soterion

ACCESS RISK MANAGER

Access Risk Manager: Identify Risk

Gain insight into your SAP access risks with business-friendly reporting.

SAP Access Risk Analysis — Incorporating Transactional Usage

Soterion for SAP analyses users' authorizations and incorporates the user's historical transactional usage data to differentiate between the potential and the actual access risks. This allows business to focus on the real access risk in the SAP environment.

Business-friendly SAP Access Risk Reporting

Soterion for SAP allows the organisation to view data from every angle by using drag and drop functionality for grouping and filtering. Graphical overviews show the organisation's access risk landscape, including high-risk areas, in relation to risk tolerance and appetite levels. Reporting on SAP access risks at department level makes it easy to define the responsibility of ownership.

Access Risk Manager: Get Clean

Remediate SAP access risks with minimal business interruption using powerful data analytics.

Resolution-driven Gap Analysis Reporting

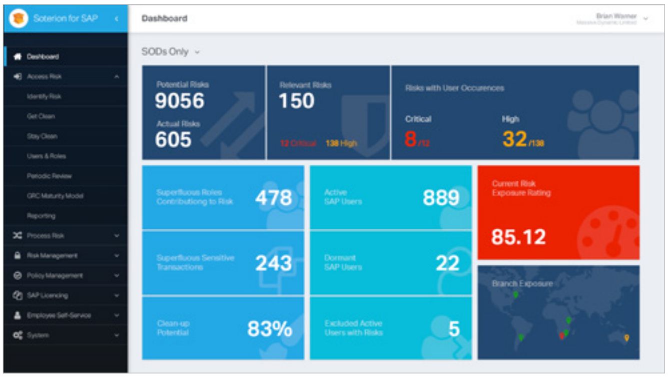
Soterion for SAP performs a Gap Analysis between potential SAP access risk and the actual SAP access risk in your authorization environment. Identifying and resolving this superfluous access is the first step in taking control of your SAP authorization landscape. Any redundant user access can then be remediated without business interruption and allows business to focus on the real access risk. Redundant user access typically contributes to 80% of the access risks in an SAP environment.

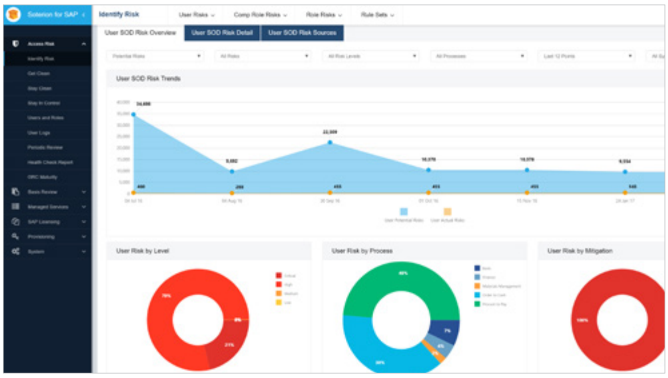
Risk Clean-up Wizards

The Risk Clean-up Wizards provide clear, focused, step-by-step suggestions on how to eradicate access risks, from the removal of superfluous allocations to the splitting of roles based on role usage analytics.

SAP Access Risk Clean-up Projection

The Risk Clean-up Projection view estimates to which degree your SAP Authorization solution can be cleaned up using Soterion for SAP's methodology. The clean-up actions focus initially on the removal of unused access contributing to risk, ensuring significant risk remediation with minimal impact on business.





Get Clean: User Risk Overview

The majority of access risk in a SAP environment is caused by functionality that is assigned to a user but is not being used. Soterion for SAP's Gap Analysis functionality enables you to align your authorization solution to what the users are actually doing in the system, thus allowing you to focus on the real access risk in your SAP environment.

Access Risk Manager: Stay Clean

Simulates "What-if" scenarios prior to making the changes in SAP - business approval is done using workflow.

Allocation Simulations and "What-If" Analysis

Soterion for SAP allows for the simulation of SAP authorization changes prior to effecting the changes in SAP. By incorporating the user's transactional usage history, business is empowered to make better access risk decisions. Change control ensures business approval of authorization changes, together with the risk impact.

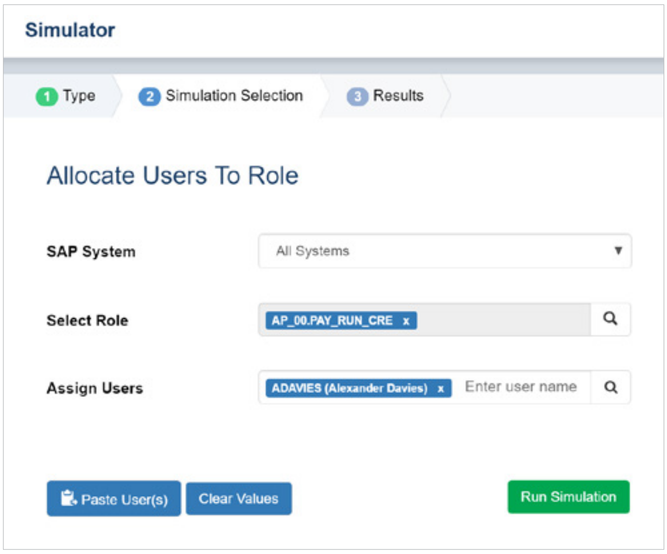
"Out-the-Box" Rule Set that is Fully Customisable

Soterion for SAP comes with an 'out-the-box' access risk rule set based on best practice for all industries. The rule set is easily customisable to cater for an organisation's specific needs.

Mitigating Controls

Soterion for SAP's unique Gap Analysis functionality enables business to focus on mitigating the actual SAP access risks. Business can graphically view the mitigation status of identified risks.

The Control Library is a central repository of mitigating controls, allowing business to easily and effectively mitigate access risk through default controls and workflow functionality.



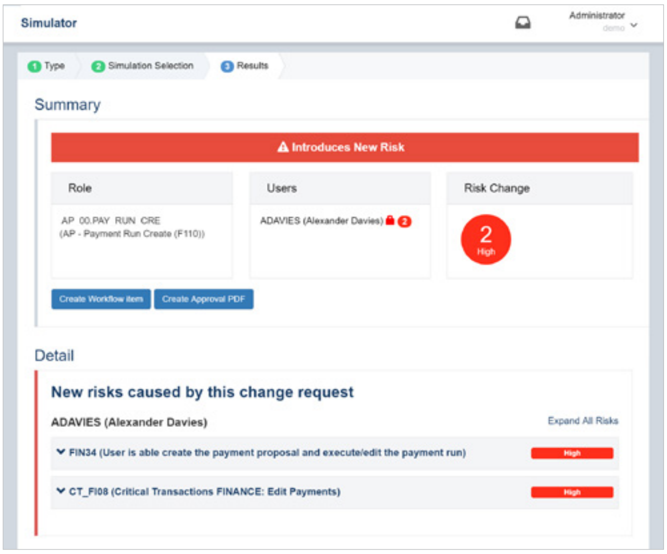
Allocate Users To Role

SAP System: All Systems

Select Role: AP_00.PAY_RUN_CRE x

Assign Users: ADAVIES (Alexander Davies) x Enter user name

Simulation



Summary

Introduces New Risk

Role	Users	Risk Change
AP 00.PAY RUN CRE (AP - Payment Run Create (F110))	ADAVIES (Alexander Davies) 2	2 High

Detail

New risks caused by this change request

ADAVIES (Alexander Davies)

- FIN34 (User is able create the payment proposal and execute/edit the payment run) High
- CT_FI08 (Critical Transactions FINANCE: Edit Payments) High

Simulation Result

Stay Clean: Allocation Simulator

Ensure that the SAP Authorization solution remains clean going forward by simulating allocations prior to affecting these changes in SAP. Soterion for SAP's Allocation Simulator identifies whether these changes will introduce any new SAP access risk violations. These changes can be sent for approval using workflow, thereby ensuring that business accepts the new risk, as well as establishing audit trails for changes and risks.

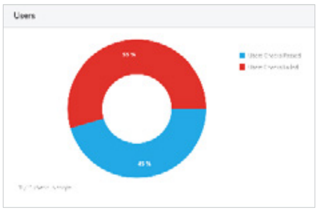
soterion

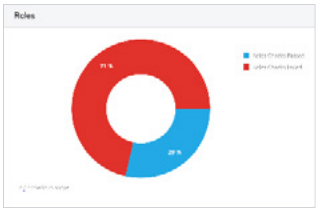
BASIS REVIEW MANAGER

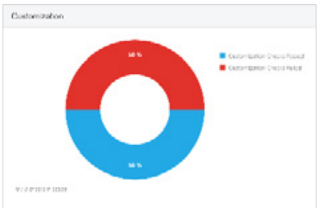
Inspecting the SAP Basis Configuration to Ensure Compliancy

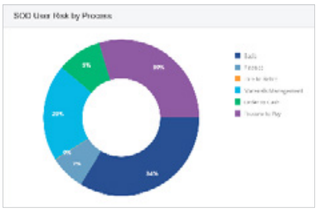
SAP Basis Configurations provide system-level controls to secure a SAP system. These configuration settings can be set up to be in line with your specific security requirements. The Soterion Basis Review Manager will inspect your SAP Basis Configuration against a set of rules that are based on industry best practices. Since these configurations usually form part of an annual external audit, our Basis Review Manager will allow you to be prepared, and will establish complete compliance to avoid adverse audit findings.

The Basis Review Manager consists of a number of checks that can be executed against your SAP system. The results will be highlighted as either passes or fails, with the option of mitigating failed reports. Examples of typical tests are:









Parameter Settings (RSPARAM)

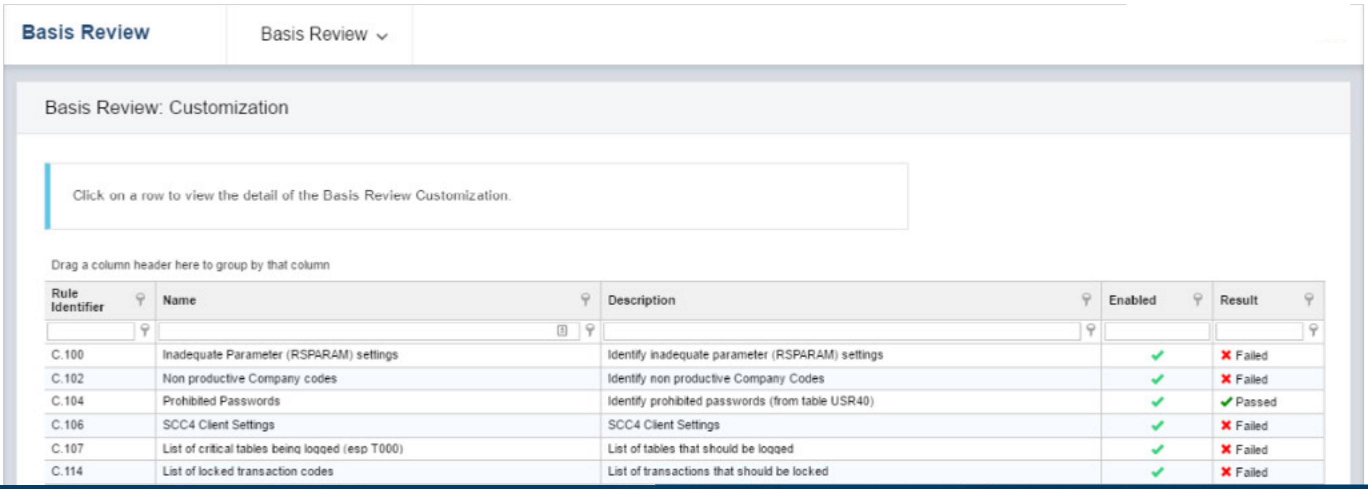
- ✓ Password lengths, expiry and complexity
- ✓ Restricting multiple logons
- ✓ Examining table logging

Role Checks

- ✓ Roles that are in the Production environment, but not assigned to users
- ✓ Roles that were created or changed in the Production environment
- ✓ Roles with wildcards for transactions

User Checks

- ✓ Users who have developer keys in the Production environment
- ✓ Test users who are working in the Production environment
- ✓ Users who have SAP standard roles in the Production environment



Basis Review: Customization

Click on a row to view the detail of the Basis Review Customization.

Drag a column header here to group by that column

Rule Identifier	Name	Description	Enabled	Result
C.100	Inadequate Parameter (RSPARAM) settings	Identify inadequate parameter (RSPARAM) settings	✓	✗ Failed
C.102	Non productive Company codes	Identify non productive Company Codes	✓	✗ Failed
C.104	Prohibited Passwords	Identify prohibited passwords (from table USR40)	✓	✓ Passed
C.106	SCC4 Client Settings	SCC4 Client Settings	✓	✗ Failed
C.107	List of critical tables being logged (esp T000)	List of tables that should be logged	✓	✗ Failed
C.114	List of locked transaction codes	List of transactions that should be locked	✓	✗ Failed

soterion

Let's talk: **info@soterion.com** **www.soterion.com**

soterion

ELEVATED RIGHTS MANAGER

Granting Sensitive Access in a Safe and Structured Environment

From time to time, users need temporary or emergency access for a limited period - often called **firefighter access**. This module allows you to do this effortlessly, while adhering to audit requirements.

Soterion's Elevated Rights Manager grants sensitive access in an automated workflow-driven process, and enables your management team to perform a structured review of any activities that were performed during the Elevated Rights Access check-out period.

Our Process

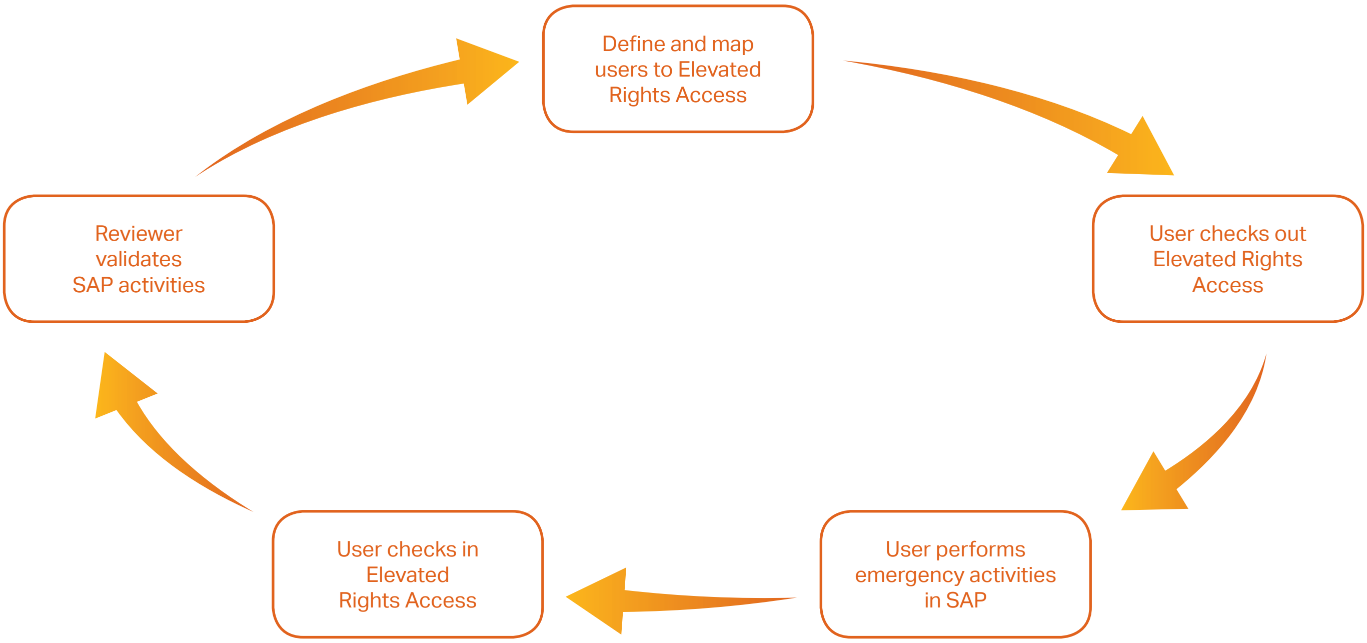
The Elevated Rights Manager can be tailored to your specific business environment. Elevated Rights Access may be granted to either a role or to an SAP user.

Elevated Rights Roles

Wide access roles can be assigned to pre-approved SAP Users when performing a check out. The particular SAP user will use their SAP User ID to perform the required activities in SAP.

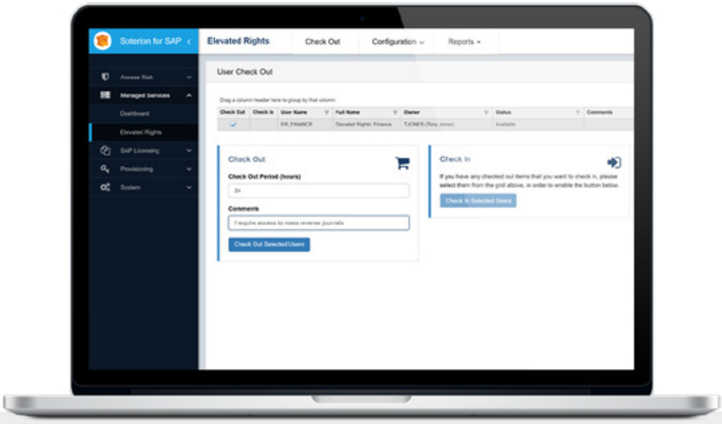
Elevated Rights SAP Users

An SAP user account containing requisite wide access will be unlocked, and the password will be sent to a pre-approved entitled SAP User. The relevant SAP User account will be used to perform the necessary activities in SAP.


Define and map users to Elevated Rights Access
User checks out Elevated Rights Access
User performs emergency activities in SAP
User checks in Elevated Rights Access
Reviewer validates SAP activities

Checking Out Elevated Rights Access

When a user performs a check out, the Elevated Rights Access will be assigned to them for a predefined period to enable them to perform the required emergency activities. Once completed, the user will be able to check the Elevated Rights Access back in. Alternatively, it will automatically be checked in once the allocated period has expired.



User Check Out

Drag a column header here to group by that column

Check Out	Check In	User Name	Full Name	Owner	Status	Comments
✓		ER_FINANCE	Elevated Rights: Finance	TJONES (Tony Jones)	Available	

Check Out

Check Out Period (hours): 24

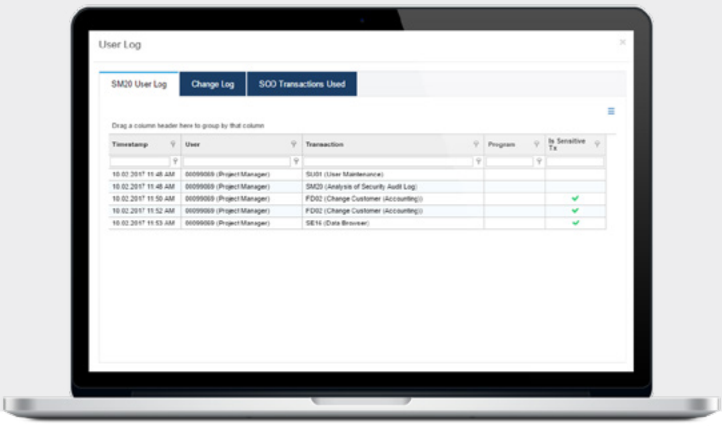
Comments: I require access to mass reverse journals

Check Out Selected Users

Check In

If you have any checked out items that you want to check in, please select them from the grid above, in order to enable the button below.

Check In Selected Users

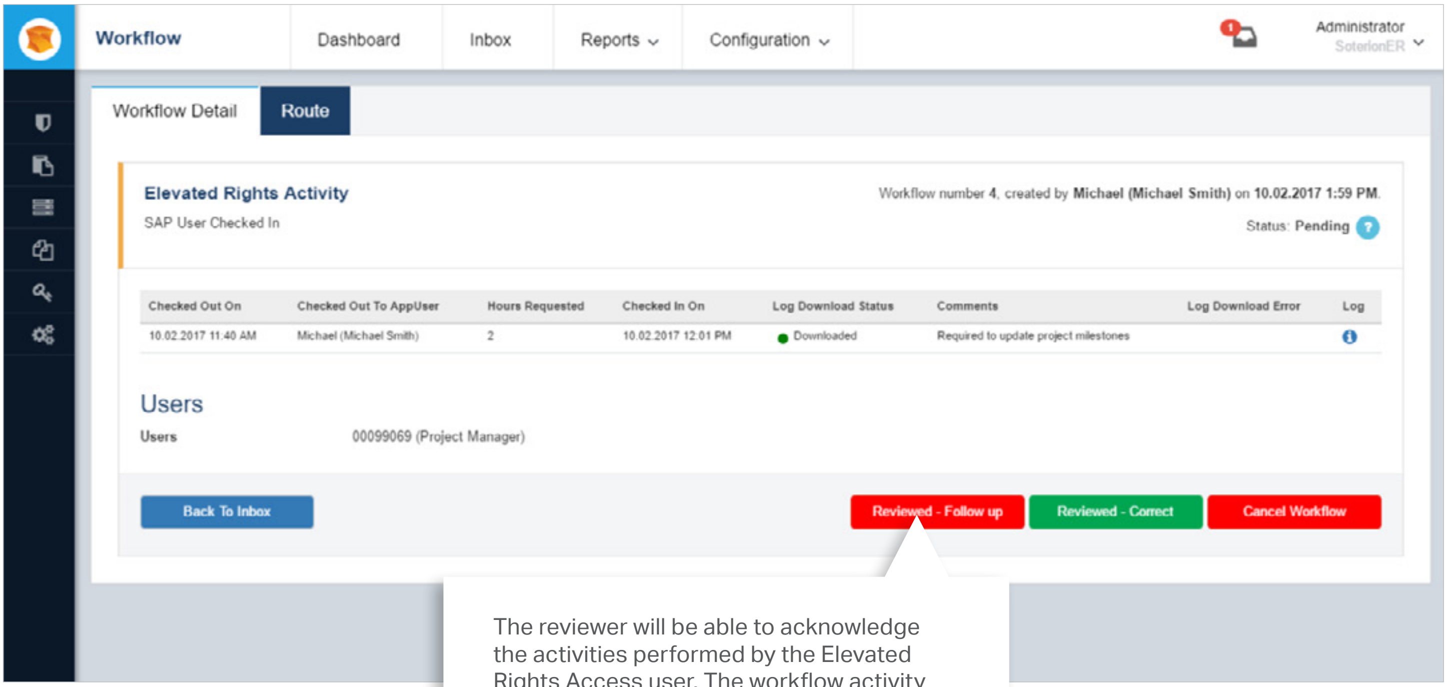

User Log

Drag a column header here to group by that column

Timestamp	User	Transaction	Program	Is Sensitive Tx
10.02.2017 11:48 AM	00099069 (Project Manager)	SU01 (User Maintenance)		
10.02.2017 11:48 AM	00099069 (Project Manager)	SM20 (Analysis of Security Audit Log)		
10.02.2017 11:50 AM	00099069 (Project Manager)	FD02 (Change Customer (Accounting))		✓
10.02.2017 11:52 AM	00099069 (Project Manager)	FD02 (Change Customer (Accounting))		✓
10.02.2017 11:53 AM	00099069 (Project Manager)	SE16 (Data Browser)		✓

Review of Elevated Rights Access Activities

All changes in SAP will be logged and downloaded to the Soterion Elevated Rights Manager for review. All transactions that were executed and any sensitive fields that were changed can be reviewed by the reviewer. Any sensitive transactions that were executed (SOD or Critical Transactions) will also be highlighted for their attention.



Elevated Rights Activity

SAP User Checked In

Workflow number 4, created by Michael (Michael Smith) on 10.02.2017 1:59 PM.

Status: Pending

Checked Out On	Checked Out To AppUser	Hours Requested	Checked In On	Log Download Status	Comments	Log Download Error	Log
10.02.2017 11:40 AM	Michael (Michael Smith)	2	10.02.2017 12:01 PM	● Downloaded	Required to update project milestones		ℹ

Users

Users 00099069 (Project Manager)

The reviewer will be able to acknowledge the activities performed by the Elevated Rights Access user. The workflow activity can be marked for **"Review - Follow up"** if there are any queries.

soterion

PERIODIC REVIEW MANAGER

Aligning Your GRC Capabilities with Your Business Objectives

Periodically reviewing your SAP user access, analysing the associated risks and evaluating the necessary controls will align your GRC capacity with your individual business targets. This process will significantly enhance the insight into your GRC environment, as well as being an audit and statutory requirement in many business environments.

A Mature GRC Capability Includes Periodically Reviewing a User's Access, Risks and Controls

The Periodic Review Manager provides a platform where user access reviews can be performed by business users in a simple, workflow-driven web environment while facilitating external rule set and control reviews.

Soterion's Periodic Access Review Manager ensures central control, but decentralised management throughout the entire user access review process.

Rule Set Review

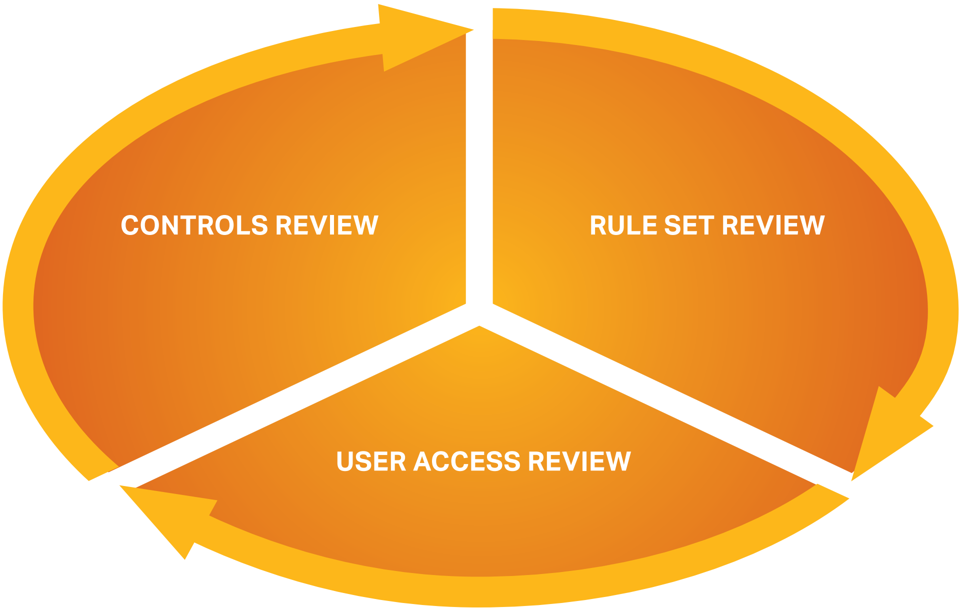
Regularly reviewing and updating your risk rule set will ensure continued relevancy in an evolving business environment.

Controls Review

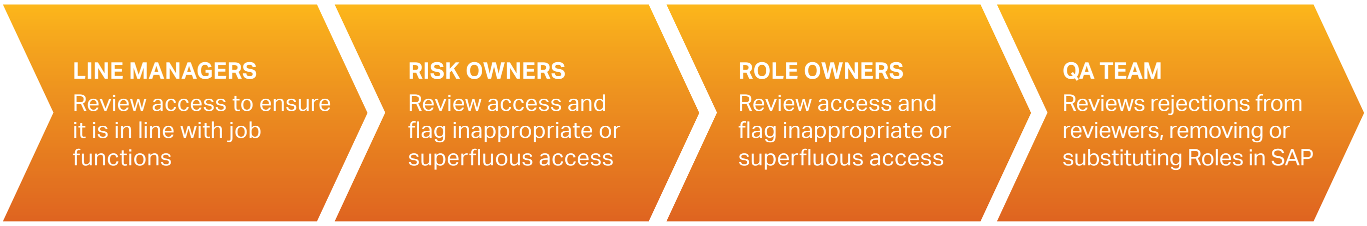
Periodic reviews will consistently optimise the efficiency of your mitigating controls by identifying any gaps in control effectiveness.

User Access Review

Review your SAP user access allocations to ensure that all assignments are still relevant. Recertify user access by identifying and removing redundant and superfluous access.



Persons Involved in a Review



LINE MANAGERS
Review access to ensure it is in line with job functions

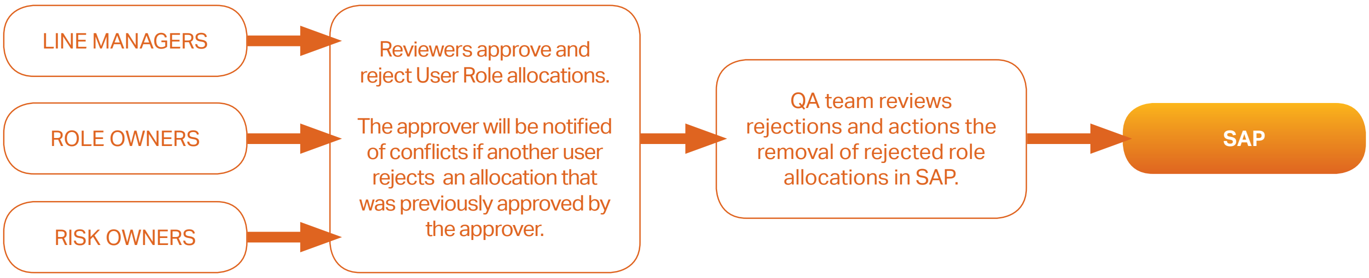
RISK OWNERS
Review access and flag inappropriate or superfluous access

ROLE OWNERS
Review access and flag inappropriate or superfluous access

QA TEAM
Reviews rejections from reviewers, removing or substituting Roles in SAP

Any combination of line managers, risk owners and role owners may accept or reject user role allocations in the context of a particular risk scenario. Business users will be able to participate from any web-enabled device. The Administrator will have access to an illustrated view of the overall progress of all reviewers. Queries and disputes can be effectively regulated, and business users will be regularly updated via email.

The Review Process



LINE MANAGERS

ROLE OWNERS

RISK OWNERS

Reviewers approve and reject User Role allocations.

The approver will be notified of conflicts if another user rejects an allocation that was previously approved by the approver.

QA team reviews rejections and actions the removal of rejected role allocations in SAP.

SAP

A review set is a snapshot of the user access landscape in SAP at the time of its creation. Each review set also contains a list of owners and approvers for users, risks and roles.

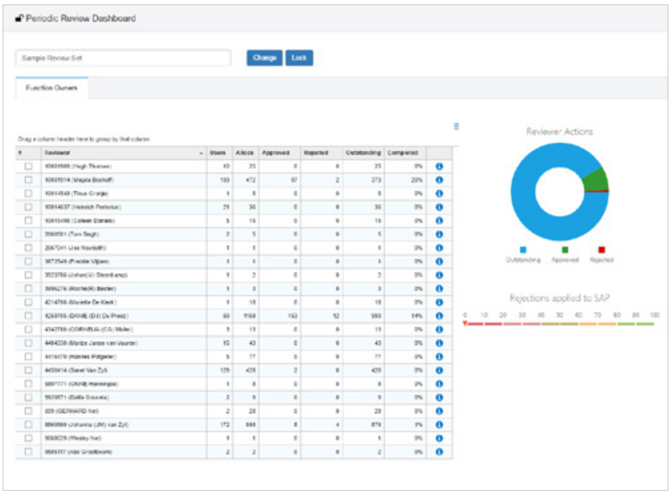
Reviewers can Perform User Role Approvals and Rejections

An automated email from the Administrator will prompt all relevant users to participate in the review process by simply logging into their Review Inbox from any web-enabled device and using the URL specified in the email.

When logging in, the user will be presented with an Inbox that will detail the role allocations and associated risks in separate tabs.

The user can approve or reject role allocations and if necessary, will be able to add comments.

The user will be able to view (and revert) allocations that were previously approved or rejected by them. The user will have access to view and remediate allocations where conflicts exist — that is allocations that were previously approved, but have been rejected by another user.



Periodic Review Dashboard

Sample Review Set

Drag a column header here to group by that column

	Reviewer	Users	Allocs	Approved	Rejected	Outstanding	Completed	
□	10001569 (Hugh Thomas)	10	25	0	0	25	0%	ℹ
□	10001014 (Magda Boshoff)	103	472	97	2	373	20%	ℹ
□	10014549 (Tinus Cronje)	1	5	0	0	5	0%	ℹ
□	10014637 (Heinrich Pretorius)	29	36	0	0	36	0%	ℹ
□	10015490 (Coleen Daniels)	5	15	0	0	15	0%	ℹ
□	2060501 (Tom Singh)	2	5	0	0	5	0%	ℹ
□	2067041 (Jan Noordhoff)	1	1	0	0	1	0%	ℹ
□	3572549 (Freddie Viljoen)	1	1	0	0	1	0%	ℹ
□	3523786 (Johan(J) Steenkamp)	1	2	0	0	2	0%	ℹ
□	3996276 (Roche(R) Bester)	1	3	0	0	3	0%	ℹ
□	4214766 (Mariette De Klerk)	1	18	0	0	18	0%	ℹ
□	4250765 (DANIE (DJ) Du Preez)	60	1158	163	12	983	14%	ℹ
□	4342788 (CORNELIA (C.G.) Muller)	3	15	0	0	15	0%	ℹ
□	4484338 (Marize Janse van Vuuren)	15	43	0	0	43	0%	ℹ
□	4416479 (Hannes Potgieter)	5	77	0	0	77	0%	ℹ
□	4435414 (Sarel Van Zyl)	129	428	2	0	426	0%	ℹ
□	5897771 (OKKIE Hanekom)	1	8	0	0	8	0%	ℹ
□	5920671 (Della Gouws)	2	9	0	0	9	0%	ℹ
□	609 (GERHARD Nel)	2	29	0	0	29	0%	ℹ
□	8860668 (Johanna (JM) van Zyl)	172	888	8	4	876	1%	ℹ
□	9068029 (Wesley Nel)	1	1	0	0	1	0%	ℹ
□	9989117 (Abe Grootboom)	2	2	0	0	2	0%	ℹ

EMPLOYEE SELF-SERVICE MODULE

SAP User Role Provisioning will be Revolutionised by Soterion's Employee Self-Service (ESS) Module

Soterion's ESS Module will enable you to decentralise the provisioning of SAP user access. This functionality will reduce the time it takes users to obtain their required access, as well as lowering the costs associated with having large SAP Security teams to support the user provisioning process in your business.

Role Provisioning

Roles in SAP can either be assigned directly to a user's SAP User ID or via their SAP HR position. Soterion's Business Role option will provide you with an alternative and more efficient method of provisioning access to users.

A Business Role is a role container in our system that includes all the applicable single and composite roles for a specific job function. It is similar to the SAP Composite role, but has the following benefits for your business:

Standardisation and Flexibility

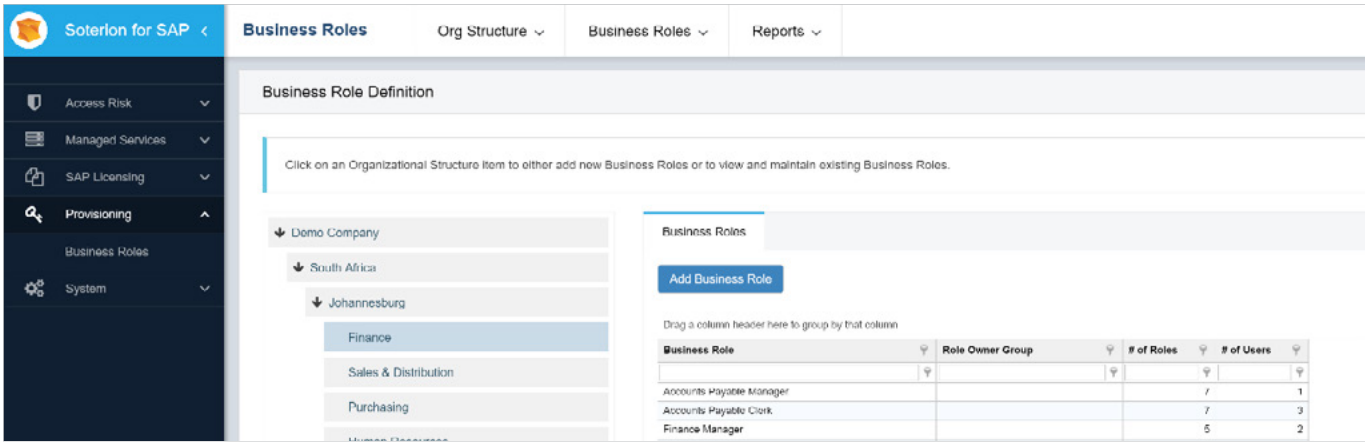
Business Roles will enable the standardisation of job functions, while facilitating the removal of irrelevant access to a specific user's job function.

Effortless Navigation

Soterion's Organisational Structure gives the user easy access to the required results.

Provisioning Using the Business Role Concept

The Business Role concept resides in an organisational structure within the Soterion application. This will enable specific SAP Roles to be assigned to the applicable Business Roles, consequently simplifying the selection process for all relevant users.



Business Role Definition

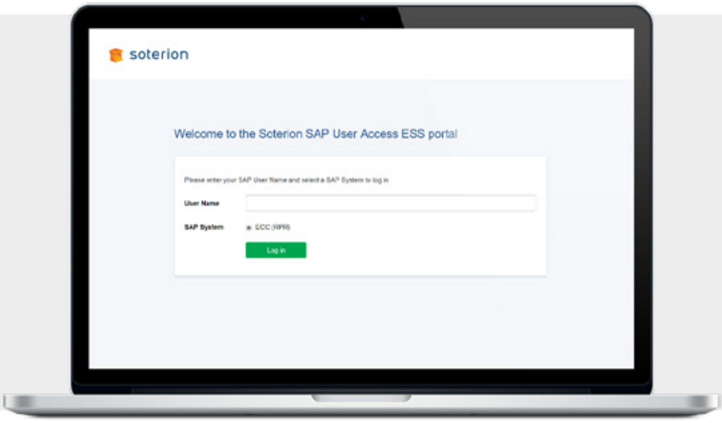
Click on an Organizational Structure item to either add new Business Roles or to view and maintain existing Business Roles.

Drag a column header here to group by that column

Business Role	Role Owner Group	# of Roles	# of Users
Accounts Payable Manager		7	1
Accounts Payable Clerk		7	3
Finance Manager		5	2

Soterion’s ESS Module

Users may access the Soterion ESS portal from any web browser in order to provision access to themselves or to other users.



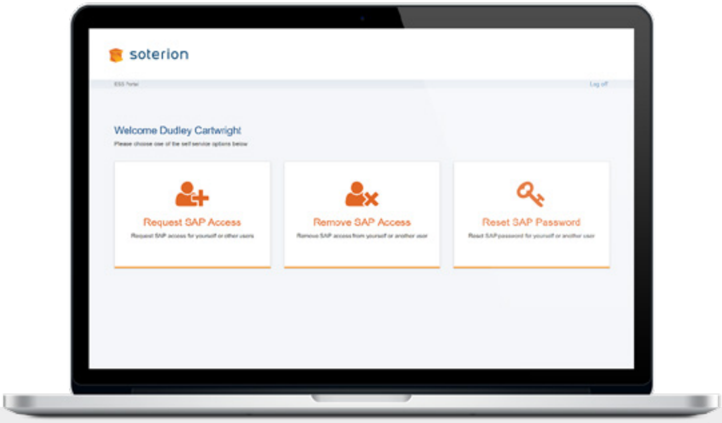
soterion

Welcome to the Soterion SAP User Access ESS portal

Please enter your SAP User Name and select a SAP System to log in

User Name

SAP System ● ECC (RPR)



soterion

ESS Portal

Welcome Dudley Cartwright

Please choose one of the self service options below

Request SAP Access
Request SAP access for yourself or other users

Remove SAP Access
Remove SAP access from yourself or another user

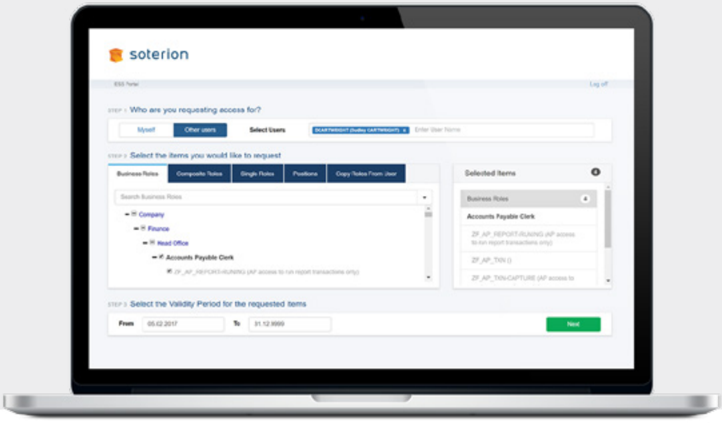
Reset SAP Password
Reset SAP password for yourself or another user

ESS will enable users to:

- ✓ Request additional SAP access
- ✓ Remove existing SAP access
- ✓ Reset SAP passwords

ESS users will be able to provision access to users using the following options:

- ✓ Business Roles
- ✓ SAP Composite Roles
- ✓ SAP Single Roles
- ✓ SAP HR Positions



soterion

ESS Portal

STEP 1 Who are you requesting access for?

Select Users: DCARTWRIGHT (Dudley CARTWRIGHT) × Enter User Name

STEP 2 Select the items you would like to request

Search Business Roles

- Company
  - Finance
    - Head Office
      - Accounts Payable Clerk
        - ZF_AP_REPORT-RUNING (AP access to run report transactions only)

Selected Items 4

Business Roles

Accounts Payable Clerk

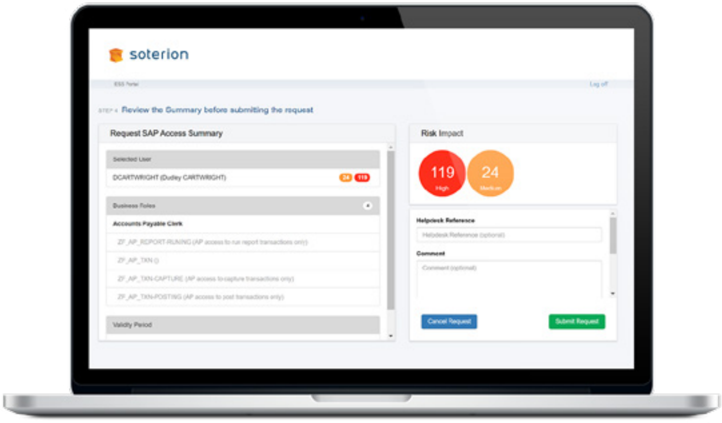
ZF_AP_REPORT-RUNING (AP access to run report transactions only)

ZF_AP_TXN ()

ZF_AP_TXN-CAPTURE (AP access to

STEP 3 Select the Validity Period for the requested items

From 05.02.2017 To 31.12.9999



soterion

ESS Portal

STEP 4 Review the Summary before submitting the request

Request SAP Access Summary

Selected User

DCARTWRIGHT (Dudley CARTWRIGHT) 24 119

Business Roles

Accounts Payable Clerk

ZF_AP_REPORT-RUNING (AP access to run report transactions only)

ZF_AP_TXN ()

ZF_AP_TXN-CAPTURE (AP access to capture transactions only)

ZF_AP_TXN-POSTING (AP access to post transactions only)

Validity Period

Risk Impact

119 High

24 Medium

Helpdesk Reference: Helpdesk Reference (optional)

Comment: Comment (optional)

The ESS module will perform a Risk Impact Analysis on the proposed request.

A workflow task will be created for the change request and will automatically be provisioned in SAP once it is approved.

soterion

SOTERION SAP LICENSING MANAGER

Optimise Expenditure and Retain Compliance by Taking Control of Your SAP License Management

SAP License Management is a crucial element in creating an economical and compliant strategy for effective software asset management. Soterion's SAP Licensing Manager can provide you with the insight you need to tailor your SAP license agreement to your organisation's specific requirements, ensuring optimal contract management and complete compliance whilst reducing unplanned and excess costs.

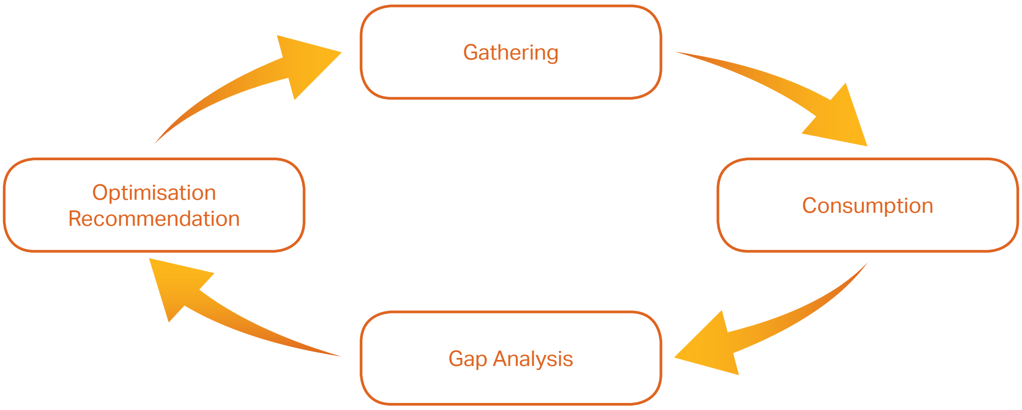
Our Background

Our specialised experience and in-depth comprehension of pre-SAP license audits ensure that our clients can confidently monitor productivity and manage cost, while governing SAP license compliance.

Key Points

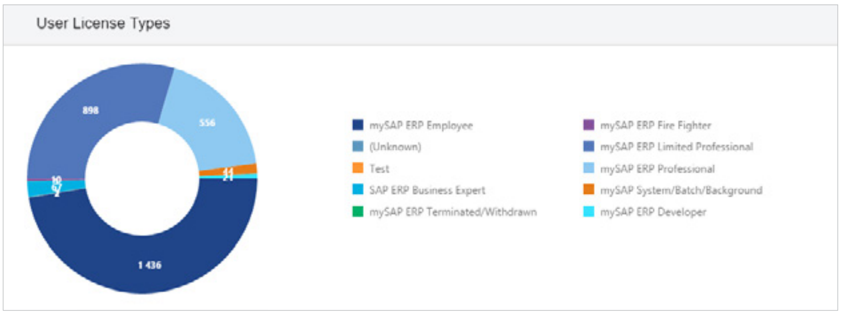
Our Approach

- ✓ **Gathering (Bill of Material)**
  Collate SAP license agreements and compare with SAP License Bill of Material.
- ✓ **Gap Analysis**
  Compare the consumption figures with the Bill of Material and determine whether it is within licensing thresholds to avoid facing unplanned excess charges.
- ✓ **Consumption**
  Determine configuration and usage of various licensing categories.
- ✓ **Optimisation Recommendations**
  Determine optimisation opportunities based on the actual usage of license categories. This will include activities such as locking or expiring dormant user accounts.



SAP Licensing Categories typically fall into the following areas:

- ✓ Named users (including indirect usage)
- ✓ Master records
- ✓ Throughput
- ✓ Hardware



User License Optimisation Recommendations

User Maintenance

- ✓ Dormant users
- ✓ Users locked and not expired
- ✓ Users never logged on

User Classification

- ✓ **Users inconsistently classified** are deemed to be in the higher license category by SAP. Named SAP user licenses must be aligned across the various SAP systems.
- ✓ **Users not classified** will be categorised by SAP as a Professional license type (high end category) during the annual license audit.

45

USERS LOCKED, BUT NOT EXPIRED
These Users are locked, but have not been expired by changing their “Valid To” dates. A User that is locked, but not expired, is considered to be an active SAP Named User.

612

USERS NEVER LOGGED ON
These Users have never logged on to the SAP System. Consider whether these accounts could be locked and expired.

User Classification

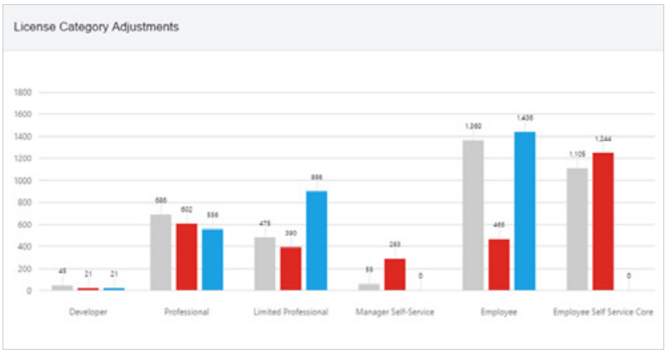
- ✓ **Users inconsistently classified** are deemed to be in a higher license category by SAP. Named SAP user licenses must be aligned across the various SAP systems.
- ✓ **Users not classified** will be categorised by SAP as a Professional license type (high end category) during the annual license audit.

User License Category Adjustment Recommendations

The graph summarises the reclassification recommendations based on usage.

Since it is not possible to include the SAP user usage data in the classification process in the standard version of SAP, most SAP clients follow the SAP license classifications methodology that is based on role allocations. This methodology can be used successfully if the specific SAP roles allocated to users are well aligned with what the users are indeed doing in SAP.

However, research shows that SAP users on average use only 20% of the functionality allocated to them, resulting in the unnecessary allocation of higher SAP license categories access to the majority of users (80%).



Going Forward

Soterion SAP Licensing Manager uses its database as a repository for future SAP license reviews, hence reducing the time and resources you will require to maintain your SAP licenses.

Our solution also allows you to store agreements, documents and notes to demonstrate your SAP license compliance which will minimise the number of consulting days you will need on future SAP licensing audits.