SBN 2020
SAP USER CONFERENCE
Virtual Event | October 20-22 & 27-29

Introduction Security Weaver

Martin de Lange

Security Weaver

Where can we help? Being in Control!

"Can we find a spot to go over the results of your compliance audit?"

SECURITY WEAVER

Know what's happening in your SAP- and related system(s)

Being Compliant

Having an efficient Solution

serco

Example of Customers in Europe

‘Security Weaver is a *preferred* choice for any SAP-centric organization looking for a reasonable total cost of ownership solution……’

Source: Gartner, Market Guide for SOD Controls Monitoring Tools Published

Feel free to get in contact at any time!

Simone van Kipperssuis
Business Development Nordics
simone@securityweaver.com
+31 6 51 85 55 56

serco

Do you know what's happening in your SAP-system(s)?

serco

Gerald West

20th October 2020

Do you know how many....

Users having risky access…?

Invoices getting paid twice…?

Changes to sensitive fields on vendors…. ?

SoD-conflicts being exploited….?

Users performing risky actions…?

Critical configuration changes…?

Continuous Controls Monitoring (CCM) brings ….

Agenda

Background

- Provides outsourcing services to governments & public sector (mainly Defence, Health, Citizen Services, Justice & Immigration, Transport)
- Main operations in UK, Europe, Middle East, ASPAC and North America
- Running SAP since 2007 - ECC (x2), SRM, CRM, BW, BPC, BO, PI, SolMan, SuccessFactors, SAP Concur
- Over 35,000 SAP users

Part 1 – Controls Approach

Overview of Controls Approach

Dimensions

- People
- Process
- Technology
- Data

Initiatives

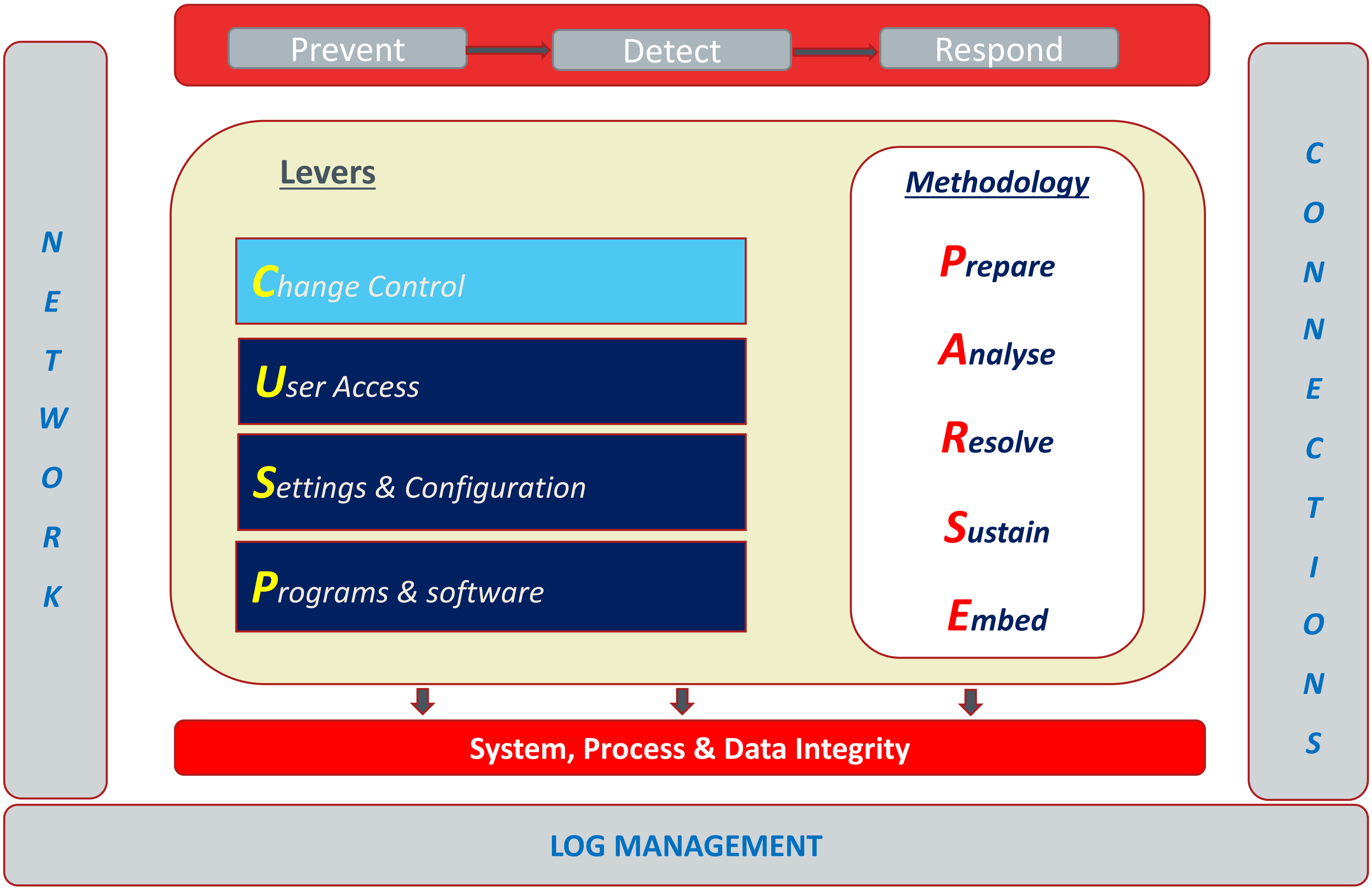
ENABLE

- **Define** – Define processes, policies and standards
- **Engage** – Engage and Educate User Community
- **Simplify** – Make it Easy to Do The Right Thing
- **Know** – Identify Risks and Control Mechanisms

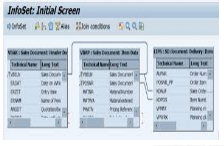
EXECUTE

- **Control** – Implement and Maintain Effective Controls
- **Assure** – Establish Robust Assurance and Testing
- **Report** – Analyse Controls Environment and Detect Exceptions

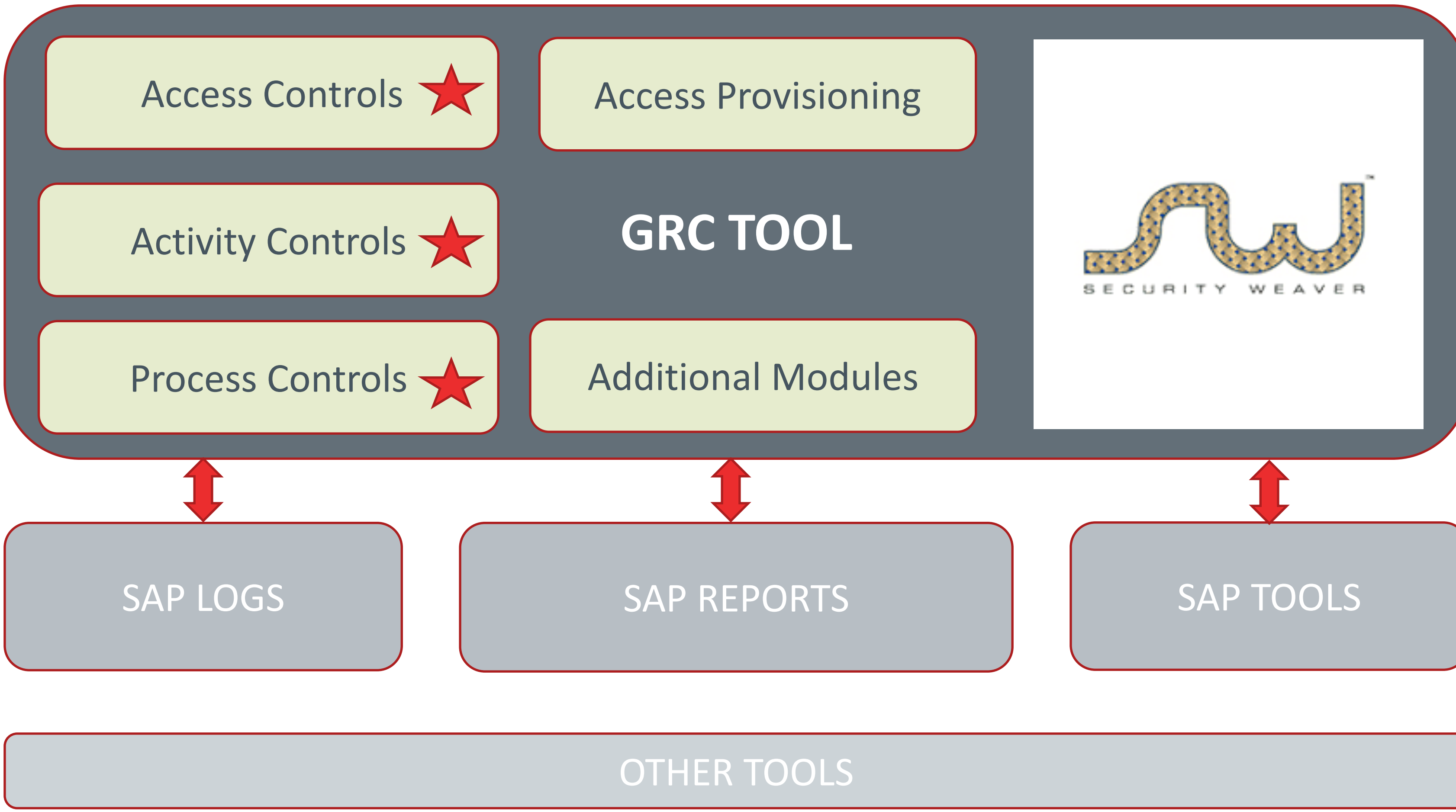
Controls Approach – The Technology Shield



Continuous Controls Monitoring – The RACE

Report	Create report on controls-relevant dataset	
Alert	Capture exceptional scenario via a variant and automate with a batch job	
Check	Investigate the exceptions reported	
Execute	Take the required corrective action	

Controls Platform – Overview



★ CCM Focus

Controls Platform – Security Weaver Use Cases

Separations Enforcer – Critical authorizations, Segregation of Duties (SoD), Sensitive access, Organisational access, Personal Data Access

Secure Enterprise – Non-SAP/Cross-System SoD and Critical Authorizations

Emergency Repair – Firefighter (Exceptional) Access

Process Auditor – Master Data Checks, Configuration and Settings Monitoring, Transaction Monitoring

Transaction Archive - User Intelligence, Alerts, Forensics

Licence Management – Compliance, Optimization, Simulation

Reset Password – Self-service password reset for all SAP systems

Controls Platform – Value Streams

- **Risk reduction**
  - Manages user access risks
  - Ensures secure settings and configuration
  - Checks for data integrity (reduces risk of fraud/error)
  - Accelerates and enhances detection of risky events/transactions

- **Cost savings**
  - Reduces cash leakage (e.g. identifying duplicate invoices)
  - Avoids process re-work costs (e.g. flagging duplicate vendors)
  - Slashes the cost of SAP password resets
  - Cuts down effort and cost of role maintenance

Part 2 – Continuous Controls Monitoring (CCM) Use Cases

CCM Use Cases – Access Controls

Key Objective

Monitor and manage segregation-of-duties, critical access & data access

Tools

SW Separations Enforcer

SW Secure Enterprise

Tips/Lessons/Ideas

1. Use single-sided SoD conflicts for critical/data access rulesets
2. Leverage usage information
3. Report on FF assignments

Prepare
- Review and refine risk ruleset
- Understand risk scenarios
- Identify risk owners and process

Analyse
- Review risk report with risk owners
- Devise "get clean" solution options

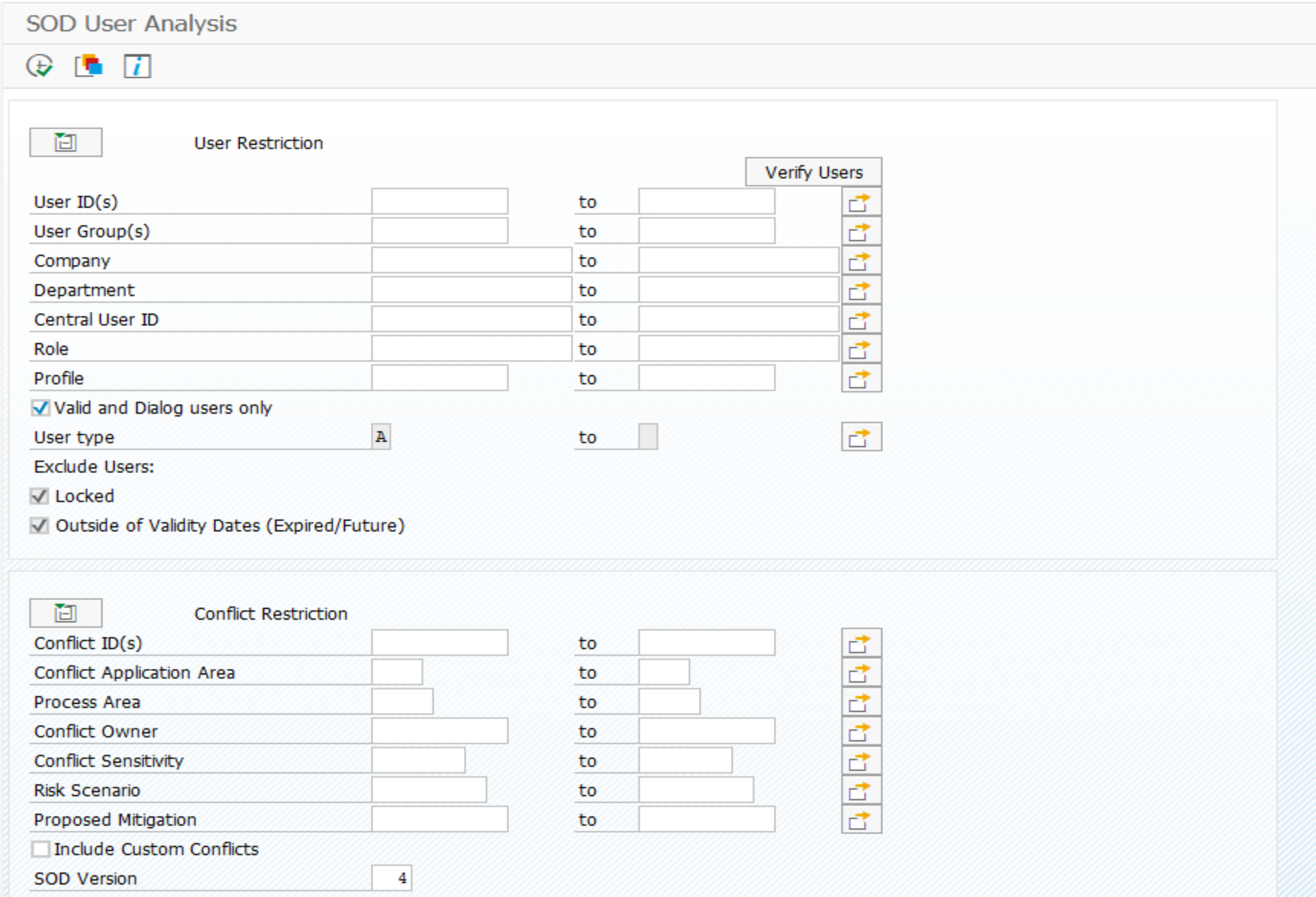
Resolve
- Remediate roles (single/composite)
- Remediate/Mitigate users

Sustain
- Automate risk reports
- Establish ongoing resolution process

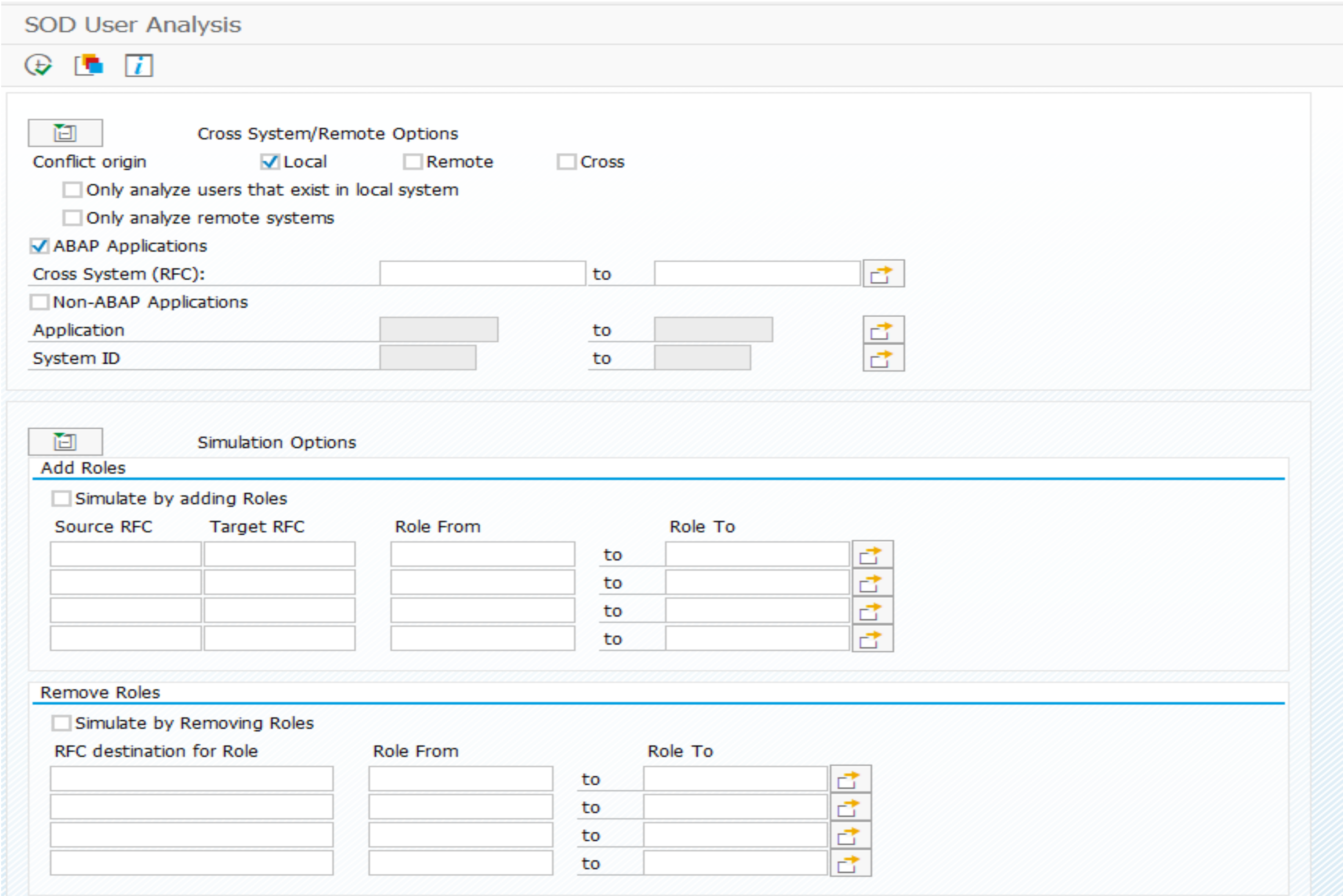
Embed
- Incorporate risk analysis & resolution into provisioning process

serco

Continuous Controls Monitoring – Access Controls Example



Continuous Controls Monitoring – Access Controls Example



Continuous Controls Monitoring – Access Controls Example

SOD User Analysis

SOD Live Options

- (•) Standard SOD Analysis
- ( ) Analyze Authorizations and check if Users executed conflicting T-Codes
- ( ) Analyze Authorizations and check if changes were made in conflicting Tcodes

Time frame for historical data 28.03.2020 to 26.04.2020

Output Options

- (•) SOD Conflict Summary
- ( ) SOD Conflict details (Advanced use; Auth. Details)
- ( ) SOD Conflict details tree (Advanced use; Auth. Details)
- ( ) SOD Conflict details - Simplified View

List display

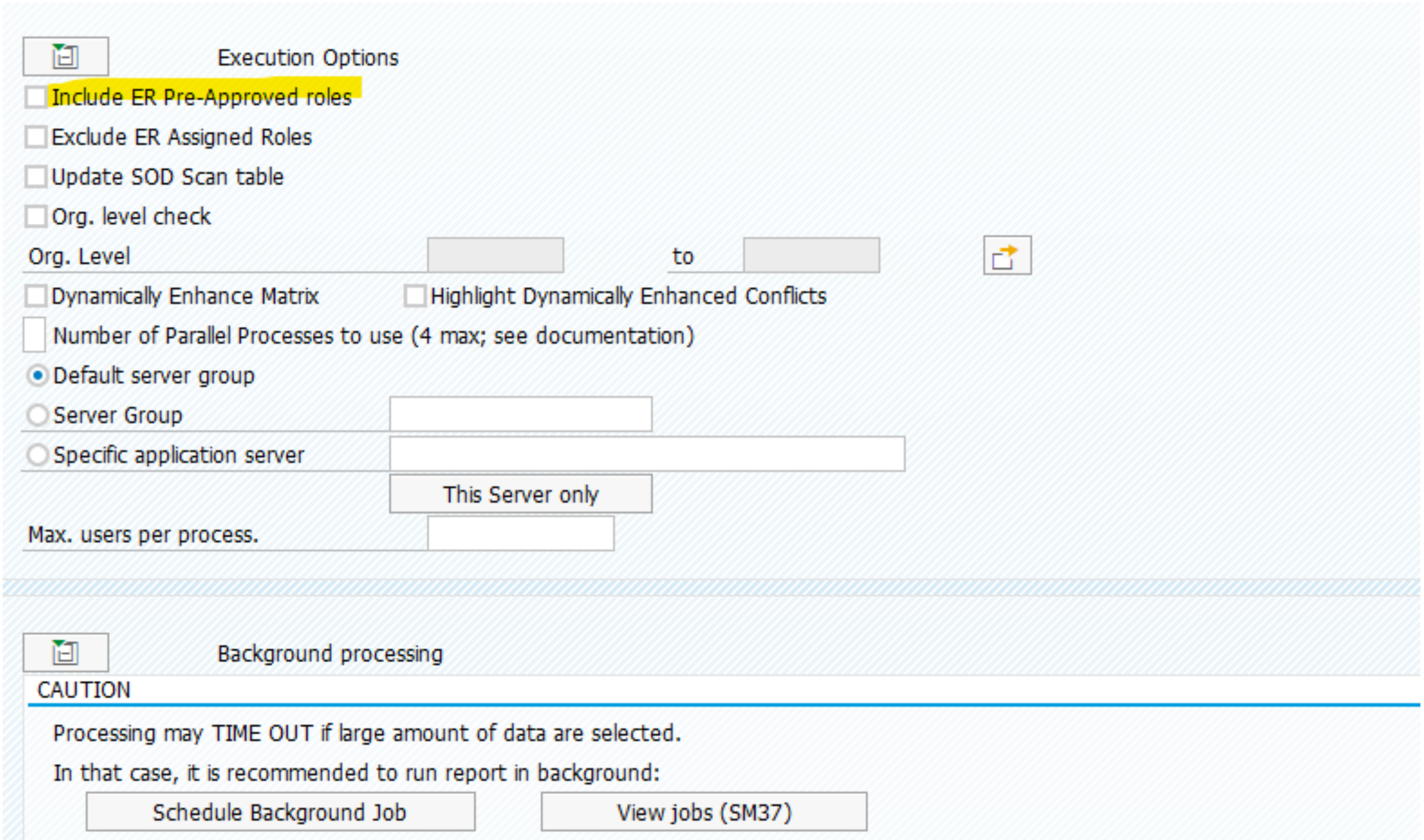
Layout Summary output

- [x] Show Mitigated Conflicts
- [ ] Show Users w/o Conflicts
- [ ] Highlight Conflicts
- [ ] Show Composite Role(s)

- [x] Output results (screen/spool)

serco

Continuous Controls Monitoring – Access Controls Example



serco

Continuous Controls Monitoring – Access Controls Example

Security Weaver: Segregation of Duties Analysis SOD Version 004

Tree output | Show Texts | Add Historical Usage | Propose Remediation | Simplified View

Details: User(s) with SOD conflicts

SOD version: 004 : Customized Version
User & Date: [redacted] on 27.04.2020 17:09:09
Summary 1 User(s) analyzed. Avg 1 SOD Conflict(s) in 1 user(s)

User ID	Sens	Con ID	SW: Risk Description	Risk	Func. ID	Tcode	Sys-Cli	Object	Authorization	Field Name	From	To	Role	Profile
[redacted]	HIGH	BC04	Functional Configuration (Direct Data Maintenance in Tables) & System Administration		BC10	SE16	EP1600	S_TABU_DIS	T-E184831300	ACTVT	02		ZXXTEMP_SW	T-E1848313
									T-E285049700		02		ZXXSWPA01	T-E2850497
									T-E285049701		02			
									T-E285677503		02		ZXXSA04	T-E2856775
									T-P355539305		02		/PSYNG/SW_ER_ADMINISTRATOR	T-P3555393
									T-P355844800		02		/PSYNG/SP_CHANGE	T-P3558448
									T-P355931700		02		/PSYNG/SW_ADMIN	T-P3559317
									T-P355931702		02			
								S_TCODE	T-E193950800	TCD	SE16		ZXXSA12	T-E1939508
									T-E195050300		SE16		ZXXSA13	T-E1950503
									T-E285650700		SE16		ZXXEA01	T-E28565071
									T-E285677500		SE16		ZXXSA04	T-E2856775
									T-E285677600		SE16		ZXXSA05	T-E2856776
						SM30		S_TABU_DIS	T-E184831300	ACTVT	02		ZXXTEMP_SW	T-E1848313
									T-E285049700		02		ZXXSWPA01	T-E2850497
									T-E285049701		02			
									T-E285677503		02		ZXXSA04	T-E2856775
									T-P355539305		02		/PSYNG/SW_ER_ADMINISTRATOR	T-P3555393
									T-P355844800		02		/PSYNG/SP_CHANGE	T-P3558448
									T-P355931700		02		/PSYNG/SW_ADMIN	T-P3559317
									T-P355931702		02			
								S_TCODE	T-E285650700	TCD	SM30		ZXXEA01	T-E28565071
									T-E285677500		SM30		ZXXSA04	T-E2856775
					BC17	SM04		S_ADMI_FCD	T-E195050300	S_ADMI_FCD	PADM		ZXXSA13	T-E1950503
									T-E285677500		PADM		ZXXSA04	T-E2856775
									T-E285677600		PADM		ZXXSA05	T-E2856776
								S_TCODE	T-E195050300	TCD	SM04		ZXXSA13	T-E1950503
									T-E285650700		SM04		ZXXEA01	T-E28565071
									T-E285677500		SM04		ZXXSA04	T-E2856775
									T-E285677600		SM04		ZXXSA05	T-E2856776
						SM13		S_ADMI_FCD	T-E285677500	S_ADMI_FCD	UADM		ZXXSA04	T-E2856775
									T-E285677600		UADM		ZXXSA05	T-E2856776
								S_TCODE	T-E285677500	TCD	SM13		ZXXSA04	T-E2856775
									T-E285677600		SM13		ZXXSA05	T-E2856776
						SM20		S_ADMI_FCD	T-E285650700	S_ADMI_FCD	SM21		ZXXEA01	T-E28565071
									T-E285677500		SM21		ZXXSA04	T-E2856775
								S_TCODE	T-E195050300	TCD	SM20		ZXXSA13	T-E1950503

CCM Use Cases - Activity Controls

Key Objective

Monitor and report on user activity

Tools

SW Transaction Archive

Tips/Lessons/Ideas

1. Check executed SoD analysis
2. Drill-down to change documents for forensic analysis
3. Note user terminals

Prepare

- Set up data capture rules
- Set up integration to other logs
- Define rules and alert recipients

Analyse

- Run activity reports & review results
- Identify sensitive/risky actions

Resolve

- Follow up with relevant users
- Modify access as appropriate

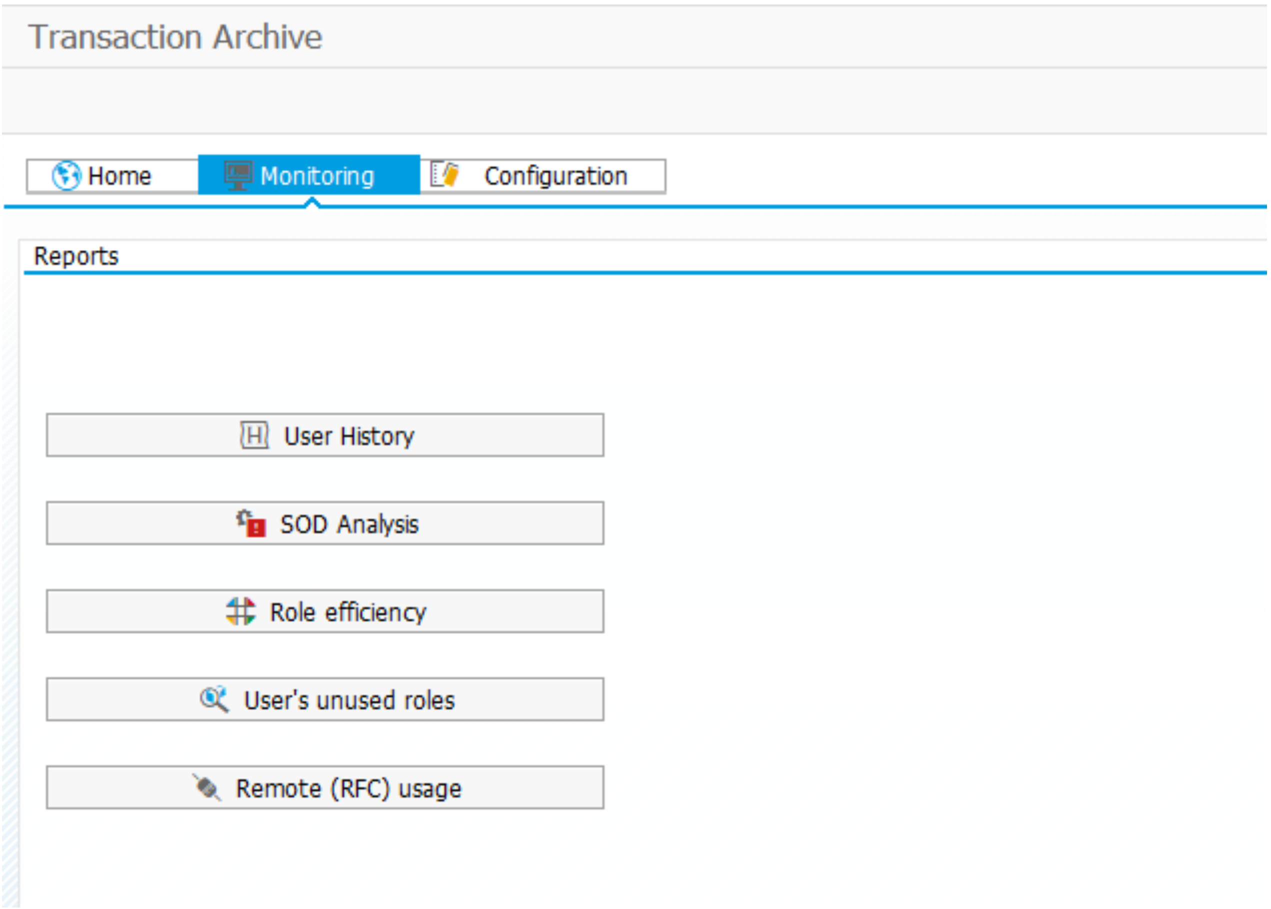
Sustain

- Schedule reports to run regularly
- Create sensitive action alerts

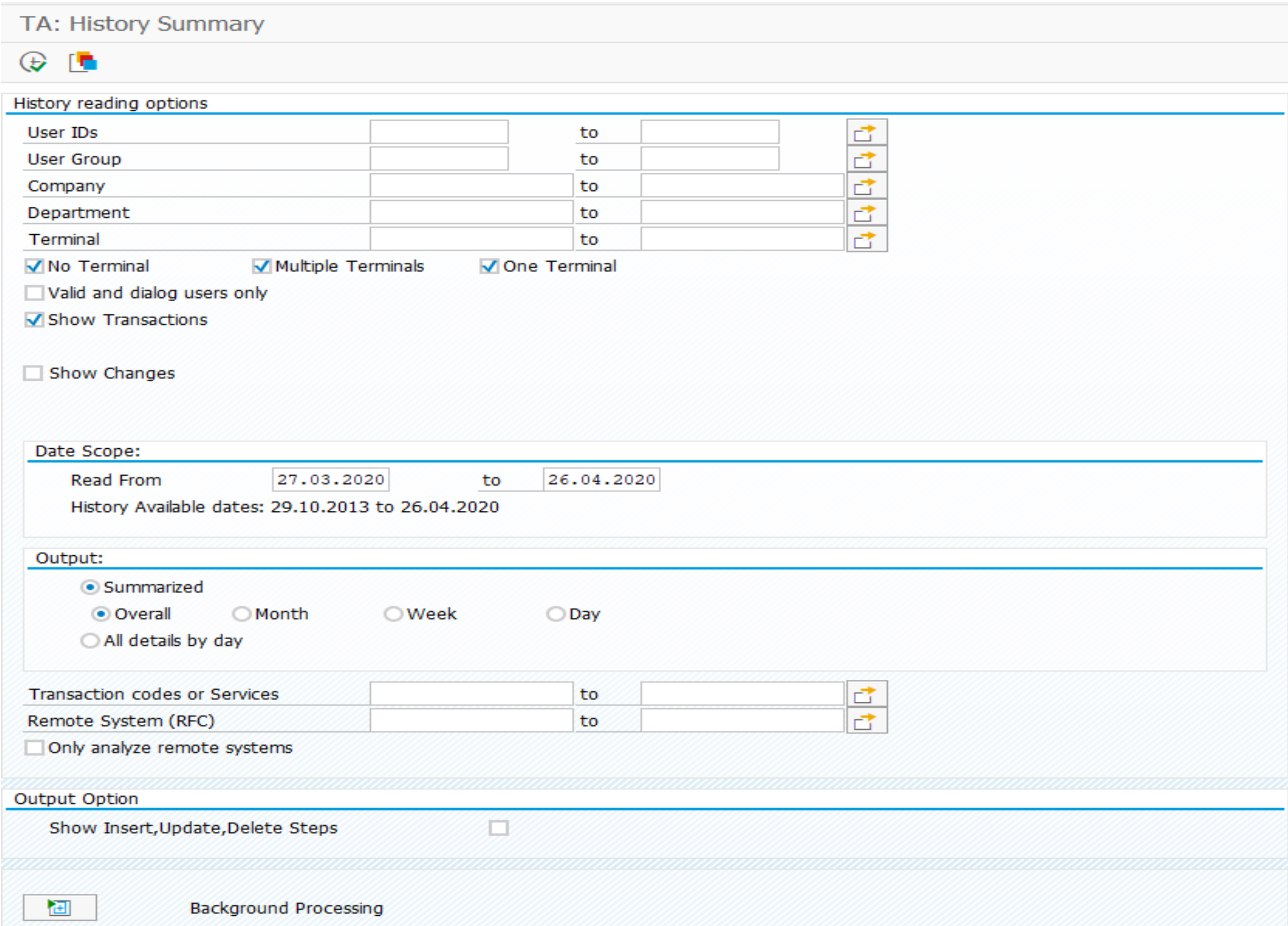
Embed

- Incorporate user activity monitoring into controls processes

User Intelligence – Transaction Archive Examples



Transaction Archive – User History Example



TA: History Summary

History reading options

User IDs		to	
User Group		to	
Company		to	
Department		to	
Terminal		to	

☑ No Terminal ☑ Multiple Terminals ☑ One Terminal

☐ Valid and dialog users only

☑ Show Transactions

☐ Show Changes

Date Scope:

Read From 27.03.2020 to 26.04.2020

History Available dates: 29.10.2013 to 26.04.2020

Output:

◉ Summarized

◉ Overall ○ Month ○ Week ○ Day

○ All details by day

Transaction codes or Services		to	
Remote System (RFC)		to	

☐ Only analyze remote systems

Output Option

Show Insert,Update,Delete Steps ☐

Background Processing

Transaction Archive – User History Example

TA: History Summary

History Summary

RFC	User ID	User Full Name	Terminal	Interactio	Data Type	Tcode or Service	Description
HP1600	[redacted]	Gerald West	1[redacted]	29		(None)	No transaction code
			L-[redacted]	72		/PSYNG/LM	SW: License Management
				24		/PSYNG/TA	Transaction Archive
				61		PFCG	Role Maintenance
				79		SE16N	General Table Display
				12		SESSION_MANAGER	Session Manager Menu Tree Display
				125		SQ00	SAP Query: Start queries
				30		SU01D	User Display
				0		SU53	Evaluate Authorization Check

- Terminal now included to indicate where user is accessing from
- Pencil icon allows drill down into change documents

serco

CCM Use Cases – Process Controls

Key Objective

Monitor and manage configuration and data integrity

Tools

SW Process Auditor

Tips/Lessons/Ideas

1. Start with simple IT controls
2. Assemble a broad working group
3. Invest in design

Prepare

- Review standard controls
- Refine and customize as required
- Define rules and alert recipients

Analyse

- Execute controls & review results
- Devise remediation options

Resolve

- Update configuration/data
- Update and close cases

Sustain

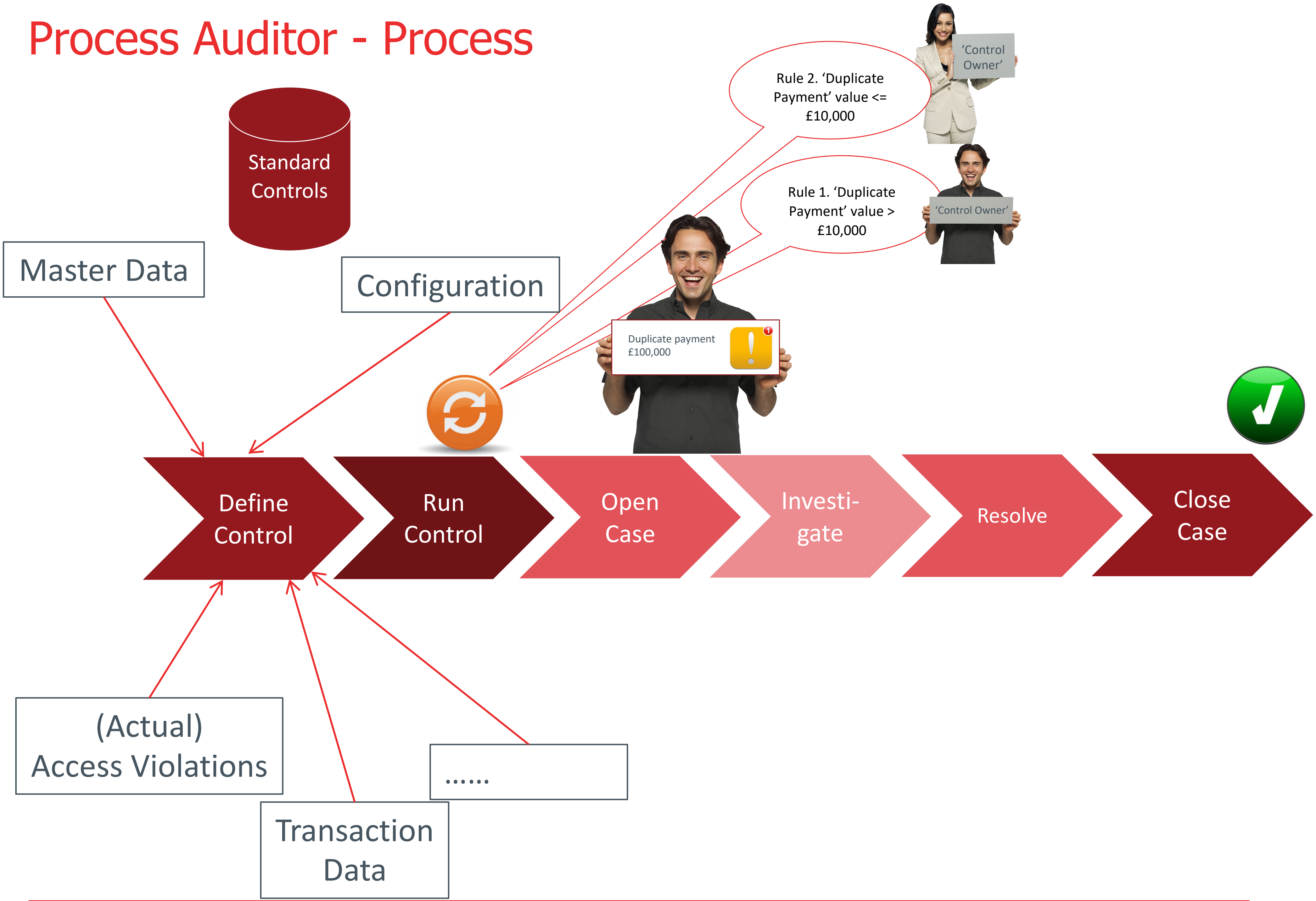
- Schedule controls to run regularly
- Establish ongoing resolution process

Embed

- Incorporate controls into core processes as appropriate

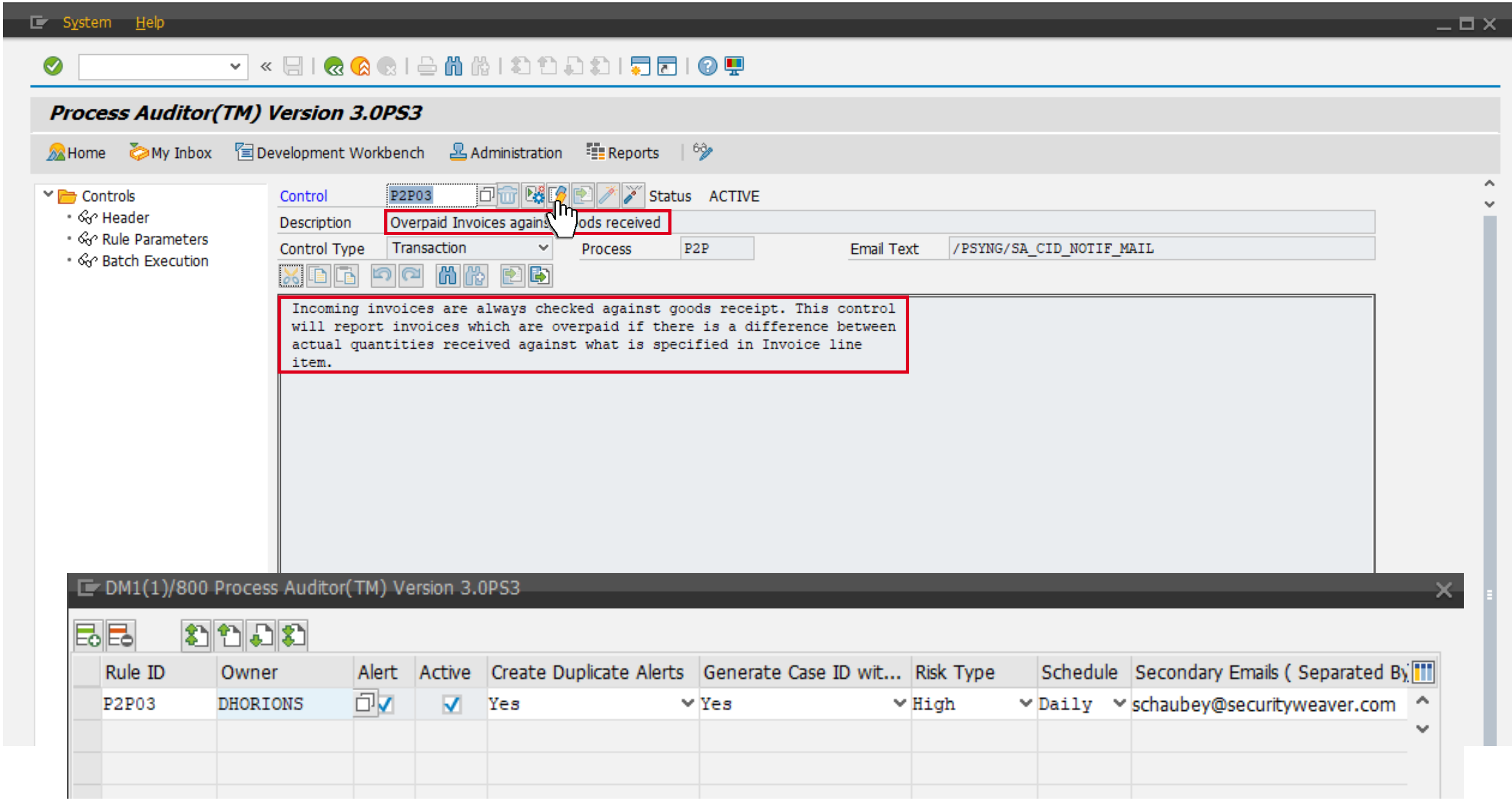
Part 3 – Process Controls (CCM with Process Auditor)

Process Auditor - Process



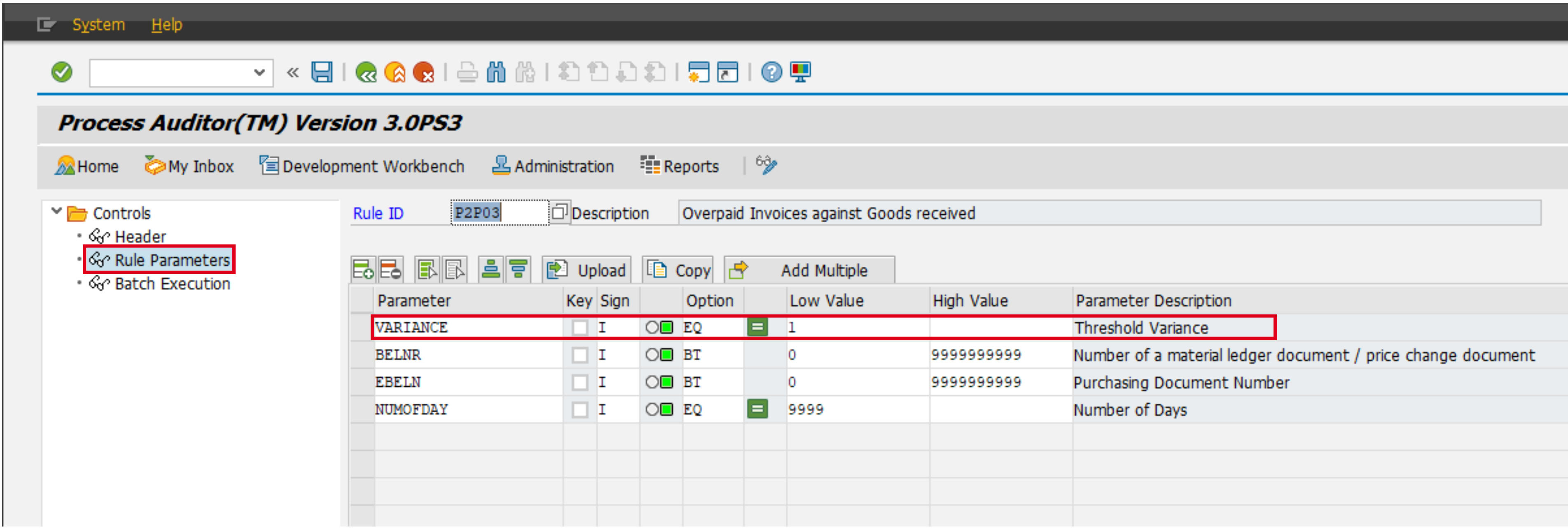
serco

Example control – 'Overpaid invoices against goods received'



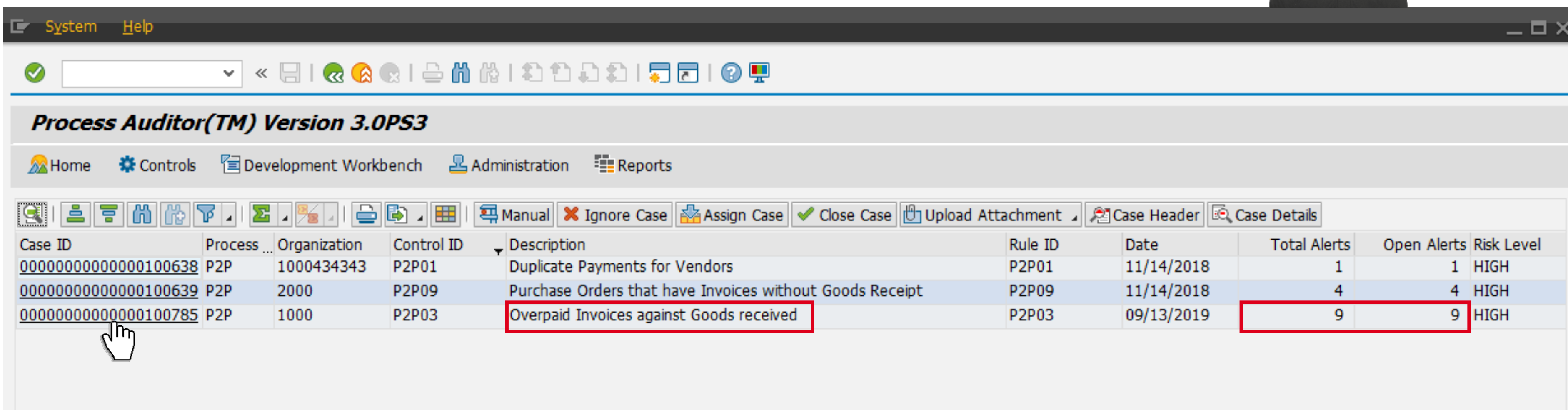
serco

Example control – 'Overpaid invoices against goods received'



Parameter	Key	Sign	Option	Low Value	High Value	Parameter Description
VARIANCE		I	EQ	1		Threshold Variance
BELNR		I	BT	0	9999999999	Number of a material ledger document / price change document
EBELN		I	BT	0	9999999999	Purchasing Document Number
NUMOFDAY		I	EQ	9999		Number of Days

Example control – ‘Overpaid invoices against goods received’



Case ID	Process ...	Organization	Control ID	Description	Rule ID	Date	Total Alerts	Open Alerts	Risk Level
000000000000000100638	P2P	1000434343	P2P01	Duplicate Payments for Vendors	P2P01	11/14/2018	1	1	HIGH
000000000000000100639	P2P	2000	P2P09	Purchase Orders that have Invoices without Goods Receipt	P2P09	11/14/2018	4	4	HIGH
000000000000000100785	P2P	1000	P2P03	Overpaid Invoices against Goods received	P2P03	09/13/2019	9	9	HIGH

Example control – ‘Overpaid invoices against goods received’

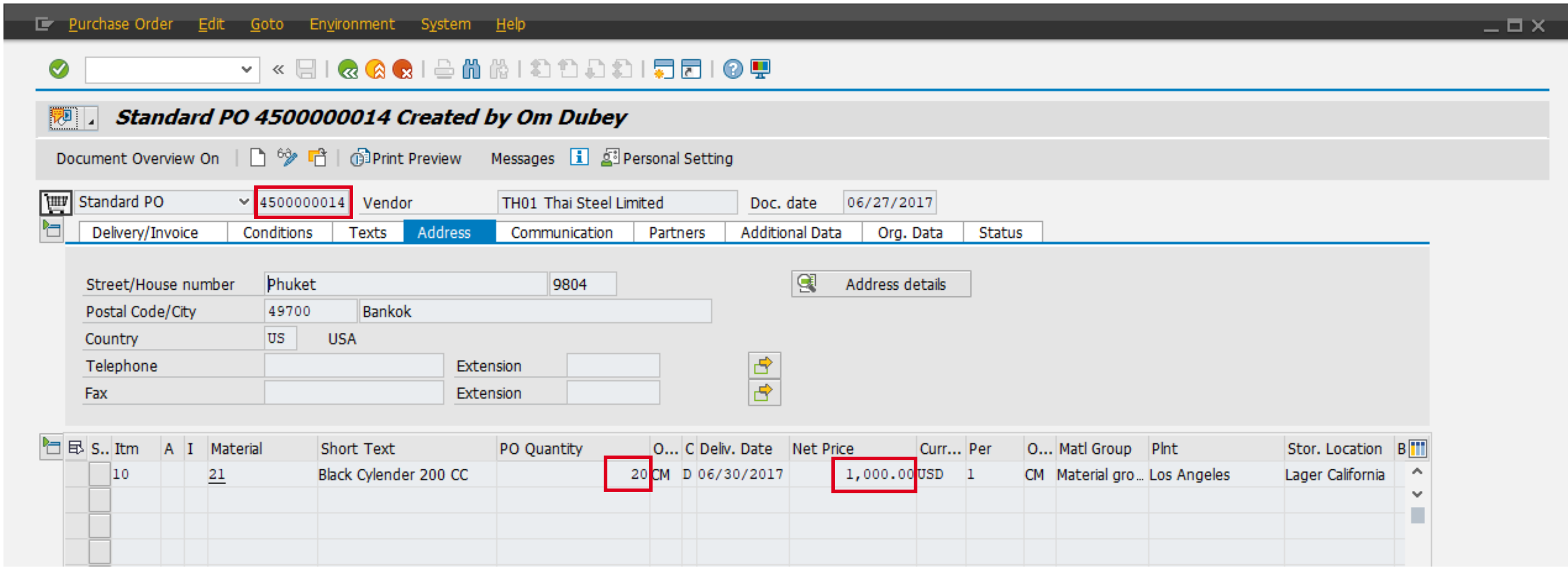
System Help

P2P03:Overpaid Invoices against Goods received

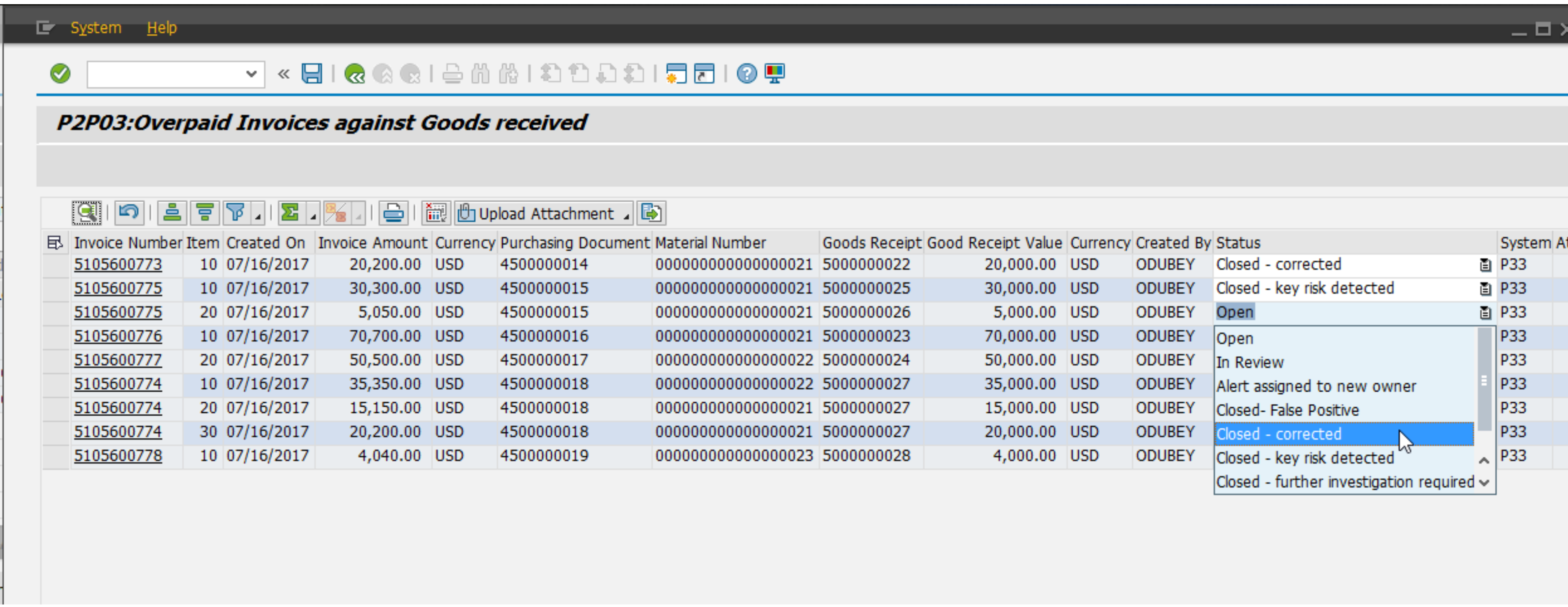
Upload Attachment

Invoice Number	Item	Created On	Invoice Amount	Curren...	Good Receipt Val...	Curren...	Purchasing Document	Material Number	Goods Receipt	Created By	Status	Syste...
5105600776	10	07/16/2017	70,700.00	USD	70,000.00	USD	4500000016	000000000000000021	5000000023	ODUBEY	Open	P33
5105600777	20	07/16/2017	50,500.00	USD	50,000.00	USD	4500000017	000000000000000022	5000000024	ODUBEY	Open	P33
5105600774	10	07/16/2017	35,350.00	USD	35,000.00	USD	4500000018	000000000000000022	5000000027	ODUBEY	Open	P33
5105600775	10	07/16/2017	30,300.00	USD	30,000.00	USD	4500000015	000000000000000021	5000000025	ODUBEY	Open	P33
5105600773	10	07/16/2017	20,200.00	USD	20,000.00	USD	4500000014	000000000000000021	5000000022	ODUBEY	Open	P33
5105600774	30	07/16/2017	20,200.00	USD	20,000.00	USD	450[illegible]018	000000000000000021	5000000027	ODUBEY	Open	P33
5105600774	20	07/16/2017	15,150.00	USD	15,000.00	USD	45000[illegible]018	000000000000000021	5000000027	ODUBEY	Open	P33
5105600775	20	07/16/2017	5,050.00	USD	5,000.00	USD	4500000015	000000000000000021	5000000026	ODUBEY	Open	P33
5105600778	10	07/16/2017	4,040.00	USD	4,000.00	USD	4500000019	000000000000000023	5000000028	ODUBEY	Open	P33

Example control – 'Overpaid invoices against goods received'

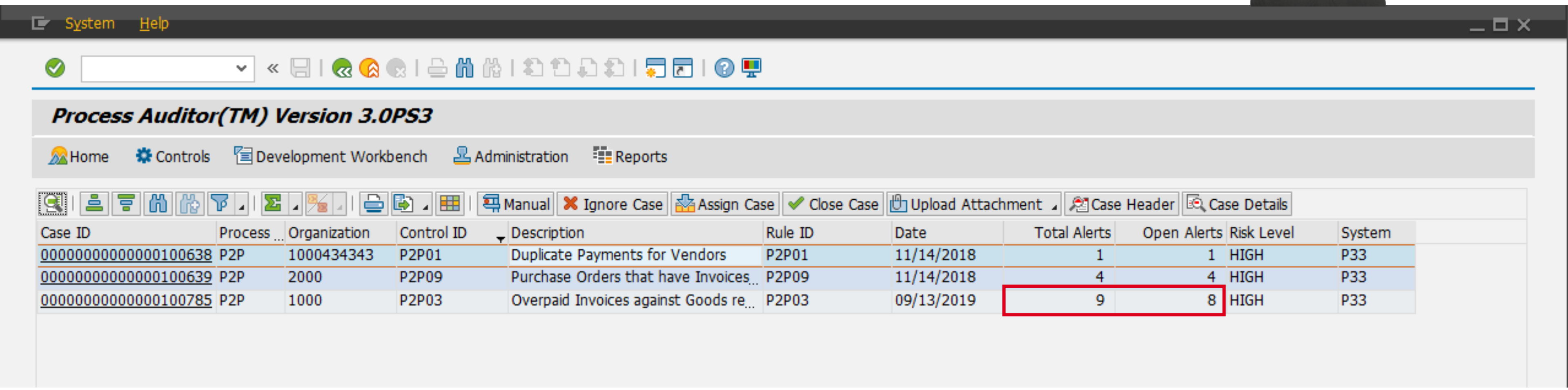


Example control – 'Overpaid invoices against goods received'



Invoice Number	Item	Created On	Invoice Amount	Currency	Purchasing Document	Material Number	Goods Receipt	Good Receipt Value	Currency	Created By	Status	System At
5105600773	10	07/16/2017	20,200.00	USD	4500000014	000000000000000021	5000000022	20,000.00	USD	ODUBEY	Closed - corrected	P33
5105600775	10	07/16/2017	30,300.00	USD	4500000015	000000000000000021	5000000025	30,000.00	USD	ODUBEY	Closed - key risk detected	P33
5105600775	20	07/16/2017	5,050.00	USD	4500000015	000000000000000021	5000000026	5,000.00	USD	ODUBEY	Open	P33
5105600776	10	07/16/2017	70,700.00	USD	4500000016	000000000000000021	5000000023	70,000.00	USD	ODUBEY		P33
5105600777	20	07/16/2017	50,500.00	USD	4500000017	000000000000000022	5000000024	50,000.00	USD	ODUBEY		P33
5105600774	10	07/16/2017	35,350.00	USD	4500000018	000000000000000022	5000000027	35,000.00	USD	ODUBEY		P33
5105600774	20	07/16/2017	15,150.00	USD	4500000018	000000000000000021	5000000027	15,000.00	USD	ODUBEY		P33
5105600774	30	07/16/2017	20,200.00	USD	4500000018	000000000000000021	5000000027	20,000.00	USD	ODUBEY		P33
5105600778	10	07/16/2017	4,040.00	USD	4500000019	000000000000000023	5000000028	4,000.00	USD	ODUBEY		P33

Example control – 'Overpaid invoices against goods received



Case ID	Process ...	Organization	Control ID	Description	Rule ID	Date	Total Alerts	Open Alerts	Risk Level	System
000000000000000100638	P2P	1000434343	P2P01	Duplicate Payments for Vendors	P2P01	11/14/2018	1	1	HIGH	P33
000000000000000100639	P2P	2000	P2P09	Purchase Orders that have Invoices...	P2P09	11/14/2018	4	4	HIGH	P33
000000000000000100785	P2P	1000	P2P03	Overpaid Invoices against Goods re...	P2P03	09/13/2019	9	8	HIGH	P33

Process Auditor Examples – Standard Controls

Business Controls

- Duplicate Payments for Vendors
- Zero Value Line Item in Purchase Order
- 3-way match - Changes to configuration for Price variances
- Critical vendor master data changes
- Aged GR/IR balance greater than £x
- Invoices cleared for payment without goods receipt
- Unmatched credit notes greater than x days old
- Employees and Vendors with Same Name or Address
- Changes in Payment Terms for customer or Vendors

IT Controls

- Detect Changes Made in Production Client Settings
- Detect If Changes To Customization Settings Are Allowed In Production Client
- Detect If Profile Parameter No Automatic User SAP* Is Not Activated
- Detect If Login Minimum Password Length Is Not Set To Proper Value
- Detect if Profile Parameter Login Fails To User Lock Is Not Set To Proper Value

Process Auditor Examples – Custom Controls

Type	Control Testing Rules
Config.	3 way match - Changes to configuration for Price variances
Config.	Changes to Critical/Sensitive vendor master data fields
Master Data	Double invoice check in vendor master data
Transaction	Aged GR/IR balances greater than £x
Transaction	Invoices cleared for payment without goods receipt
Transaction	Limit Orders - Invoice value exceeding PO value
Transaction	OTV - bank account used more than 3 x
Transaction	Unmatched credit notes greater than x days old
Transaction	Unmatched Direct Debit payments
Transaction	Duplicate invoices

Case Study - Duplicate Invoice Check

Features

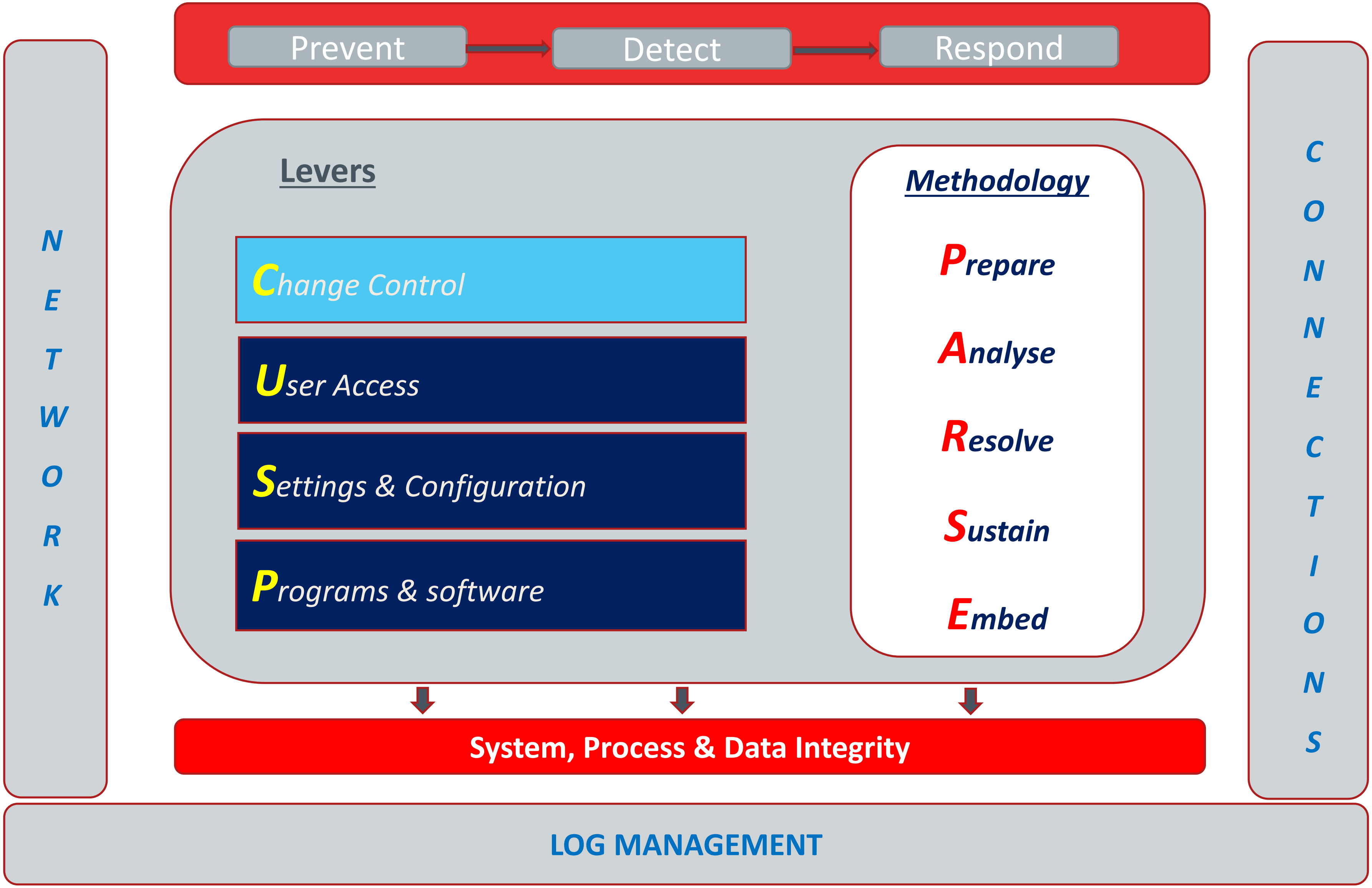
- Possible duplicates identified by matching on 5 fields – Vendor Number, Vendor Name, Invoice Reference Number, Invoice Date, Gross Value
- Grades assigned to possible duplicates based on number of matching fields => Allows prioritization and focus
- Fuzzy logic built into matching on Vendor Name and Invoice Reference
- Parameters to control fuzziness of matches e.g. minimum length of matching string for truncation, maximum length difference between strings
- Ability to control size of comparison set as well as selection set
- Upstream check as well as pre-payment check
- Performance enhancements with upfront indexing

CCM Roadmap

- Expand portfolio of standard IT and business controls
- Formalise key IT alerts by creating custom IT controls in Process Auditor
- Create additional custom business controls for P2P, O2C and RTR processes
- Upgrade modules and implement web/Fiori apps
- Integrate Process Auditor with other SW modules (e.g. Transaction Archive)
- Develop user intelligence and expand CCM accordingly

Part 5 – Wrap Up

Protecting SAP – The Technology Shield



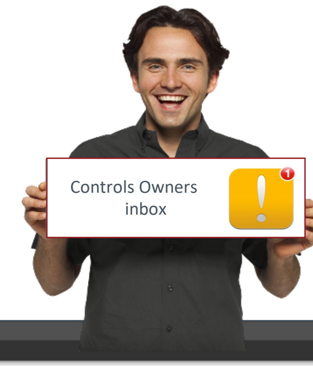
Summary/ Key Points

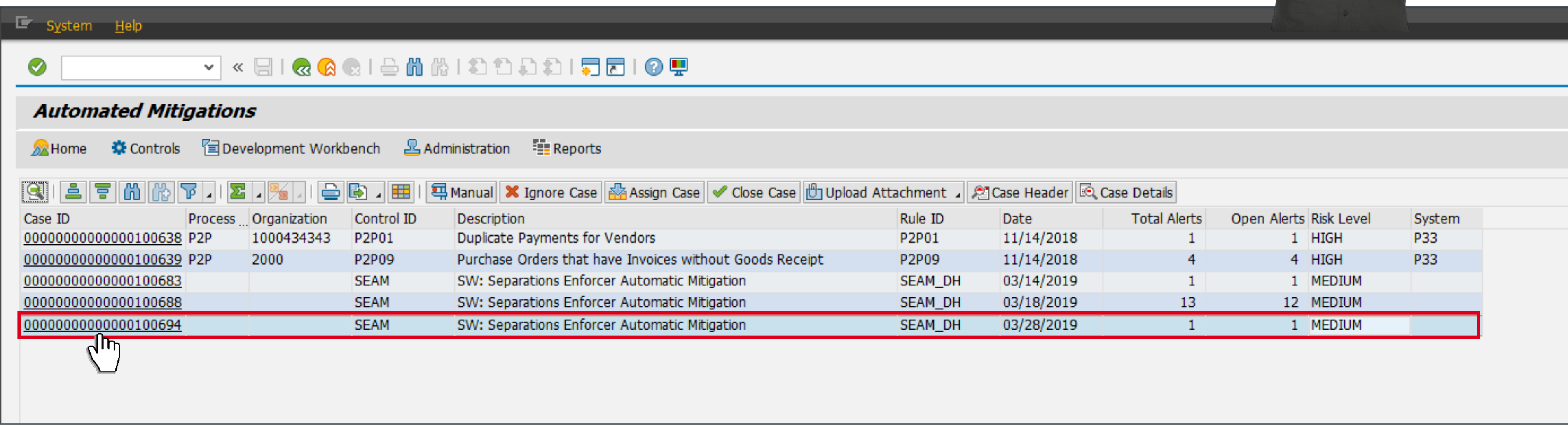
- Driving value from controls monitoring requires all 4 dimensions of People, Process, Technology and Data to be effective
- Manage Change Control, User Access, Settings & Configuration and Programs & Software as the levers of a Technology Shield
- Use a simple 5-Step PARSE methodology (Prepare, Analyse, Resolve, Sustain, Embed) to manage controls
- Enhance your Controls Platform with the right GRC Tool to drive effective prevention, detection and response
- Move from informal alerts to case management – formalise the management of controls exceptions by employing a process controls solution alongside informal alerts
- Unlock early value with IT Controls for system protection and business controls for cash leakage reduction

Questions?

APPENDIX

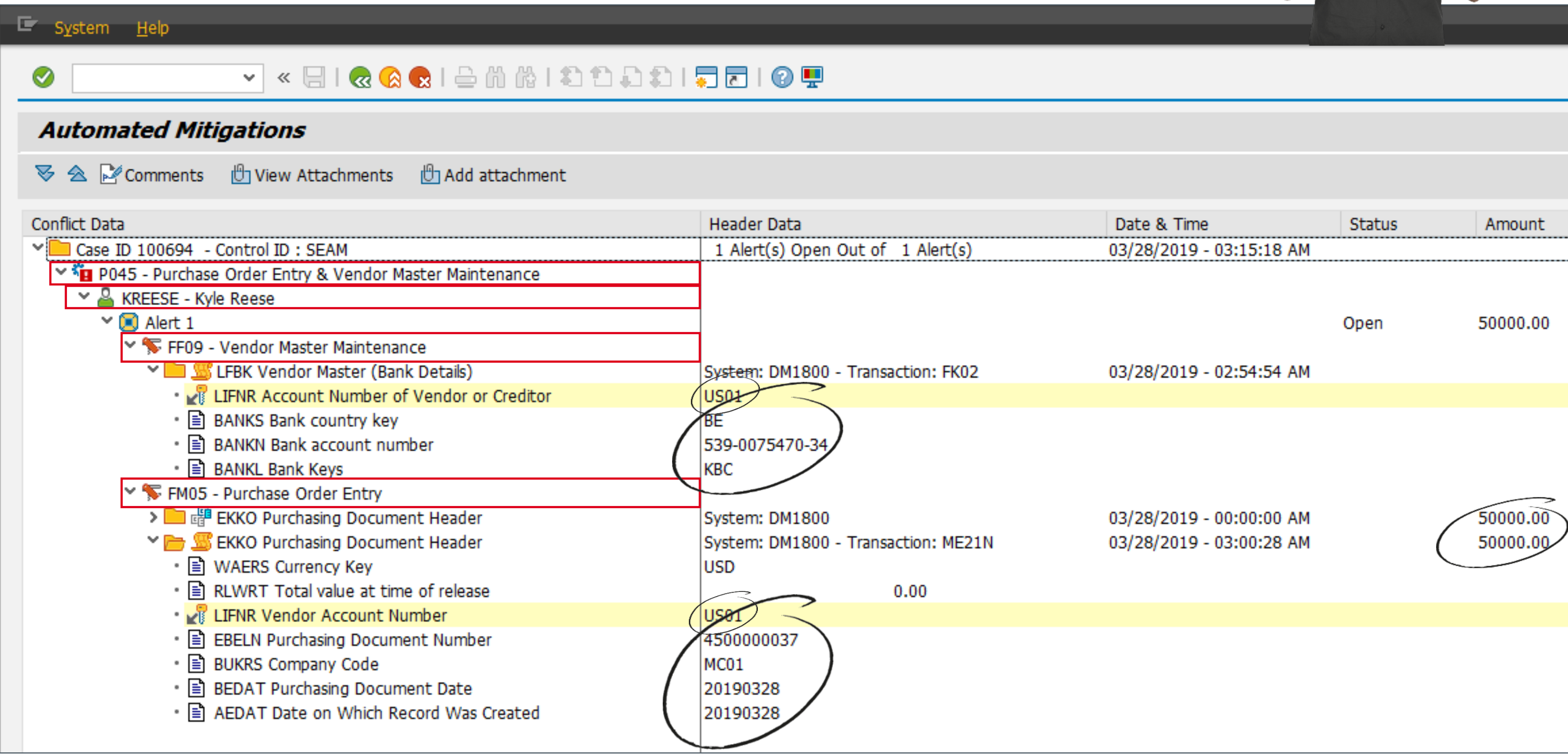
Example control: SoD-violation





Case ID	Process ...	Organization	Control ID	Description	Rule ID	Date	Total Alerts	Open Alerts	Risk Level	System
0000000000000100638	P2P	1000434343	P2P01	Duplicate Payments for Vendors	P2P01	11/14/2018	1	1	HIGH	P33
0000000000000100639	P2P	2000	P2P09	Purchase Orders that have Invoices without Goods Receipt	P2P09	11/14/2018	4	4	HIGH	P33
0000000000000100683			SEAM	SW: Separations Enforcer Automatic Mitigation	SEAM_DH	03/14/2019	1	1	MEDIUM	
0000000000000100688			SEAM	SW: Separations Enforcer Automatic Mitigation	SEAM_DH	03/18/2019	13	12	MEDIUM	
0000000000000100694			SEAM	SW: Separations Enforcer Automatic Mitigation	SEAM_DH	03/28/2019	1	1	MEDIUM	

Example control: SoD-violation



serco

CCM Roadmap

- Expand portfolio of standard IT and business controls
- Formalise key IT alerts by creating custom IT controls in Process Auditor
- Create additional custom business controls for P2P, O2C and RTR processes
- Upgrade and implement web/Fiori version of Process Auditor
- Integrate Process Auditor with other SW modules (e.g. Transaction Archive)
- Develop user intelligence and expand CCM accordingly

www.serco.com

Serco Group plc.
Serco House
16 Bartley Wood Business Park
Bartley Way, Hook
Hampshire RG27 9UY
United Kingdom

For general enquiries contact:
T: +44 (0)1256 745 900
E: generalenquiries@serco.com