Deloitte.

Access Control Monitoring Solution (ACMS)

One stop solution for all your user access management needs

Introduction

Segregation of Duties (SoD) - A building block for sustainable user access risk management.

The principle of SoD is based on shared responsibilities of key business process that distributes access to the critical functions of that process to more than one person. Without this segregation in key processes, there is a higher possibility of errors and fraud risks.

Business need

With growing regulatory requirements, organisations need a centralised platform where they can manage user access risks across business applications. In the absence of a Governance Risk Compliance (GRC) solution, businesses today are facing challenges to:

- Manage, monitor, report and mitigate key risks arising from loosely defined user access.
- Improve compliance stature while reducing the cost of controls operation
- Compare cross-application user access, thereby increasing their exposure to financial frauds
- Obtain comprehensive insights for effective and timely decision-making

ACMS overview

Access Control Monitoring Solution (ACMS) is an ABAP based SAP custom program (compatible with SAP ECC and HANA versions) that helps organisations manage their SoD and critical access through a centralised platform in a robust manner.

Powered by Deloitte India's Risk Advisory knowledge and content, it gives our clients access to the golden SoD rulebook and mitigation controls library, for industry benchmarking. ACMS also provides stakeholder specific landing pages, and visualisation dashboards tailored to suit the varied reporting and monitoring needs of businesses.

Engagement models

SoD diagnostics/ health check

- Analyses of system health pertaining to user access
- Data extraction from SAP by running scripts in production environment
- Offline analysis with output –
  - SOD violation report / matrix
  - SOD dashboard
  - Detailed user and role level conflict reports
  - Custom transaction analysis for redundancy

User access review advisory

- ACMS deployment in production environment to set up user access review and monitoring
- Cross system SOD comparison for third party applications
- Online ongoing monitoring with
  - SOD reports and dashboards
  - Pre-check for SOD conflicts
  - UAR ageing reports
  - Tracking of remediation / mitigation actions
  - Rulebook and mitigation controls maintenance
  - Tool support

ACMS tool implementation

- ACMS deployment in production environment to set up user access review and monitoring
- Tool implementation, building content and hand over including
  - End-User training
  - User Manuals and tool documentation
  - Tool maintenance support (if needed)
  - Standard reports and visualisation packs

Access Control Monitoring Solution (ACMS)

Benefits of ACMS

Business challenges	How ACMS can help
High technology implementation cost for a centralised GRC solution (hardware and software licenses)	Custom solution deployed on existing SAP landscape. No additional hardware or software cost to be incurred
Difficulty in managing cross application SoD conflicts	One stop solution for compliant user access management for SAP and other third-party applications
Unavailability of user-friendly reports to review and monitor user access conflicts	Insightful reports with SOD heat map tailored to meet stakeholder requirements
Lack of awareness with users regarding sensitive and conflicting access (while requesting/approving access)	Capability of pre-check for SOD conflicts and sensitive access before granting user access
Difficulty in tracking actions for remediation and mitigation of identified conflicts	Centralised solution to initiate and track mitigation / remediation actions for SOD conflicts
Lack of access to industry leading practices to manage access related risks	Includes Deloitte global SOD rulebook and standard reports for SOD and sensitive access management
Dealing with audit findings related to SOD, sensitive access and user access review controls	Offers capability to monitor, mitigate and track user access review activities on a single platform, while maintaining required documentation to support future reviews

Access Control Monitoring Solution (ACMS)

Deployment approach

We propose a three-phased approach to implement ACMS to minimise operational impact and provide a model that is tailored for your needs

Risk content benchmarking

- Baseline existing rulebook against business process
- Analyse custom transactions
- Identify critical transactions
- Design benchmarked SOD rulebook

Tool design and deployment

- Design and blueprint ACMS features
- Develop and customise tool
- Conduct Unit testing in development environment
- Conduct User Acceptance testing in quality environment

Go live and training

- Create user manuals
- Train end users
- Set up reports and dashboards

Key differentiators

1. Content

Tailor made rule book

Combining Deloitte's golden rule book with clients' existing SoD rulebook and custom transaction landscape, to build a tailor made best practice rulebook

Mitigation controls library

Providing access to Deloitte's global library of suggested mitigation plans combined with clients' risk and controls matrix to create a centralised library for access risks

Standardised visualisation pack

Standard dashboards, SoD and violation reports with key KPIs for effective decision making

2. Reduced cost of controls with ACMS

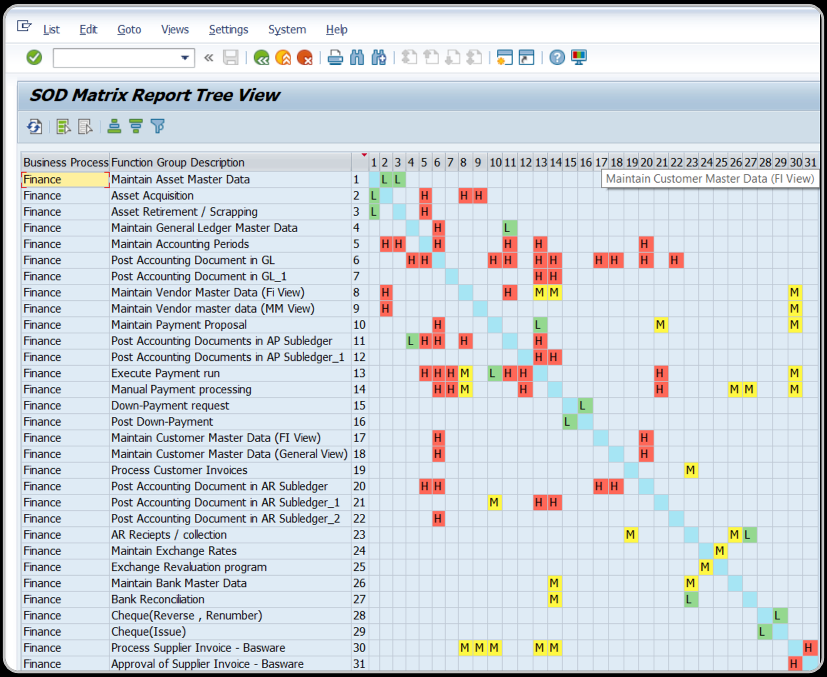
Cost element	Tangible Benefit with ACMS
Hardware	No cost
Software	No cost
License Cost	Works with existing SAP licenses
Dashboarding	Tableau / PowerBi (existing client licenses)
Support & Maintenance	Existing SAP support team

Access Control Monitoring Solution (ACMS)

Sample reports

SOD risk matrix

Business process wise SOD matrix report (with risk categorisation of conflict)



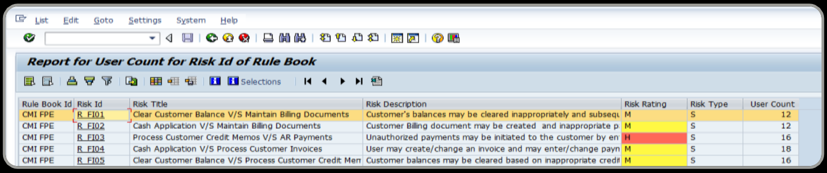
SOD Matrix Report Tree View

Maintain Customer Master Data (FI View)

Business Process	Function Group Description		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Finance	Maintain Asset Master Data	1		L	L																												
Finance	Asset Acquisition	2	L				H			H	H																						
Finance	Asset Retirement / Scrapping	3	L				H																										
Finance	Maintain General Ledger Master Data	4						H					L																				
Finance	Maintain Accounting Periods	5		H	H			H					H		H							H											
Finance	Post Accounting Document in GL	6				H	H					H	H		H	H			H	H		H		H									
Finance	Post Accounting Document in GL_1	7													H	H																	
Finance	Maintain Vendor Master Data (Fi View)	8		H									H		M	M																M	
Finance	Maintain Vendor master data (MM View)	9		H																												M	
Finance	Maintain Payment Proposal	10						H							L								M									M	
Finance	Post Accounting Documents in AP Subledger	11				L	H	H		H					H																		
Finance	Post Accounting Documents in AP Subledger_1	12													H	H																	
Finance	Execute Payment run	13					H	H	H	M		L	H	H									H									M	
Finance	Manual Payment processing	14						H	H	M				H									H					M	M			M	
Finance	Down-Payment request	15																L															
Finance	Post Down-Payment	16															L																
Finance	Maintain Customer Master Data (FI View)	17						H														H											
Finance	Maintain Customer Master Data (General View)	18						H														H											
Finance	Process Customer Invoices	19																							M								
Finance	Post Accounting Document in AR Subledger	20					H	H											H	H													
Finance	Post Accounting Document in AR Subledger_1	21										M			H	H																	
Finance	Post Accounting Document in AR Subledger_2	22						H																									
Finance	AR Reciepts / collection	23																			M							M	L				
Finance	Maintain Exchange Rates	24																									M						
Finance	Exchange Revaluation program	25																								M							
Finance	Maintain Bank Master Data	26														M									M								
Finance	Bank Reconciliation	27														M									L								
Finance	Cheque(Reverse , Renumber)	28																													L		
Finance	Cheque(Issue)	29																												L			
Finance	Process Supplier Invoice - Basware	30								M	M	M			M	M																	H
Finance	Approval of Supplier Invoice - Basware	31																														H	

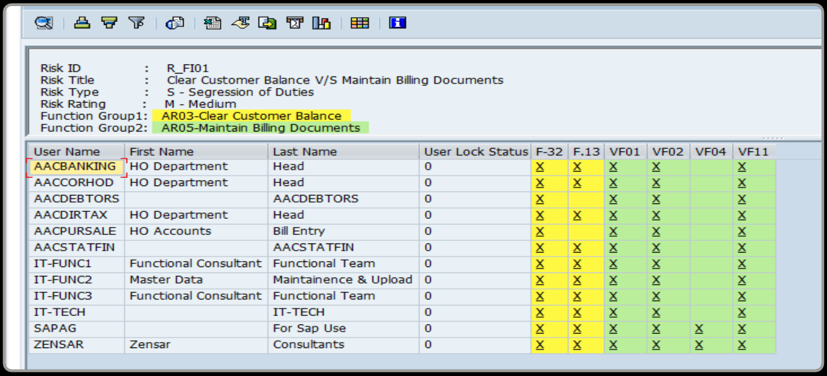
User violation report

User wise access violation report, with drill down reporting to identify and review conflicting authorisations



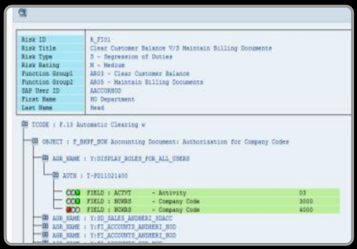
Report for User Count for Risk Id of Rule Book

Rule Book Id	Risk Id	Risk Title	Risk Description	Risk Rating	Risk Type	User Count
CMI FPE	R_FI01	Clear Customer Balance V/S Maintain Billing Documents	Customer's balances may be cleared inappropriately and subsequ	M	S	12
CMI FPE	R_FI02	Cash Application V/S Maintain Billing Documents	Customer Billing document may be created and inappropriate p	M	S	12
CMI FPE	R_FI03	Process Customer Credit Memos V/S AR Payments	Unauthorized payments may be initiated to the customer by en	H	S	16
CMI FPE	R_FI04	Cash Application V/S Process Customer Invoices	User may create/change an invoice and may enter/change payn	M	S	18
CMI FPE	R_FI05	Clear Customer Balance V/S Process Customer Credit Men	Customer balances may be cleared based on inappropriate credi	M	S	16



Risk ID : R_FI01
Risk Title : Clear Customer Balance V/S Maintain Billing Documents
Risk Type : S - Segression of Duties
Risk Rating : M - Medium
Function Group1: AR03-Clear Customer Balance
Function Group2: AR05-Maintain Billing Documents

User Name	First Name	Last Name	User Lock Status	F-32	F.13	VF01	VF02	VF04	VF11
AACBANKING	HO Department	Head	0	X	X	X	X		X
AACCORHOD	HO Department	Head	0	X	X	X	X		X
AACDEBTORS		AACDEBTORS	0	X		X	X		X
AACDIRTAX	HO Department	Head	0	X	X	X	X		X
AACPURSALE	HO Accounts	Bill Entry	0	X		X	X		X
AACSTATFIN		AACSTATFIN	0	X	X	X	X		X
IT-FUNC1	Functional Consultant	Functional Team	0	X	X	X	X		X
IT-FUNC2	Master Data	Maintainence & Upload	0	X	X	X	X		X
IT-FUNC3	Functional Consultant	Functional Team	0	X	X	X	X		X
IT-TECH		IT-TECH	0	X	X	X	X		X
SAPAG		For Sap Use	0	X	X	X	X	X	X
ZENSAR	Zensar	Consultants	0	X	X	X	X	X	X



Risk ID	R_FI01
Risk Title	Clear Customer Balance V/S Maintain Billing Documents
Risk Type	S - Segression of Duties
Risk Rating	M - Medium
Function Group1	AR03 - Clear Customer Balance
Function Group2	AR05 - Maintain Billing Documents
SAP User ID	AACCORHOD
First Name	HO Department
Last Name	Head

```
TCODE : F.13 Automatic Clearing w
  OBJECT : F_BKPF_BUK Accounting Document: Authorisation for Company Codes
    AGR_NAME : Y:DISPLAY_ROLES_FOR_ALL_USERS
      AUTH : T-FD11021400
        FIELD : ACTVT     - Activity          03
        FIELD : BUKRS     - Company Code      3000
        FIELD : BUKRS     - Company Code      4000
    AGR_NAME : Y:SD_SALES_ANDHERI_SDACC
    AGR_NAME : Y:FI_ACCOUNTS_ANDHERI_HOD
    AGR_NAME : Y:FI_ACCOUNTS_ANDHERI_HOD
```

Connect with us

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Peeyush Vaish
Partner, Risk Advisory
Deloitte India
peeyushvaish@deloitte.com

Senthil Kaliyamurthy
Partner, Risk Advisory
Deloitte India
senthilvelk@deloitte.com

Shuchi Sangal
Partner, Risk Advisory
Deloitte India
ssangal@deloitte.com

Nitin Naredi
Partner, Risk Advisory
Deloitte India
nitinnaredi@deloitte.com

Deloitte.

This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTI LLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed

on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.