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**

![Pie chart showing data classification categories](chart.png)

- User: 14%
- Credit Card: 11%
- Development: 23%
- Sarbanes Oxley: 36%
- Customer - Confidential: 16%
Data Classification – What is it?

- **Who owns your data**

  - Branch: 27%
  - Insurance: 22%
  - HR: 13%
  - Systems: 9%
  - Development: 14%
  - Credit Card: 7%
  - User: 8%
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

User 1

Group A

Group B

Group C

Group D

User 2

Access List

Access List

Access List

Access List

Access List
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

- XBridge Datasniff
- RACF Database
- Naming Standards
- Access Monitor
- Support Teams
- Local Knowledge
Sources for Data Ownership

- Service Management
- Support Teams
- Service Database
- RACF Database
- Local Knowledge

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

- Reduced Risk of Fraud
- Focused Monitoring
- Recertification
- Audit
- Who has privileged access
- Compliance
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

Define RBAC Rules

- Personal userid connected to one role group
- Role group describes the business role
- Role group contains all the access
- All role groups will have an ‘owner’
RBAC - Sources of data

Sources

- Access Monitor
- HR Data
- RACF
- Local Knowledge
- Business Org. Chart
- Global Address List
- Phone List
RBAC Stages – An overview

1. Analyse and prepare mainframe environment
2. Identify logical grouping
3. Engage with managers and users
4. Devise RBAC implementation plan
5. Test RBAC implementation
6. Implement RBAC
7. Update/Develop Processes
RBAC Implementation Tools

- RSM RBAC tool
- RSM DB2 RBAC Tools
- Access Monitor data
- RACF Offline
- CARLa code
RBAC Benefits – Some examples

User 1
Role Group A
Access List

User 2
Role Group B
Access List
RBAC Benefits – Some examples

- Reduced Risk
- Fraud
- Security Management
- Joiners
- Movers
- Leavers
- Who is who
- Least Privilege Access
- Who does what
- Recertification
- Audit
- Monitor
MAINTAINING THE ENVIRONMENT
Tools – Maintain the environment

- In-House Security Panels
- IBM zSecure Command Verifier
- IBM zSecure Alert
- RSM ExceptionReporter
- RSM RealtimeDashboard
### Mainframe Monitoring Process Reports

Report Produced on Tuesday 12 Feb 2013 @ 19:42:24

Using files dated: 130212

<table>
<thead>
<tr>
<th>File Status</th>
<th>JDEV</th>
<th>JPRD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C002</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C004</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C006</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C012</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C022</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C024</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C026</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Complex

- **JDEV**: 166, 4, 45, 0, 1, 3, 4, 3, 0, 237
- **JPRD**: 8, 6443, 3, 29, 965, 1, 50, 28, 0, 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: Ready
- JPRD: Ready
- \(\text{Sum} = 0\)
Tools – RSM RealtimeDashboard
RESULTS
Reduction in Privileged Accesses

Before

After

0 200.000 400.000 600.000 800.000

373.669

737.468
Reduction in Privileged Users

Before: 12.949
After: 7.347

Graph showing the reduction in privileged users before and after a certain intervention.
Questions
Contact Details

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