Role Risks
Rule Sets
Administrator
Relevant Risks
154
Actual Risks
1,475
Show Clean-up Projections
Critical
High
Active SAP Users
201
Current Risk Exposure Rating
24.27
Superfluous Roles Contributing to Risk
1,818
Dormant SAP Users
5
Superfluous Sensitive Transactions
1,034
Excluded Active Users with Risks
0
Clean-up Potential
46%

SOTERION SAP **ACCESS RISK ASSESSMENT**

- Segregation of Duty
- Critical Transaction

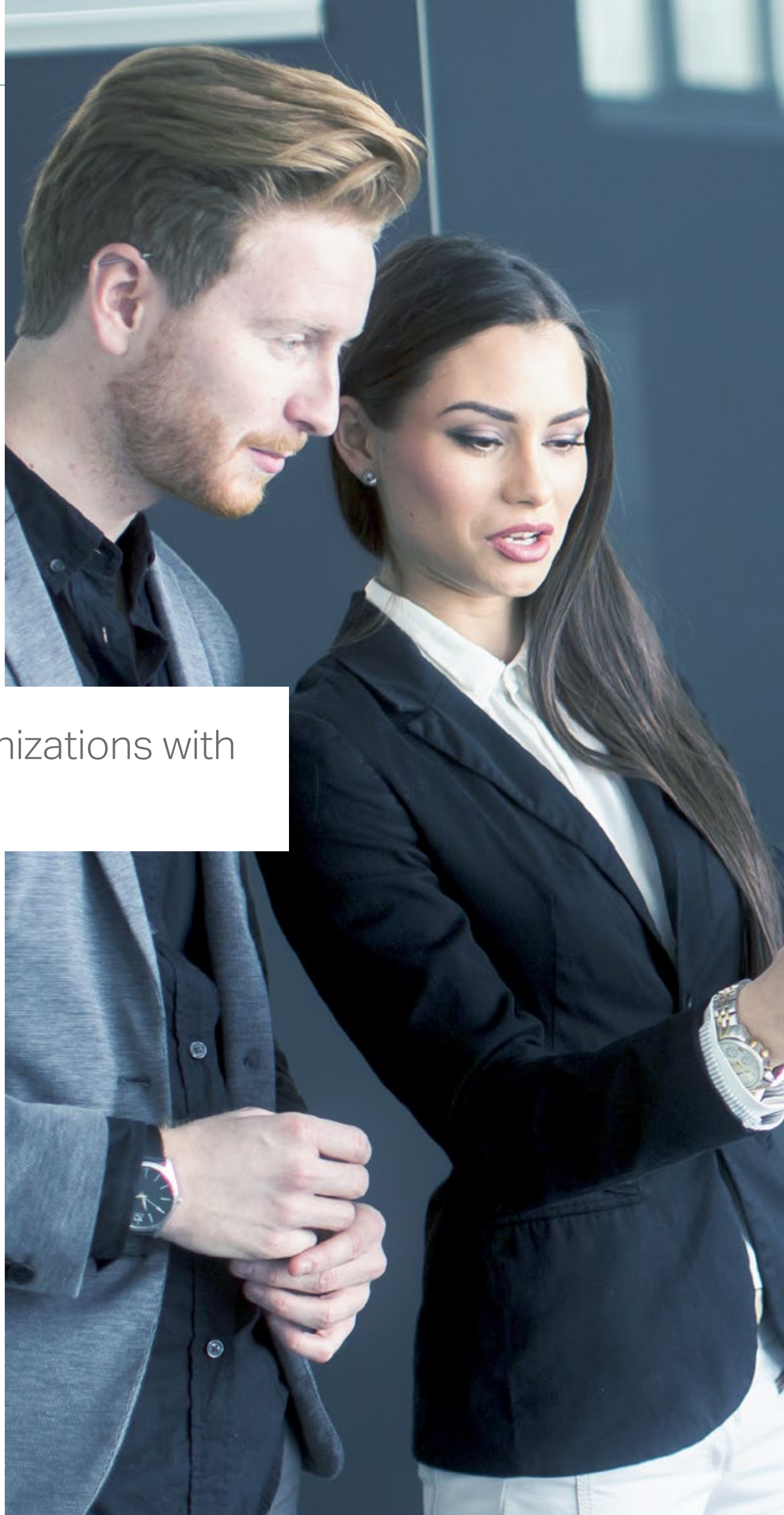
soterion

soterion.com

Content

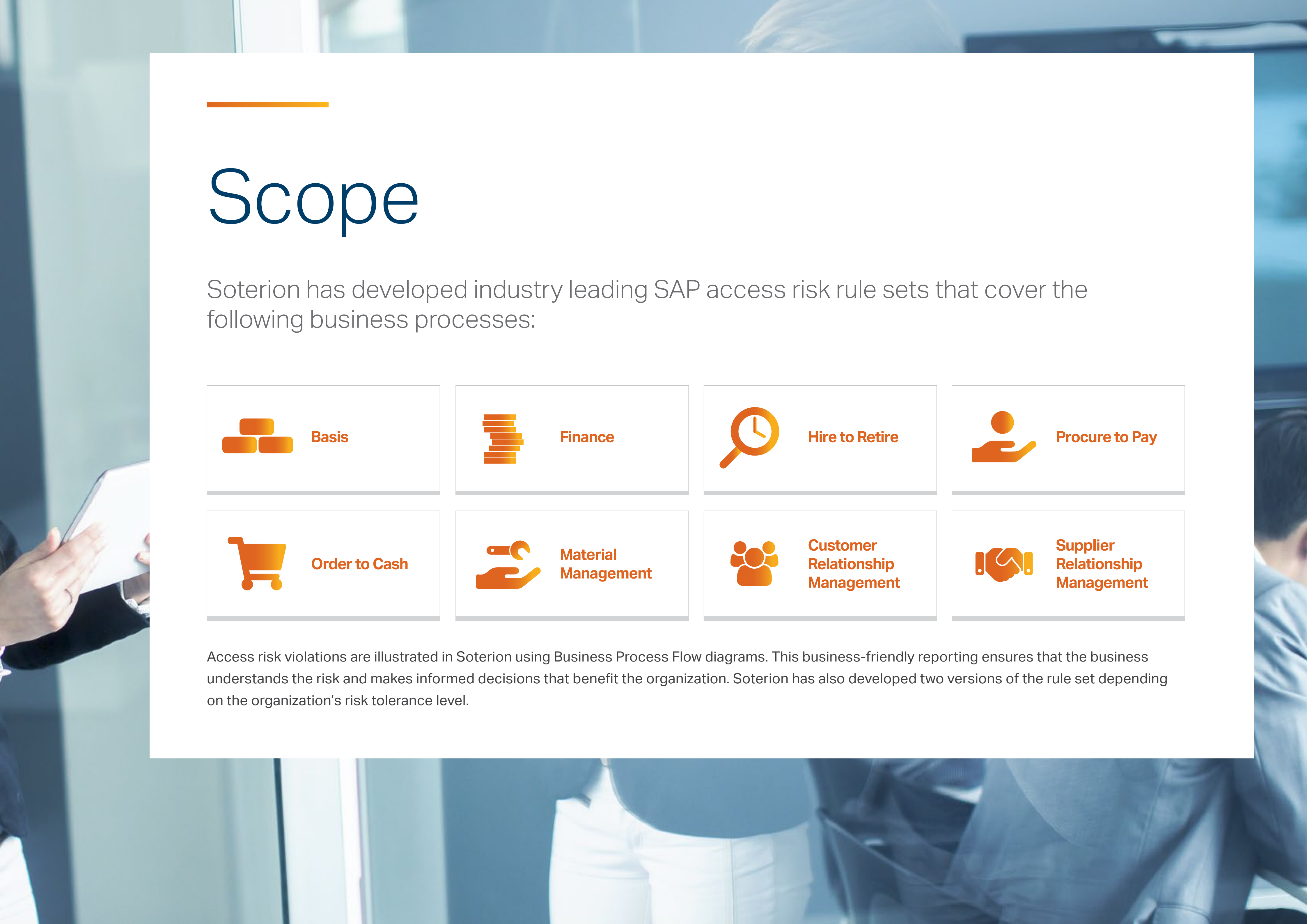
Objective of the SAP Access Risk Assessment

The objective of Soterion's access risk assessment is to provide organizations with some insight into their SAP access risk exposure.



Access control is one of the primary tools available to an organization to prevent incidents of fraud, as well as data privacy leaks and breaches. The SAP Authorization solution is the mechanism used to ensure there is adequate access control. Unfortunately, SAP Authorization creep typically results in SAP users being assigned wider access, over time, than what is required to carry out their job function. This increases the organization's access risk exposure year on year.

The Soterion SAP access risk assessment will highlight the users that have segregation of duty or critical transaction access, the role/profile from where the user gets this access, as well as whether the user is executing the transaction code. The Soterion assessment will typically recommend a number of role clean-up or risk remediation suggestions that could be carried out to reduce the organization's access risk exposure.



Scope

Soterion has developed industry leading SAP access risk rule sets that cover the following business processes:

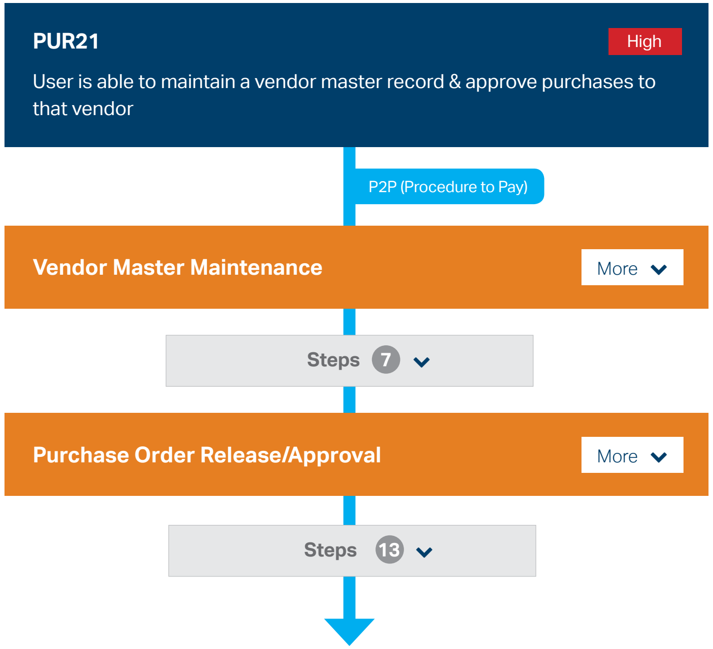
- Basis
- Finance
- Hire to Retire
- Procure to Pay
- Order to Cash
- Material Management
- Customer Relationship Management
- Supplier Relationship Management

Access risk violations are illustrated in Soterion using Business Process Flow diagrams. This business-friendly reporting ensures that the business understands the risk and makes informed decisions that benefit the organization. Soterion has also developed two versions of the rule set depending on the organization's risk tolerance level.

Process Flow Diagrams

Standard Tolerance

Soterion's Standard rule set is applicable for organizations that would like to monitor access risks at a more granular level. The majority of the risks in this rule set are a combination of 2 conflicting functions.



PUR21 High

User is able to maintain a vendor master record & approve purchases to that vendor

P2P (Procedure to Pay)

Vendor Master Maintenance More

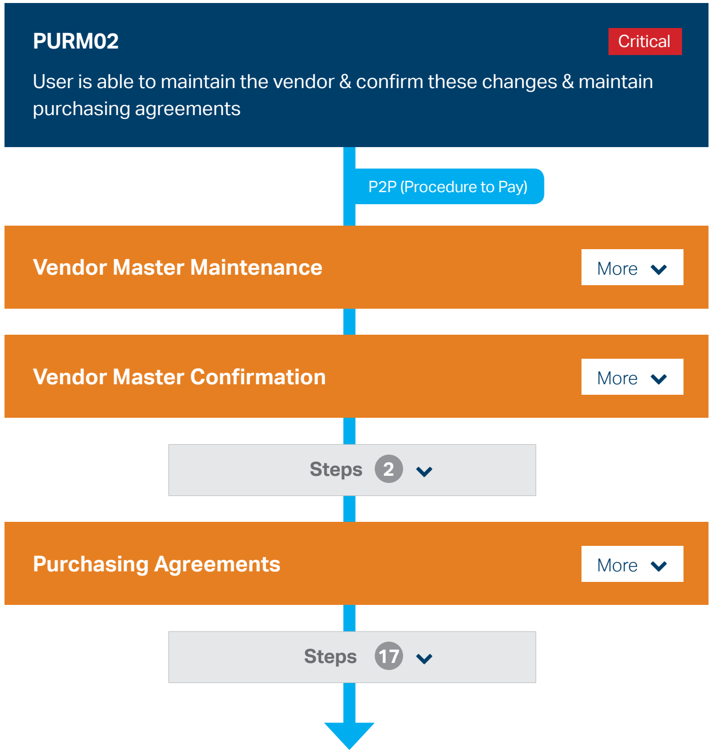
Steps 7

Purchase Order Release/Approval More

Steps 13

High Tolerance

Soterion's High Tolerance rule set is applicable for organizations that are more risk tolerant and would like to monitor access risks where users have multiple functions of a business process. The majority of the risks in this rule set are a combination of 3 or more conflicting functions.



PURM02 Critical

User is able to maintain the vendor & confirm these changes & maintain purchasing agreements

P2P (Procedure to Pay)

Vendor Master Maintenance More

Vendor Master Confirmation More

Steps 2

Purchasing Agreements More

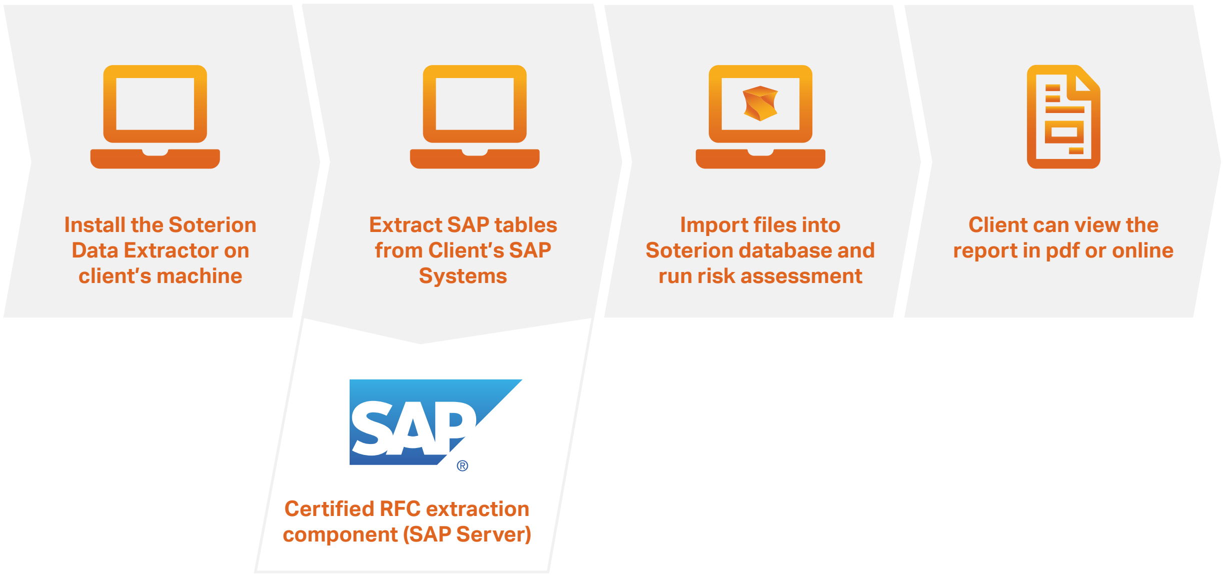
Steps 17

■ Risk 🟦 Business Process 🟧 Relevant Process Step ⬜ Other Process Step

Process

Organizations who wish to have a Soterion access risk assessment done on their SAP system will need to download the Soterion Data Extractor from the Soterion website.

The Data Extractor will be installed on a user's PC/laptop (no ABAPs required). The user will use their SAP User logon credentials to extract the SAP authorization related tables, which will be uploaded to Soterion's data center (Azure) in your geographic jurisdiction in an encrypted format. Soterion will run the risk assessment on the customer's data.



Install the Soterion Data Extractor on client's machine

Extract SAP tables from Client's SAP Systems

Import files into Soterion database and run risk assessment

Client can view the report in pdf or online

Certified RFC extraction component (SAP Server)

Findings

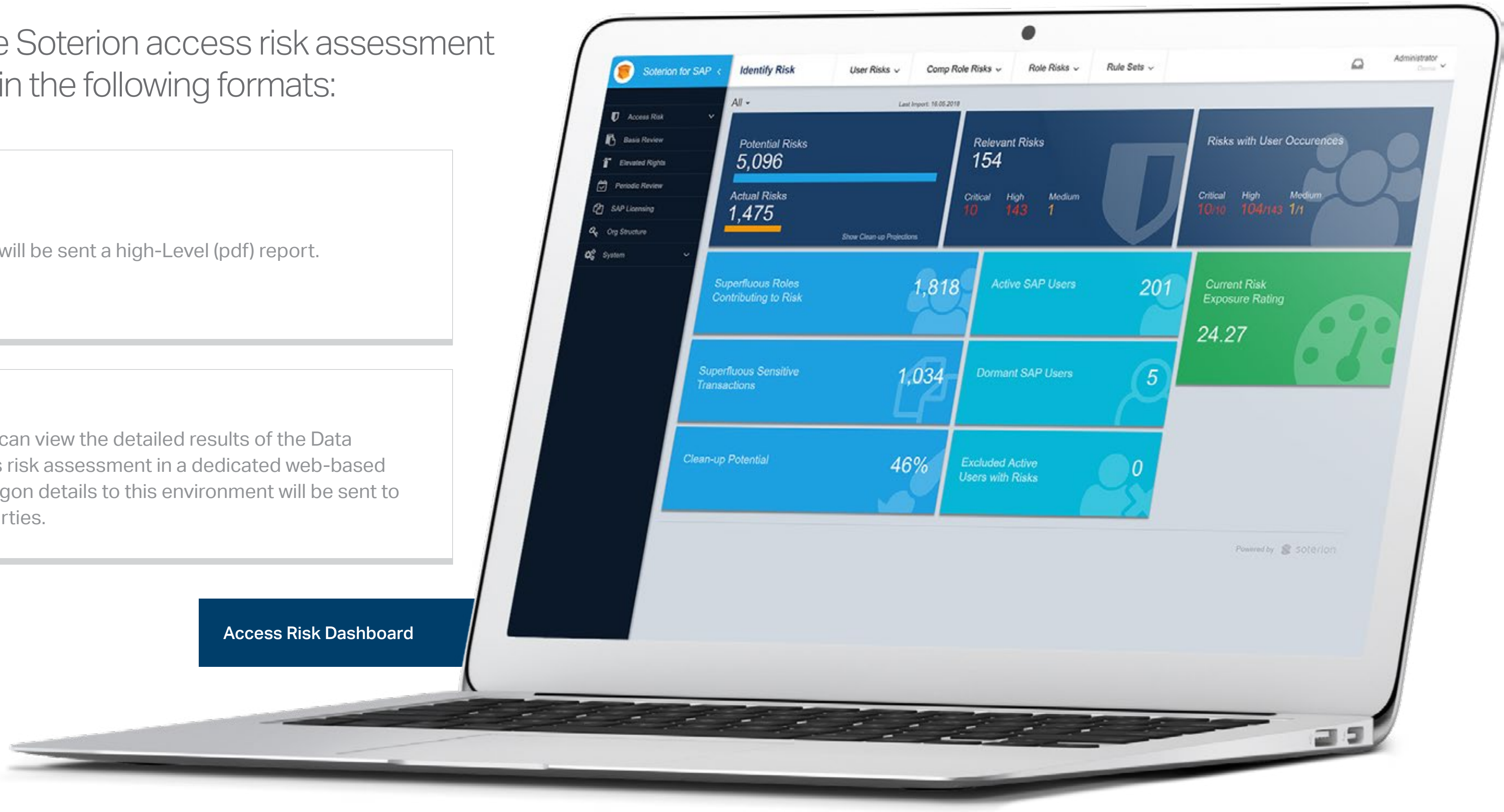
The results of the Soterion access risk assessment will be displayed in the following formats:

Summary

The customer will be sent a high-Level (pdf) report.

Detailed

The customer can view the detailed results of the Data Privacy access risk assessment in a dedicated web-based application. Logon details to this environment will be sent to the relevant parties.



Last Import: 16.05.2018

Potential Risks 5,096

Actual Risks 1,475

Relevant Risks 154

Critical 10 High 143 Medium 1

Risks with User Occurences

Critical 10/10 High 104/143 Medium 1/1

Superfluous Roles Contributing to Risk 1,818

Active SAP Users 201

Current Risk Exposure Rating 24.27

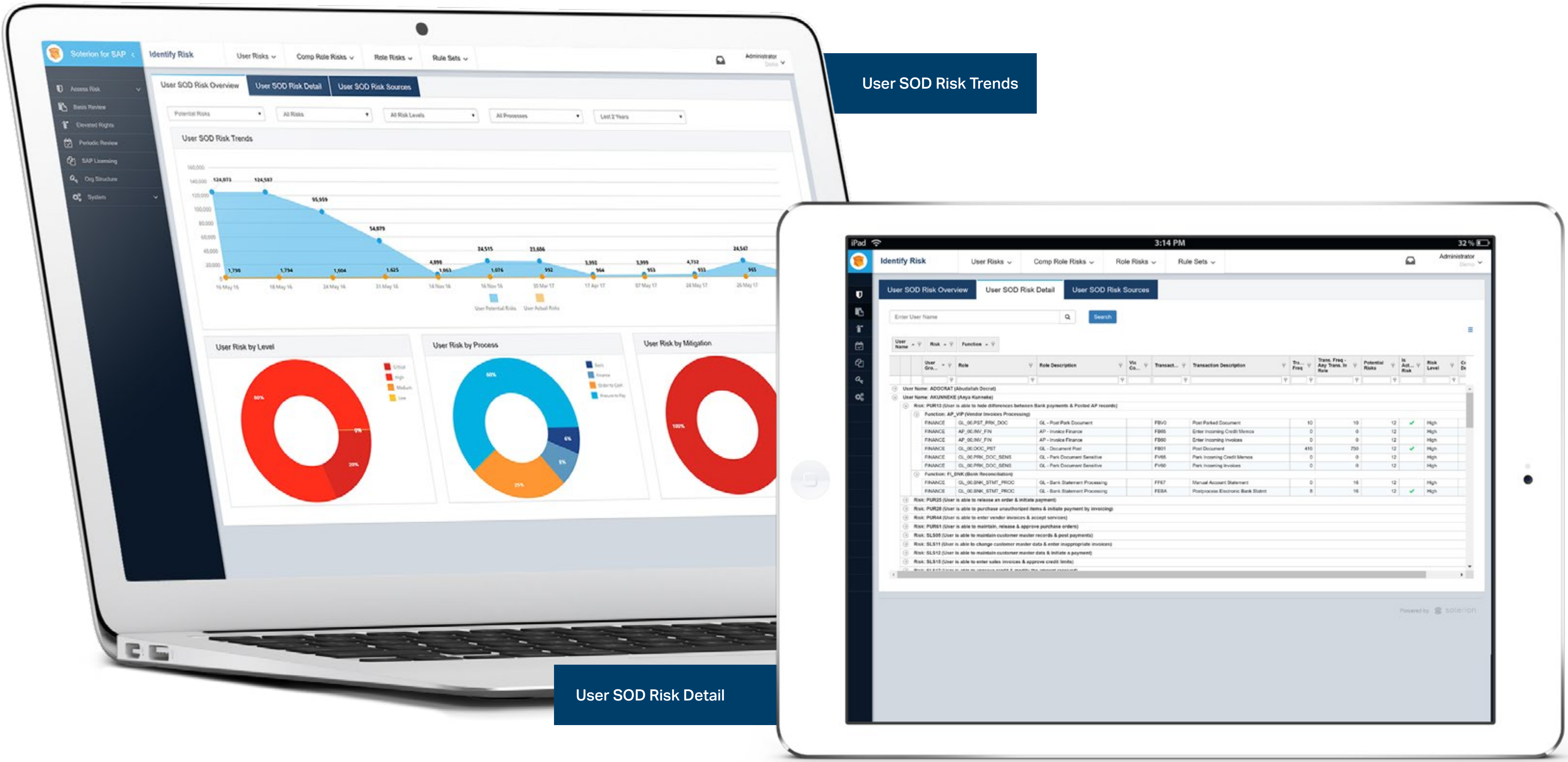
Superfluous Sensitive Transactions 1,034

Dormant SAP Users 5

Clean-up Potential 46%

Excluded Active Users with Risks 0

Access Risk Dashboard



User SOD Risk Trends

User Name ▲ | Risk ▲ | Function ▲

User Name: ADOCRAT (Abudallah Docrat)

User Name: AKUNNEKE (Aaya Kunneke)

Risk: PUR13 (User is able to hide differences between Bank payments & Posted AP records)

Function: AP_VIP (Vendor Invoices Processing)

User Gro...	Role	Role Description	Vio Co...	Transact...	Transaction Description	Tra... Freq	Trans. Freq - Any Trans. In Role	Potential Risks	Is Act... Risk	Risk Level
FINANCE	GL_00.PST_PRK_DOC	GL - Post Park Document		FBV0	Post Parked Document	10	10	12	✓	High
FINANCE	AP_00.INV_FIN	AP - Invoice Finance		FB65	Enter Incoming Credit Memos	0	0	12		High
FINANCE	AP_00.INV_FIN	AP - Invoice Finance		FB60	Enter Incoming Invoices	0	0	12		High
FINANCE	GL_00.DOC_PST	GL - Document Post		FB01	Post Document	416	750	12	✓	High
FINANCE	GL_00.PRK_DOC_SENS	GL - Park Document Sensitive		FV65	Park Incoming Credit Memos	0	0	12		High
FINANCE	GL_00.PRK_DOC_SENS	GL - Park Document Sensitive		FV60	Park Incoming Invoices	0	0	12		High

Function: FI_BNK (Bank Reconciliation)

User Gro...	Role	Role Description	Vio Co...	Transact...	Transaction Description	Tra... Freq	Trans. Freq - Any Trans. In Role	Potential Risks	Is Act... Risk	Risk Level
FINANCE	GL_00.BNK_STMT_PROC	GL - Bank Statement Processing		FF67	Manual Account Statement	0	16	12		High
FINANCE	GL_00.BNK_STMT_PROC	GL - Bank Statement Processing		FEBA	Postprocess Electronic Bank Statmt	8	16	12	✓	High

Risk: PUR25 (User is able to release an order & initiate payment)

Risk: PUR28 (User is able to purchase unauthorized items & initiate payment by invoicing)

Risk: PUR44 (User is able to enter vendor invoices & accept services)

Risk: PUR61 (User is able to maintain, release & approve purchase orders)

Risk: SLS05 (User is able to maintain customer master records & post payments)

Risk: SLS11 (User is able to change customer master data & enter inappropriate invoices)

Risk: SLS12 (User is able to maintain customer master data & initiate a payment)

Risk: SLS15 (User is able to enter sales invoices & approve credit limits)

User SOD Risk Detail

Follow Up

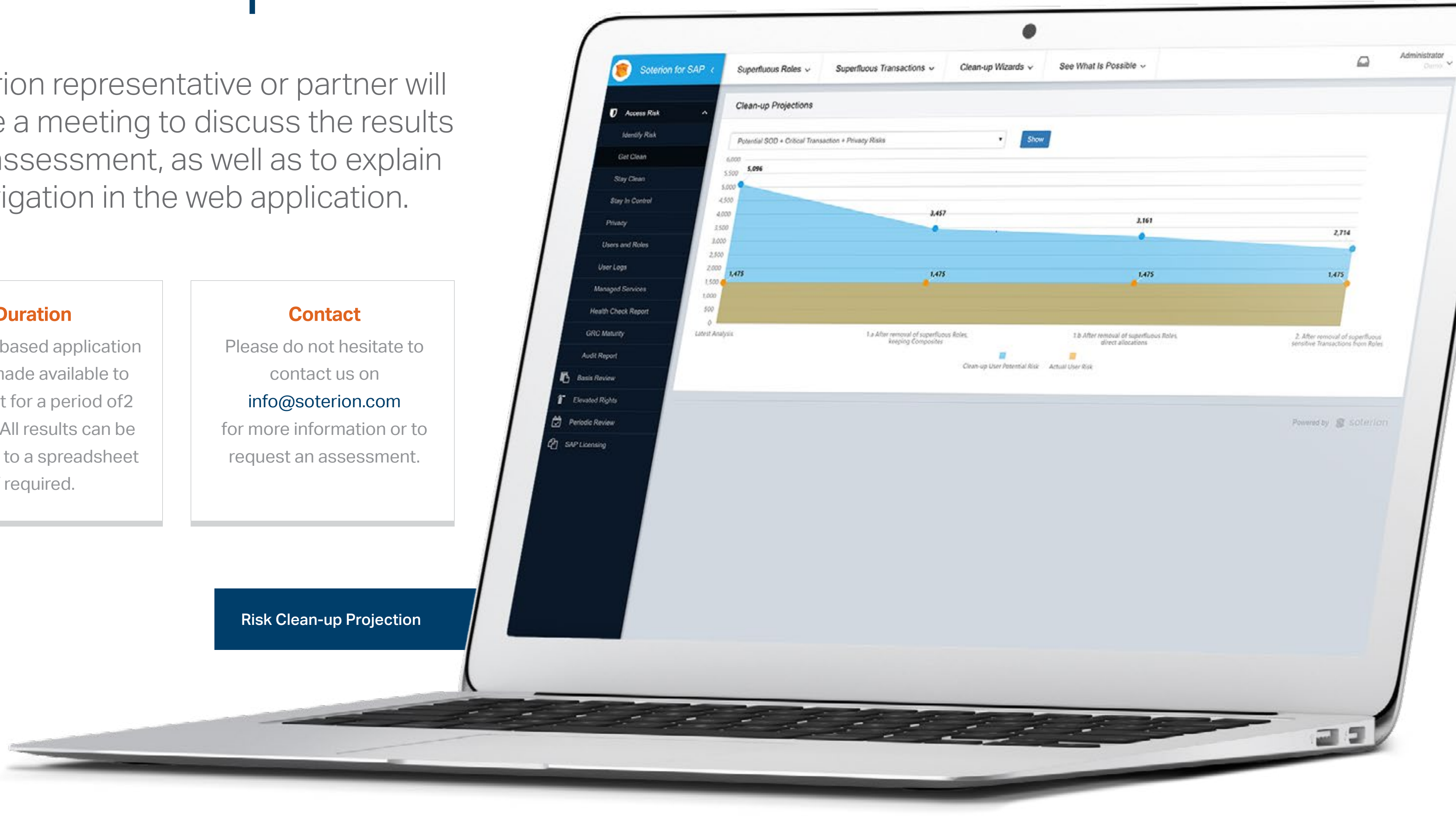
A Soterion representative or partner will arrange a meeting to discuss the results of the assessment, as well as to explain the navigation in the web application.

Duration

The web-based application will be made available to the client for a period of2 months. All results can be exported to a spreadsheet if required.

Contact

Please do not hesitate to contact us on info@soterion.com for more information or to request an assessment.



Risk Clean-up Projection

NETHERLANDS

Kingsfordweg 151,
1043 GR Amsterdam,
Holland

Telephone: +31 (0) 20 491 7841

AUSTRALIA

53 Walker Street
North Sydney
NSW 2060

Telephone: +61 2 9045 0238

SOUTH AFRICA

Block A, Wedgefield Office Park
17 Muswell Road
South Bryanston
Johannesburg 2021

Telephone: +27 11 540 0232

ASIA PACIFIC

10 Anson Road, International
Plaza #49-09, 079903
Singapore

Telephone: +65 9883 9267

soterion

info@soterion.com www.soterion.com