- Framework and architecture
- EAM (Firefighter)
- ARA (SoD Scanning, SoD Review)
- ARM (Position Bases Access Control, User Access Review)
- BRM (Rolemanagement)
- S/4 FIORI Role Concept
- FIORI Access Request app
- Provisioning to Active Directory/Legacy
- Roadmap IAM & GRC
- Wrap-up



Introduction Vitens

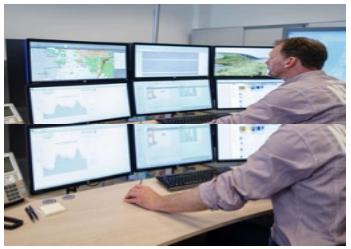


Introduction Vitens

- Vitens is the largest drinking water company in the Netherlands
- Service 5 provinces
- 5.6 MLN customers
- 49.000 km water mains
- Centrally controlled water distribution
- Drinking water laboratory in Leeuwarden







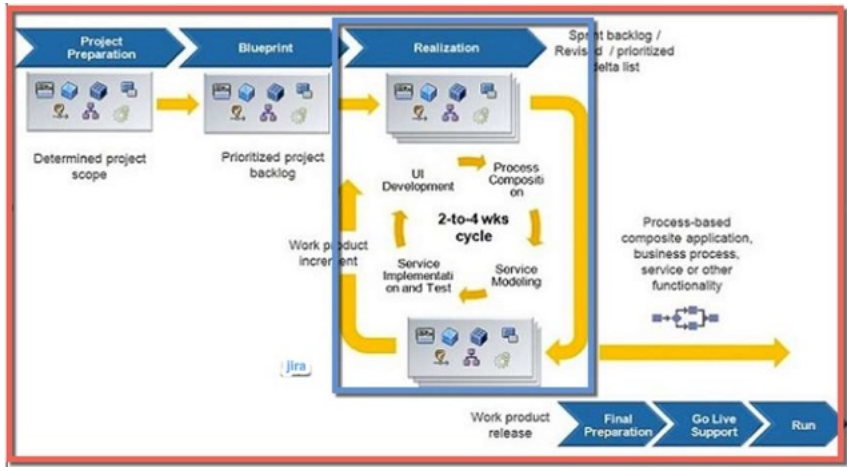


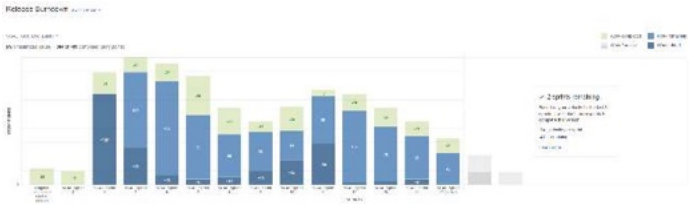


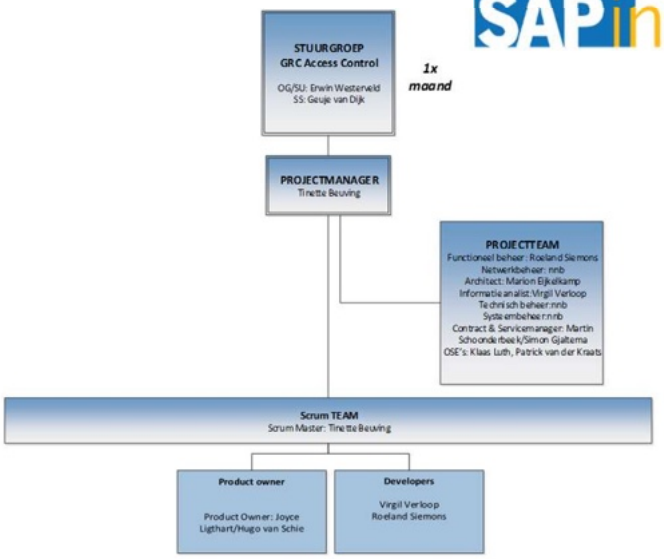
Introduction project

- In 2016 the project ‘Implementation Authorization Policies’ was completed. With it a full redesign of the authorization roles and the procedures was delivered. In this project we used the CSI tool as a risk analysis tool;
- Vitens decided to automate it’s authorization processes with SAP GRC. Not only the access risk analysis module, but a full integration of the GRC modules (Nov 2017 – Dec 2018)
- In 2019 the S/4HANA Redesign project and the IAM project started
- IAM – connect SAP GRC to Active directory/Legacy, update procedures, deprovision current MS IAM system and redesign and clean up roles
- S/4HANA redesign - complete redesign of the Vitens SAP landscape. Transfer current systems to S/4HANA, Succesfactors and C4C

Project approach

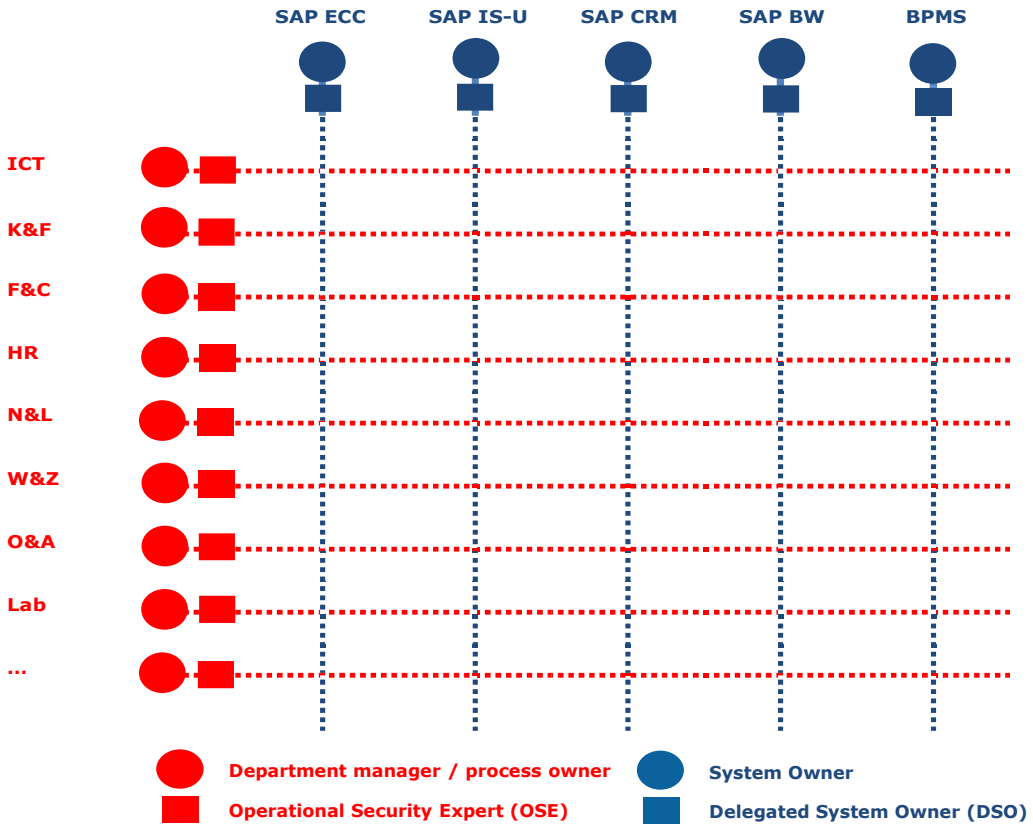








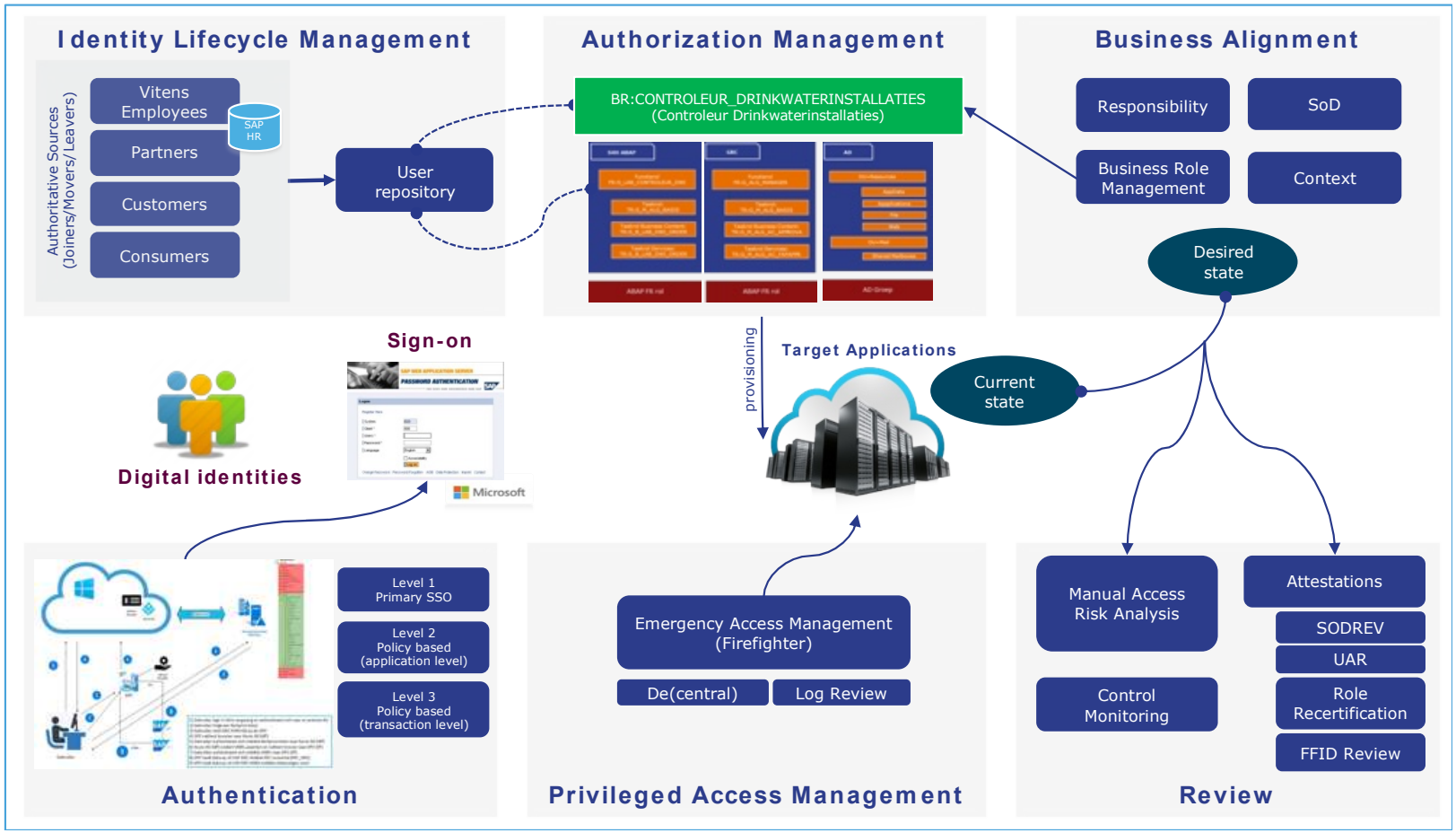
Security organisation



Framework and architecture

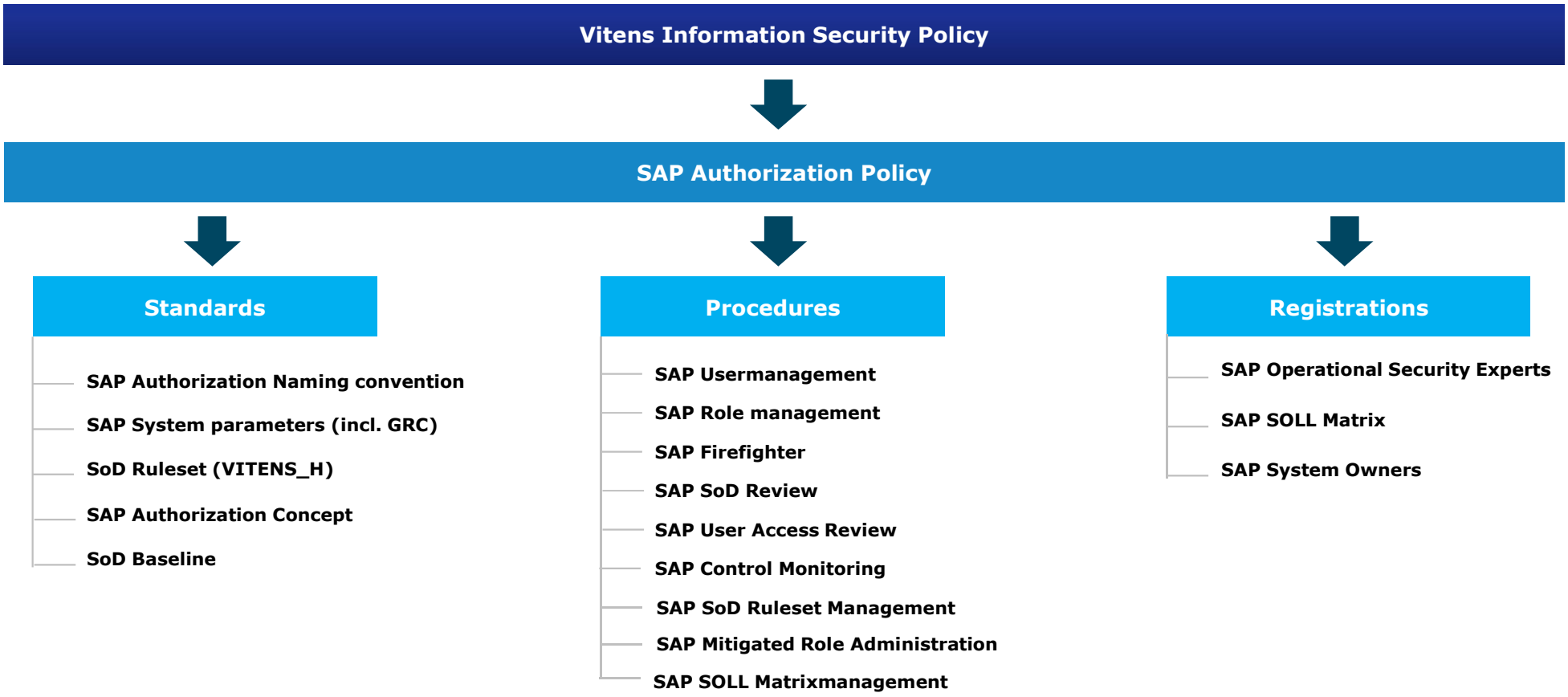


Framework

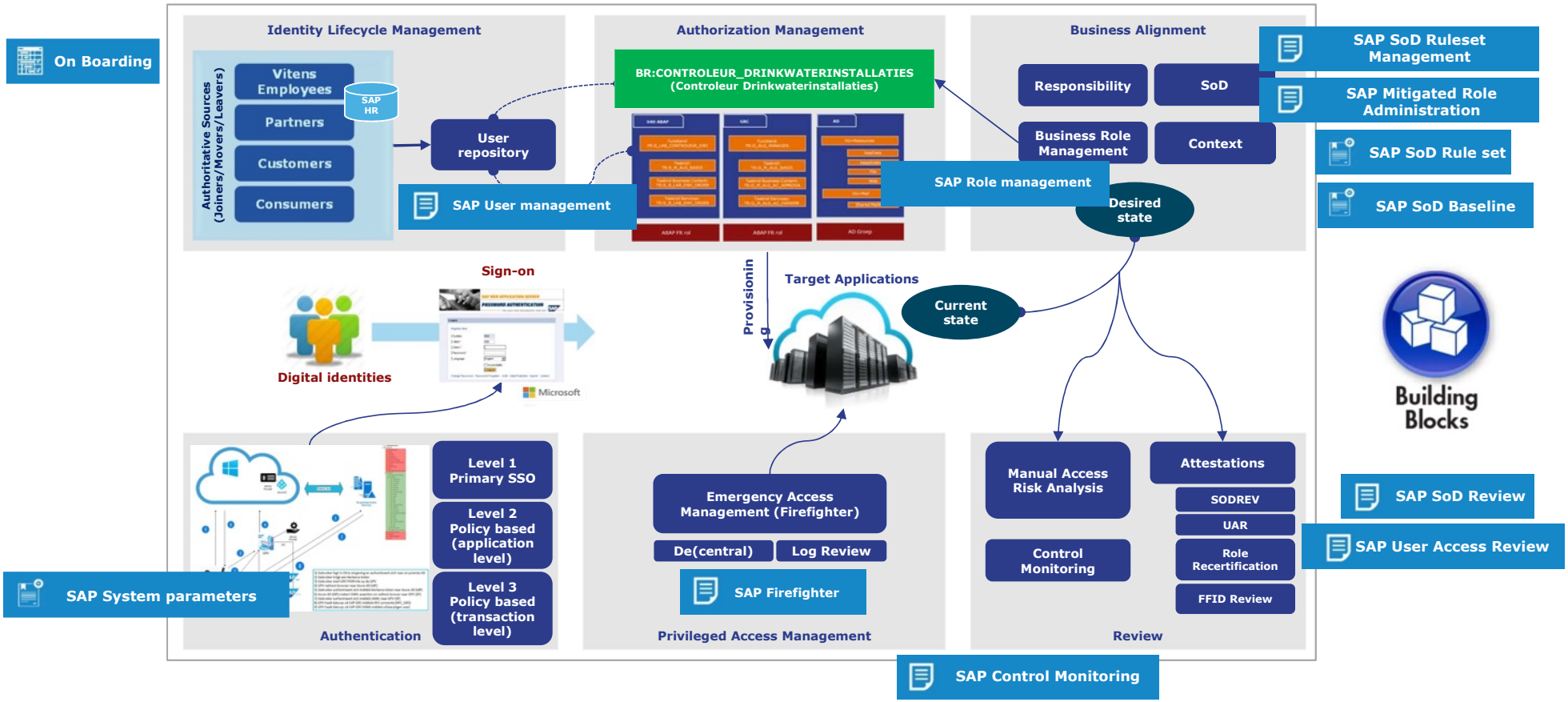


Building Blocks

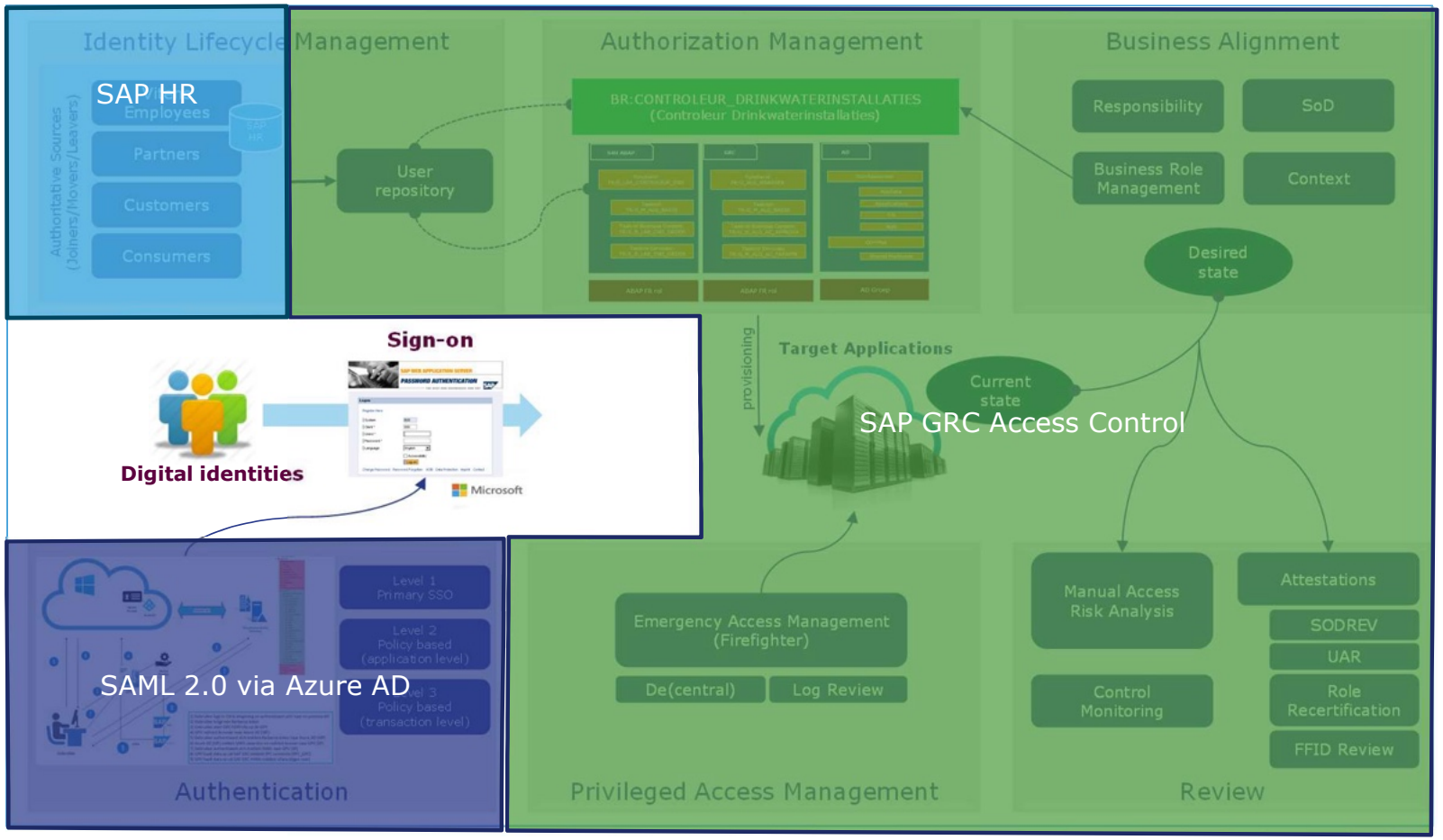
Documentation Structure



Documentation Mapping to Framework

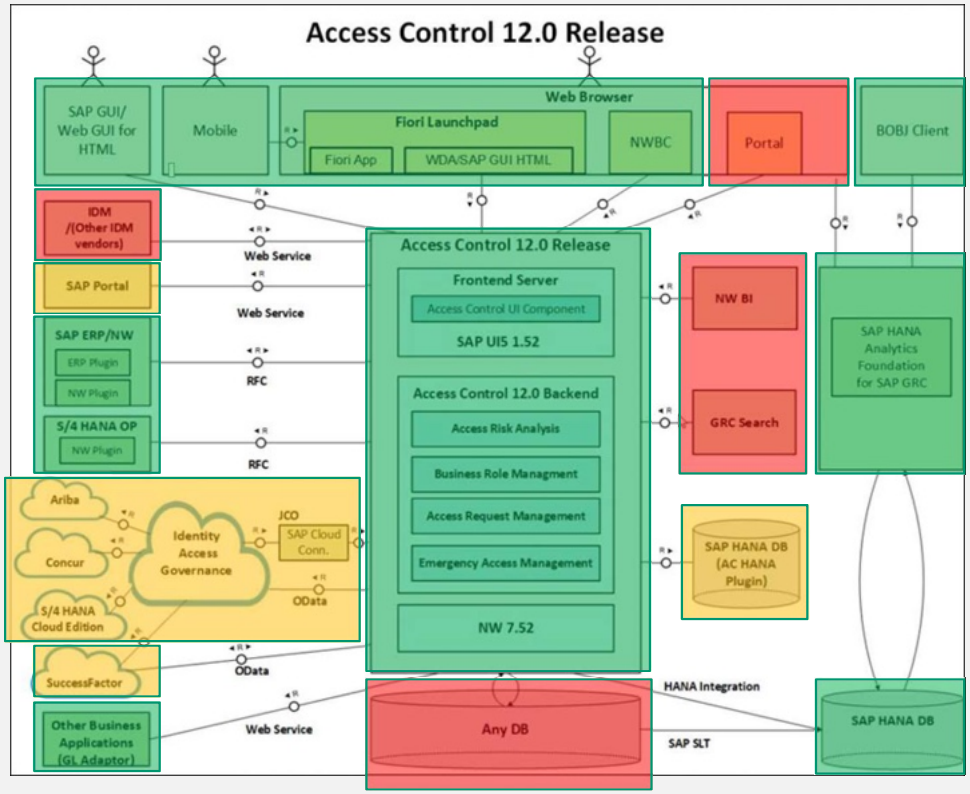


Framework solution overlay



Solution

SAP GRC AC 12.0 Architecture



- No portal integration we are using NWBC and FIORI
- SAP Portal will be provisioned via Web Service. Later integration with SuccessFactors
- Integration to BW is not neccessary because we can use GRC Analytics Foundation together with BO front end tools
- GRC search only neccessary for PC and RM to search in documents
- Integration with IDM is not applicable (we are using GRC as IDM tool)
- Integration with non SAP software is not applicable.
  We are only using the LDAP/AD connector in component “Other Business Applications” and do not need to buy a GL adaptor
- Any DB with SLT is not neccessary because we run native on HANA (HANA integration)
- Integration with S/4 is done via RFC with NW plugin, same for other SAP systems
- Identity & Access Governance is not being used yet but will be to provision C4C and Azure AD
- AC HANA plugin only for GRC HANA. S/4 not (yet) using analytical/smart business/factsheets FIORI apps.

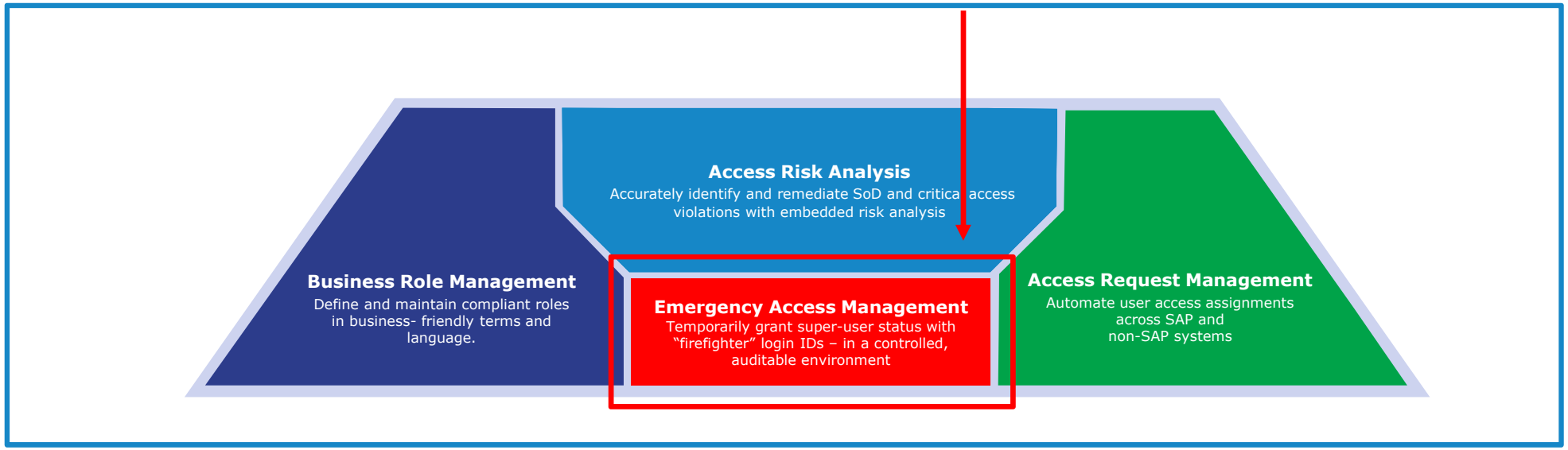
Emergency Access Management (Firefighter)



Emergency Access Management (Firefighter)

1 Firefighter (central and decentral)

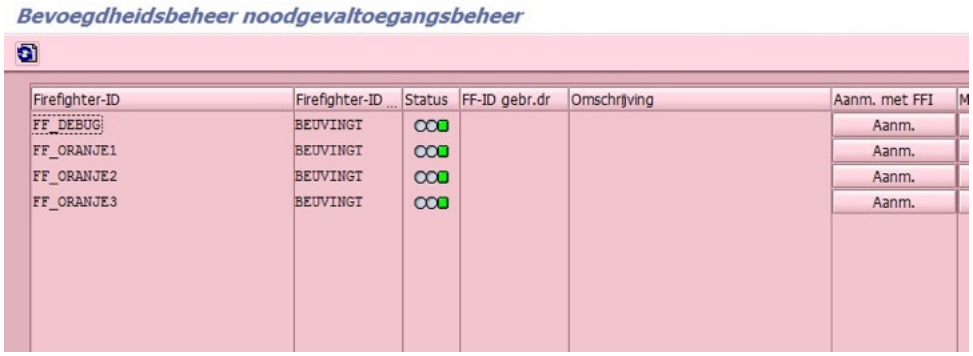
2 Firefight log review



Central and Decentral

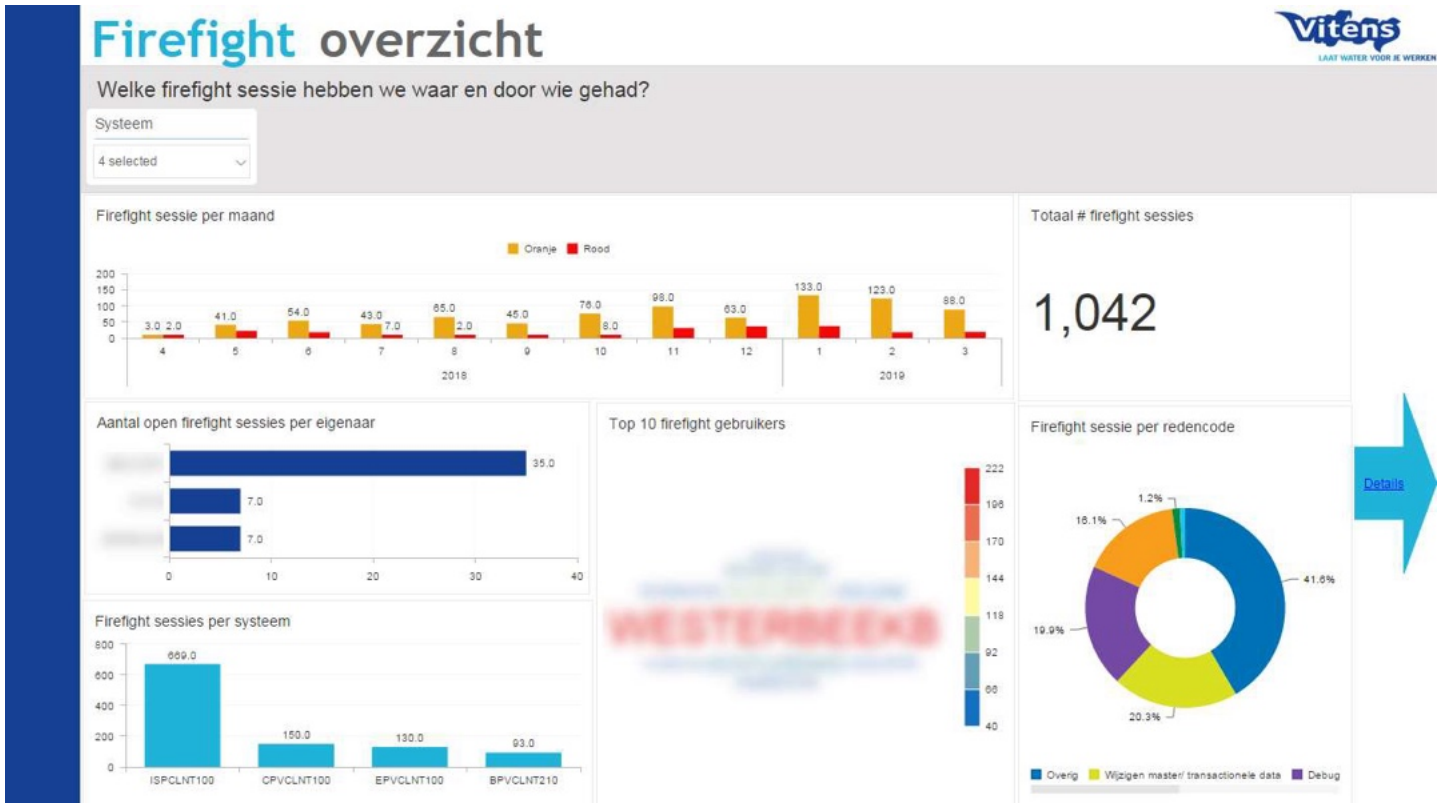
Firefighter is able to firefight:
- Central (GRx) and
- Decentral (S/4HANA/ECC/ISU/CRM/BI)

For each session the firefighter needs to fill in a form with:
- Reason code
- Ticket number
- Description of transaction codes





Firefight Dashboard



Access Risk Analysis

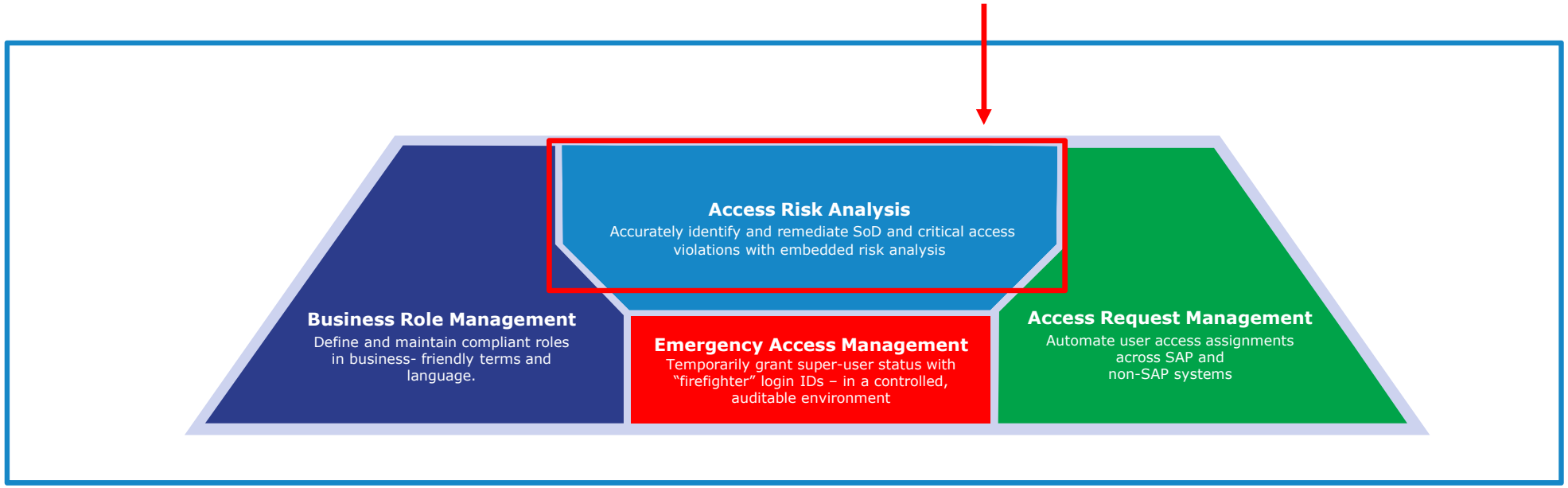


Access Risk Analysis (SoD management)

1 SoD Ruleset

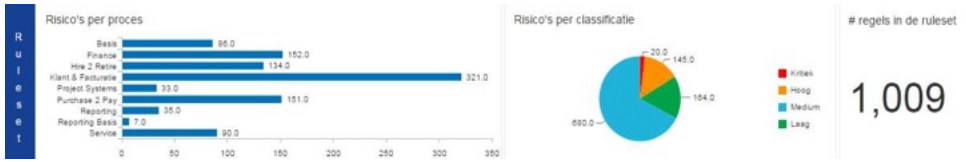
2 SoD Review

3 Adhoc scan



SoD Ruleset

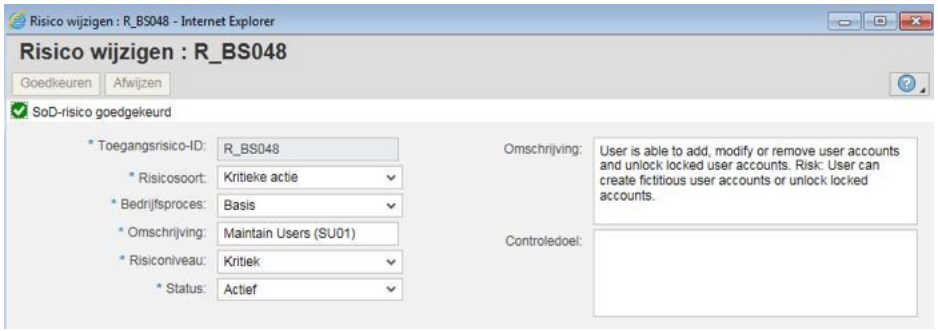
- Translation from CSI ruleset, 97% match
- Ruleset devided (Critical/High vs Medium/Low)
  - Performance reasons
  - SODREV reasons
- Change management on ruleset is active (ruleset is treated as masterdata)
- The following steps have been followed:



Regelstelsel-ID	Omschrijving
VITENS_H	Vitens Ruleset Hoog/Kritiek
VITENS_M	Vitens Ruleset Medium/Laag

Steps

1. Export CSI ruleset
2. Mapping processes, risks and functions with new ones
3. Translation by Protiviti
4. Validation translation by Vitens
5. Install tool
6. Upload ruleset
7. Run SoD analysis
8. Validate risks on role level
9. Validate risks on user level
10. Troubleshooting
    a. Adjust risk in GRC
    b. Adjust risk in CSI
11. QA
12. Go Live

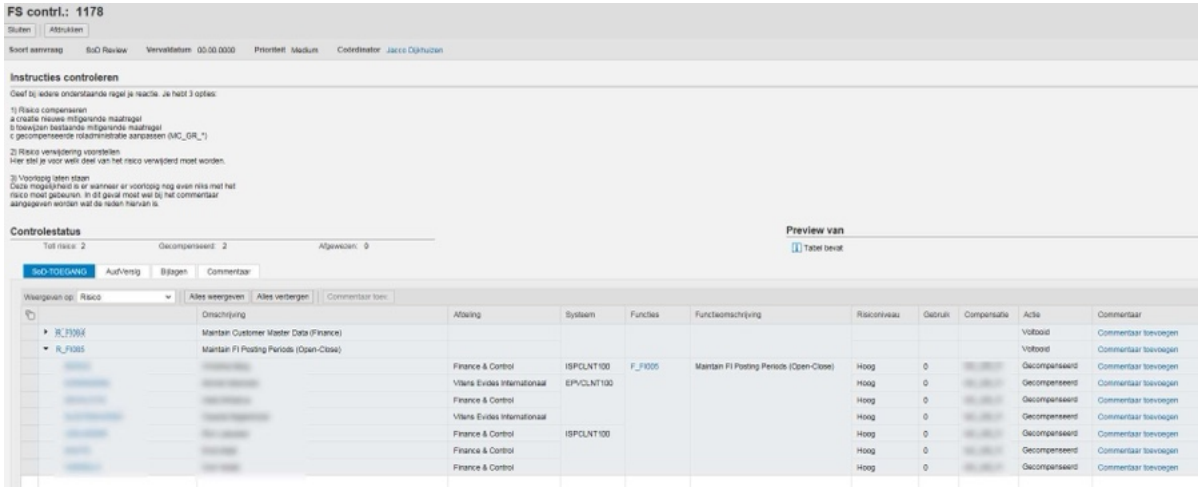


Risk ➔ Risk Owners
Function ➔ Security Team (4 eyes principle)

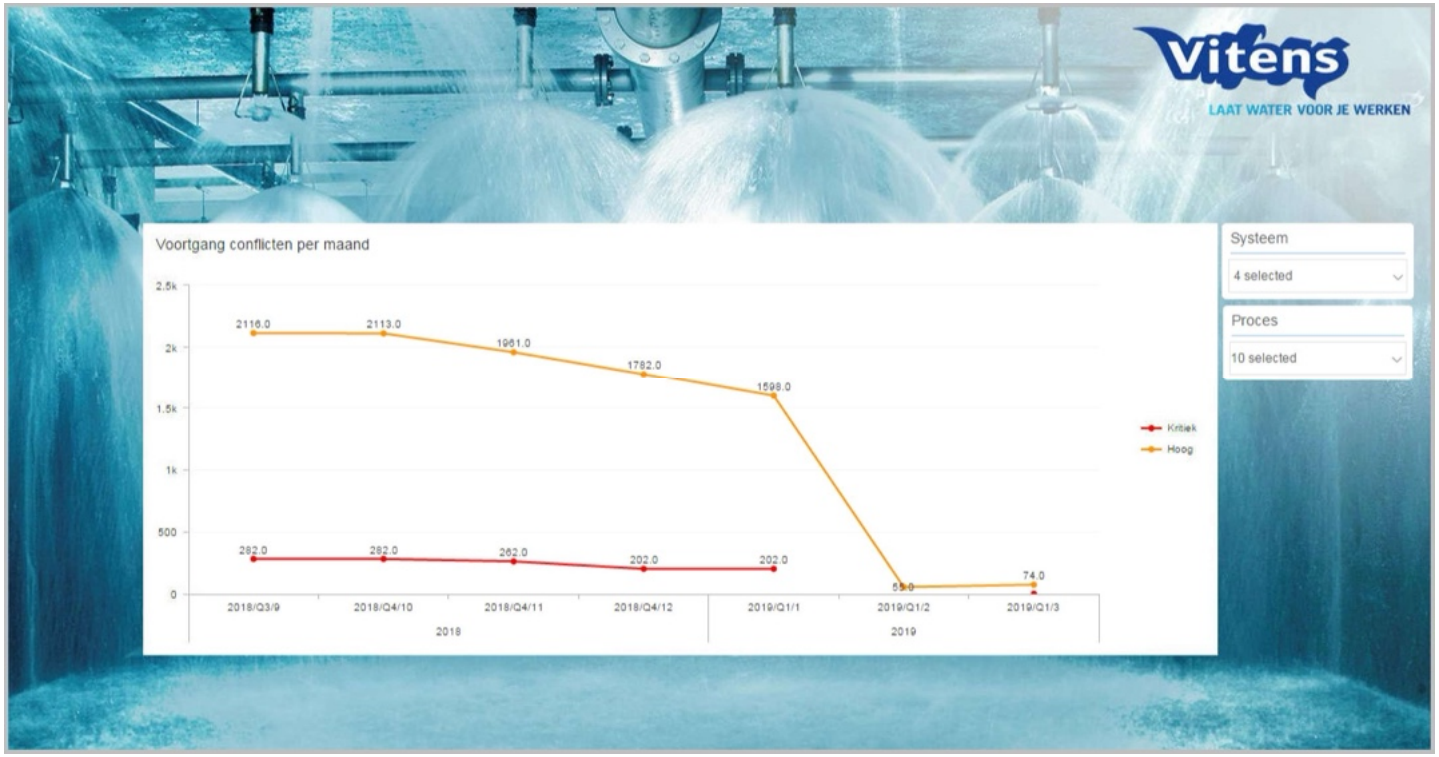
SoD Review (Safety Net)

Includes the following functionality:

- **Plan periodic jobs**
- **5 reaction types**
- **Submit by OSE**
- **Submit (formal close by DSO)**



Access Risk Dashboard







Access Risk Dashboard

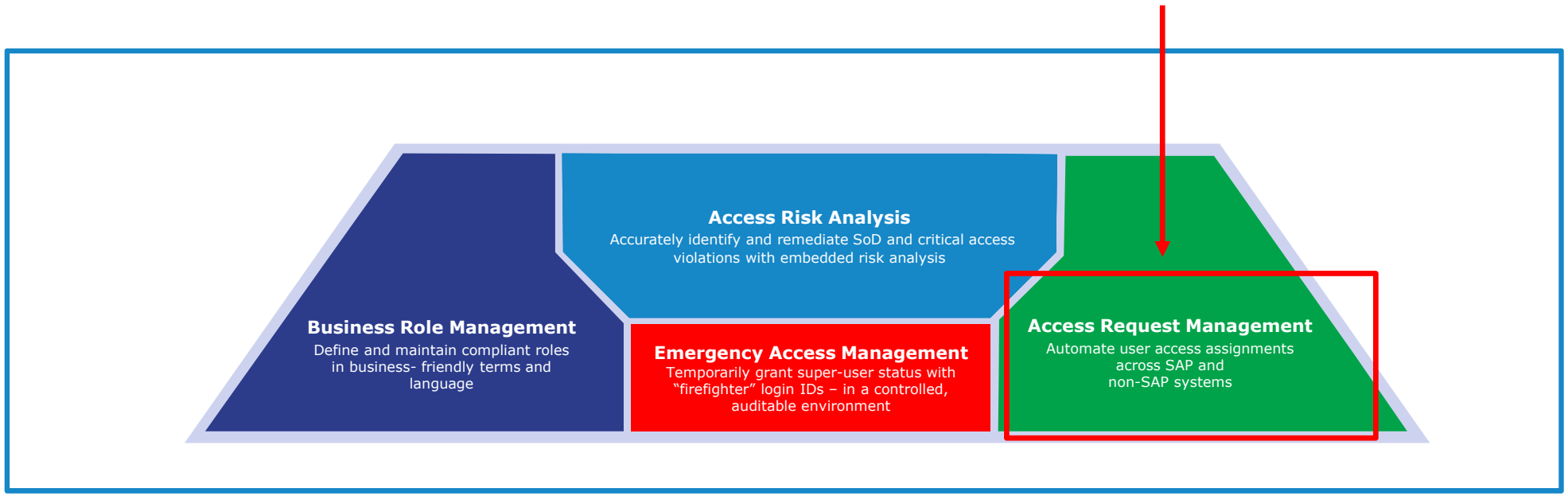


Access Request Management

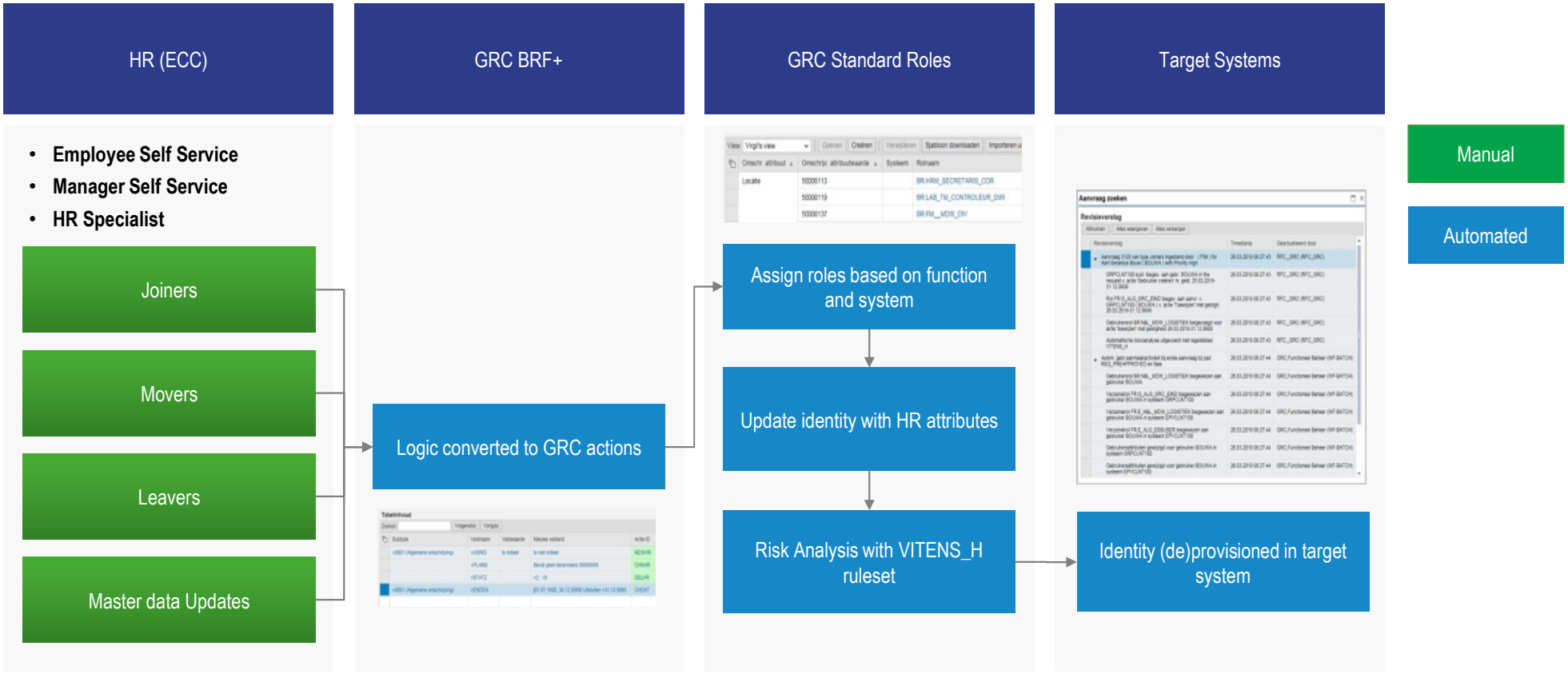


Access Request Management (usermanagement)

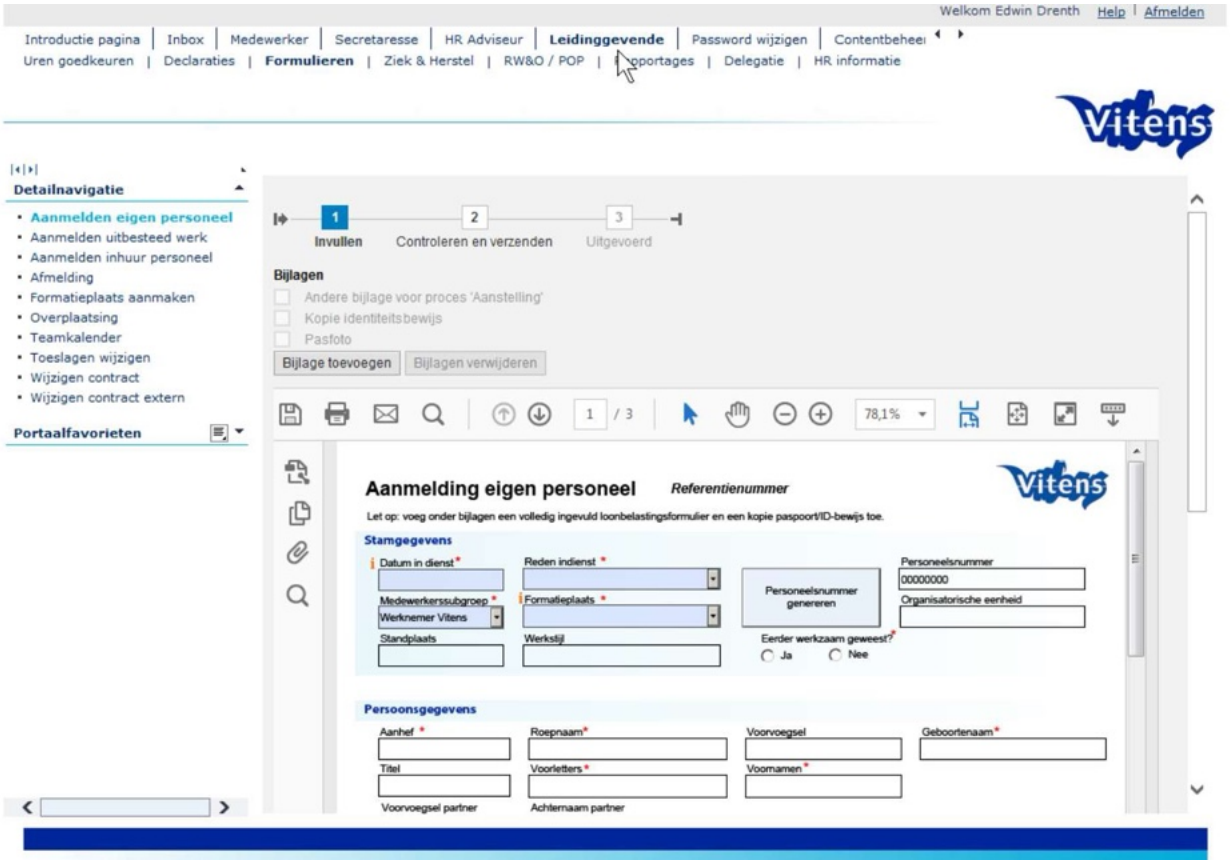
1. Position Based Access Control (90%)
2. Requests by user (10%)
3. Password Self Service
4. User Access Review



Position Based Access Control



Onboarding form (PDF)



Position Based Access Control via Standard role

Business role assignment based on function code (via location)

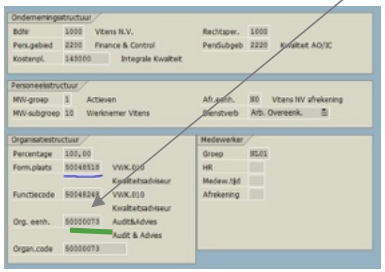
Generic role assignment based on system

Standaardrol - Alle

Query wijzigen Nieuwe query definiëren Personaliseren

View: Virgil's view | Openen | Creëren | Verwijderen | Sjabloon downloaden | Importeren uit bestand | Afdrukken | Afdrukversie | Export

Omschr. attribuut	Omschrijv. attribuutwaarde	Systeem	Rolnaam	Constellatie	Laatst geactualiseerd	Geactualiseerd door
Locatie	50048518		BR:KWALITEITSADVISEUR		17.10.2018 15:07:23	Virgil Verloop
Locatie	50049821		BR:FBA		17.10.2018 15:09:25	Virgil Verloop
Systeem	GRDCLNT100	GRDCLNT100	FR:G_ALG_GRC_EIND	GRC straat	22.06.2018 05:38:09	Virgil Verloop

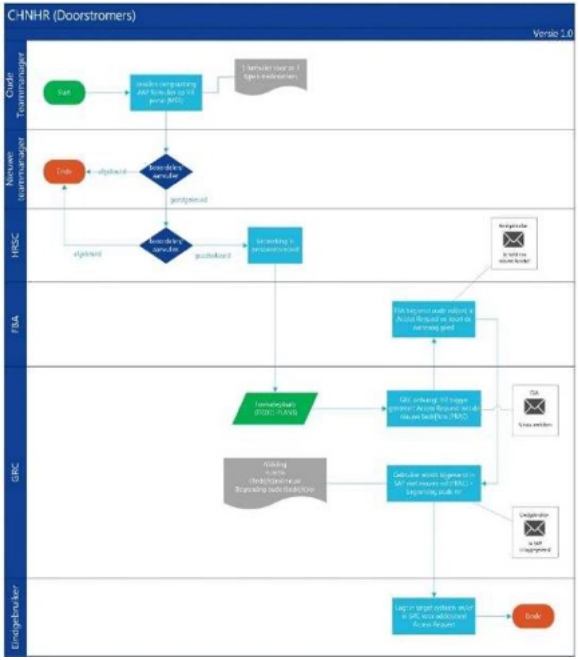


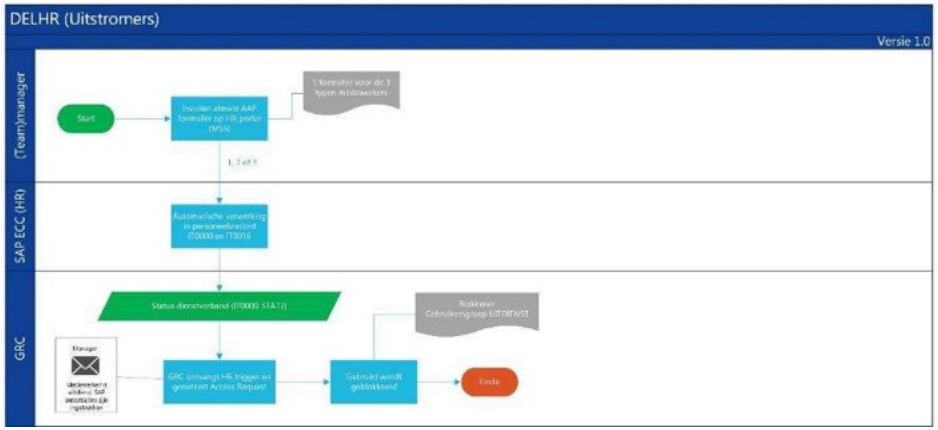
Manual activities:

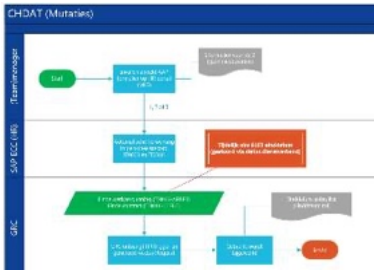
- **PPOME provisioning (org model in i.e. CRM)**
- **License code in UMR > role based classification in USMM**

Movers, Leavers and Masterdata Updates

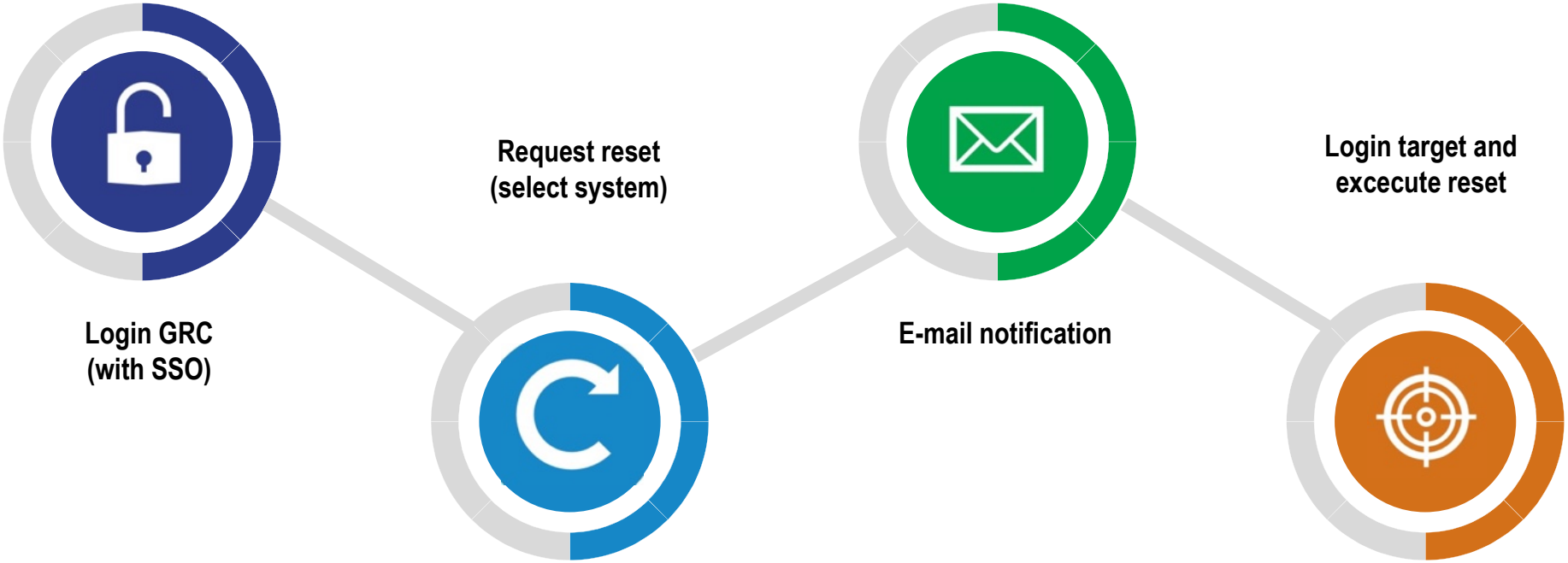
- We have similar processes for movers, leavers and masterdata updates



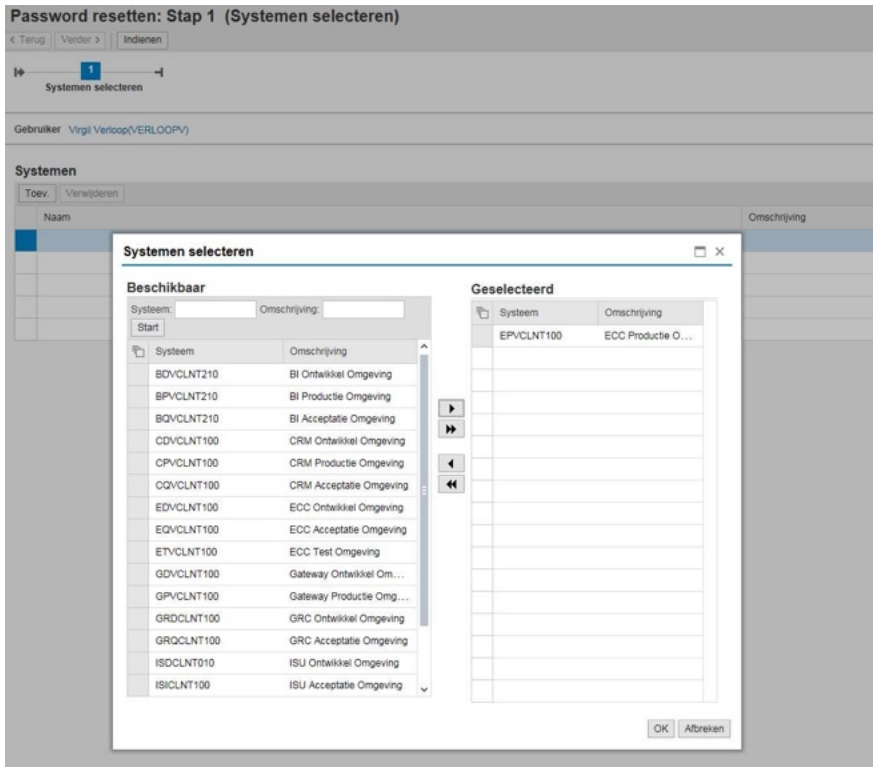




Password Self Service



Password reset menu





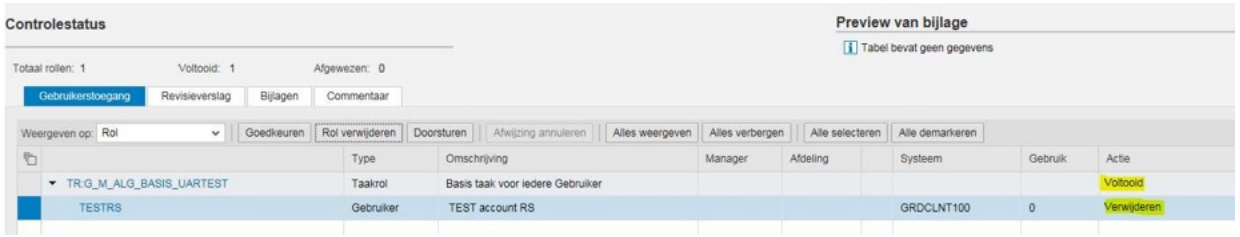
- Password reset possible on production and non production systems
- Reset is not possible when user has an admin lock
- Valid @vitens.nl e-mail address is mandatory in UMR

User Access Review

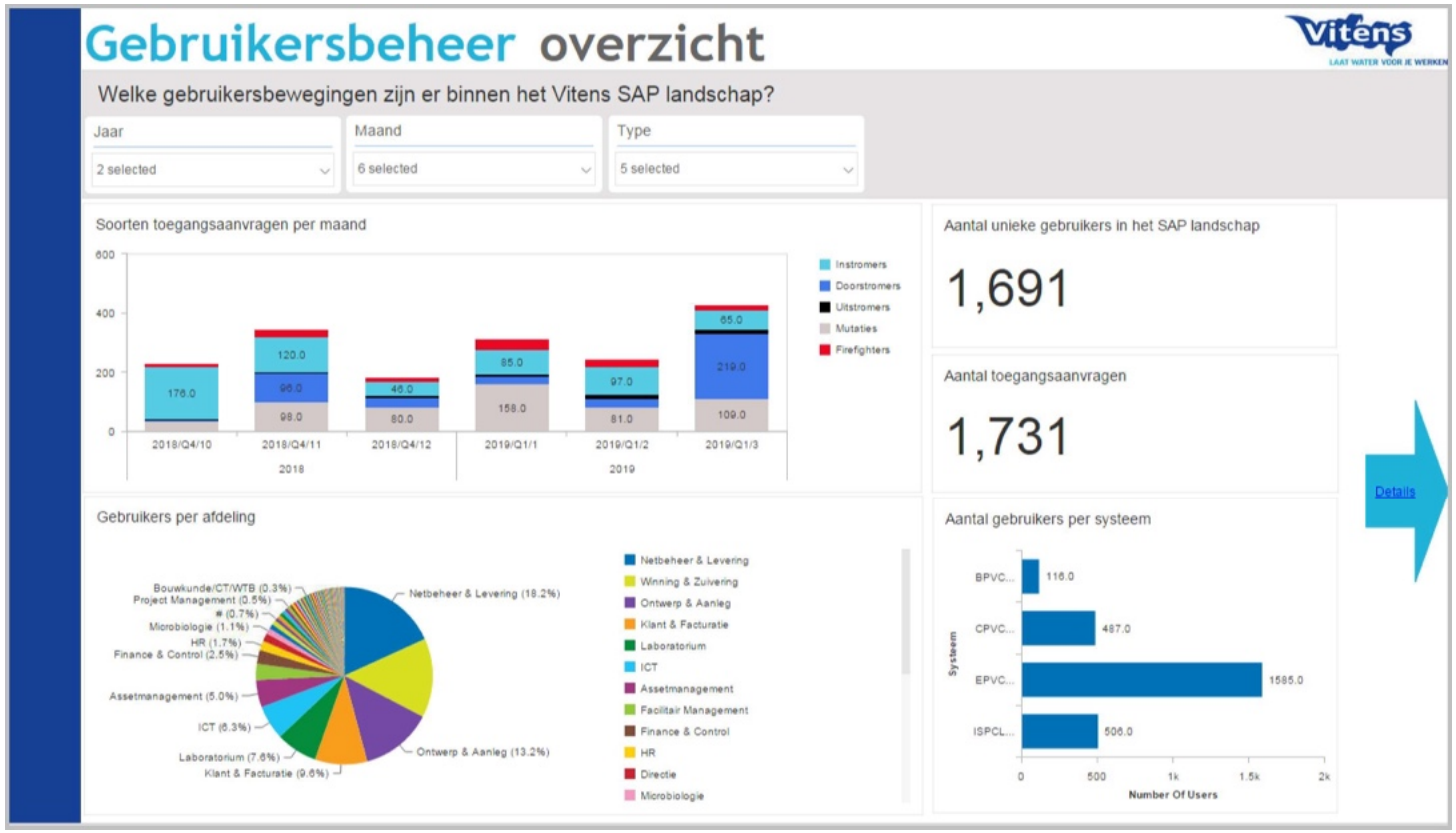
Periodic control (twice a year) of user role assignments

The OSE (Operational Security Expert) has two weeks to finish the UAR
- After that the UAR work item escalates to the DSO (Delegated System Owner)

The following actions are allowed for every line item:
- Approve
- Delete(role is immediately deleted!)
- Forward to another OSE



Access Request Dashboard



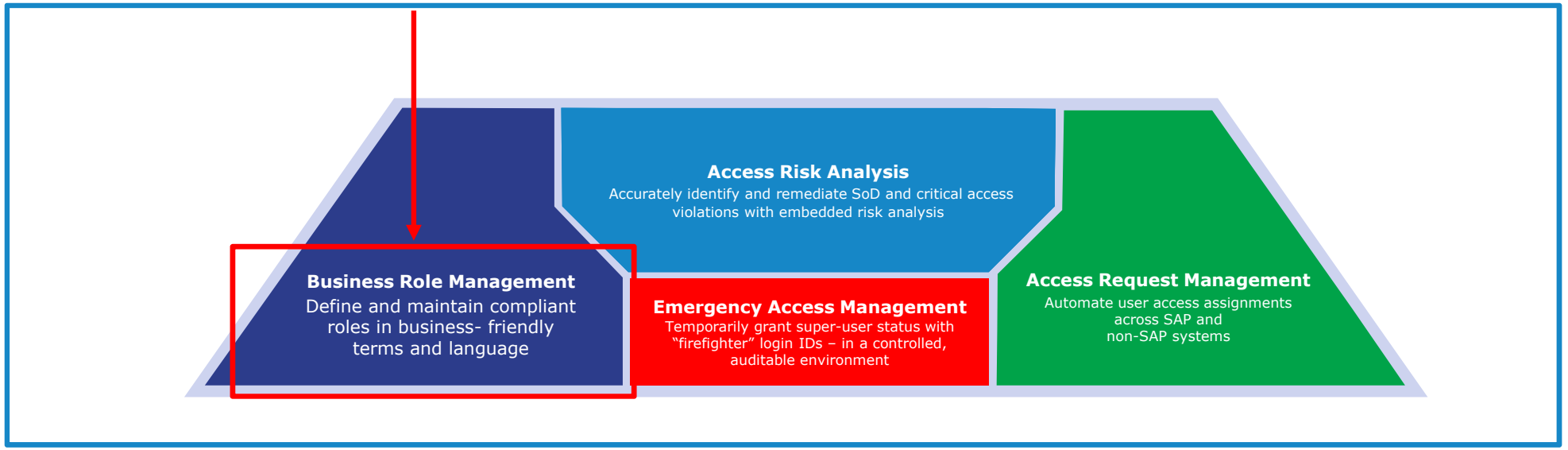
Business Role Management



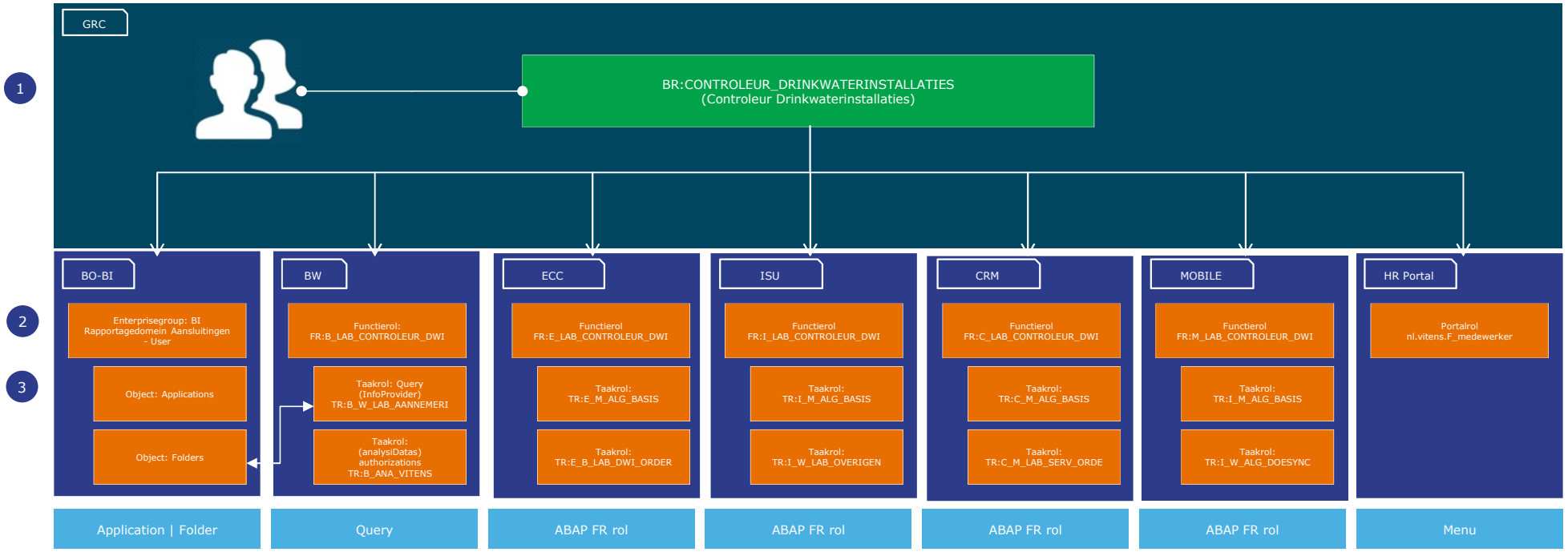
Business Role Management (Rolbeheer)

1 Business role hierarchy

2 Role management process

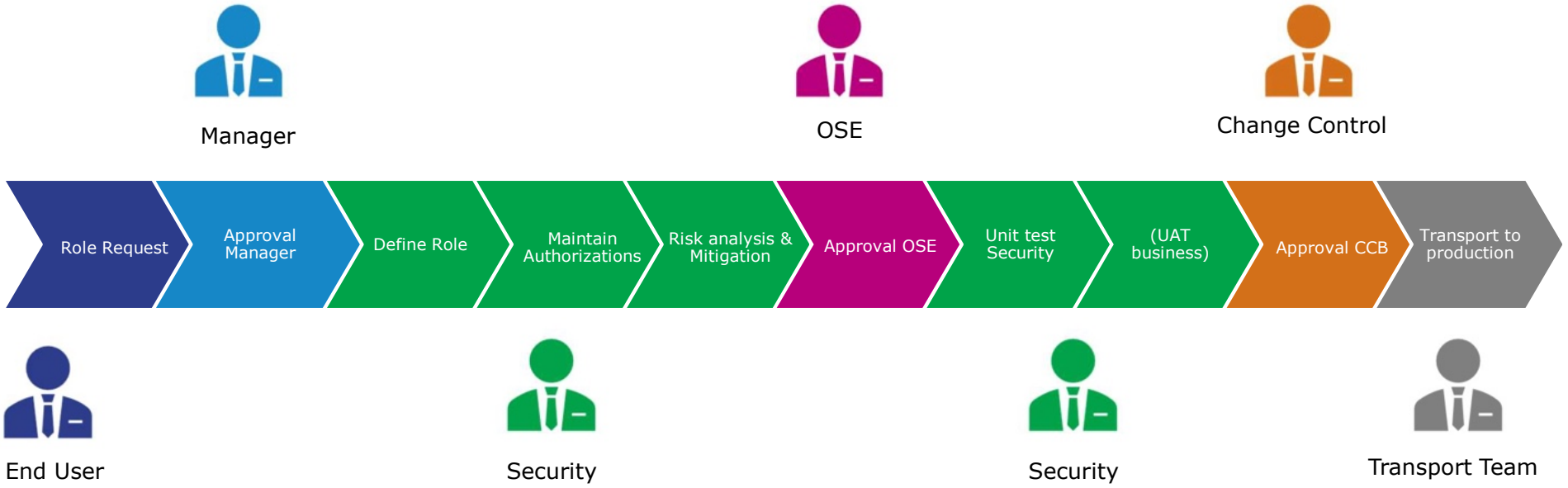


GRC Business Role Hierachy

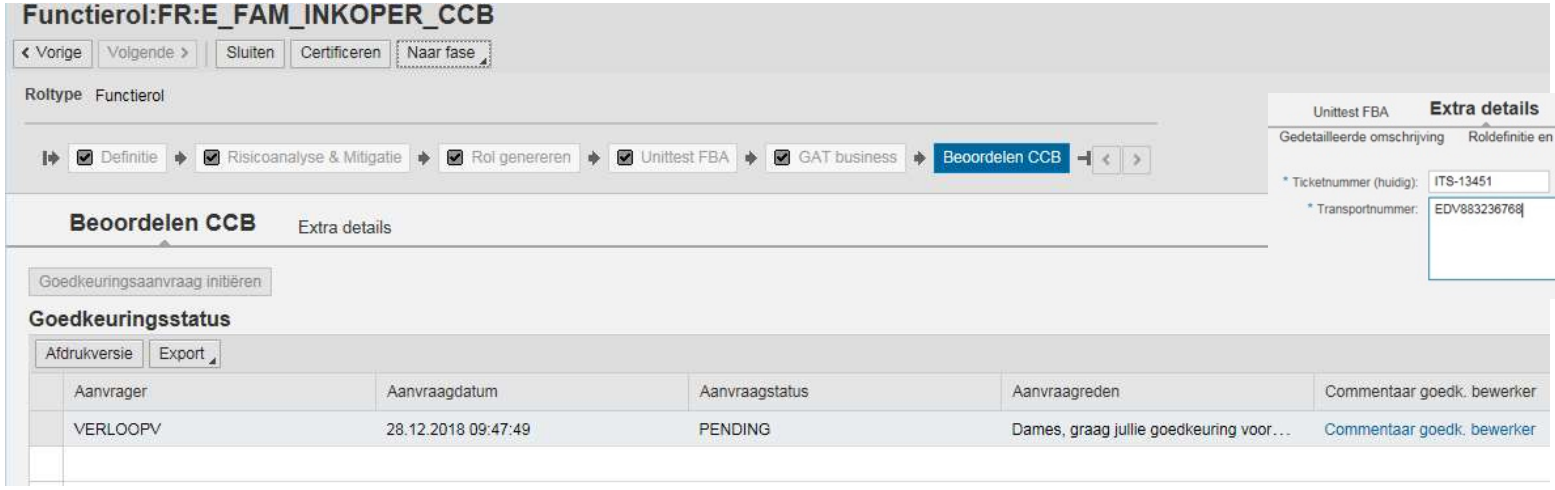


1) Business role (can be requested in GRC) - owner
2) Function role (can be requested in GRC) - owner
3) Task role (can be requested in GRC) – owner

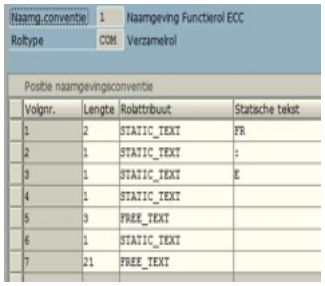
Role Management Simplified

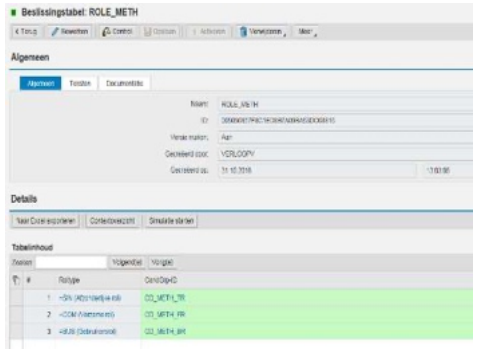


Composite Role Methodology (Example)

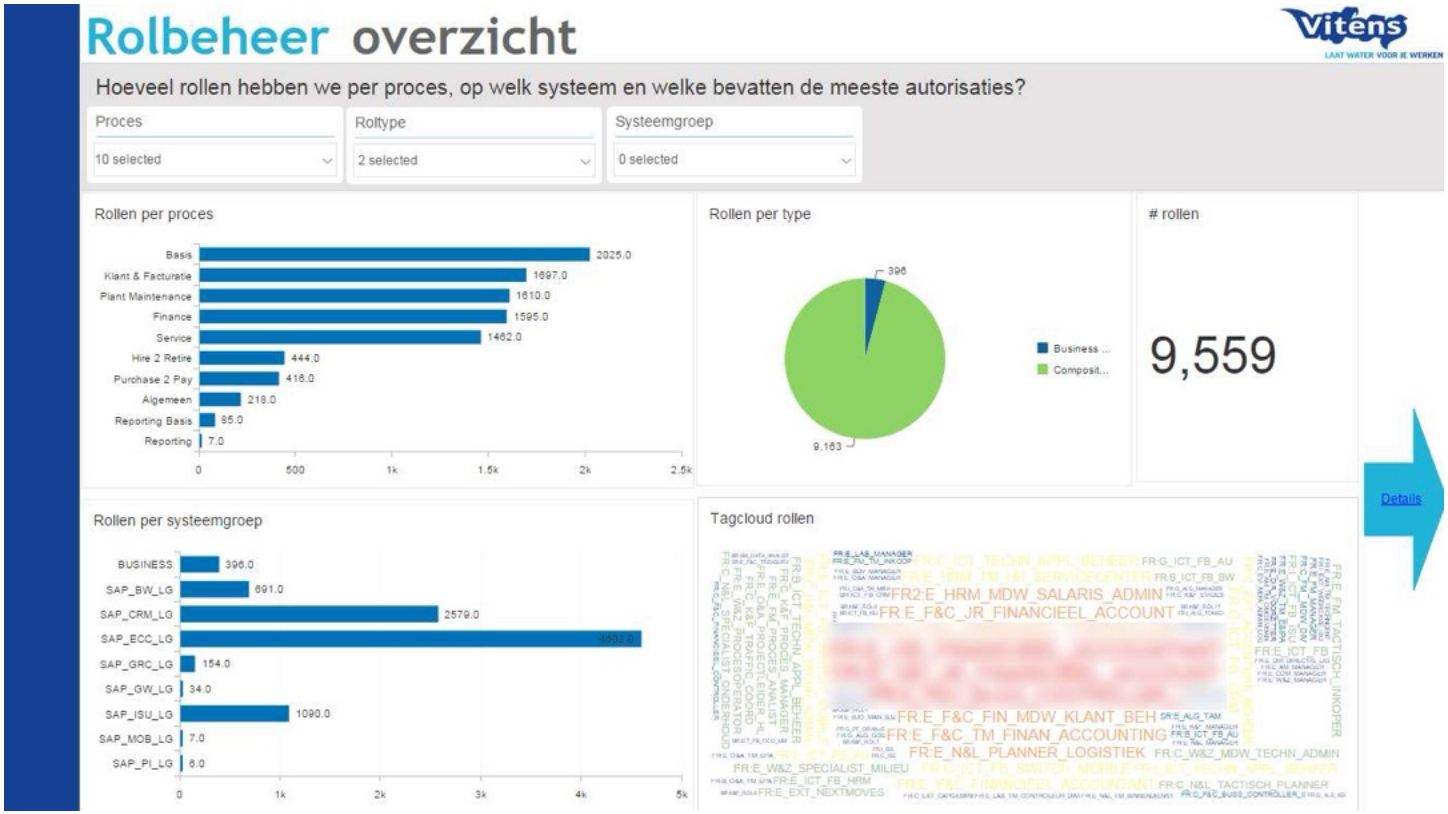




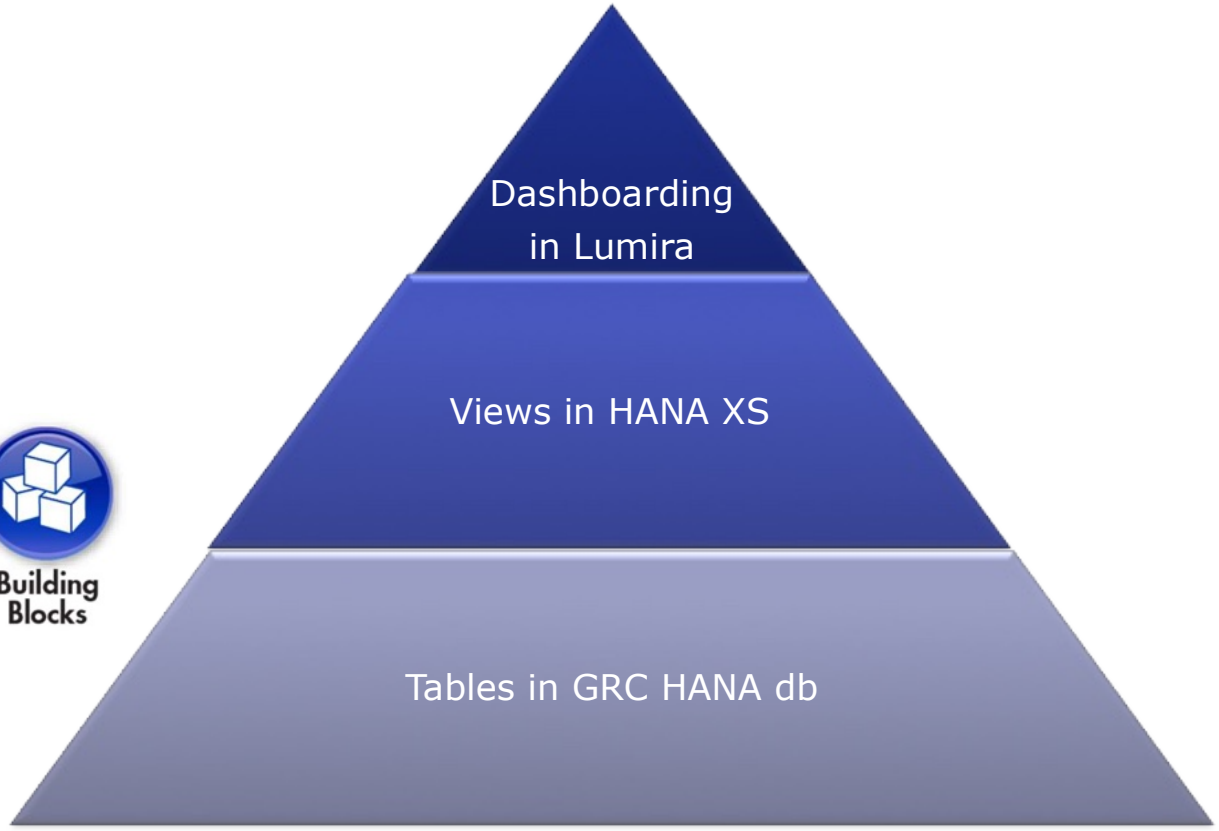


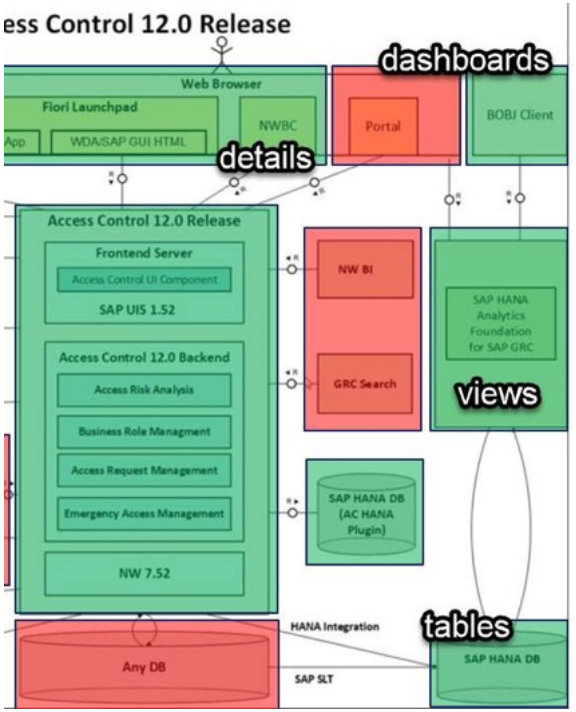


Business Rolemanagement Dashboard



Analytics architecture



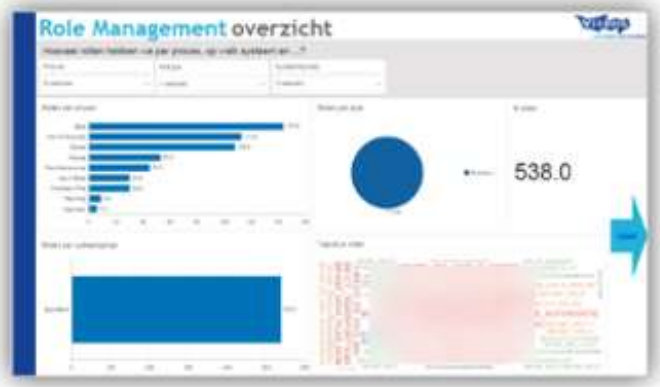


Dashboarding in Lumira









S/4 FIORI Role Concept

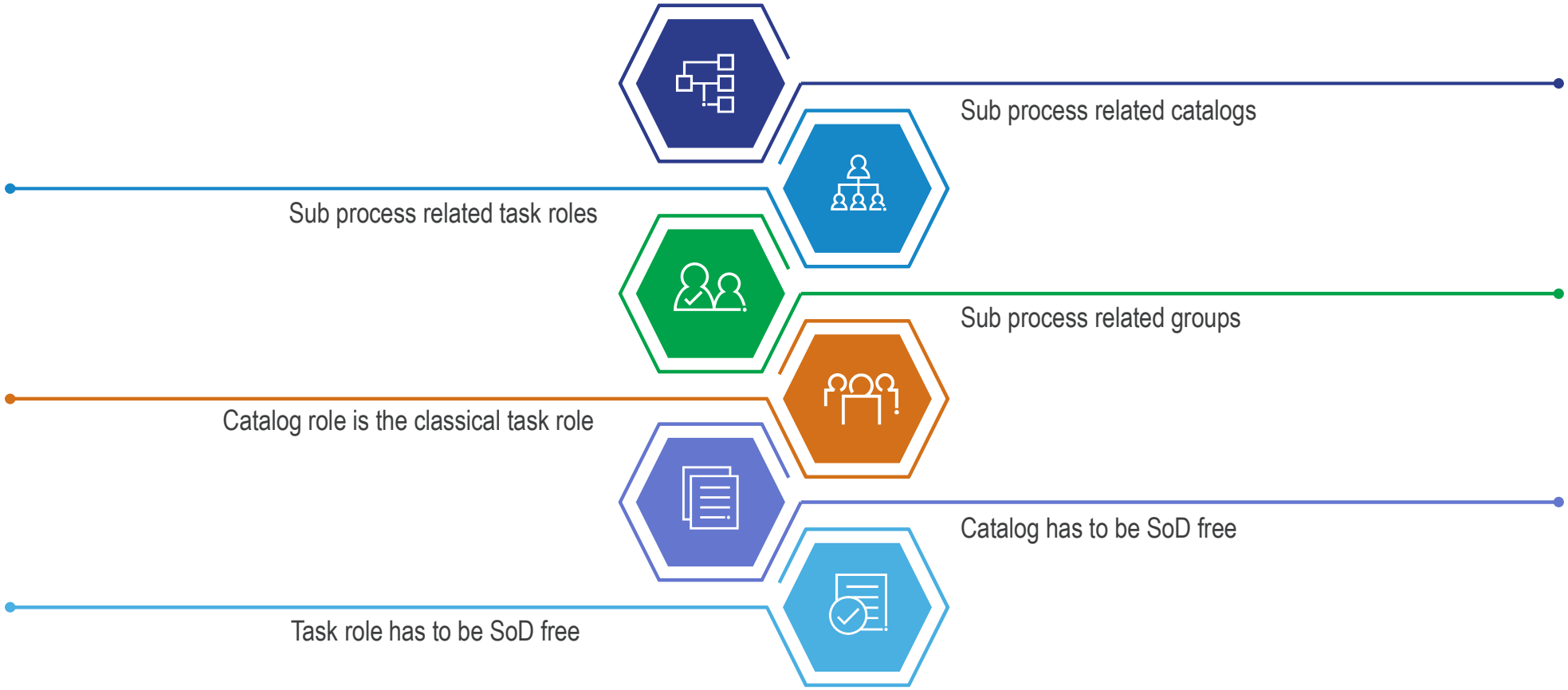


S/4 HANA Authorization Model

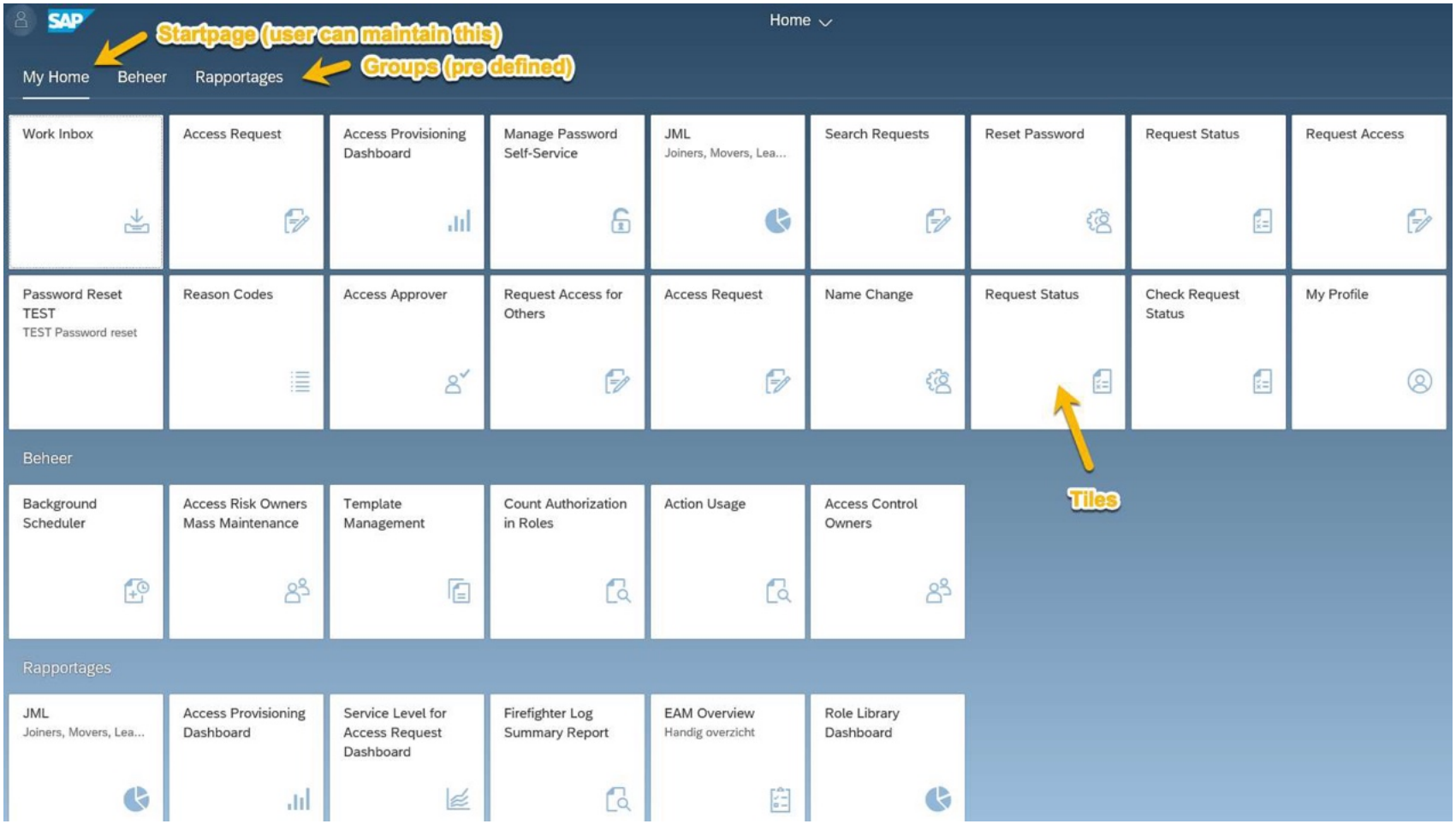


- Function –task role model
- Task role is connected to catalog
- Groups are linked to task roles
- Authorizations (TADIR) in task roles are generated based on the catalog

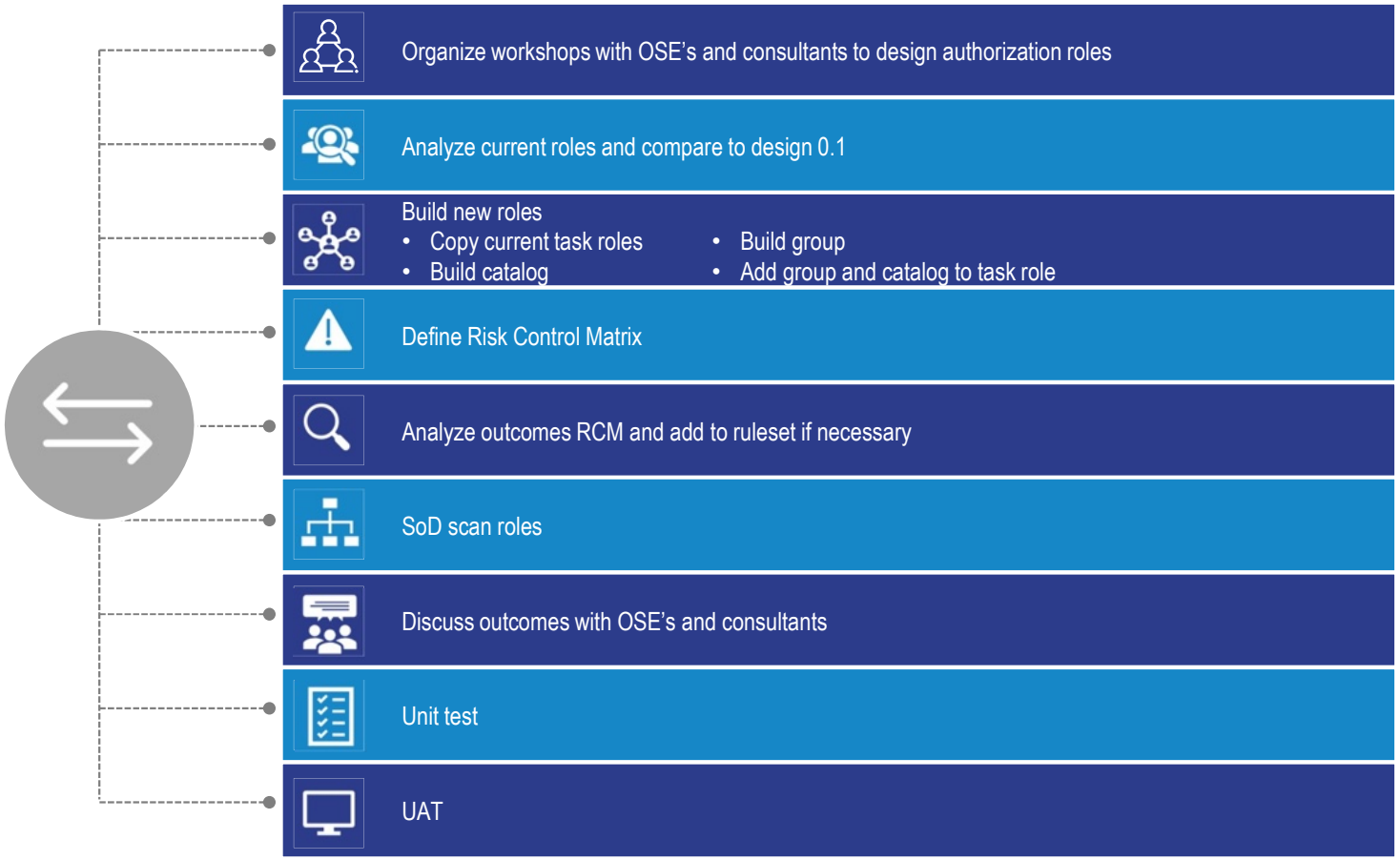
Principles


Sub process related catalogs
Sub process related task roles
Sub process related groups
Catalog role is the classical task role
Catalog has to be SoD free
Task role has to be SoD free

FIORI Startup Screen



Role Design/Build Approach



Fiori – Tiles

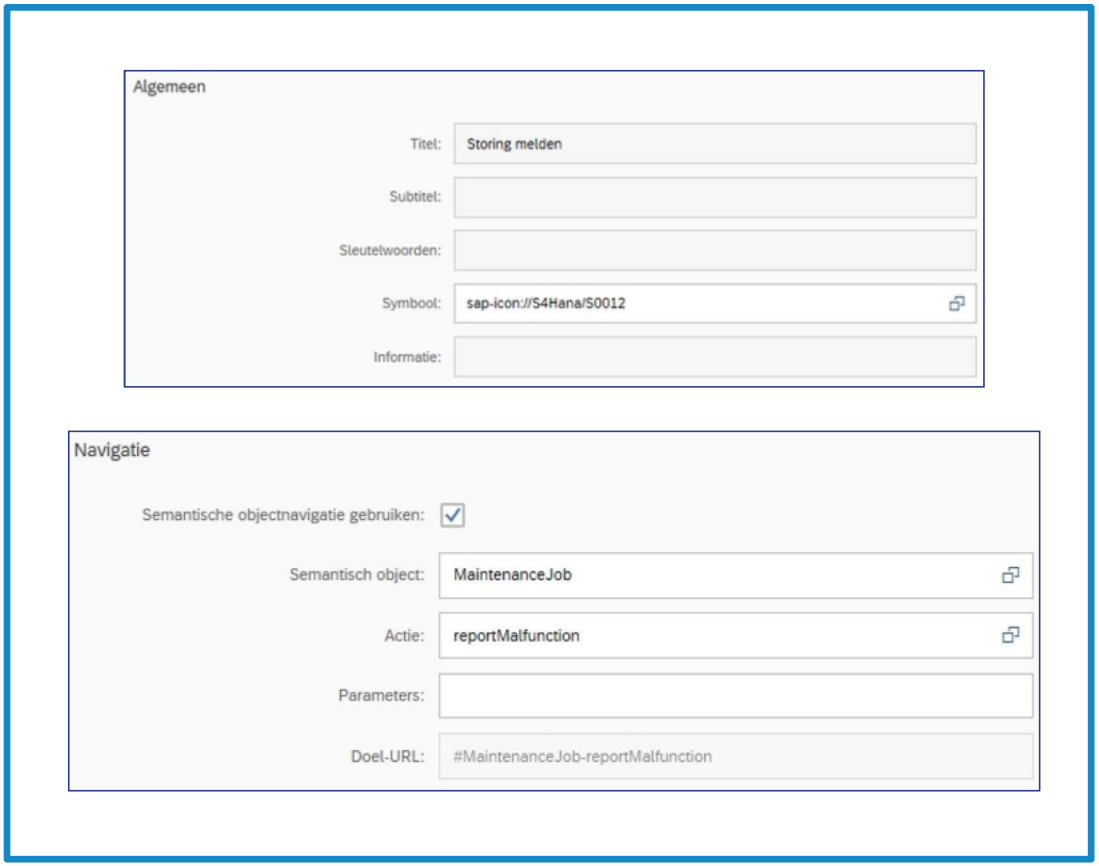
A tile consists of the following data:

Common

- Title
- Subtitle
- Keywords
- Symbol

Navigation

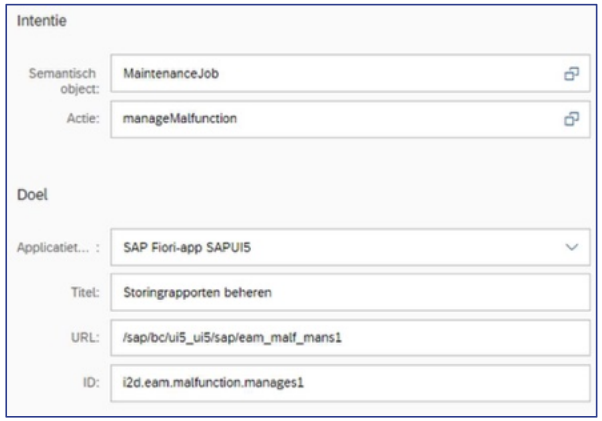
- Semantic object
- Action
- Parameters
- Target-URL

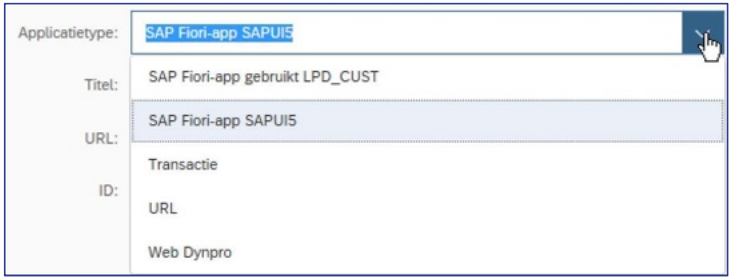


Fiori – Target Mapping

In the target mapping the combination of Semantic object and Action (= Intention) is linked to the app (= Target), transaction or Web Dynpro which has to be executed.

In the Target you can define the app, transaction or Web Dynpro which has to be started



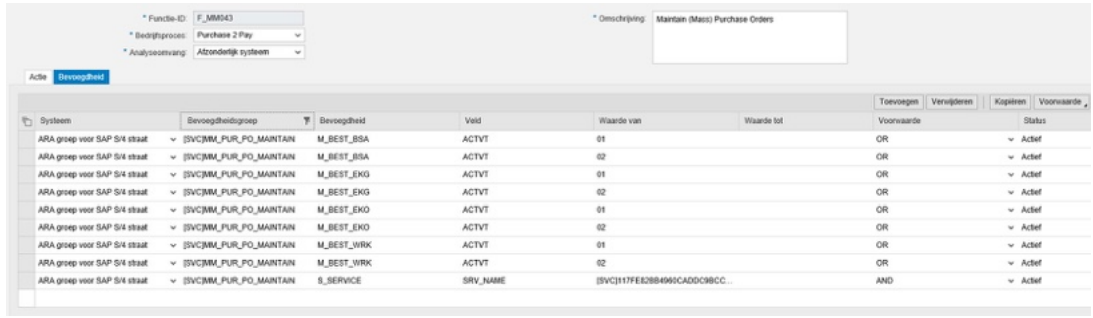


GRC Integration to S/4



GRC Ruleset Upgrade Approach for S/4HANA

- Download ruleset from GRC PRD in spreadsheet format
- Benchmark and analysis ruleset (Protiviti)
  - Disable obsolete tcodes
  - Modified authorization objects
  - New S/4 tcodes (S/4HANA 1809)
  - Generated FIORI oData services from table USOBHASH
  - Mapping FIORI apps to tcodes for placement in GRC function
  - FIORI apps without tcode mapping manual placement in GRC function
- Download active ruleset from GRC PRD (SPRO)
- Upload active ruleset to GRC DEV (SPRO)
- Append ruleset (VITENS_H) to GRC DEV on connector SAP_S4_LG (new adjustments from Protiviti analysis)
- Role level scan ECC PRD (validate new ruleset is still working on old system)
- Role level scan S/4 DEV (validate new ruleset works for new FIORI roles)
- Final acceptance Vitens



GRC Connection to S/4

Activities to connect to S/4 system

- Install GRC plug on S/4 system
- Extend sync jobs on GRC
- Configure GRC parameters on S/4
- Import S/4 function/task roles with attributes in GRC
- Extend business roles in GRC with S/4 composite roles (joiners/movers/leavers get S/4 authorizations)
- SPRO extensions for S/4 system (leaver process, connections, user parameters etc.)
- Create firefight roles in S/4
- Testing (unit test, UAT and production validation)



Issues

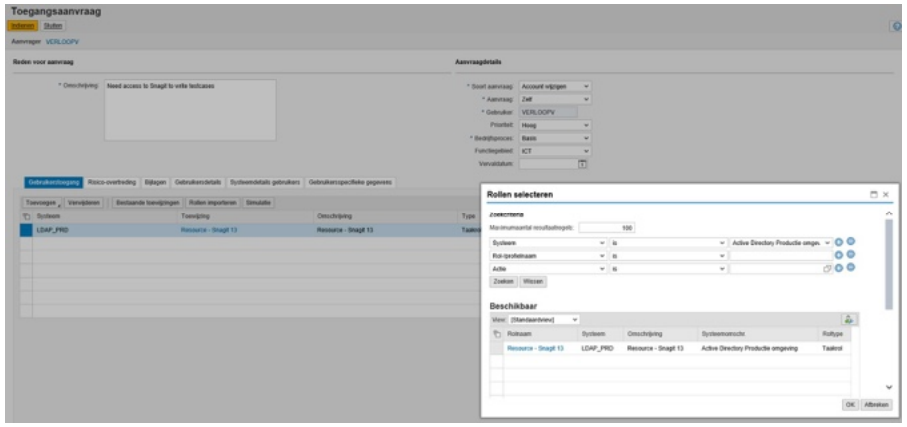
- Firefighters need to use FIORI launchpad instead of tcodes. We created composite roles per module with broad catalogues. Firefighters can login to S/4 and need to start tcode /UI/FLP for FIORI launchpad
- Link between oData services [SVC] and FIORI app [FAPP] is not transparent
- Link with FIORI app ID is also not available in the system
- Limited hits (false negatives) due to incorrect usage action tab, see note 2655122 for correct usage

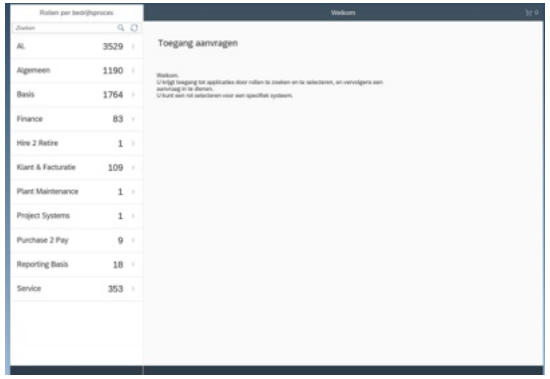
FIORI Access Request App



FIORI Access Request App

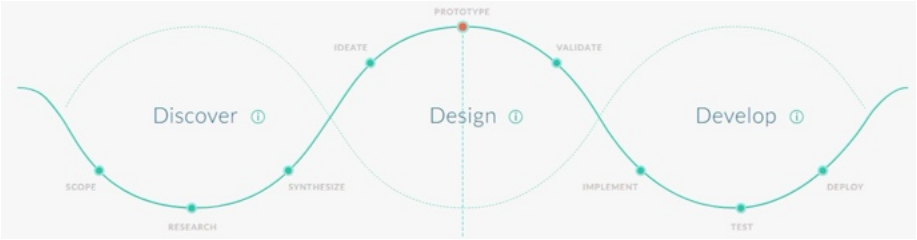
- Currently 90% of our access request is via the PBAC trigger and manual access requests are rare
- When expanding to Active Directory the expectation is that manual access request become more common (i.e. access to MS Visio etc.), thus the Access Request app becomes an important part of the IAM solution
- The current NWBC request app takes about 10 clicks to select the role
- GRC has a standard FIORI request app delivered in 12.0 but is not that user friendly
- Custom app development was necessary to meet expectations from the business

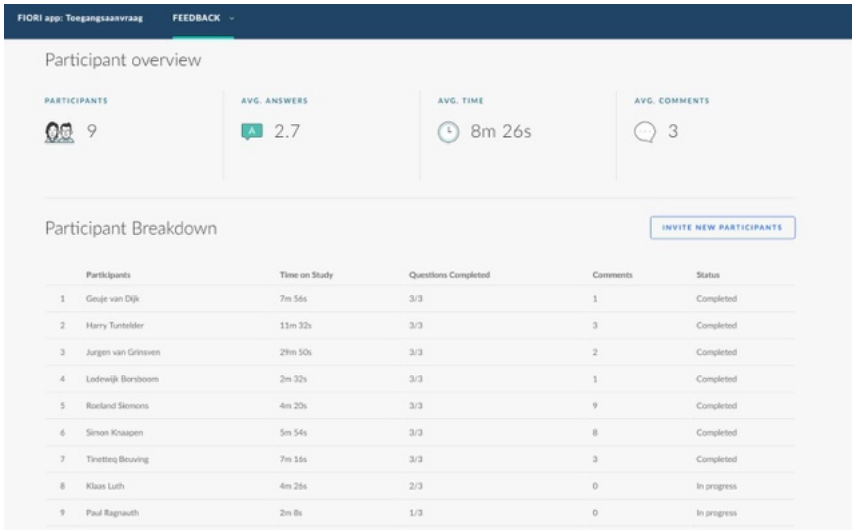




FIORI App Development Process

(supported by build.me)

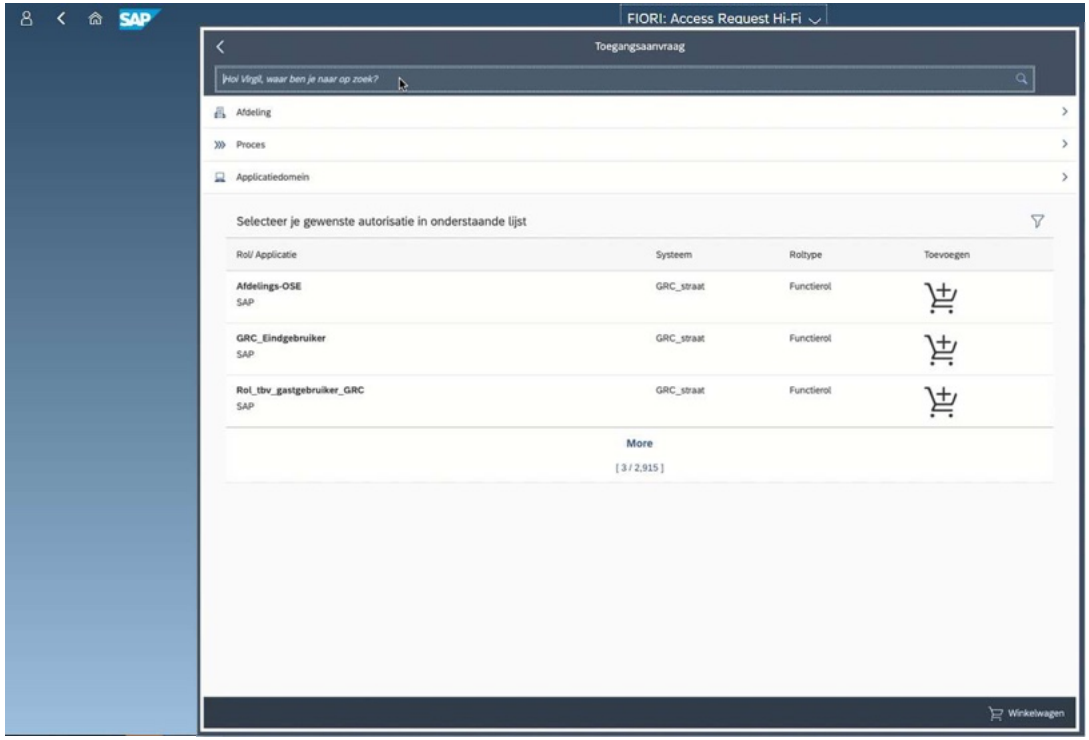






- Discover, design and develop
- Feedback from participants
- Heatmap to view hotspots

FIORI High-Fidelity Design



- Based on web shops:
  - Amazon.com
  - Coolblue.nl
- Search bar on top
- Navigate per category
- Use real data with Excel upload feature
- Collect feedback and iterate
- Transfer to SAP Cloud platform and connect oData services (role search/ order submission)
- Publish on GRC development
- Transport to GRC production

Provisioning to Active Directory/Legacy



Provisioning to Active Directory

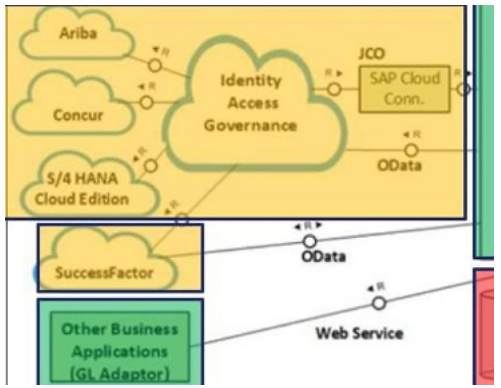
Provision on premise AD using SAP GRC AC

Extend business roles with AD “groups”

AD processes can make use of the existing processes for:

- Joiners/Movers/Leavers/Updates
- Business Role model
- User Access Review
- SoD Review (AD critical access risks)
- Access Request process
- Reporting

Azure Cloud can be provisioned via the Identity Access Governance cloud



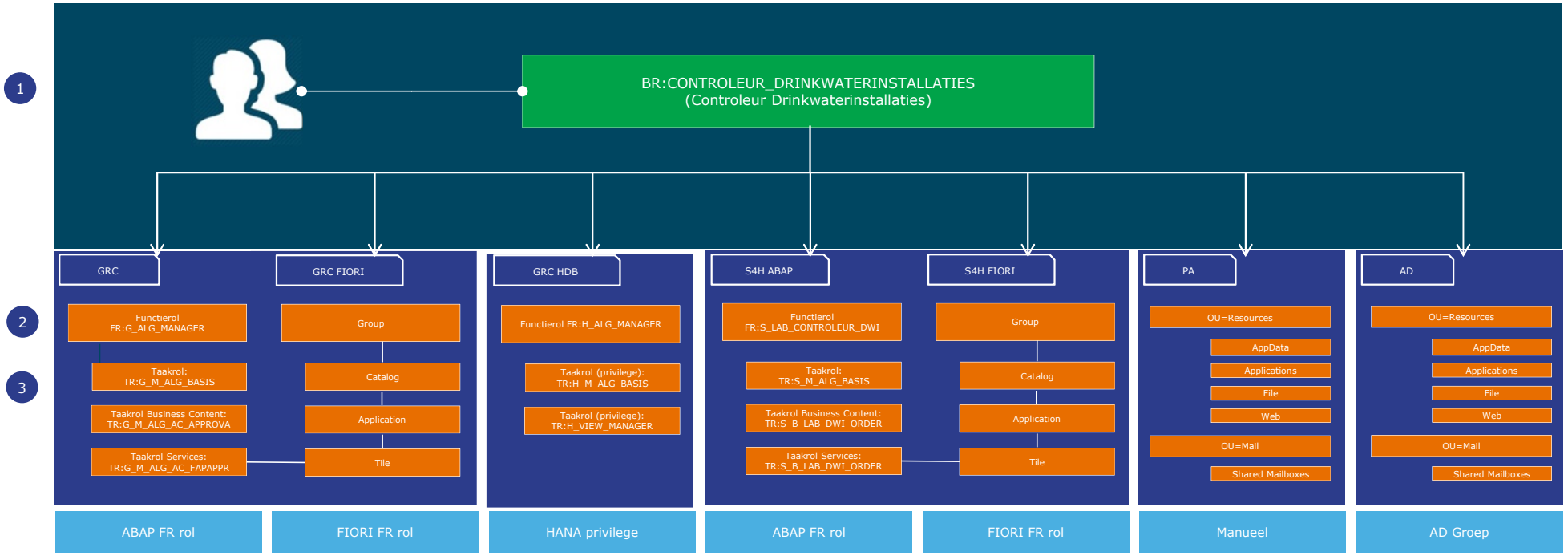
Manual Provisioning



Nr	User or Role Data Type	Logische padnaam	Omschrijving	Sytax -groep	Fysiek pad	Fys. Bestand	File ID
1	Action Master	Z_PA_ACTION	File Connector for PA Actions	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_ACTION.TXT	LEGACY_ACTION
2	Permission Master	Z_PA_PERMISSION	File Connector for PA Permissions	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_PERMISSION/TXT	LEGACY_PERMISSION
3	Profile Master	Z_PA_PROFILES	File Connector for PA Profiles	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_PROFILE.TXT	LEGACY_PROFILE
4	Profile Action	Z_PA_PROFILE_ACTIONS	File Connector for PA Profile Actions	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_ACTIONS.TXT	LEGACY_ACTIONS
5	Profile Permission	Z_PA_PROFILE_PERMISSIONS	File Connector for PA Profile Permissions	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_PROFILE_PERMISSION.T	LEGACY_PROFILE_PERMISSION
6	Role Master	Z_PA_ROLES	File Connector for PA Roles	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_ROLE.TXT	LEGACY_ROLE
7	Role-Action	Z_PA_ROLE_ACTIONS	File Connector for PA Role Actions	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_ROLE_ACTION.TXT	LEGACY_ROLE_ACTION
8	Role-Permission	Z_PA_ROLE_PERMISSIONS	File Connector for PA Role Permissions	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_ROLE_PERMISSION.TXT	LEGACY_ROLE_PERMISSION
9	User Master	Z_PA_USERS	File Connector for PA Users	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_DEFAULT_USER.TXT	LEGACY_DEFAULT_USER
10	User Action	Z_PA_USER_ACTIONS	File Connector for PA User Actions	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_USER_ACTION.TXT	LEGACY_USER_ACTION
11	User Permission	Z_PA_USER_PERMISSIONS	File Connector for PA User Permissions	UNIX	/usr/sap/trans/PA/<FILENAME>	LEGACY_USER_PERMISSION.TXT	LEGACY_USER_PERMISSION

- Legacy system connector
- File based provisioning

GRC Business Role Hierachy



1) Business role (can be requested in GRC) - owner
2) Function role (can be requested in GRC) - owner
3) Task role (can be requested in GRC) – owner

IAM Chain - User Creation (part 1)

1. Create on boarding (HR portal)
2. Processing in HR backend system
3. GRC detects new employee and generates User ID/Mail on GRC
4. GRC writes User ID/Mail back to HR backend system
5. GRC triggers joiner process based on IT0105-0001 and creates access request
6. User creation with all relevant attributes in GRC system
7. LDAP SYNC creates user in Active Directory with all relevant attributes
8. Active Directory script enables account, creates home drive and moves to correct OU and syncs account to Azure AD (cloud)
9. Azure AD generates mailbox and Office 365

IAM Chain - Authorizations Assignment (part 2)

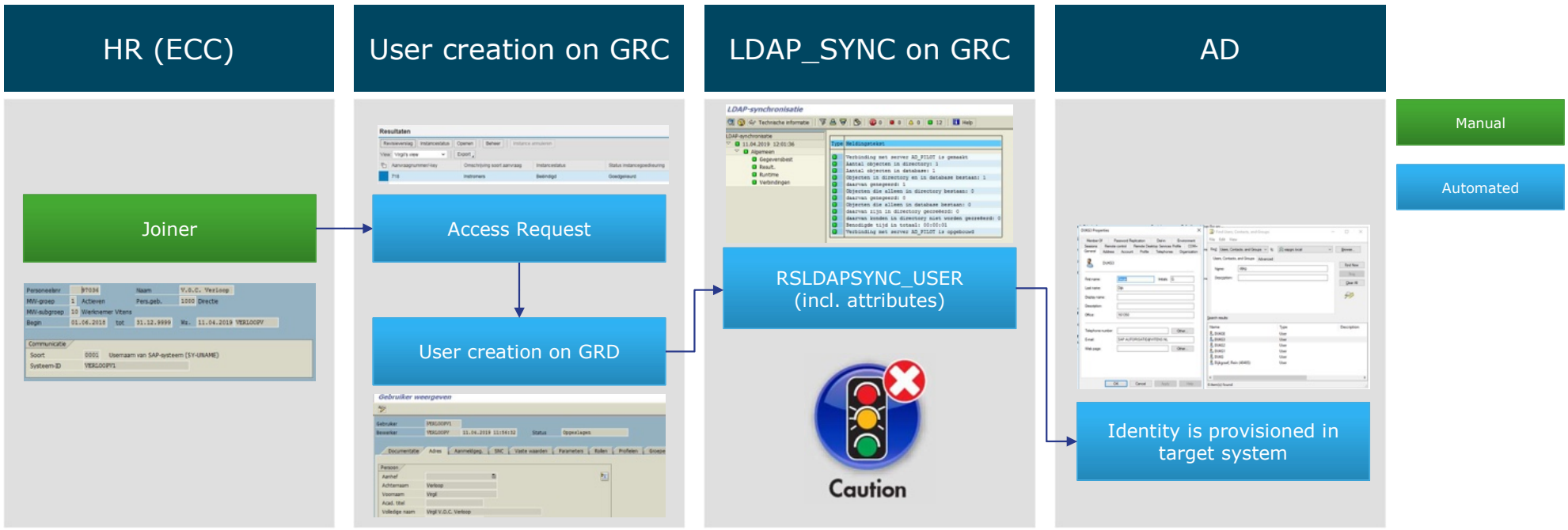


1. Pre Employment Screening (PES) needs to be completed by HR
2. HR sets PES indicator to OK in HR system
3. GRC generates second trigger and assigns authorization based on PBAC
4. GRC generates initial password
5. Initial Windows password is sent to manager via e-mail

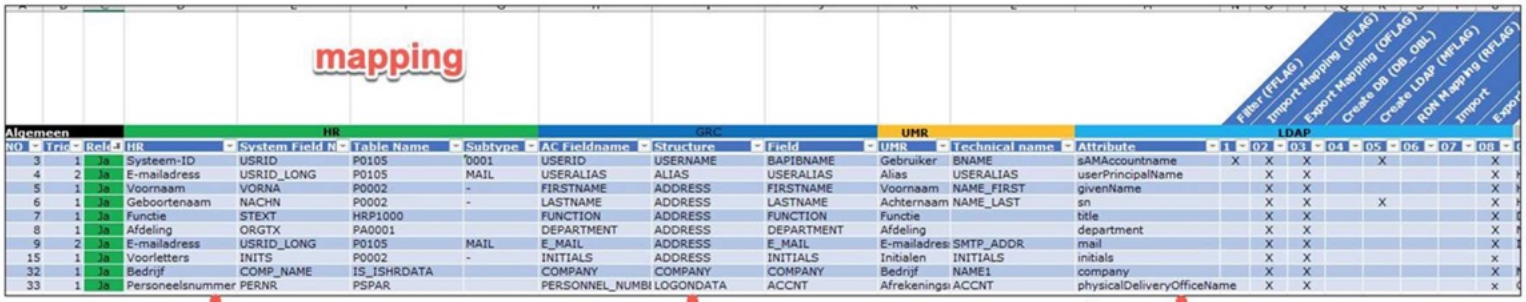


6. Provisioning to target systems (SAP and non SAP)
7. Welcome e-mail is sent to new employee

AD account creation



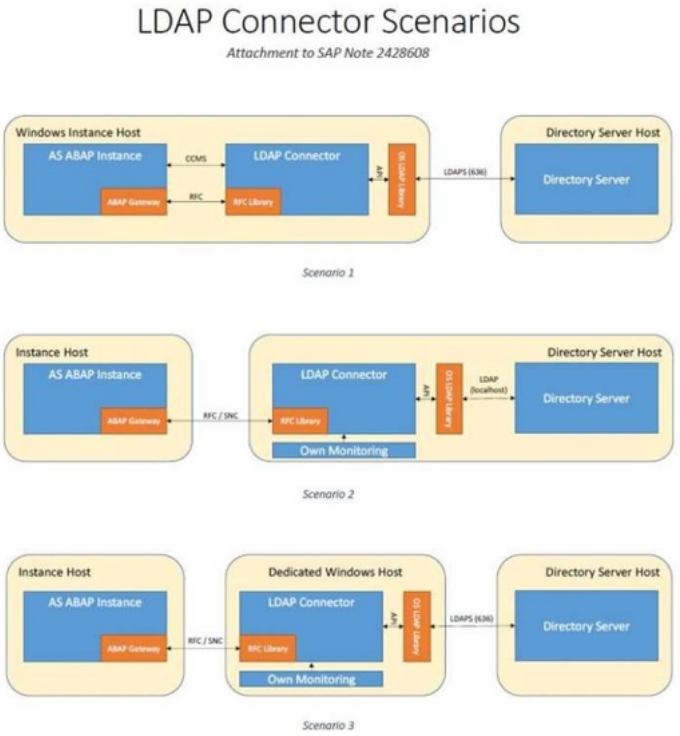
Attribute mapping HR ➔ GRC ➔ UMR ➔ LDAP (AD)





Secure LDAP with LDAPS

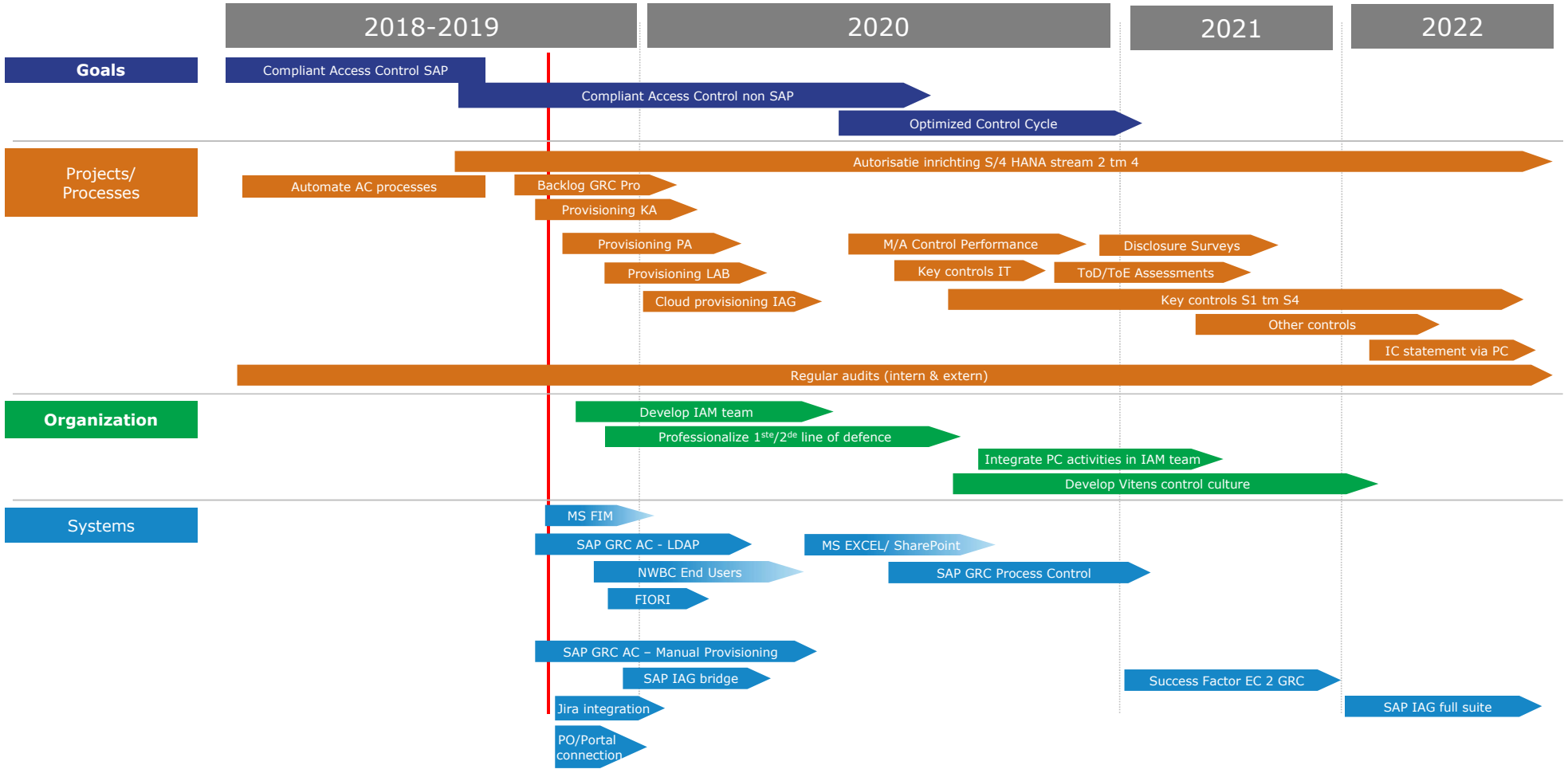
- Within Vitens there are new guidelines on security hardening. One of them is that all LDAP communications need to be secured via LDAPS
- The LDAP connector in SAP GRC does not implement the LDAP protocol itself but uses the LDAP client library of the Operating System
- There are 3 scenario's available, see image
- Vitens will use scenario 3 because we are on linux and we don't want extra software on the Directory Server
- See SAP Note 2428608 for further information



Roadmap IAM & GRC



Roadmap GRC & IAM



Wrap-up



Where to Find More Information

- https://help.sap.com/viewer/product/SAP_ACCESS_CONTROL/12.0.03/en-US
  - Access Control help page
- https://help.sap.com/viewer/product/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE/latest/en-US
  - Identity & Access Governance help page
- https://wiki.scn.sap.com/wiki/display/GRC/GRC+10.0+-+HR+Trigger+configuration
  - HR trigger wiki
- https://blogs.sap.com/2016/05/02/connecting-sap-grc-ac-10x-to-microsoft-active-directory/
  - Blog explaining how to connect GRC to AD

Key Points to Take Home

- The “Default Roles” feature can help to create system wide business roles and can maximize automation in your joiner process
- Automate your attestations to keep your solution healthy
- Treat your ruleset as masterdata and activate risk and function approvals for a closed audit loop
- SAP Lumira is free for GRC and can visualize your solution the way you want
- Active Directory can be integrated using the standard LDAP(S) connector
- Don’t forget Business Role Management to optimize your rolemangement process



Your Turn!

Tinette Beuving
Virgil Verloop

tinette.beuving@vitens.nl
virgil.verloop@profilus.nl







Thank You
Any Questions?

Please remember to complete your session evaluation

Disclaimer

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.



Wellesley Information Services, 20 Carematrix Drive, Dedham, MA 02026
Copyright © 2019 Wellesley Information Services. All rights reserved.