



Implementation of RBAC and Data Classification

Steve Tresadern
Rui Miguel Feio

RSM Partners

December 2014
v1.7



Agenda

- **Introductions**
- **Data Classification & Ownership**
- **Role-Based Access Control (RBAC)**
- **Maintain the environment**
- **Results**
- **Q&A**

Who are we?

- ***Steve Tresadern***

- ***27 years mainframe experience***
- ***Former z/OS Systems Programmer***
- ***Experience in Cryptography, RACF, Compliance***

- ***Rui Miguel Feio***

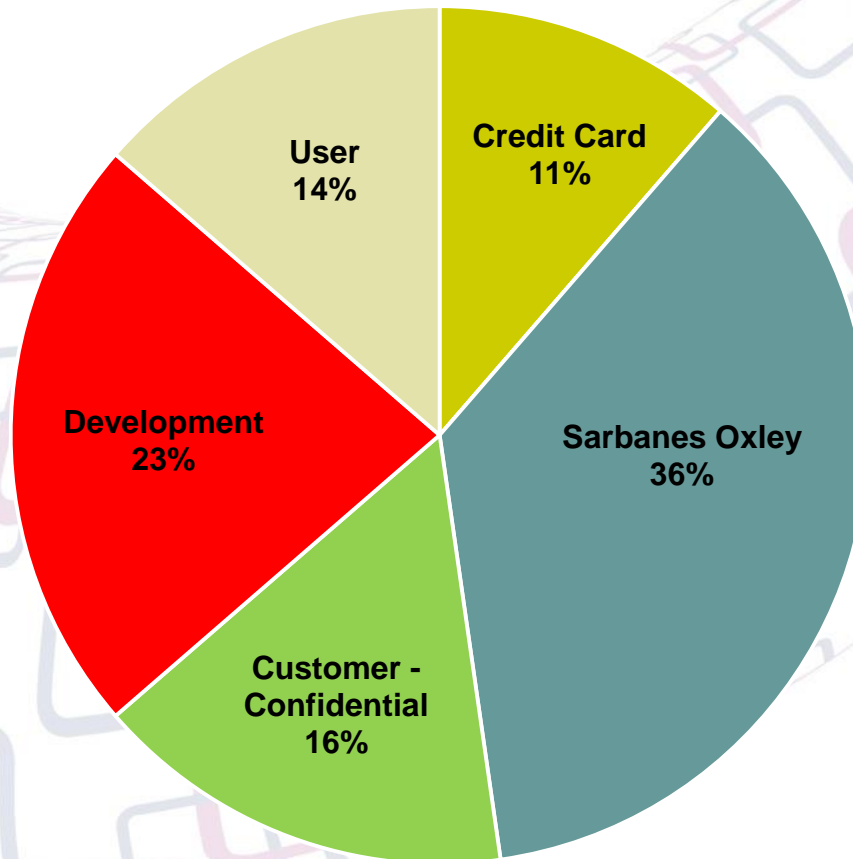
- ***15 years mainframe experience***
- ***Experience in z/OS, RACF, zSecure, Development***
- ***Last 4 years working in Security and implementing RBAC***



**DATA CLASSIFICATION
&
OWNERSHIP**

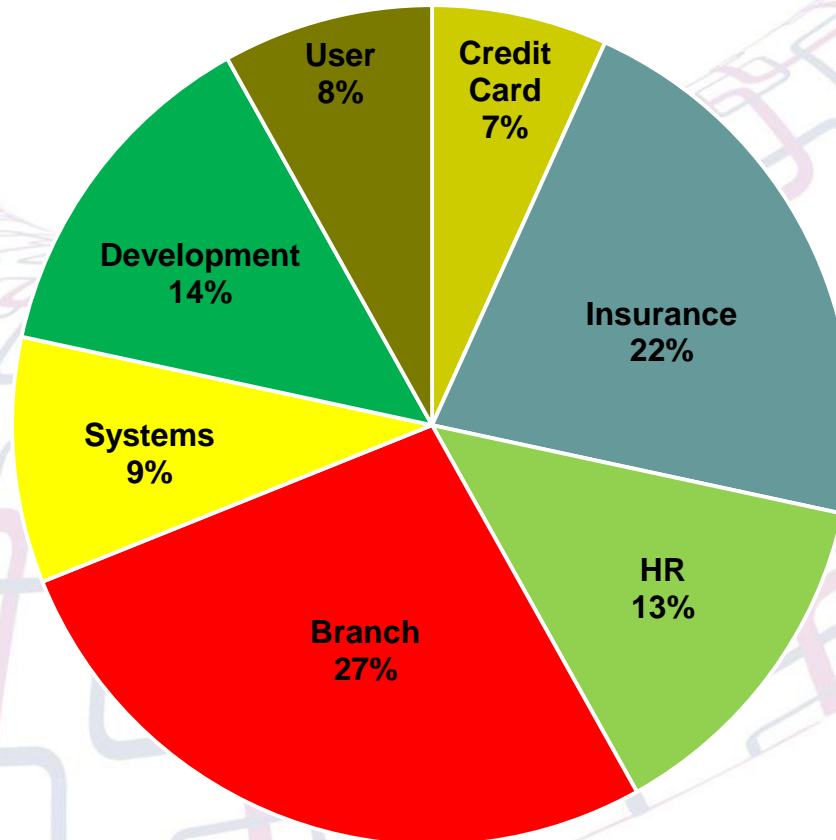
Data Classification – What is it?

- *Understanding what your data is*



Data Classification – What is it?

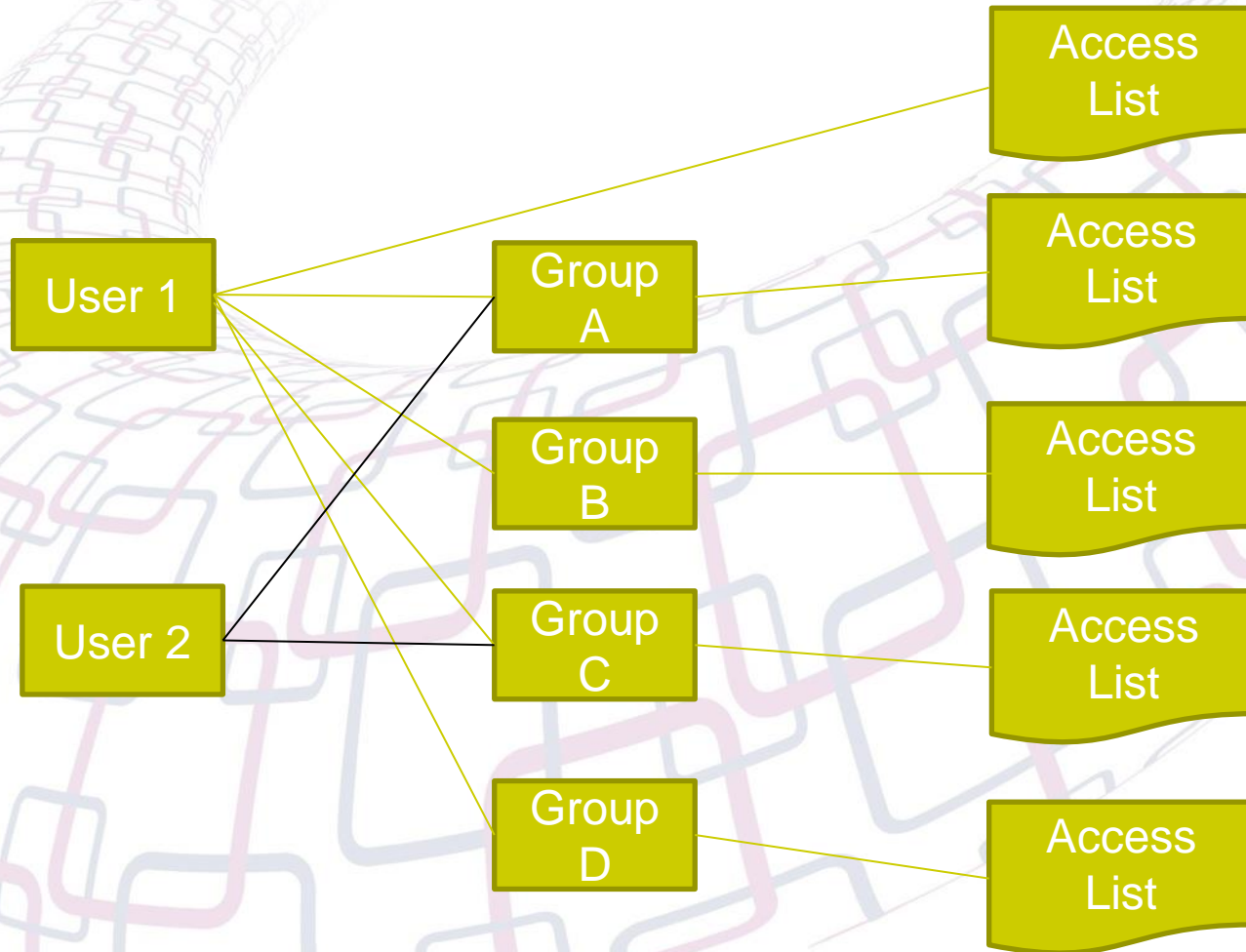
- *Who owns your data*



Data Classification – Reasons to do it

- *Audit requirements*
- *Compliance*
- *Who has privileged access?*
- *Who is accessing confidential information?*
- *Reduce the risk of fraud?*

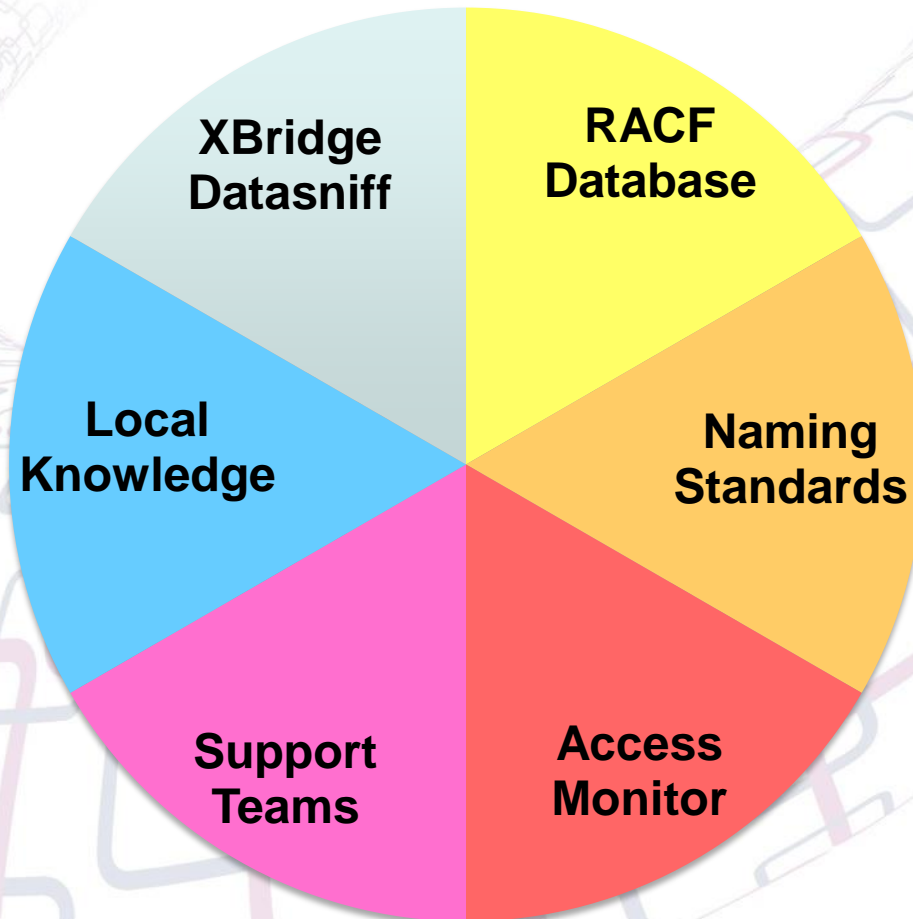
Data Classification – Reasons to do it



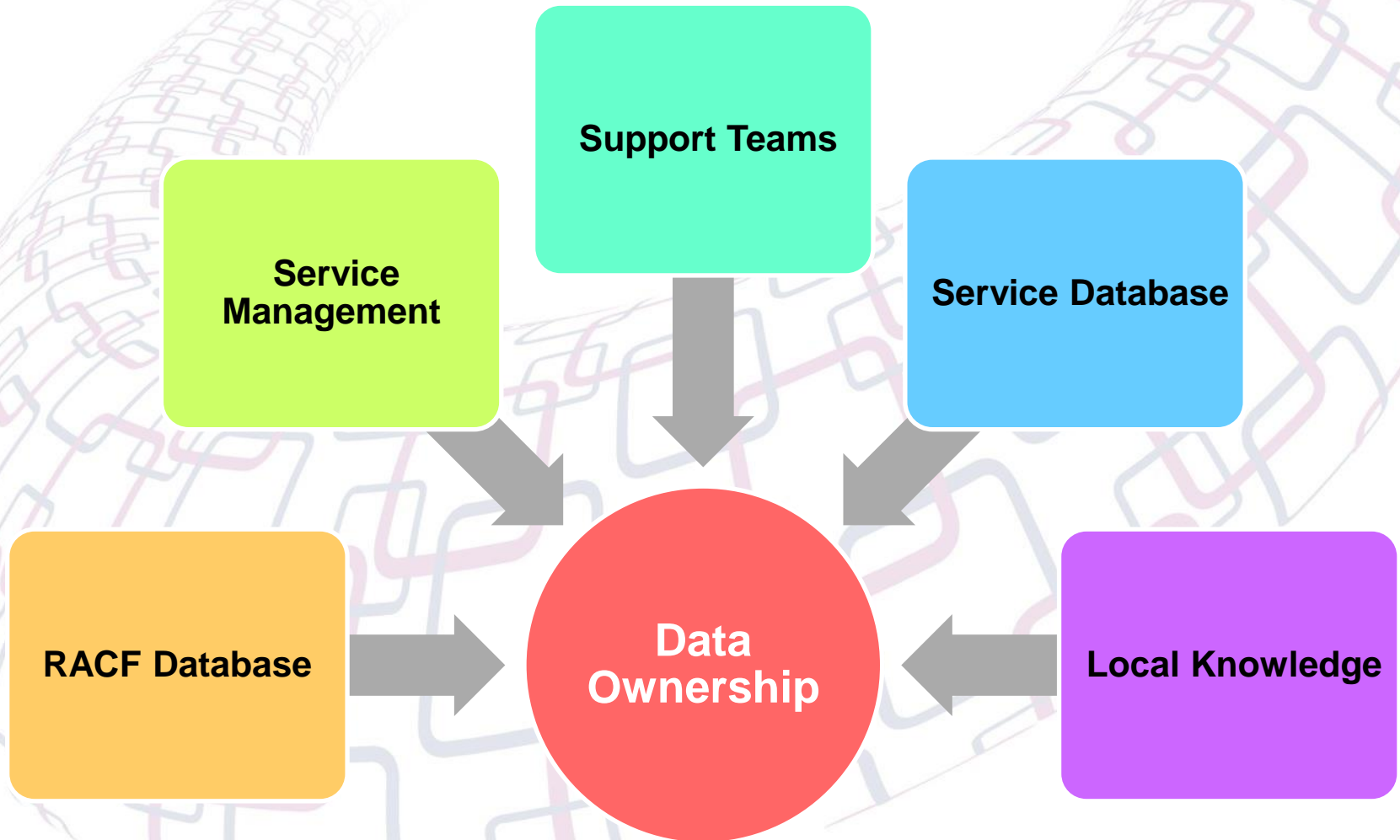
Data Classification – Aims

- ***Every dataset and resource profile must be;***
 - ***Classified in terms of confidentiality and integrity.***
 - ***All linked to an application.***
 - ***The basic security correctly defined***
 - ***Understand who has privileged access***
- ***All applications have a business/data owner.***
 - ***Ideally they should approve all access***
 - ***Review who has access***

Sources for Data Classification



Sources for Data Ownership



Data Classification – Challenges

- **Lack of knowledge in support teams**
- **Development Team Processes**
- **Business areas cooperation**
- **Non-RACF based security**
- **Unravelling of the environment**
- **Service Database – Up to date?**

Data Classification Benefits





ROLE-BASED ACCESS CONTROL (RBAC)

RBAC – Reasons to do it

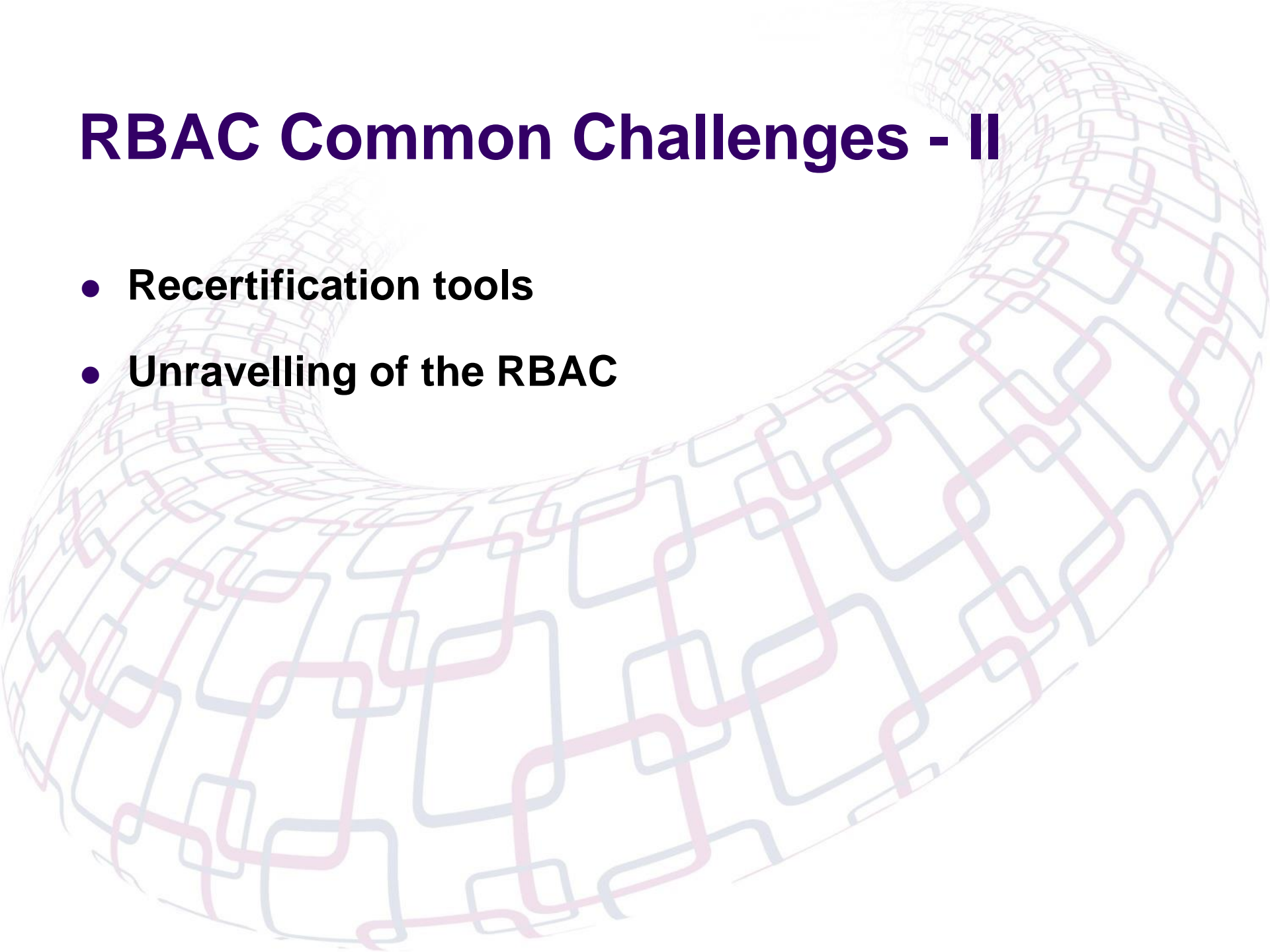
- ***Business organisation keeps changing***
- ***Managing the mainframe security environment***
- ***Audit requirements***
- ***Compliance***
- ***Recertification***
- ***Remove access not required***

RBAC Common Challenges - I

- **Historical code**
- **Global Access Table (GAT)**
- **Lack of technical knowledge**
- **Business areas cooperation**
- **Least Privilege access implementation**
- **DB2**

RBAC Common Challenges - II

- **Recertification tools**
- **Unravelling of the RBAC**



RBAC – Define Standards and Rules

Personal userid
connected to one role
group

Role group describes
the business role

**Define
RBAC Rules**

Role group contains all
the access

All role groups will
have an 'owner'

RBAC - Sources of data



RBAC Stages – An overview

Analyse and prepare mainframe environment



Identify logical grouping



Engage with managers and users



Devise RBAC implementation plan



Test RBAC implementation



Implement RBAC

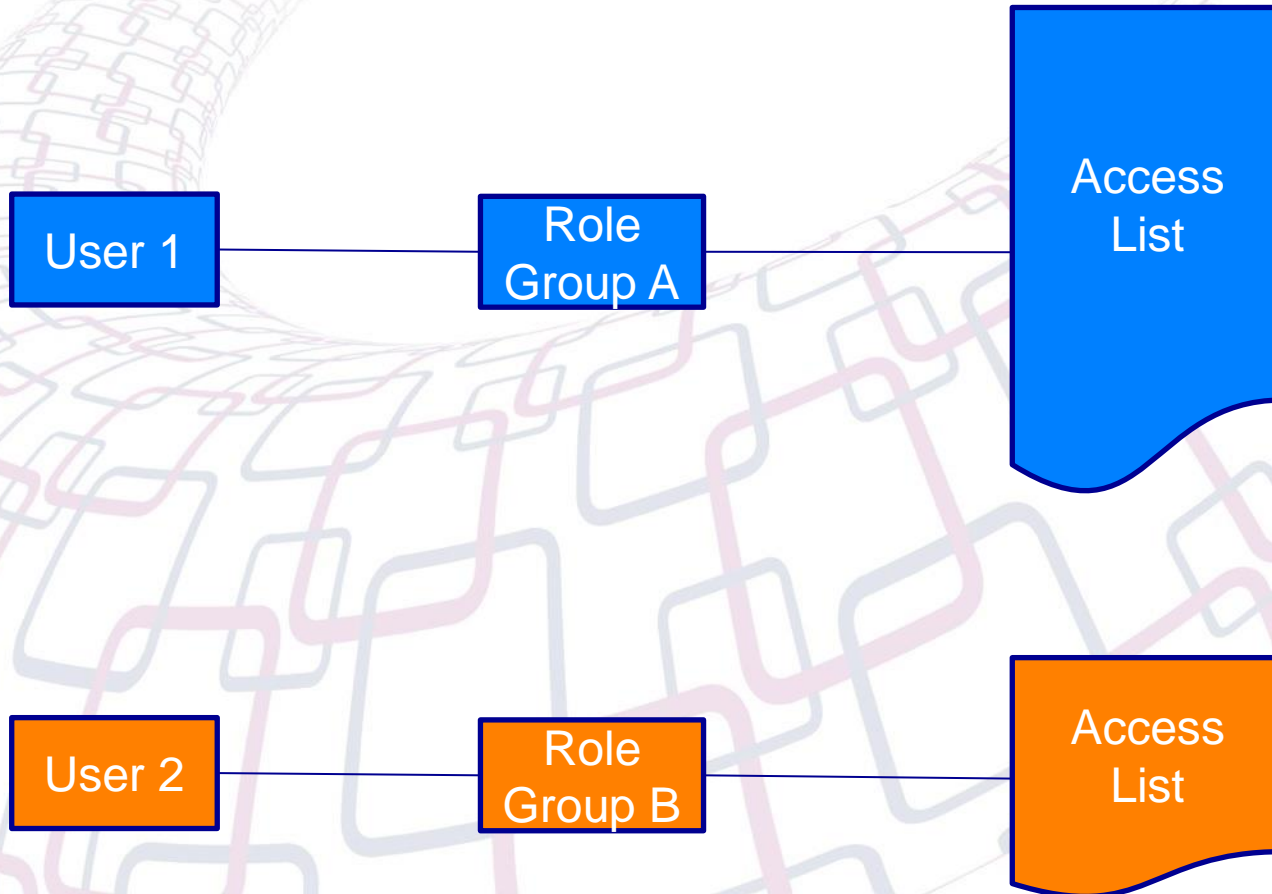


Update/Develop Processes

RBAC Implementation Tools

- **RSM RBAC tool**
- **RSM DB2 RBAC Tools**
- **Access Monitor data**
- **RACF Offline**
- **CARLa code**

RBAC Benefits – Some examples



RBAC Benefits – Some examples





MAINTAINING THE ENVIRONMENT

Tools – Maintain the environment

- **In-House Security Panels**
- **IBM zSecure Command Verifier**
- **IBM zSecure Alert**
- **RSM ExceptionReporter**
- **RSM RealtimeDashboard**

Tools – RSM ExceptionReporter

Mainframe Monitoring Process Reports

Report Produced on Tuesday 12 Feb 2013 @ 19:42:24
 Using files dated: 130212
 File Status JDEV JPRD

Control	Title	Complex	
		JDEV	JPRD
C002	RACF Profiles in WARNING mode overview	166	8
C004	Overview of User Accounts that have a Weak password	4	6443
C006	Overview of User Accounts with non-expiring passwords	45	8
C008	UID=0 accounts overview	0	29
C010	Profiles with UACC or ID(*) on ACL >= READ	0	0
C012	Overview of User Accounts Inactive for 90 days	0	0
C014	Started class Trusted & Privileged Started Task overview report	1	965
C016	Unexpected activity by accounts with OPERATIONS attribute	1	1
C018	RACF commands issued by system level SPECIAL accounts overview	8	50
C020	Updates to APF Protected Libraries	4	0
C022	RACF database name location or attributes changed	8	28
C024	Non-Compliant Audit Setting for RACF dataset Profile	0	0
C026	Non-Compliant Owner for RACF dataset Profile	0	0
Totals		237	7532

Key

- Complex All data present
- Complex Some data is missing
- Complex Dataset missing for this complex
- 0 No exceptions reported
- 4 Some exceptions present
- Missing Dataset missing for this complex

Overview JDEV JPRD C002 C004 C006 C008 C010 C012 C014 C016

Normal View Ready Sum=0

Tools – RSM RealtimeDashboard





RESULTS

Reduction in Privileged Accesses

Before

737.468

After

373.669

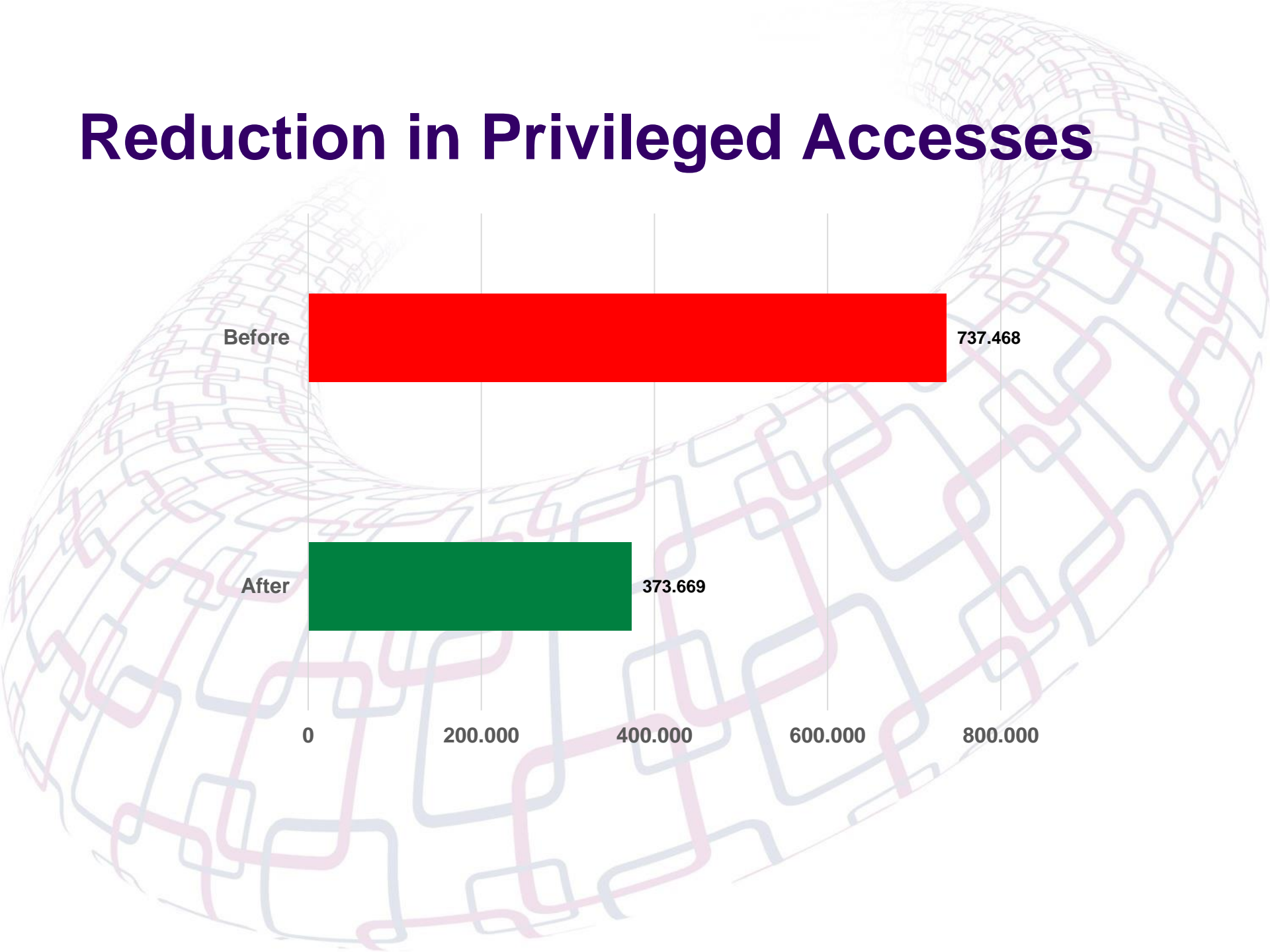
0

200.000

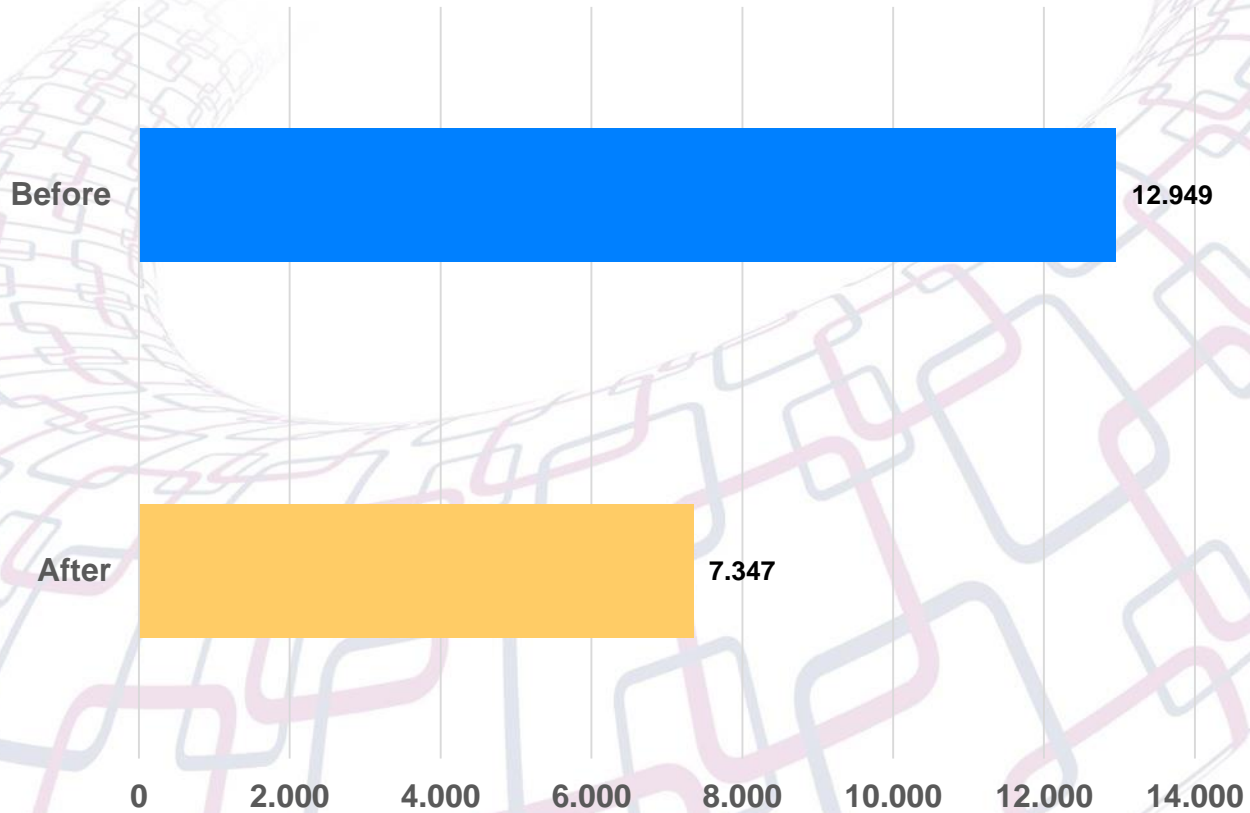
400.000

600.000

800.000



Reduction in Privileged Users



Questions



Contact Details

- Rui Miguel Feio - ruif@rsmpartners.com
- Steve Tresadern - stevet@rsmpartners.com
- RSM Partners - www.rsmpartners.com
- RSM Software – www.rsmsoftware.com