Team Polymaths

Smartsheet: Streamlining Identity Access Management for SOX Controls

Adrian Lavergne | Lelo Gemtessa

Nikhil Shenoy | Kinjal Raut

MAY 2024

The Team

Lelo Gemtessa

PM

Adrian Lavergne

UX

Nikhil Shenoy

Developer

Kinjal Raut

Developer

Background

Federal regulation (SOX) requires publicly traded companies to conduct periodic user access reviews to ensure access rights align with authorized employees' roles and responsibilities.

Problem

The current quarterly user access review process involves manual, time-consuming labor with scattered data.

Objective

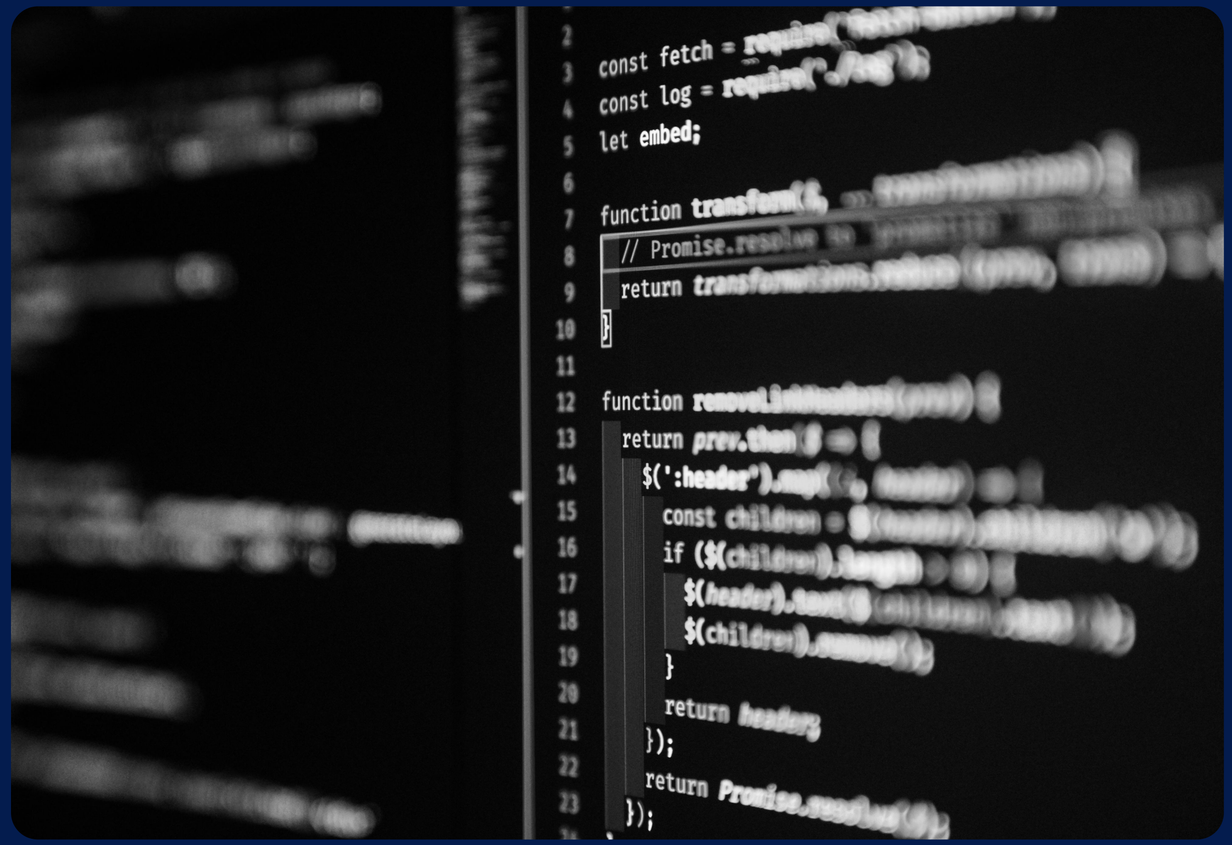
Our objective is to streamline the user access review process. This is to increase accuracy, decrease security risks, and reduce manual labor.

Phase 1

Development

Previous Work

- Integration between the in-scope systems and Smartsheet portal
- Access Request Automation
- Saving 1400 billable hours/quarter



Pain Points

Inefficient Account Review Process

Without a streamlined flagging system based on researched parameters, identifying which accounts needed to be reviewed regularly would have been a challenging and potentially subjective task.

Manual Identity Access Process

Pre-automated system, the Identity Access Management (IAM) process involved excessive manual effort, including filtering evidence sheets and importing data for QUAR. This process was prone to errors and inefficient.

Time Intensive

Manual IAM processes require significant human resources. These repetitive and time-consuming tasks detracts from focusing on higher-value activities, such as strategic planning or improving security protocols.

Solution Implementation

Automated Access Review Sheets

Enhanced the Python script to automatically create user access review sheets and implement flagging to remove inactive, non-privileged and service accounts.

KPI Tracking

- ~2000 total accounts removed this quarter
- 600 billable hours of labor saved / FY

Flagging Non Privileged Accounts

Email	Id	Name	Role
john.smith@smartsheet.com	0055a000007pXXWAA2	John Smith	Plan
jane.doe@smartsheet.com	0055a0000089CMYAA2	Jane Doe	Plan
adrian.l@smartsheet.com	0055a000007qLZaAAM	Adrian L	Plan
nikhil.shenoy@smartsheet.com	0055a00000AqIZXAA3	Nikhil Shenoy	Developer
jim.carrey@smartsheet.com	0055a000007pUHfAAM	Jim Carrey	Plan
lelo.gemtassa@smartsheet.com	0050b000005CsKZAA0	Lelo Gemtassa	User
jiya.parekh@smartsheet.com	0055a00000AqYw8AAF	Jiya Parekh	Member
riya.jain@smartsheet.com	0055a000007q9XMAAY	Riya Jain	Plan
matt.doe@smartsheet.com	0055a00000AVo40AAD	Matt Doe	Developer
john.rick@smartsheet.com	0055a00000AVo40BBD	John Rick	User
marissa.mar@smartsheet.com	0055a00000AVo58KKW	Marissa Mar	Developer

Row Attachment

	Account Owner	Department	Position	System	Account Name	System Entitlement
1	nikhil.shenoy@sma			System A	Nikhil Shenoy	Developer
2	matt.doe@smartsh			System A	Matt Doe	Developer
3	Marissa Mar			System A	Marissa Mar	Developer

QUAR Sheet

Non-Privileged Roles	Complete	System Count	Output Count	Master Sheet Count
user, plan, member	☑	11		3

Evidence Sheet

Flagging Service Accounts

Name	mail	SamAccountName	Descriptio	Group Nar	User Mana	Group Managed By
Aniket Chatterjee	Aniket.Chatterjee@smartsheet.com	achatterjee	Sr. SE I	Artifactory	Richard.N	Artifactory Owners
Richard Noble	Richard.Noble@smartsheet.com	rnoble	Manager, I	Artifactory	Iain.J.Wat	Artifactory Owners
Nathan Higgins	Nathan.Higgins@smartsheet.com	nhiggins	Sr. SE II	Artifactory	Richard.N	Artifactory Owners
Martin Waite	Martin.Waite@smartsheet.com	mwaite	Sr. SE II	Artifactory	Richard.N	Artifactory Owners
Jonathan Ricci	jonathan.ricci@smartsheet.com	jricci	SE II	Artifactory	Richard.N	Artifactory Owners
Freddie Leighton	frederick.leighton@smartsheet.com	fleighton	SE II	Artifactory	Richard.N	Artifactory Owners
Dudu Hazal OK	dudu.hazalok@smartsheet.com	dhazalok	Sr. SE I	Artifactory	Richard.N	Artifactory Owners
Administrator		Administrator	Built-in ac	Administrators		
Victoria Walsh - X	vwalsh-x@smartsheet.com	vwalsh-x		Administrators		
Config LocalAdmin		ConfigMgrLocalAdmin	SCCM loca	Administrators		
SVC_SS_APOLLO Service Account		svc_ss_apollo	Service Ac	Administrators		
SVC_VScan_SVR_Win Service Account		svc_vscan_svr_win	Service Ac	Administrators		
bi-service-ad-auth		bi-service-ad-auth	This accou	bdp-airflow-users		bdp-airflow-admins
Anand Siloju	Anand.Siloju@smartsheet.com	asiloju	Sr. Data Er	bdp-airflo	john.wiltse	bdp-airflow-admins
Vikram Bhamidipati	Vikram.Bhamidipati@smartsheet.com	vbhamidipati	Principal D	bdp-airflo	john.wiltse	bdp-airflow-admins
John Wiltse	john.wiltse@smartsheet.com	jwiltse	Director, B	bdp-jenkin	kaushik.mi	bdp-jenkins-admins
Chris Acuna	chris.acuna@smartsheet.com	cacuna	Sr. Technic	bdp-jenkin	muthuram	bdp-jenkins-admins
Monica Poinescu	Monica.Poinescu@smartsheet.com	mpoinescu	Sr Softwar	bdp-jenkin	john.wiltse	bdp-jenkins-admins
Djordje Savovic	Djordje.Savovic@smartsheet.com	dsavovic	SDET II	bdp-jenkin	john.wiltse	bdp-jenkins-admins

Row Attachment

Mail	Account Name	System Entitlement	Status	Service Accounts
Email	Name	Role	Active	
mail	SamAccountName	Group Name	Active	svc_vscan_svr_win, svc_lm_monitoring, svc-rpa-stripe, svc_scom_action, itautosvc, svc_scom_action_sql, bi-service-ad-auth, svc_ss_apollo

Evidence Sheet

Aniket.Chatterjee			SA1.Active Directory	achatterjee	Artifactory Owners
Richard.Noble@			SA1.Active Directory	rnoble	Artifactory Owners
Nathan.Higgins@sr			SA1.Active Directory	nhiggins	Artifactory Owners
Martin.Waite@smar			SA1.Active Directory	mwaite	Artifactory Owners
jonathan.ricci@sma			SA1.Active Directory	jricci	Artifactory Owners
frederick.leighton@			SA1.Active Directory	fleighton	Artifactory Owners
dudu.hazalok@sma			SA1.Active Directory	dhazalok	Artifactory Owners
			SA1.Active Directory	Administrator	Administrators
vwalsh-x@smartsh			SA1.Active Directory	vwalsh-x	Administrators
			SA1.Active Directory	ConfigMgrLocalAdm	Administrators
canderson-x@sma			SA1.Active Directory	canderson-x	Administrators
sbell-x@smartshee			SA1.Active Directory	sbell-x	Administrators
csachs-x@smartsh			SA1.Active Directory	csachs-x	Administrators
john.wiltse@smarts			SA1.Active Directory	jwiltse	bdp-airflow-admins
Monica.Poinescu@			SA1.Active Directory	mpoinescu	bdp-airflow-users
Djordje.Savovic@s			SA1.Active Directory	dsavovic	bdp-airflow-users

QUAR Sheet

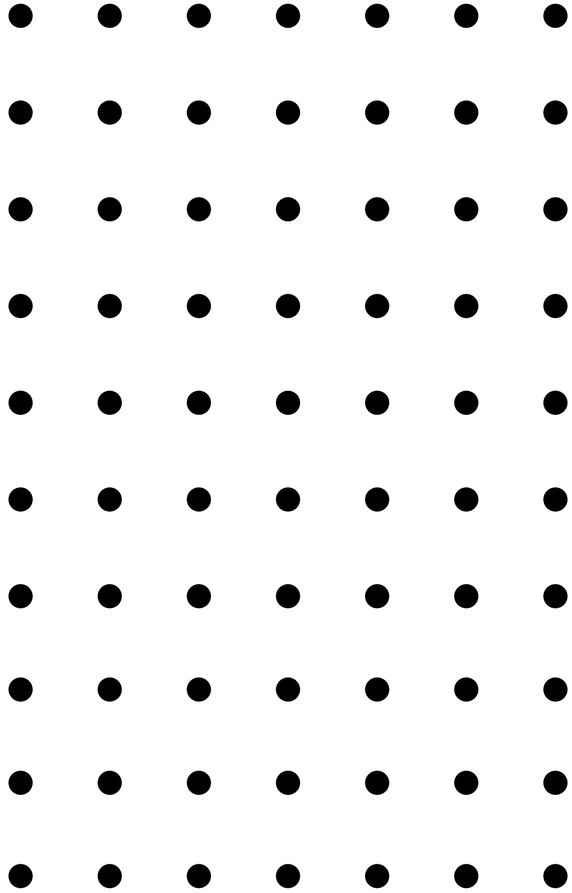
The Benefits

Streamlined Reviews

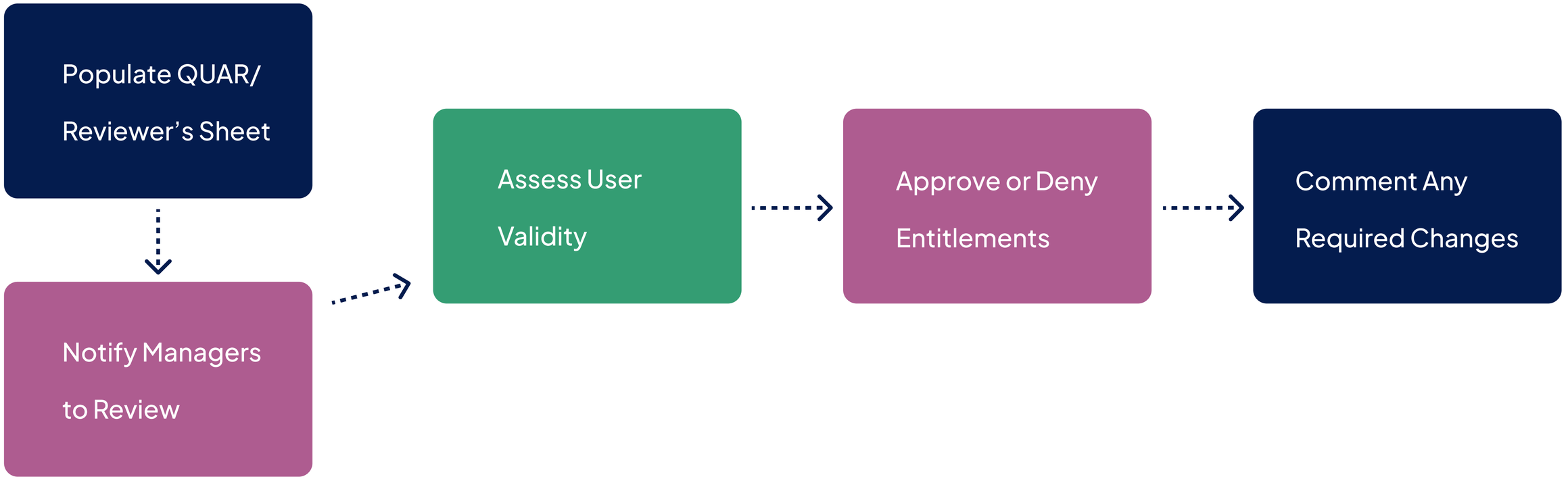
- Automated workflows reduce manual effort
- Reduce risk of unauthorized access
- Improved accuracy of user access data

Phase 2

User Experience



User Access Review Process



Pain Points

Resource Intensive

Current process requires significant manpower and managerial oversight

Lack of Understanding

Reviewers are required to understand the roles / entitlements they are reviewing without resources

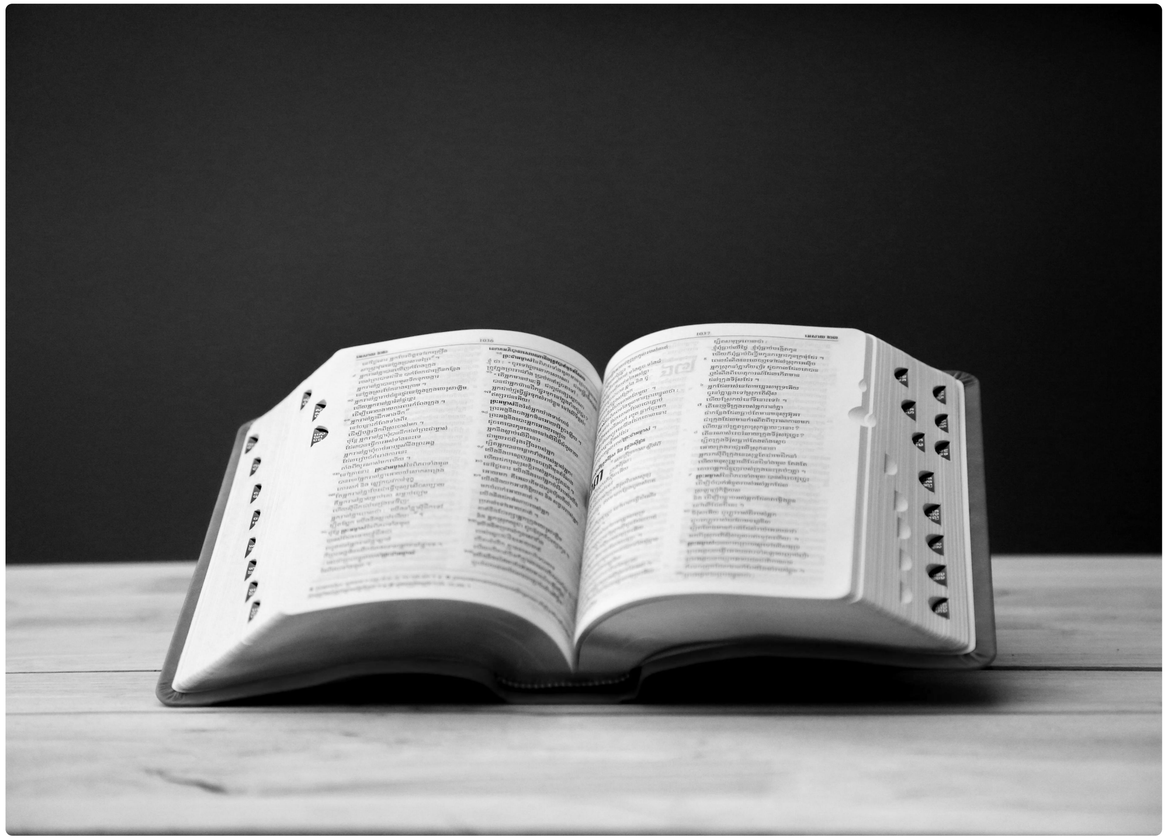
Security Risks

Manual efforts and incompetence may lead to incomplete or inaccurate reviews

Solution Implementation

Centralized Data Dictionary

We interviewed all system owners in scope for SOX and created a data dictionary defining all user access and their risks so managers can understand what their reviewing at a glance.



Before

Uncategorized systems with no definitions or risk levels led to uninformed decision making.

	Risk Type	Privilege	Definition
1		Fidelis Data Sync Pro	
2		Xenon API Gateway	
3		Triton WorkFlow Automation	
4		Comet Comms Suite	
5		Radiant API V9	
6		Data Map Integrator N-4	
7		Nemrat File Transfer Protocol S1	
8		Cascade Batch Process System	
9		Cobalt Sync Custom	
10		Spectrum Access Provisioner	
11		Argon Resource Engine w/o 2F	
12			

After

Definitions and risk levels are included. Color coded for fast info at a glance.

Risk Type	Privilege	Definition
	High Risk	
	Spectrum Access Provisioner	Admins can manage access controls and provisions to verify
	Triton WorkFlow Automation	Admins can manage access controls and permissions, ensur
	Nemrat File Transfer Protocol S1	Users have the ability to transfer sensitive files across networ
	Radiant API V9	System administrators can configure API integrations, manag
	Medium Risk	
	Cascade Batch Process System	Allows users to set up, execute, and monitor batch processin
	Argon Resource Engine w/o 2F	Users can manage resource allocation and monitor system p
	Xenon API Gateway	Users can manage API configurations, monitor traffic, and en
	Low Risk	
	Comet Comms Suite	Provides tools for managing internal communications, setting
	Cobalt Sync Custom	Read-only users can customize data synchronization settings
	Data Map Integrator N-4	Provides limited tools for mapping and transforming data fron

The Benefits

Improved efficiency

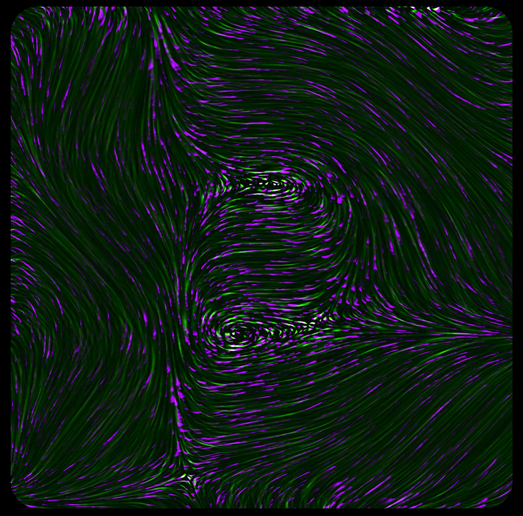
- Increase manager’s comprehension of system access and risks.
- Facilitates quicker audits with readily accessible data.
- Improves communication and collaboration between teams.

Phase 3
Outcomes

IMPACT

Our solution has improved compliance efforts, optimizing access reviews and centralizing entitlement management, resulting in decreased cost and security risks.

Future Opportunities



Further Automation

Utilizing NLP to securely assist system owners.

System UX Writing

Enhancing system comprehensibility.

Robust Notifications

Iterating upon internal IT notification systems.

Thank You!

Adrian Lavergne | Lelo Gemtessa

Nikhil Shenoy | Kinjal Raut