

# **SAS® Metadata Security Journey** **prepare to be audited!**

**SAS® Metadata Security 301**  
AUDITING YOUR SAS ENVIRONMENT

# Authors



## Charyn Faenza

Vice President And Manager  
First National Bank

Charyn is responsible for the architecture and development of F.N.B.s corporate profitability, stress testing and analytics platforms.



## Michelle Homes

Co-founder and Business Dev Manager  
Metacoda

Michelle Homes is an enthusiastic and active member of the SAS community and social sphere, and helps SAS customers keep their SAS platforms secure.



# **SAS<sup>®</sup> Metadata Security 301**

## AUDITING YOUR SAS ENVIRONMENT

Charyn Faenza and Michelle Homes

# Introduction

## Overview

The Security Journey & the Three As



Regulatory Compliance & Responding to Audit Requests



Assessment & Remediation of Risks



Secure Development



Operational Requests



- Scenario 1: Testing a Specific User's Access
- Scenario 2: Reviewing Admin Privilege Assignments
- Scenario 3: Reviewing Changes to User Security
- Scenario 4: Change Control & Testing Process for Security Changes
  
- The Departmental Access Report
  
- Confirming Users Only Have Access To What They're Supposed To

# Introduction

## What If?



What would happen in your organization if someone accessed data they shouldn't?

When was your last SAS platform security project?

When was it last tested? How extensive was it? How long did it take?

Have there been any changes since it was last tested? Whether they are deliberate, accidental, expected or unexpected.

How do you know if it's still secure today?

# SECURITY JOURNEY

**SAS® Metadata Security 301**  
AUDITING YOUR SAS ENVIRONMENT

# Security Journey

## The Three As



### **AUTHENTICATION**

Who are you?



### **AUTHORIZATION**

What are you allowed  
to do?

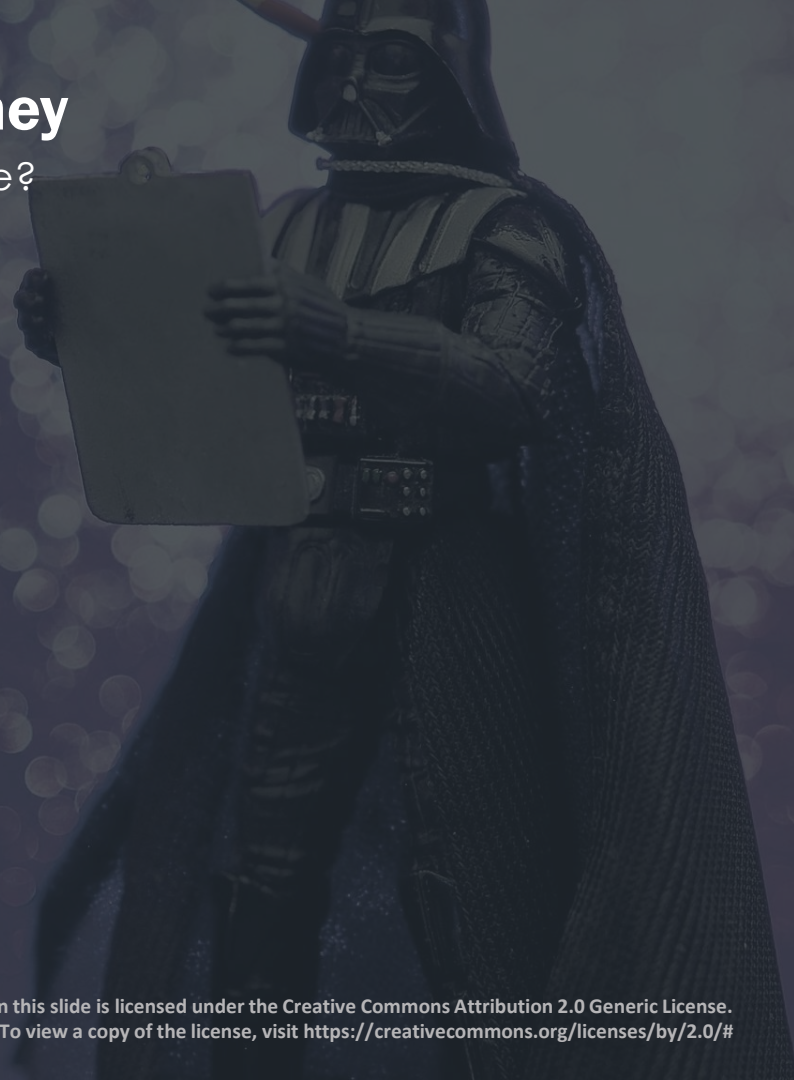


### **AUDITING**

What can you access?  
What can you do?

# Security Journey

Audit, Friend or Foe?



## TOOLS OF THE TRADE

SAS Management Console

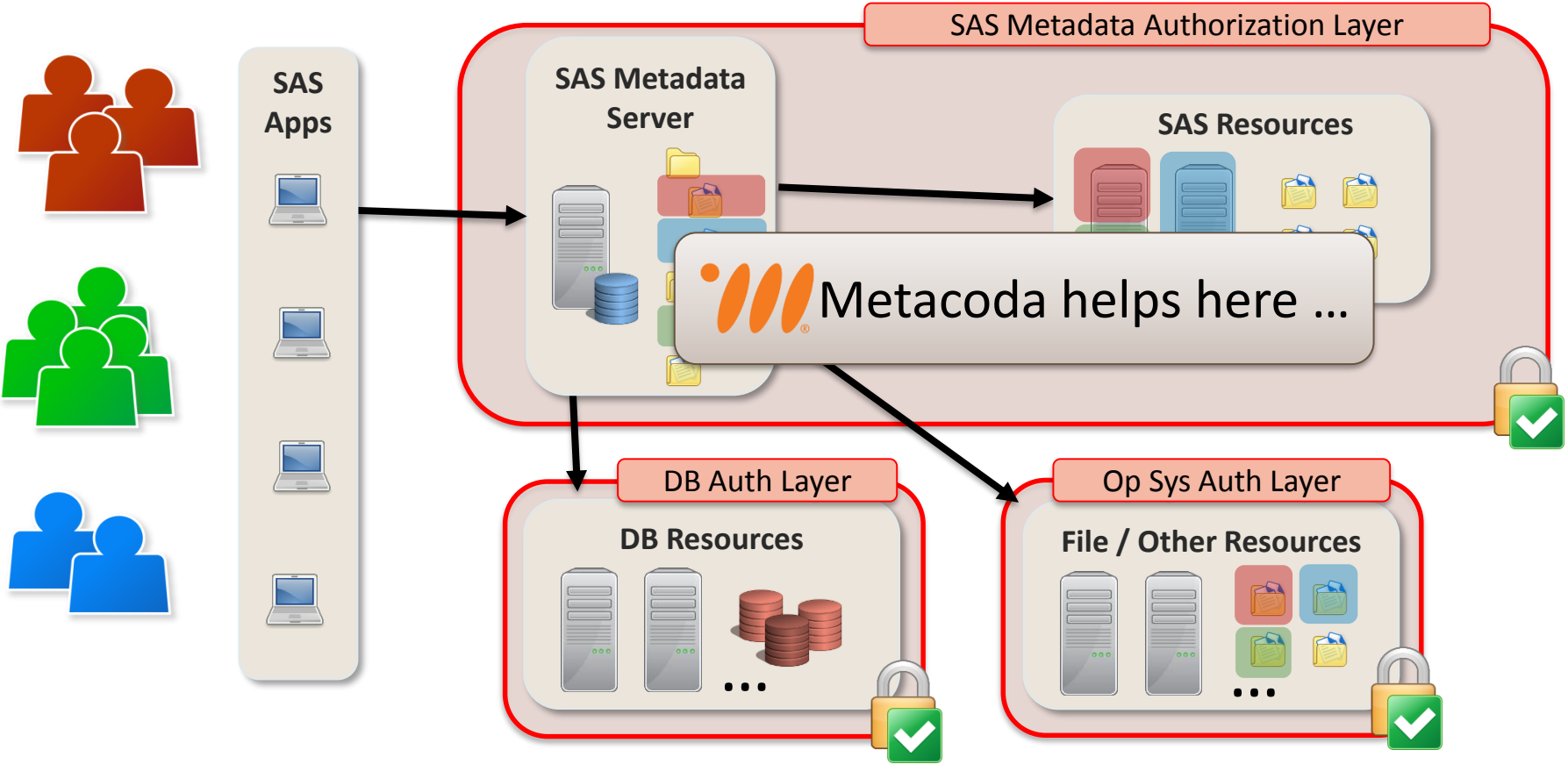
SAS Environment Manager

SAS Visual Analytics Administration Console

Metacoda



# Where Does Metacoda Help?



# REGULATORY COMPLIANCE

**SAS® Metadata Security 301**  
AUDITING YOUR SAS ENVIRONMENT

# Regulatory Compliance

## Common Regulations

### Gramm-Leach-Bliley Act (USA)

The Safeguards Rule requires financial institutions to protect the consumer information they collect.

- Designate responsible party
- Identify applications hosting or transacting customer information
- Assess risks to customer information
- Design, monitor and test assessment program
- Hold service providers to same standards
- Continue to evaluate and adjust programs

### Dodd-Frank Wall Street Reform (USA)

Intended to promote financial stability by improving accountability and transparency in the financial system.

- Sets the baseline for what is “reasonable and appropriate” security around consumer financial data
- Institutions must be ready to prove their security controls and document them
- Controls must include time to detect, respond and report breaches impacting sensitive data
- Size and maturity of the organization is a consideration in what is reasonable

### Sarbanes-Oxley Act (USA)

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

- Sections 302 and 404 indirectly charge information systems to support accounting and oversight for the accuracy of reporting

### General Data Protection Regulation (EU)

Intended to strengthen and unify data protection for individuals within the European Union.

- Designate a data protection officer
- Process personal data only for specific purposes
- All customer to take their data with them
- Delete personal data once its purpose is fulfilled
- Recognize an individual's ‘Right to be Forgotten’

### Payment Card Industry Data Security Standards

Industry standards for self-regulation of security.

- Protect cardholder data
- Manage vulnerabilities
- Provide strong access controls
- Monitor and test
- Maintain policy

# Responding to Audit Requests

## Scenario 1: Testing a Specific User's Access

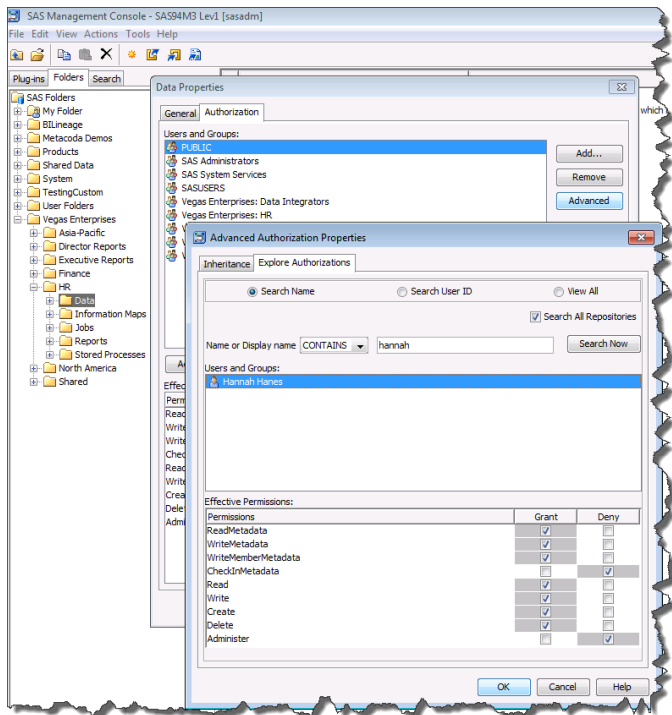
Auditors may request evidence that a specific user, most often an administrator, has been assigned the appropriate level of access.

In Scenario 1 the auditor requests a report detailing what Hanna, the HR Director in our demonstration company, has access to. The following information is desired:

- What security groups is she a member of, directly and indirectly
- What folders are visible and/or accessible to her

# Responding to Audit Requests

## Scenario 1: Testing a Specific User's Access



### SAS MANAGEMENT CONSOLE

Right-clicking on a single SAS metadata folder provides details on the users and groups with direct and indirect access on the specific folder

### METACODA

The Identity Permissions Explorer plug-in generates a report of all folder applicable permission settings for users or groups

# Responding to Audit Requests

## Scenario 1: Testing a Specific User's Access

The screenshot displays the SAS Management Console interface. The left pane shows a tree view of the repository structure, including folders like 'Reports', 'Information Maps', 'Jobs', and 'Stored Processes'. The main pane shows a table of users with their effective permissions. The user 'demojackson' is selected, and a detailed view of their permissions is shown below.

ID	Display Name	Description	Login Ids
25	Gayle Gordon	Sales Director (NZ)	demogayle (DefaultAuth)
26	Harry Hines	Account Rep. (NZ)	demojackson (DefaultAuth)
27	Harry Hines	Account Rep. (NZ)	demojackson (DefaultAuth)
28	Ian Irons	HR Consultant	demoian (DefaultAuth)
29	Ivy Ives	Sales Director (AU)	demoivy (DefaultAuth)
30	Jack Jamieson	NSW State Manager (AU)	demojack (DefaultAuth)

Type	Name	Access Level	RM	WM	WMM	CM	R	W	C	D
1	Folder	Stored Processes	Update metadata & data	✓	✓	✓	✗	✓	✓	✓
2	Folder	Reports	Update metadata & data	✓	✓	✓	✗	✓	✓	✓
3	Folder	Jobs	Update metadata & data	✓	✓	✓	✗	✓	✓	✓
4	Folder	Information Maps	Update metadata & data	✓	✓	✓	✗	✓	✓	✓
5	Folder	Data	Update metadata & data	✓	✓	✓	✗	✓	✓	✓
6	Folder	.	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓

Visual inspection & review

# Responding to Audit Requests

## Scenario 1: Testing a Specific User's Access

**metacoda** Identity Permissions Explorer Report

Effective Permissions and Access Levels for a Single Identity on Multiple Metadata Objects

User (external): Hannah Hanes

Metadata Folder Tree

- SAS Folders
  - BILineage
- Metacoda Demos
  - ProtectedWithACEWithSASDemo
  - ProtectedWithACTWithUsers
  - ProtectedWithEmptyACT
  - Unprotected
- Portal Application Tree
  - BI Dashboard Administrators Permissions Tree
  - BI Dashboard Users Permissions Tree
  - BI Web Services Users Permissions Tree
  - CORPQ\_VegasFinEUG Permissions Tree
  - Data Management Administrators Permissions Tree
  - Data Management Business Approvers Permissions Tree
  - Data Management Business Users Permissions Tree
  - Data Management Executives Permissions Tree
  - Data Management Power Users Permissions Tree
  - Data Management Stewards Permissions Tree
  - demosef1g1 Permissions Tree
  - demosef1g2 Permissions Tree
  - PUBLIC Permissions Tree
  - RolesTree
    - DefaultRole
      - DESKTOP\_PROFILE
        - Default
        - Sticky
        - Home
          - Home Column 1

Report output displaying effective permissions and access levels across all folders

# Responding to Audit Requests

## Scenario 1: Testing a Specific User's Access

Repository: Foundation

Filter: name, display name, description, or login ids contain

	Display Name	Name	Description
10	Eve Evans	demoeve	Sales Director (CA)
11	Famke Foster	demofamke	Report Developer I
12	Fred Faulkner	demofred	Account Rep. (CA)
13	Gareth Gale	demogareth	Report Developer II
14	Gayle Gordon	demogayle	Sales Director (NZ)
15	Hannah Hanes	demohannah	HR Director
16	Harry Hanes	demoharry	Account Rep. (NZ)
17	Ian Irons	demoian	HR Consultant
18	Ivy Ives	demoivy	Sales Director (AU)
19	Jack Jamieson	demojack	NSW State Manager (AU)
20	Jane Jacobs	demojane	SAS Platform Administrator
21	Jane Jacobs (Unrestricted)	AdminJane	SAS Platform Administrator

Groups (3:8) Roles (0:8) Capabilities (290/415) Logins (1) Int. Login (0) ACT Part. (0)

Filter: name contains

Level	Name
1	0 Hannah Hanes
2	1 Vegas Enterprises: Directors
3	1 Vegas Enterprises: Finance / AU (Global)
4	1 Vegas Enterprises: Finance (Universal)
5	2 SASUSERS
6	3 BI Dashboard Users
7	4 PUBLIC
8	5 Vegas Enterprises: HR
9	5

Reviewing identity hierarchy and group membership



# Responding to Audit Requests

## Scenario 1: Testing a Specific User's Access

### Identity Hierarchy and Group Membership Report

**metacoda** Metadata Security Report

User: Hannah Hanes

Display Name	Hannah Hanes
Name	demohannah
Description	HR Director
Title	HR Director
Protected	No
ACE Identity	No
Logins	Yes
Internal	No
Login Ids	demohannah (DefaultAuth)

Groups Tree / Identity Hierarchy (direct group memberships: 3; total distinct group memberships: 8)

Filters:  
Show duplicate group membership paths: **Off**

- Hannah Hanes
  - Vegas Enterprises: Directors
  - Vegas Enterprises: Finance / AU (Global)
    - Vegas Enterprises: Finance (Universal)
      - Vegas Enterprises: Finance (Domain Local)
        - SASUSERS
        - BI Dashboard Users
        - PUBLIC
  - Vegas Enterprises: HR

# Responding to Audit Requests

## Scenario 2: Reviewing Administrative Privilege Assignments

Auditors typically request a listing of all individuals with administrative access.

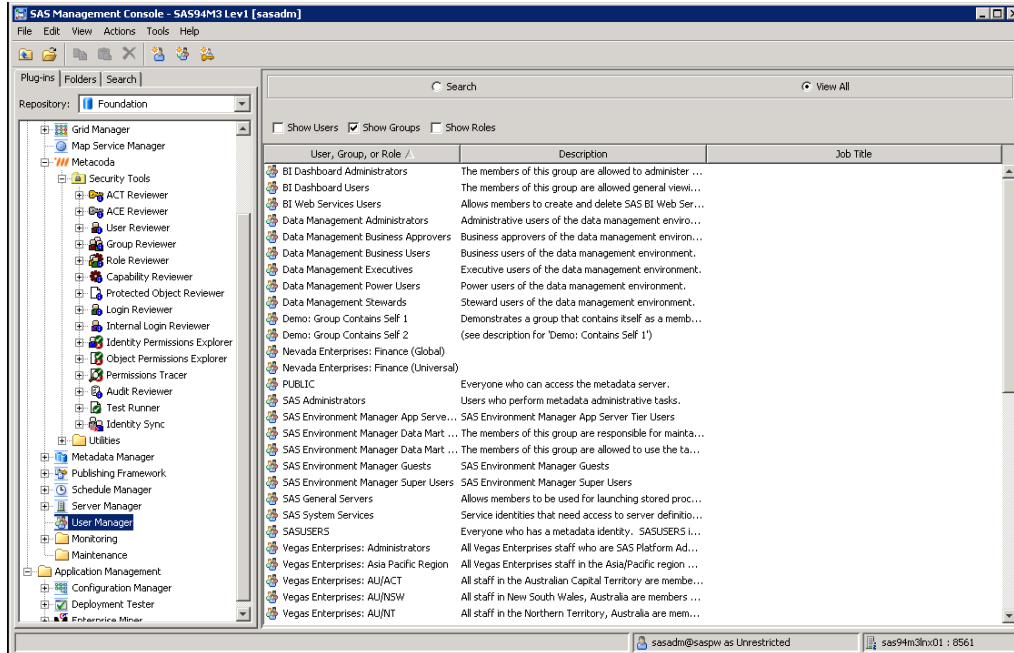
- Administrative groups in SAS Management Console can be provided.
- A risk is that administrative roles may be added to non-administrative groups, or groups that are not obviously administrative.

In Scenario 2 the auditor requests a list of all users with administrative access. The following information is desired:

- Who has access to change/update users, create users/groups, and manipulate repositories and metadata servers
- Who is able to create unrestricted users with access to all metadata and has the ability to provide all capabilities in SAS Management Console

# Responding to Audit Requests

## Scenario 2: Reviewing Administrative Privilege Assignments



### SAS MANAGEMENT CONSOLE

Groups can be reviewed by filtering by group in the User Manager

### METACODA

The Role Reviewer plug-in allows the admin to filter by the administrative roles *User Administration, Operation and Unrestricted*

# Responding to Audit Requests

## Scenario 2: Reviewing Administrative Privilege Assignments

The screenshot displays the SAS Metadata Server administrative console. On the left, a tree view shows the 'Security Tools' folder expanded to 'Role Reviewer'. The main area shows a search filter for 'metadata' and a table of results. The table lists three repositories: 'Foundation', 'Foundation', and 'Foundation', all with 'Display Name' as 'Metadata Server: Unrestricted'. Below this, a 'Members' section shows a list of users for the 'Metadata Server: Unrestricted' role, including 'Jane Jacobs (Unrestricted)', 'Koby Kogan (Unrestricted)', 'SAS Administrator', and 'SAS Environment Manager Service Account'. A smaller table on the right lists these members with their names.

Repository	Display Name	Description
1 Foundation	Metadata Server: Operation	Supports adding repositories and o
2 Foundation	Metadata Server: Unrestricted	Provides all capabilities in SAS Mana
3 Foundation	Metadata Server: User Administration	Supports management of users, p

Member Name
1 Jane Jacobs (Unrestricted)
2 Koby Kogan (Unrestricted)
3 SAS Administrator
4 SAS Environment Manager Service Account

Examining the unrestricted users

# Responding to Audit Requests

## Scenario 2: Reviewing Administrative Privilege Assignments

The screenshot displays the SAS Metadata Server Role Reviewer interface. On the left, a tree view shows the 'Security Tools' folder expanded to 'Role Reviewer'. The main window is titled 'Filter: name, display name or description contains metadata'. It contains a table with the following data:

	Repository	Display Name	
1	Foundation	Metadata Server: Operation	Supports adding reposi
2	Foundation	Metadata Server: Unrestricted	Provides all capabilit
3	Foundation	Metadata Server: User Administration	Supports management

Below this table, the 'Members (2:10)' section is expanded for 'Metadata Server: User Administration'. It shows a tree view of members, with 'Barbara Bennings' selected. To the right, a table lists the members:

	Member Name
1	Barbara Bennings
2	SAS Administrators
3	Jane Jacobs (Unrestricted)
4	Koby Kogan (Unrestricted)
5	SAS Administrator
6	SAS Demo User
7	SAS Environment Manager Servi
8	Vegas Enterprises: Administrat
9	Jane Jacobs
10	Koby Kogan

Examining users and groups that have an admin type role using the Role Reviewer plug-in

# Responding to Audit Requests

## Scenario 3: Reviewing Changes to User Security

Changes to user security since the last audit are a frequent focus of auditors.

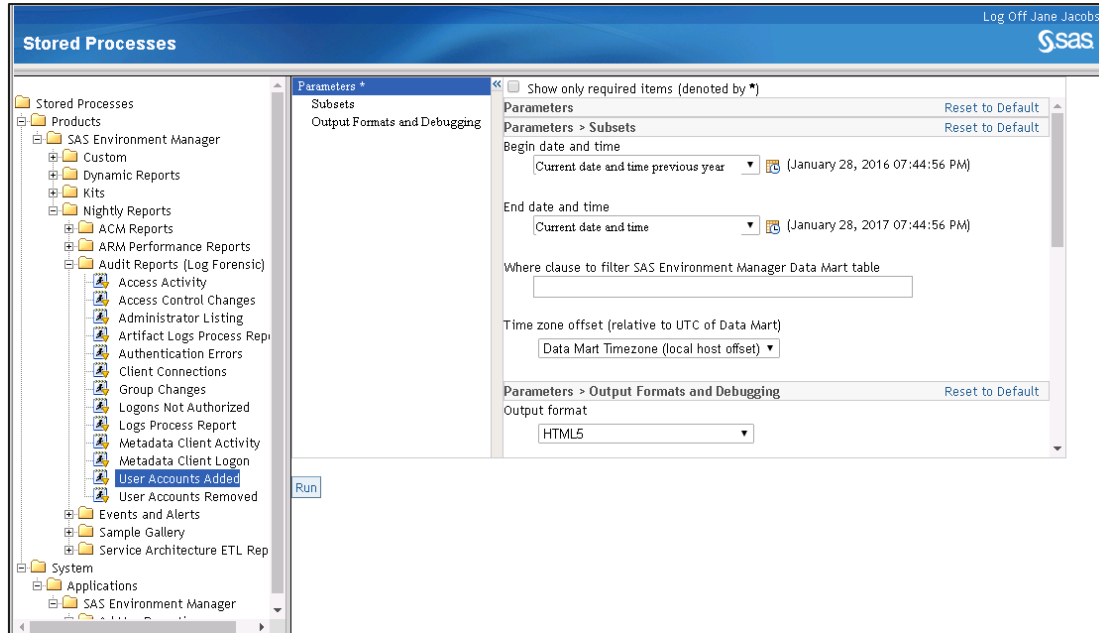
SAS provides several reports in the SAS Environment Manager Report Center to assist with tracking historical changes.

In Scenario 3 the auditor requests a list of all changes made to several SAS administration roles. The following information is desired:

- What user were added/removed from administrative roles
- When were the changes made
- Who made the changes

# Responding to Audit Requests

## Scenario 3: Reviewing Changes to User Security




The screenshot displays the SAS Environment Manager interface. On the left, a tree view shows the 'Stored Processes' hierarchy, with 'Audit Reports (Log Forensic)' expanded to show 'User Accounts Added'. The main panel shows the 'Parameters' configuration for the selected process, including options for 'Begin date and time', 'End date and time', 'Where clause to filter SAS Environment Manager Data Mart table', 'Time zone offset', and 'Output format' (set to HTML5). A 'Run' button is visible at the bottom of the configuration panel.

Several reports are available within SAS Environment Manager to support audit requests

# Responding to Audit Requests

## Scenario 3: Reviewing Changes to User Security

Stored Processes Log Off Jane Jacobs 

Stored Processes

- Products
  - SAS Environment Manager
    - Custom
    - Dynamic Reports
    - Kits
    - Nightly Reports
      - ACM Reports
      - ARM Performance Reports
      - Audit Reports (Log Forensic)
        - Access Activity**
        - Access Control Changes
        - Administrator Listing
        - Artifact Logs Process Report
        - Authentication Errors
        - Client Connections
        - Group Changes
        - Logons Not Authorized
        - Logs Process Report
        - Metadata Client Activity
        - Metadata Client Logon
        - User Accounts Added
        - User Accounts Removed
      - Events and Alerts
      - Sample Gallery
      - Service Architecture ETL Report

- System

**Event Summary Totals**

	Count
Audit Record Event	N
314071.SASADM@SASPW: Access Control change	108
314071.SASADM@SASPW: Added AccessControlTemplate	90
314071.SASADM@SASPW: Added IdentityType	12
314071.SASADM@SASPW: Added Internal Login ObjId	6
314071.SASADM@SASPW: Added Login with UserId	3
314071.SASADM@SASPW: Added Member IdentityType	30
314071.SASADM@SASPW: Changed AccessControlTemplate	96
314071.SASADM@SASPW: Changed IdentityType	21
314071.SASADM@SASPW: Changed Internal Login ObjId	12
314071.SASADM@SASPW: Changed Login UserId	3
319696.SASDEMO: Access Control change	6
319696.SASDEMO: Removed IdentityType	9
319696.SASDEMO: Removed Member IdentityType	15
334065.SASADM@SASPW: Added Member IdentityType	15
334065.SASADM@SASPW: Changed IdentityType	3
337459.SASADM@SASPW: Changed IdentityType	3
340344.SASADM@SASPW: Added IdentityType	3
342396.SASADM@SASPW: Access Control change	57
342396.SASADM@SASPW: Added AccessControlTemplate	3
342396.SASADM@SASPW: Added Authentication Domain Name	3
342396.SASADM@SASPW: Added Login with UserId	3
342396.SASADM@SASPW: Added Member IdentityType	138
342396.SASADM@SASPW: Changed AccessControlTemplate	6
342396.SASADM@SASPW: Changed IdentityType	57
342396.SASADM@SASPW: Changed Login UserId	3

Summarizing security changes



# Responding to Audit Requests

## Scenario 3: Reviewing Changes to User Security

Log Off Jane Jacobs

Stored Processes

SAS

Stored Processes

- Products
  - SAS Environment Manager
    - Custom
    - Dynamic Reports
    - Kits
    - Nightly Reports
      - ACM Reports
      - ARM Performance Reports
      - Audit Reports (Log Forensic)
        - Access Activity
        - Access Control Changes
        - Administrator Listing
        - Artifact Logs Process Report
        - Authentication Errors
        - Client Connections
        - Group Changes
        - Logons Not Authorized
        - Logs Process Report
        - Metadata Client Activity
        - Metadata Client Logon
        - User Accounts Added
        - User Accounts Removed
      - Events and Alerts
      - Sample Gallery
      - Service Architecture ETL Report
    - System

Audit Report Userids\_Added

Administrator	Txn Start Date/Time	Metadata Userid	Userid	Log_Line
sasadm@saspw	22JAN2017:10:11:46	testoustomep		2017-01-22T10:11:46,898 INFO [02500770] 314071:sasadm@saspw - 314071:SASADM@SASPW: Added Login with UserId=testoustomep, ObjId=A5A4PC82.AC000001, AuthDomain=DefaultAuth to IdentityType= Name=, ObjId=.
	22JAN2017:21:31:36	demomaria		2017-01-22T21:31:36,070 INFO [02727822] 346918:sasadm@saspw - 346918:SASADM@SASPW: Added Login with UserId=demomaria, ObjId=A53NPRYA.A50000TB, AuthDomain=DefaultAuth to IdentityType= Name=, ObjId=.
	22JAN2017:21:31:36	demosusan		2017-01-22T21:31:36,070 INFO [02727822] 346918:sasadm@saspw - 346918:SASADM@SASPW: Added Login with UserId=demosusan, ObjId=A53NPRYA.A50000TC, AuthDomain=DefaultAuth to IdentityType= Name=, ObjId=.
	22JAN2017:21:53:10	scott	VegasORA	2017-01-22T21:53:09,618 INFO [02736965] 342396:sasadm@saspw - 342396:SASADM@SASPW: Added Login with UserId=scott, ObjId=A53NPRYA.A50000TD, AuthDomain=OracleAuth to IdentityType=IdentityGroup Name=VegasORA, ObjId=A53NPRYA.A50000SM.
	23JAN2017:17:46:00	db2user	VegasDB2	2017-01-23T17:46:59,847 INFO [03211697] 390336:sasadm@saspw - 390336:SASADM@SASPW: Added Login with UserId=db2user, ObjId=A53NPRYA.A50000TE, AuthDomain=DB2Auth to IdentityType=IdentityGroup Name=VegasDB2, ObjId=A53NPRYA.A50000SR.
	22JAN2017:10:11:46	testoustomep		2017-01-22T10:11:46,898 INFO [02500770] 314071:sasadm@saspw - 314071:SASADM@SASPW: Added Login with UserId=testoustomep, ObjId=A5A4PC82.AC000001, AuthDomain=DefaultAuth to IdentityType= Name=, ObjId=.
	22JAN2017:21:31:36	demomaria		2017-01-22T21:31:36,070 INFO [02727822] 346918:sasadm@saspw - 346918:SASADM@SASPW: Added Login with UserId=demomaria, ObjId=A53NPRYA.A50000TB, AuthDomain=DefaultAuth to IdentityType= Name=, ObjId=.
	22JAN2017:21:31:36	demosusan		2017-01-22T21:31:36,070 INFO [02727822] 346918:sasadm@saspw - 346918:SASADM@SASPW: Added Login with UserId=demosusan, ObjId=A53NPRYA.A50000TC, AuthDomain=DefaultAuth to IdentityType= Name=, ObjId=.
	22JAN2017:21:53:10	scott	VegasORA	2017-01-22T21:53:09,618 INFO [02736965] 342396:sasadm@saspw - 342396:SASADM@SASPW: Added Login with UserId=scott, ObjId=A53NPRYA.A50000TD, AuthDomain=OracleAuth to IdentityType=IdentityGroup Name=VegasORA, ObjId=A53NPRYA.A50000SM.

Listing newly added user logins

# Responding to Audit Requests

## Scenario 3: Reviewing Changes to User Security

The screenshot shows the SAS Stored Processes interface. The left-hand navigation pane is expanded to show 'Audit Reports (Log Forensic)' > 'Group Changes'. The main window displays an 'Audit Report Group\_Changes' table with the following data:

Group Name	Administrator	Txn Start Date/Time	Audit Record Event	Userid
META: Operators Role	sasadm@saspw	23JAN2017:14:56:05	390336:SASADM@SASPW: Added Member IdentityType	SASAdministrators
	sasadm@saspw	23JAN2017:14:56:05	390336:SASADM@SASPW: Removed Member IdentityType	SASAdministrators
	sasadm@saspw	23JAN2017:14:56:05	390336:SASADM@SASPW: Removed Member IdentityType	demoalice
	sasadm@saspw	23JAN2017:14:56:06	390336:SASADM@SASPW: Added Member IdentityType	SASAdministrators
	sasadm@saspw	23JAN2017:14:56:06	390336:SASADM@SASPW: Removed Member IdentityType	SASAdministrators
META: Unrestricted Users Role	sasadm@saspw	22JAN2017:09:48:15	314071:SASADM@SASPW: Added Member IdentityType	AdminJane
	sasadm@saspw	22JAN2017:09:48:15	314071:SASADM@SASPW: Added Member IdentityType	AdminKoby
META: User and Group Administrators Role	sasadm@saspw	12JAN2017:09:10:49	Added Member IdentityType	SAS User Administrator
	sasadm@saspw	12JAN2017:09:27:34	Removed Member IdentityType	SAS User Administrator
	sasadm@saspw	23JAN2017:14:55:07	390336:SASADM@SASPW: Added Member IdentityType	SASAdministrators
	sasadm@saspw	23JAN2017:14:55:07	390336:SASADM@SASPW: Added Member IdentityType	demobarbara
	sasadm@saspw	23JAN2017:14:55:07	390336:SASADM@SASPW: Removed Member IdentityType	SASAdministrators
	sasadm@saspw	23JAN2017:14:55:07	390336:SASADM@SASPW: Removed Member IdentityType	demoalice
	sasadm@saspw	23JAN2017:14:55:07	390336:SASADM@SASPW: Added Member IdentityType	SASAdministrators
	sasadm@saspw	23JAN2017:14:55:07	390336:SASADM@SASPW: Added Member IdentityType	demobarbara
	sasadm@saspw	23JAN2017:14:55:07	390336:SASADM@SASPW: Removed Member IdentityType	SASAdministrators
	sasadm@saspw	24JAN2017:13:55:16	489752:SASADM@SASPW: Added Member IdentityType	SASUSERS

Reviewing changes to the groups with metadata server roles

# Responding to Audit Requests

## Scenario 4: Change Control & Testing Process for Security Changes

Auditors also seek to understand how administrators test for unauthorized changes to security. Metacoda provides Metadata Security Testing Framework that allows administrators to test for changes at a time interval of their choosing.

In Scenario 4 the administrator demonstrates the process for testing security changes to the HR folder to the auditor.

- A base starting point is identified
- An XML test script is created that can be modified to test all or specific items
- The Test Runner plug-in is used to run interactively or the test is scheduled to run in batch

# Responding to Audit Requests

## Scenario 4: Change Control & Testing Process for Security Changes

The image displays a sequence of screenshots from the SAS Management Console (version 9.4.1) illustrating the process of responding to an audit request by exporting a metadata security test XML file.

**Top Left Screenshot:** Shows the 'Plug-ins' pane with 'Security Tools' expanded. The 'Export Metadata Security Test XML...' option is highlighted with a red arrow.

**Top Right Screenshot:** Shows a table listing repositories. The 'Vegas Enterprises: HR' repository is selected.

Repository	Display Name	Description	Protected	ACE Identity	Logins
Foundation	Demo: Group Contains Self 1	Demonstrates a group that contains itself as a member through a nester...	No	No	No
Foundation	Vegas Enterprises: HR	This group is u...	No	Yes	No

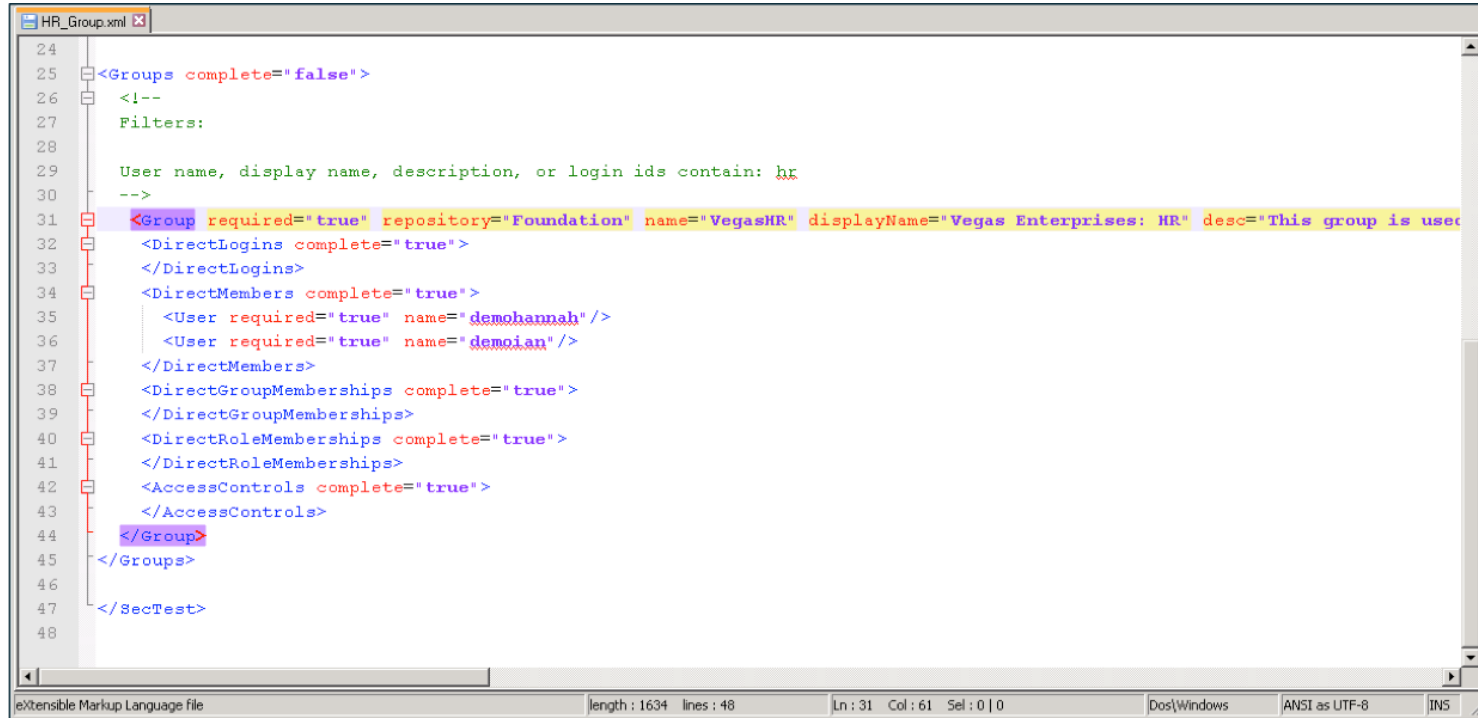
**Bottom Screenshot:** Shows the 'Export Wizard' dialog box. The 'Export Preferences: Groups' section is visible, with several options checked:

- Export Logins XML for each Group
- Export Indirect Logins XML for each Group
- Export All (Direct & Indirect) Logins XML for each Group
- Export Direct Members XML for each Group
- Export Indirect Members XML for each Group
- Export All (Direct & Indirect) Members XML for each Group
- Export Direct Group Memberships XML for each Group
- Export Indirect Group Memberships XML for each Group
- Export All (Direct & Indirect) Group Memberships XML for each Group
- Export Direct Role Memberships XML for each Group
- Export Indirect Role Memberships XML for each Group

**Right Side Text:** A yellow vertical bar is followed by the text: "Configure the Metadata Security Test XML file".

# Responding to Audit Requests

## Scenario 4: Change Control & Testing Process for Security Changes

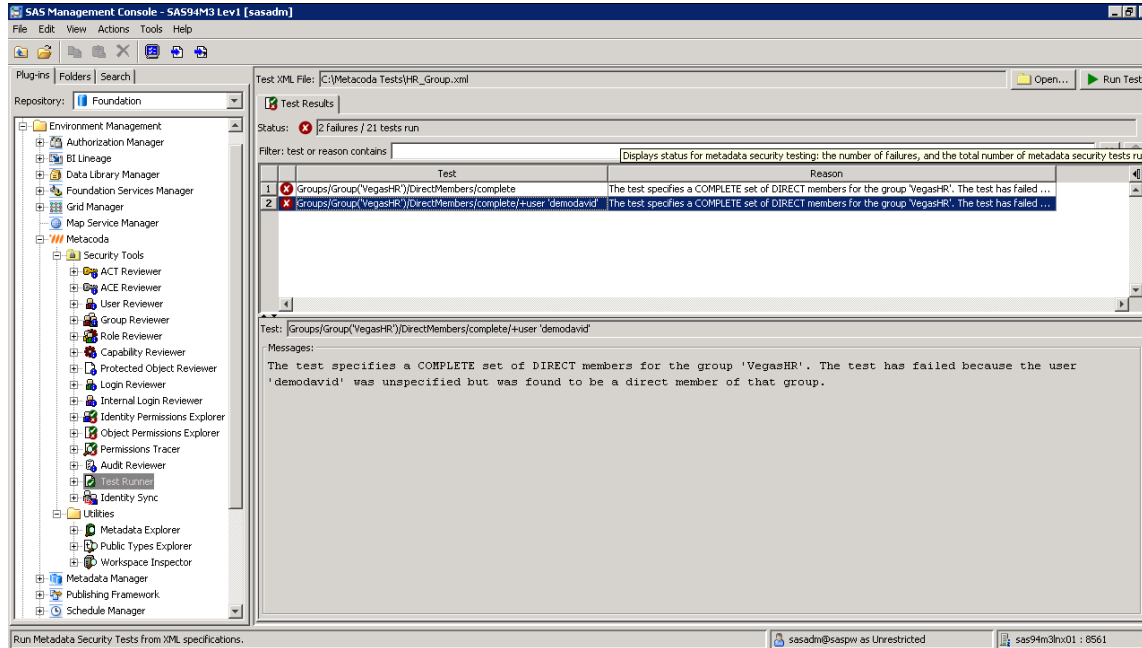


```
24
25 <Groups complete="false">
26   <!--
27     Filters:
28
29     User name, display name, description, or login ids contain: hr
30   -->
31   <Group required="true" repository="Foundation" name="VegasHR" displayName="Vegas Enterprises: HR" desc="This group is used
32     <DirectLogins complete="true">
33     </DirectLogins>
34     <DirectMembers complete="true">
35       <User required="true" name="demohannah" />
36       <User required="true" name="demoian" />
37     </DirectMembers>
38     <DirectGroupMemberships complete="true">
39     </DirectGroupMemberships>
40     <DirectRoleMemberships complete="true">
41     </DirectRoleMemberships>
42     <AccessControls complete="true">
43     </AccessControls>
44   </Group>
45 </Groups>
46
47 </SecTest>
48
```

extensible Markup Language file | length : 1634 lines : 48 | Ln : 31 Col : 61 Sel : 0 | 0 | Dos\Windows ANSI as UTF-8 INS

# Responding to Audit Requests

## Scenario 4: Change Control & Testing Process for Security Changes



The screenshot displays the SAS Management Console interface. The left-hand navigation pane shows a tree structure with 'Metacoda' expanded to 'Security Tools', where 'Test Runner' is selected. The main window shows the 'Test Results' tab for a file named 'C:\Metacoda\Tests\HR\_Group.xml'. The status indicates '2 failures / 21 tests run'. A table lists the failed tests:

Test	Reason
1 Groups(Group('VegasHR'))DirectMembers(complete)	The test specifies a COMPLETE set of DIRECT members for the group 'VegasHR'. The test has failed ...
2 Groups(Group('VegasHR'))DirectMembers(complete)+user 'demodavid'	The test specifies a COMPLETE set of DIRECT members for the group 'VegasHR'. The test has failed ...

Below the table, a detailed view of the selected test is shown:

```
Test: [Groups(Group('VegasHR'))DirectMembers(complete)+user 'demodavid']
Messages:
The test specifies a COMPLETE set of DIRECT members for the group 'VegasHR'. The test has failed because the user 'demodavid' was unspecified but was found to be a direct member of that group.
```

Test results are viewed in the Test Runner Plug-in

# ASSESSMENT & REMEDIATION OF RISKS

**SAS® Metadata Security 301**  
AUDITING YOUR SAS ENVIRONMENT

# Assessment & Remediation of Risks

## Evaluating the Security of the SAS Environment

### Security auditing has value beyond compliance

- Periodic reviews ensure a smooth, efficient audit and strengthen the overall security program
- Reviews also provide an opportunity for administrators to evaluate their environment's adherence to best practices

### The distinction between a compliance security program and a strong, effective security program that uses established best practices

- **Compliant:** Data is secured by individually adding users to individual metadata objects (data, programs, etc.)
- **Best Practice:** Data is secured through the use of ACTs that are applied to metadata folders containing metadata objects (data, programs, etc.). Users are added to groups that are granted access via the ACT.



# Assessment & Remediation of Risks

## The Departmental Access Report

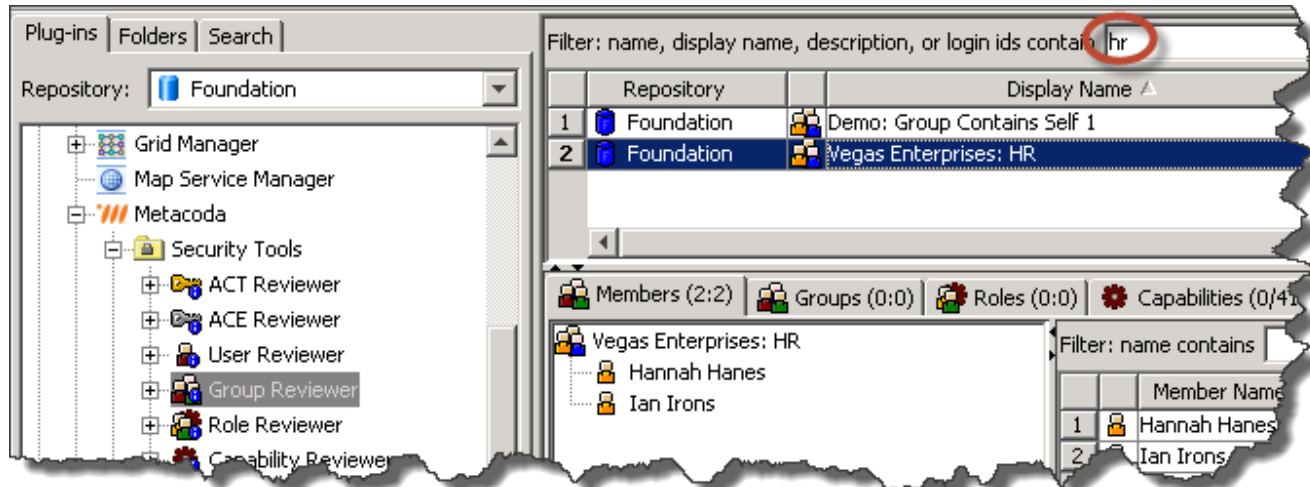
Are we complying to business security requirements?

In the following example, we want to create a report demonstrating sensitive HR data is secured.



# Assessment & Remediation of Risks

## The Departmental Access Report



Determining who has access to a departmental folder

# Assessment & Remediation of Risks

## The Departmental Access Report

Determining who has access to a departmental folder

The screenshot displays the SAS Management Console interface. The left pane shows a tree view of the repository structure, with 'Vegas Enterprises/HR' selected. The right pane shows a list of objects with a filter 'member name contains'. Below this, the 'Effective permissions for: //Vegas Enterprises/HR' table is shown, listing 20 users and their access levels across various permissions (RM, WM, WMM, CM, R, W, C, D, A).

ID	Display Name	Access Level	RM	WM	WMM	CM	R	W	C	D	A
1	SAS Administrator	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	SAS Demo User	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	SAS Environment Manager Service Account	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	Jane Jacobs	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	Koby Kogan	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Jane Jacobs (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Koby Kogan (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	SAS Administrators	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
9	Vegas Enterprises: Administrators	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	Mike Mitchell	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
11	Dorothy Dickens	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
12	Aaron Atkins	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
13	Euan Easton	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
14	Zac Zimmerman	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
15	Lisa Lowes	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
16	Jan Irons	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
17	Charles Caxton	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
18	Barbara Bennings	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
19	Hannah Hanes	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗
20	Vegas Enterprises: HR	Update folder members, Update data	✓	✗	✗	✗	✓	✓	✓	✓	✗

# Assessment & Remediation of Risks

## The Departmental Access Report

	Display Name	Access Level	RM	WM	WMM	CM	R	W	C	D	A
1	SAS Administrator	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	SAS Demo User	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	SAS Environment Manager Service Account	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	Jane Jacobs	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	Koby Kogan	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Jane Jacobs (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Koby Kogan (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	SAS Administrators	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
9	Vegas Enterprises: Administrators	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	Mike Mitchell	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
11	Dorothy Dickens	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
12	Aaron Atkins	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
13	Euan Easton	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
14	Zac Zimmerman	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
15	Lisa Lowes	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
16	Ian Irons	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
17	Charles Caxton	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
18	Barbara Bennings	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗
19	Hannah Har...	Update folder members, Update data	✓	✗	✓	✗	✓	✓	✓	✓	✗

Again, taking a deeper look at a user's access to assess a potential issue

# Assessment & Remediation of Risks

## The Departmental Access Report

The screenshot shows the Permissions Tracer tool interface. The object is '/Vegas Enterprises/HR' and the identity is 'Mike Mitchell'. The options section is checked for Role Implied, Direct ACEs, Indirect ACEs, Repository ACT, Inapplicable, Intermediate Effective, Direct ACTs, Indirect ACTs, Default, and Definitive. The table below shows the traced permissions for this user on the object.

	Path/Name	Source	Identity	Precedence	RM	WM	WMM	CM	R	W
1	/Vegas Enterprises/HR	Effective Permissions	Mike Mitchell	0	✓	✗	✓	✗	✓	✓
2	/Vegas Enterprises/HR	Direct ACT (Vegas Enterprises: Analysts (Update))	Vegas Enterprises: Data Scientists	1	✓	✗	✓	✗	✓	✓
3	/Vegas Enterprises/HR	Direct ACT (Vegas Enterprises: Hide)	PUBLIC	2	✗	✗	✗	✗	✗	✗
4	/Vegas Enterprises	Indirect ACE (Explicit)	SASUSERS	4	✓	✓	✓	✓	✓	✓
5	SAS Folders	Indirect ACE (Explicit)	PUBLIC	6	✗	✗	✗	✗	✗	✗
6	Foundation	Repository ACT (Default ACT)	SASUSERS	7	✓	✓	✓	✓	✓	✓
7	Foundation	Repository ACT (Default ACT)	PUBLIC	8	✗	✗	✗	✗	✗	✗
8		Default Deny (Repository ACT is present)	PUBLIC	9	✗	✗	✗	✗	✗	✗

The Permissions Tracer provides a complete detailed view on how the access level for a user on an object is determined

# Assessment & Remediation of Risks

## The Departmental Access Report

metacoda

Object Permissions Explorer Report

Effective Permissions and Access Levels for Multiple Identities on a Single Metadata Object

Folder: /Vegas Enterprises/HR

Row	Display Name	Access Level	RM	WM	WMM	CM	R	W	C	D	A
1	SAS Administrator	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	SAS Demo User	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	SAS Environment Manager Service Account	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	Jane Jacobs	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	Koby Kogan	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Jane Jacobs (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Koby Kogan (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	SAS Administrators	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
9	Vegas Enterprises: Administrators	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	Mike Mitchell	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
11	Dorothy Dickens	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
12	Aaron Atkins	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
13	Euan Easton	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
14	Zac Zimmerman	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
15	Lisa Lowes	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
16	Ian Irons	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
17	Charles Caxton	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
18	Barbara Bennings	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
19	Hannah Hanes	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
20	Vegas Enterprises: HR	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
21	Vegas Enterprises: Business Analysts	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
22	Vegas Enterprises: Data Scientists	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
23	Vegas Enterprises: Data Integrators	Update folder members, Update data	✓	X	✓	X	✓	✓	✓	✓	X
24	Alice Adams	View metadata & data	✓	X	X	X	X	X	X	X	X
26	Rob Baytar	View metadata & data	✓	X	X	X	X	X	X	X	X

Reports can be produced at this level of granularity, if needed, to document the administrator's findings

# SECURE DEVELOPMENT

**SAS® Metadata Security 301**  
AUDITING YOUR SAS ENVIRONMENT

# Secure Development

## Verifying Security Integrity



Reviewing security is not just the administrator's job

Developers need to use the same best practices in development that are used in production

Developers and administrators should work together throughout the development life cycle

Testing should look for both intended and unintended consequences



# Secure Development

## Verifying Security Integrity

Identifying the necessary security groups for Visual Analytics Development

SAS Management Console - SASVA73 Lev1 [sasadm]

Repository: Foundation

Filter: name, display name, description, or login ids contain director

Repository	Display Name	Description	Protected	ACE Identity	Logins	Login Ids
Foundation	Vegas Enterprises: Directors	This group is used to provide appropriate access and capabilities ...	No	Yes	No	

Members (5:5) Groups (0:0) Roles (0:0) Capabilities (0/119) Logins (0) ACT Part. (1) ACE Part. (0) ACTs (0) ACEs (0) Ext Ids (1)

Filter: name contains

Member Name	Repository	Depth	Membership Path
Carol Charleston	Foundation	1	Carol Charleston < Vegas Enterprises: Directors
Eve Evans	Foundation	1	Eve Evans < Vegas Enterprises: Directors
Gayle Gordon	Foundation	1	Gayle Gordon < Vegas Enterprises: Directors
Hannah Hanes	Foundation	1	Hannah Hanes < Vegas Enterprises: Directors
Ivy Ives	Foundation	1	Ivy Ives < Vegas Enterprises: Directors

Found 49 groups in 0.016 seconds.

sasadm@saspw es Unrestricted sasva73hxo1 : 8561

# Secure Development

## Verifying Security Integrity

The screenshot shows the SAS Visual Analytics Administration console. The left sidebar displays a folder tree with 'BONUSES' selected under 'Public > LASR'. The main area shows the 'Authorization' tab for 'BONUSES', displaying a table of effective permissions for various identities.

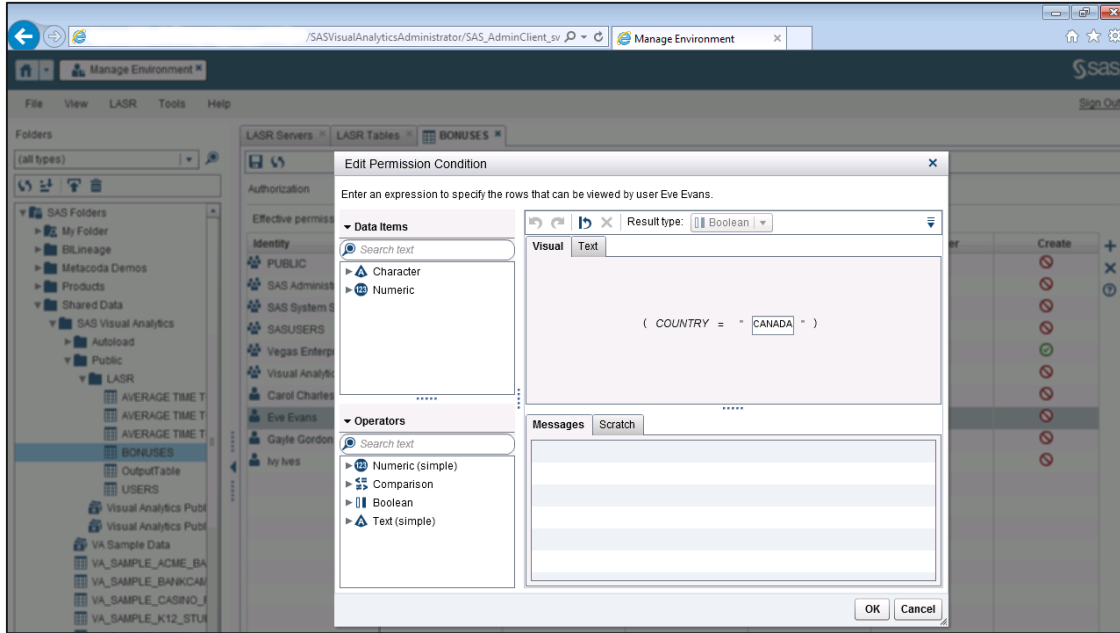
Identity	ReadMetadata	Read	WriteMetadata	Write	Administer	Create
PUBLIC	⊘	⊘	⊘	⊘	⊘	⊘
SAS Administrators	✔	✔	✔	✔	✔	⊘
SAS System Services	✔	✔	✔	✔	⊘	⊘
SASUSERS	✔	✔	✔	✔	⊘	⊘
Vegas Enterprises: Dat	✔	✔	✔	✔	⊘	✔
Visual Analytics Data A	✔	✔	✔	✔	⊘	⊘
Carol Charleston	✔	⚙	✔	✔	⊘	⊘
Eve Evans	✔	⚙	✔	✔	⊘	⊘
Gayle Gordon	✔	⚙	✔	✔	⊘	⊘
Ivy Ives	✔	⚙	✔	✔	⊘	⊘

The Visual Analytics Administration Console displays the effective permissions on the metadata object

# Secure Development

## Verifying Security Integrity

Specific row-level conditions can be displayed by right-clicking on the Identity



# Secure Development

## Verifying Security Integrity

Filter: protected object path/name or description contains bonuses

	Repository	Type	Path/Name	Protected	ACTs#	ACEs#	Perm. Cond.
1	Foundation	Table	/Shared Data/SAS Visual Analytics/Public/LASR/BONUSES	Yes	0	5	Yes

ACTs (0) ACEs (8)

	Identity	User Ref.	RM	WM	CM	R	W	C	D	Permission Condition
1	Carol Charleston (Person)	Yes								
2	Carol Charleston (Person)	Yes								COUNTRY = 'U.S.A.'/*VA <?xml version="1.0" encoding="UTF-8" standalone="yes"?><ex
3	Eve Evans (Person)	Yes								
4	Eve Evans (Person)	Yes								COUNTRY='CANADA'/*VA<?xml version="1.0" encoding="UTF-8" standalone="yes"?><ex
5	Gayle Gordon (Person)	Yes								
6	Gayle Gordon (Person)	Yes								COUNTRY = 'NZ'/*VA<?xml version="1.0" encoding="UTF-8" standalone="yes"?><ex opId
7	Ivy Ives (Person)	Yes								
8	Ivy Ives (Person)	Yes								COUNTRY = 'AUS'/*VA<?xml version="1.0" encoding="UTF-8" standalone="yes"?><ex op

The Protected Object Reviewer shows all of the permission conditions and the underlying XML

# Secure Development

## Verifying Security Integrity

The Object Permissions Explorer sorted by the access level badge to group like levels of access for review

Effective permissions for: Vegas Enterprises/Director Reports

	Display Name	Access Level	RM	WM	WPM	CM	R	W	C	D	A
1	SAS Administrator	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	SAS Demo User	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	Search Interface to SAS Content User	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	SAS Environment Manager Service Account	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	Jane Jacobs	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Koby Kogan	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Jane Jacobs (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	Koby Kogan (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
9	SAS Administrators	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	Vegas Enterprises: Administrators	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓
11	Ian Irons	Update Folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓
12	Hannah Hanes	Update Folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓
13	Vegas Enterprises: HR	Update Folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	Alice Adams	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓
15	Gayle Gordon	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓
16	Carol Charleston	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓
17	Eve Evans	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓
18	Bob Baxter	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓
19	Ivy Ives	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓
20	Vegas Enterprises: Executives	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓
21	Vegas Enterprises: Directors	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓
22	SAS Trusted User	View metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓
23	SAS System Services	View metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓
24	SAS Anonymous Web User	Hide metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓

# Secure Development

## Verifying Security Integrity

```
C:\Metacoda Tests\sasgf17audit\va-row-level-test.xml - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
var-row-level-test.xml
1 <?xml version="1.0" encoding="UTF-8"?>
2 <SecTest xmlns = "http://metacoda.com/xsd/plugins-sectest-6"
3   xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
4   xsi:schemaLocation = "http://metacoda.com/xsd/plugins-sectest-6 http://metacoda.com/xsd/plugins-sectest-6.xsd">
5
6 <Objects>
7 <Object required="true" publicType="Folder" parentFolder="/Vegas Enterprises" name="Director Reports">
8 <AccessControls complete="true">
9 <ACT required="true" name="Vegas Enterprises: Hide"/>
10 <ACT required="true" name="Vegas Enterprises: HR (Update)"/>
11 <ACT required="true" name="Vegas Enterprises: Executives (Read)"/>
12 <ACT required="true" name="Vegas Enterprises: Directors (Read)"/>
13 </AccessControls>
14 </Object>
15 <Object required="true" publicType="Table" parentFolder="/Shared Data/SAS Visual Analytics/Public/LASR" name="BONUSES">
16 <AccessControls complete="true">
17 <User required="true" name="democaxol" permissions="+RM,+R" hasCondition="true" condition="COUNTRY = &apos;U.S.A.&apos;/**VAGlt;?xml
18 <User required="true" name="demogva" permissions="+RM,+R" hasCondition="true" condition="COUNTRY = &apos;CANADA&apos;/**VAGlt;?xml
19 <User required="true" name="demogyle" permissions="+RM,+R" hasCondition="true" condition="COUNTRY = &apos;NZ&apos;/**VAGlt;?xml
20 <User required="true" name="demoiyv" permissions="+RM,+R" hasCondition="true" condition="COUNTRY = &apos;AUS&apos;/**VAGlt;?xml v
21 </AccessControls>
22 </Object>
23 </Objects>
24
25 </SecTest>
26
```

XML scripts can also be used in the development process to test security

# OPERATIONAL REQUESTS

# Operational Requests

Confirming Users Only Have Access To What They're Supposed To

Administrators also have to ensure that users only have access to the objects and capabilities that they are intended to have.

If users are members of multiple groups, unintended access may be granted through inheritance.

In the following example, a user switches from one geographic sales team to another. Not only must the administrator grant access to the new team's folder, they must also ensure that access to the prior team's folder is removed.



# Operational Requests

Confirming Users Only Have Access To What They're Supposed To

Filter: name, display name, description, or login ids contain david

Level	Name	Repository	Memberst
1	0	David Doyle	Foundation
2	1	Vegas Enterprises: U.S.A.	Foundation
3	2	Vegas Enterprises: North American Region	Foundation
4	3	Vegas Enterprises: Report Consumers	Foundation
5	4	SASUSERS	Foundation
6	5	PUBLIC	Foundation

Found 60 users in 2.652 seconds.

Filtering the User Reviewer plug-in allows the administrator to confirm the appropriate changes have been made to the user's group memberships

# Operational Requests

Confirming Users Only Have Access To What They're Supposed To

Effective permissions for: /Vegas Enterprises/North America/Canada

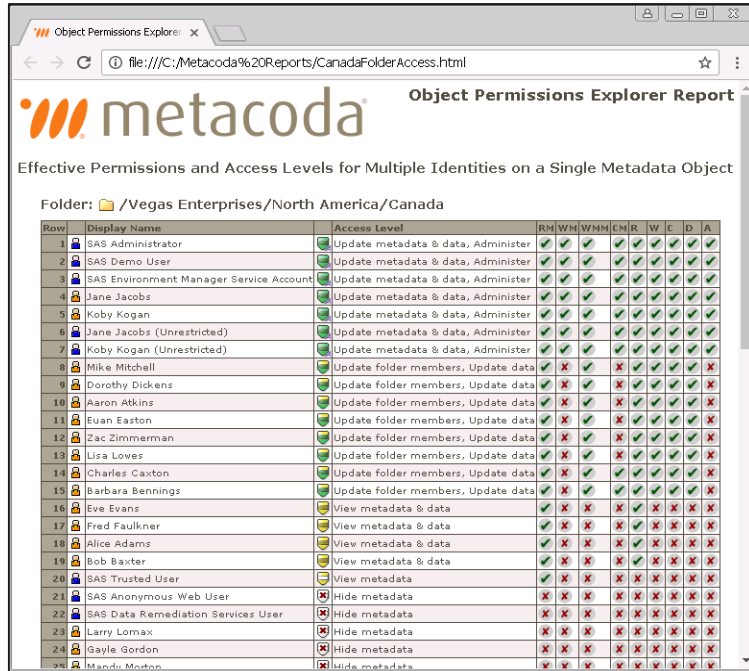
Filter: name, display name, or logins ids contain david

	Display Name	Access Level	RM	WM	WMM	CM	R	W	C	D	A
1	David Doyle	Hide metadata	X	X	X	X	X	X	X	X	X

Using the Object Reviewer plug-in allows the administrator to confirm the user's access level is correct

# Operational Requests

Confirming Users Only Have Access To What They're Supposed To



Object Permissions Explorer Report

Effective Permissions and Access Levels for Multiple Identities on a Single Metadata Object

Folder: /Vegas Enterprises/North America/Canada

Row	Display Name	Access Level	R	M	W	M	C	R	W	E	D	A
1	SAS Administrator	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	SAS Demo User	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	SAS Environment Manager Service Account	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	Jane Jacobs	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	Koby Kogan	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Jane Jacobs (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Koby Kogan (Unrestricted)	Update metadata & data, Administer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	Mike Mitchell	Update folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9	Dorothy Dickens	Update folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	Aaron Atkins	Update folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
11	Euan Easton	Update folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
12	Zac Zimmerman	Update folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
13	Lisa Lowes	Update folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	Charles Caxton	Update folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
15	Barbara Bennings	Update folder members, Update data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
16	Eve Evans	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
17	Fred Faulkner	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
18	Alice Adams	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
19	Bob Baxter	View metadata & data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
20	SAS Trusted User	View metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
21	SAS Anonymous Web User	Hide metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
22	SAS Data Remediation Services User	Hide metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
23	Larry Lomax	Hide metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
24	Gayle Gordon	Hide metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
998	Mandi Morton	Hide metadata	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

An Access Report can be created to confirm that the access has been correctly modified



---

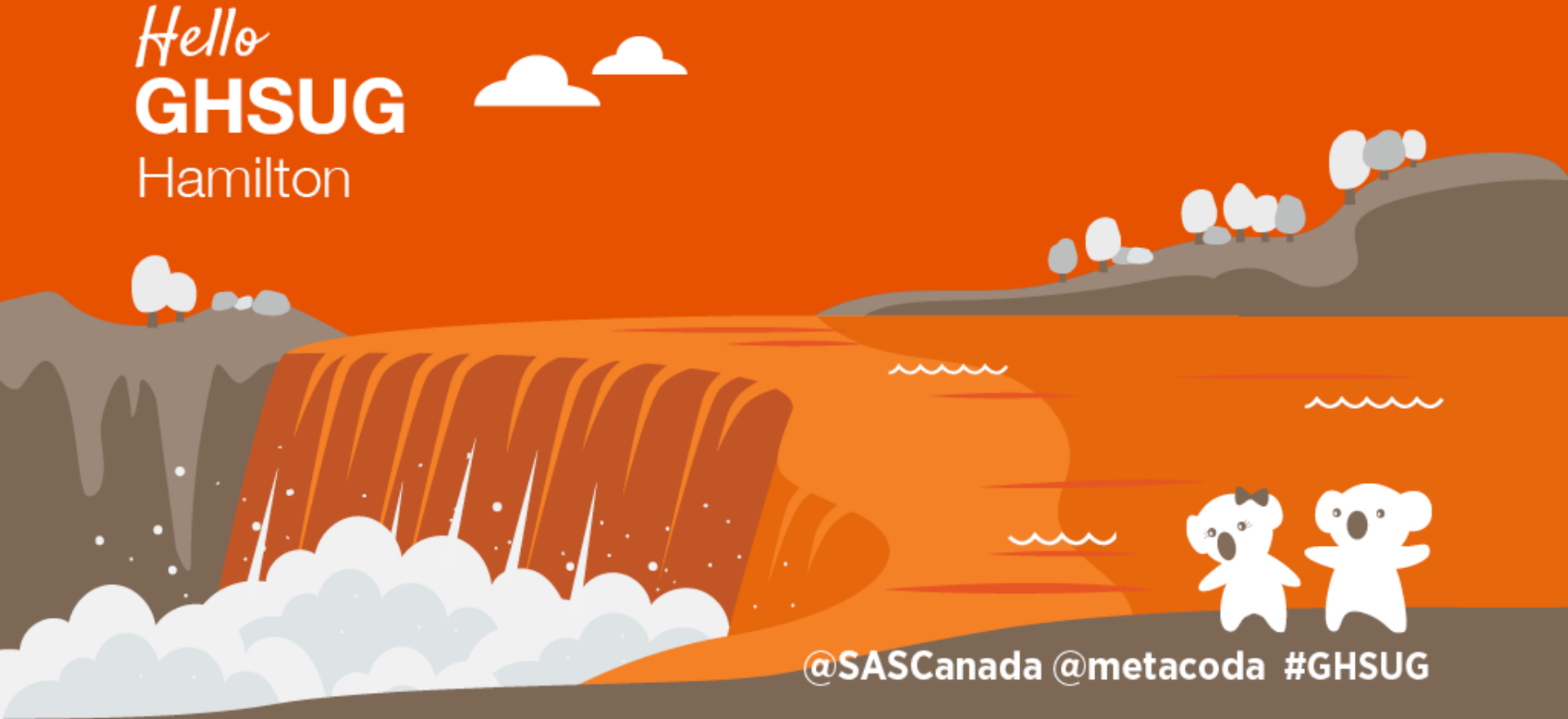
**SECURITY**  
*is a journey*  
**NOT A DESTINATION**

---

**#SASadmin @metacoda**

# QUESTIONS?

*Hello*  
**GHSUG**  
Hamilton



@SASCanada @metacoda #GHSUG

# Contact Us



Email: [info@metacoda.com](mailto:info@metacoda.com)



Web: [www.metacoda.com](http://www.metacoda.com)



Twitter: [twitter.com/metacoda](https://twitter.com/metacoda)



Facebook: [facebook.com/Metacoda](https://facebook.com/Metacoda)



LinkedIn: [linkedin.com/company/metacoda](https://linkedin.com/company/metacoda)



YouTube: [www.youtube.com/user/metacoda](https://www.youtube.com/user/metacoda)



@HomesAtMetacoda





**PRODUCTIVITY THROUGH METADATA VISIBILITY**