

ORACLE®
FUSION MIDDLEWARE **11g**

ORACLE®

Oracle Identity Analytics 11g

Das Compliance Werkzeug für Berechtigungen

Dr. Stephan Hausmann

This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Agenda

- Oracle Identity Analytics Overview
- Transparency
 - Consolidate & Correlate
- Identity-based Controls
 - Access Certification
 - Audit Policy
- Role Management & Governance
- Summary
- Q&A



Oracle Identity Analytics Overview

What Are We Hearing?

IT Ops & Security



- Manage access control across the enterprise
- Assess and control security risk

Business Managers



- Understand and attest to user access
- IT Risk and Business Productivity goals don't align

Compliance

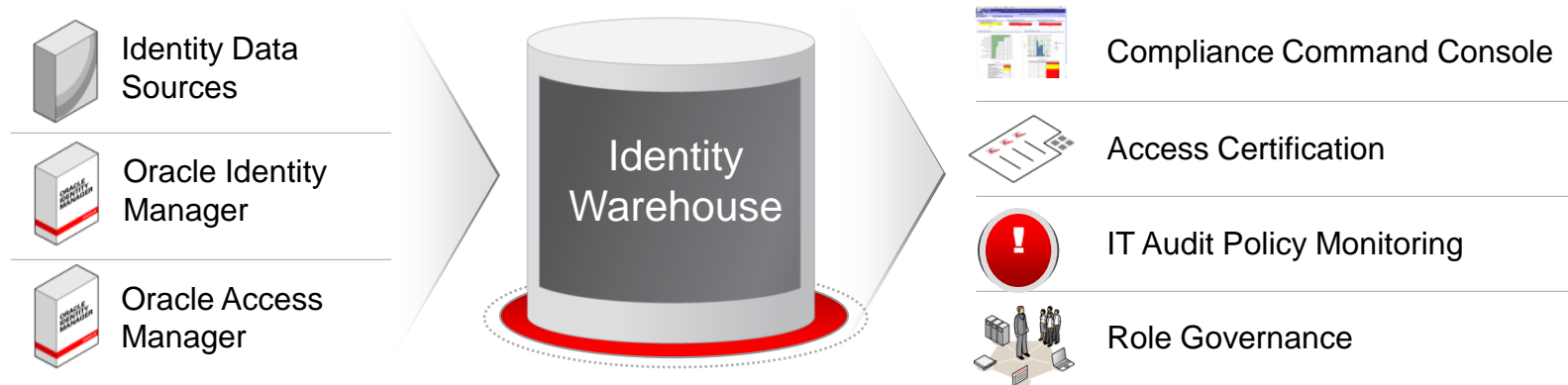


- Without automation, compliance is complex, error-prone, inconsistent
- Need to enforce and demonstrate compliance rapidly



Control IT, Security, Compliance Costs

Oracle Identity Analytics 11g



- **Compliance Command Console**
 - Actionable Dashboards, Business Reports & Comprehensive Analytics
- **Accelerated and Sustainable Compliance Automation**
 - Access Certification, IT Audit Policy Monitoring, Closed-loop Remediation, Risk based
- **Intelligent Role Governance**
 - Change Management, Attestation, Consolidation & Audit, Role Mining
- **Rich Identity Warehouse**
 - Optimized for Analysis, Mining, Correlation, Reporting on Identity, Access and Policy Data

Oracle Identity Analytics

Consolidate
& Correlate
Entitlements

Automate
Identity-based
Controls

Define
Enterprise
Roles

Assign Access
via Roles

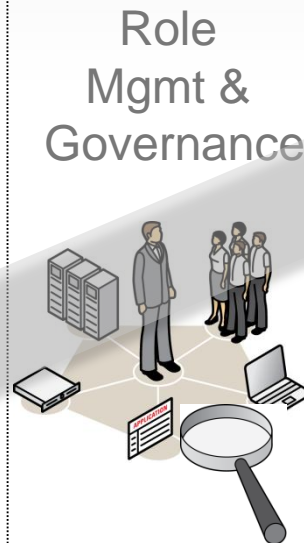
Support Business
Decisions



Phase 1



Phase 2

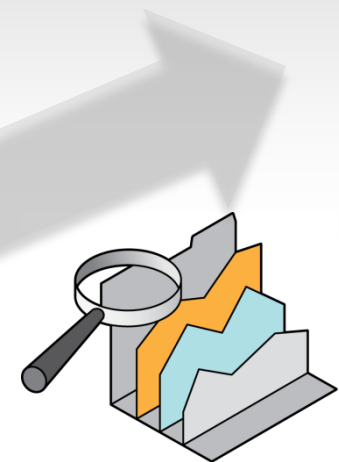


Phase 3



Integration
with
Provisioning

Phase 4

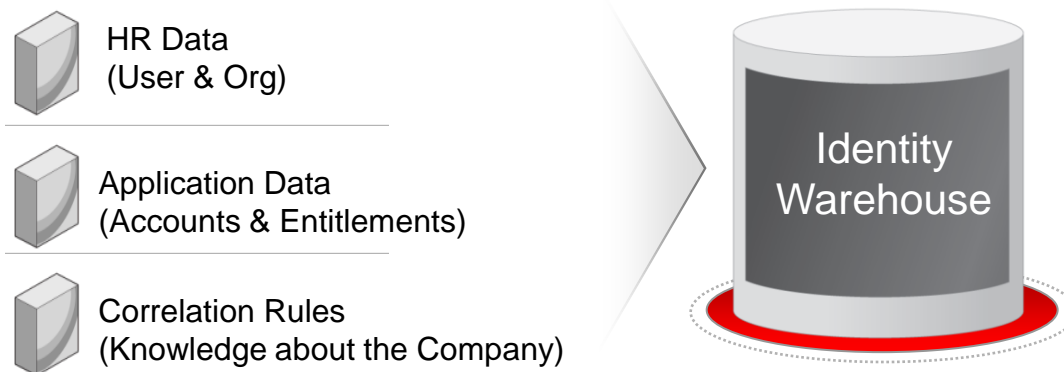


Reports,
Dashboards
& Analytics

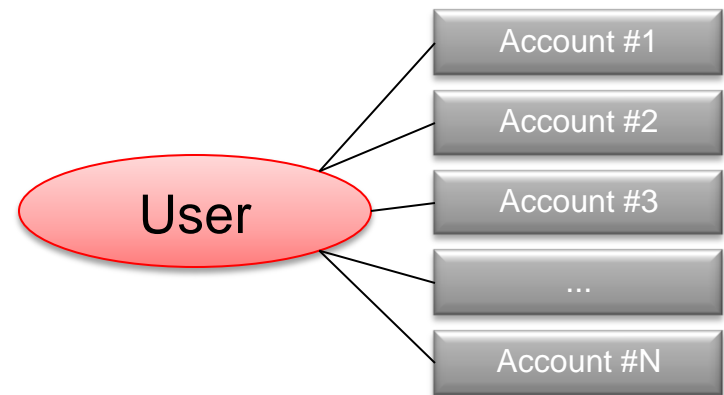
Phase 5

Transparency Consolidate & Correlate

Consolidate & Correlate



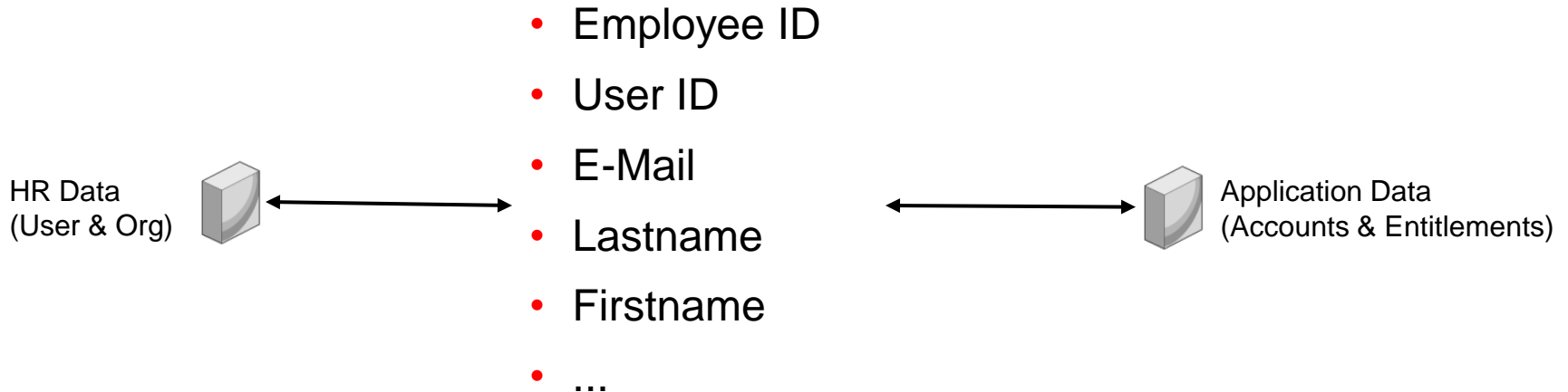
- Consolidate all account data
 - Reporting
 - Who has access to what?
- Identify all uncorrelated account data
 - orphan accounts
 - low data quality
 - manual correlation and/or increase application data quality



Import HR & Application Data

- Organizations
- User
 - Name
 - E-Mail
 - Manager
 - Assigned Organization(s), Assigned Projects, etc.
 - Jobcode, Location
 - Everything which allows a correlation to application accounts
- Application Data
 - Entitlements
 - Everything which allows a correlation to users (HR data)
 - Everything you can get is generally a good idea


Correlation Rules





- Requires knowledge about your company
- Probably different for every application
- Several correlation rules may have to be combined (or correlate with different rules and keep existing correlation)

User & Accounts

Users > Birney, Allan

 Delete User

General **Accounts** Roles Business Structures Custom Properties Relationship Map

 Change Owner  Remove Account

<input type="checkbox"/>	Account Name	Account Type	Resource	Domain	Resource Type Name	Create Date
<input type="checkbox"/>	6461143	Provisioning account	AIX	SUN	AIX	08/25/2011
<input type="checkbox"/>	ab37603	Provisioning account	DB2	SUN	DB2 Database	08/25/2011
<input type="checkbox"/>	ab37603	Provisioning account	AD	SUN	Windows Active Directory	08/25/2011
<input type="checkbox"/>	ab37603	Provisioning account	SUN	Oracle	Oracle	08/25/2011
<input type="checkbox"/>	ab37603	Provisioning account	RACF	none	RACF	08/25/2011
<input type="checkbox"/>	ab37603	Provisioning account	LDAP	SUN	LDAP	08/25/2011
<input type="checkbox"/>	ab37603	Provisioning account	MSSQLServer		Microsoft SQL Server	08/25/2011
<input type="checkbox"/>	ab37603	Provisioning account	UNIX	SUN	Red Hat Linux	08/25/2011
<input type="checkbox"/>	ab37603	Provisioning account	SUN	UDB	UDB	08/25/2011

Accounts, Entitlements & Glossary

Account Details

Account Entitlements

Attribute LDAP Groups
Value CN=BAND_2,ou=Groups,dc=identric,dc=com
Glossary Translation BAND_2
Description
Comments
Classification
Data Owner Cox, Alan
Sub Attributes
Location
Risk Summary ■

Attributes	Values
userid	translation BAND_2
firstName	CN=DEPT_INVB,ou=Groups,dc=identric,dc=com
lastName	CN=ROLE_79111,ou=Groups,dc=identric,dc=com
fullName	
mgrEmplId	
email	
Telephone Number	
Pager Number	
Employee Number	
Mobile Phone	
Home Phone	
Department	
Fax Number	
LDAP Groups	
Location	

X Cancel

Account Details

Account Entitlements

ID 2724
Name ab37603
Resource LDAP
Domain SUN
Description
Created User
Update Date
Create Date 08/25/2011
Comments
Suspended
Risk Summary ■ ■

Orphan Accounts

Users > Orphan Accounts

The screenshot displays the Oracle Identity Management console interface for 'Orphan Accounts'. On the left, a 'Resource Types' sidebar is visible, with 'LDAP(20)' selected. The main area shows a table of 20 provisioning accounts for the 'SUN' domain, all with a 'High' risk level. The table columns are Account Name, Account Type, Domain, Create Date, and Risk Level. A search bar is located at the top right, and a 'Assign To User' button is at the bottom right. The page number 'Page 1' and record count '1 - 20 of 20 Records - Display 50' are also visible.

Account Name	Account Type	Domain	Create Date	Risk Level
ab141560	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ab153570	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ab200820	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ab247170	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ab376030	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ac142810	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ac394350	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ac64100	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ac696630	Provisioning account	SUN	Thu Aug 25 2011 16:17:03 GMT+0200	High
ao5068	Provisioning account	SUN	Thu Aug 25 2011 16:17:44 GMT+0200	High
ba5392	Provisioning account	SUN	Thu Aug 25 2011 16:17:44 GMT+0200	High
cm10127	Provisioning account	SUN	Thu Aug 25 2011 16:17:45 GMT+0200	High
co15346	Provisioning account	SUN	Thu Aug 25 2011 16:17:45 GMT+0200	High
fc5981	Provisioning account	SUN	Thu Aug 25 2011 16:17:45 GMT+0200	High

- Accounts which can't be assigned automatically have to be assigned once manually
- Identify orphan accounts

Customer Example

Ressource	#Accounts	Correlated	Unmatched
Corporate LDAP	17404	17404	0
Applikation #1	6727	6495	232
Applikation #2	9851	9567	284
Applikation #3	12865	12679	186
Application #4	2003	1280	723
Application #5	3857	1757	2100
Application #6	2358	1514	844

3745 accounts deactivated in the Corporate LDAP, but 358 corresponding accounts on the others systems still active

Identity-based Controls Access Certification

Attestation Overview



- Complete Attestation Coverage
 - User Entitlement
 - Role Owner
 - Resource Entitlement
 - Data Owner
- Consolidated, correlated, granular identity data
- Flexible scheduling options and escalation workflows
- Configurable Sign-Off options and Business friendly UI
- Entitlement Glossaries
- Risk based

Access Certification Flow



1 Set Up Periodic Review



What Is Reviewed?



Who Reviews It?



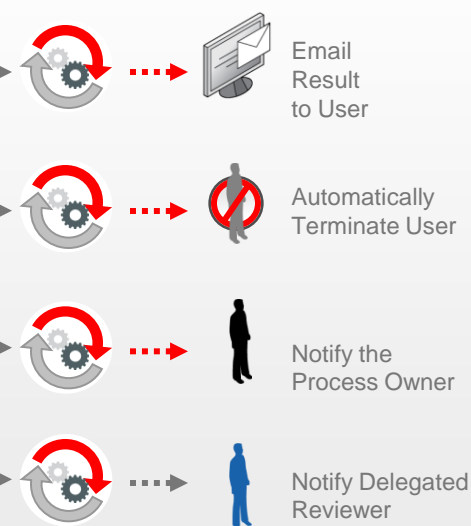
Start When?
How Often?

2 Reviewer Is Notified Goes to Self Service

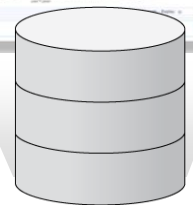
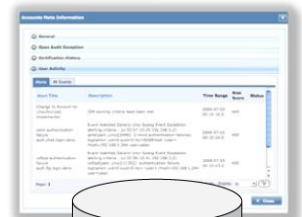
Reviewer Selections

Certify	
Reject	
Decline	
Delegate	
Comments	<input type="text"/>

3 Automated Action is taken based on Periodic Review

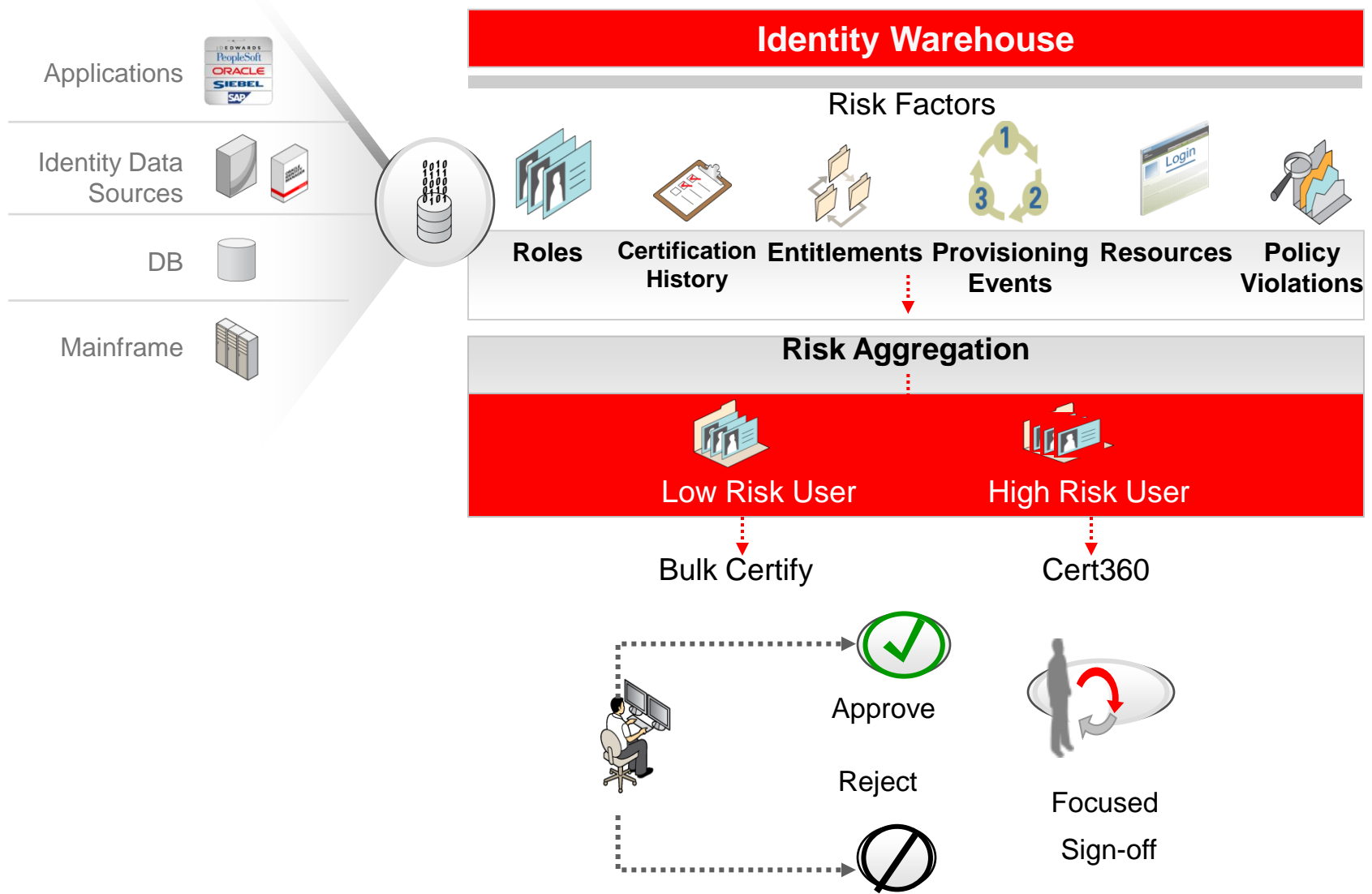


4 Report Built And Results Stored in DB



Archive
Attested Data
Attestation Actions
Delegation Paths

Risk Based Certifications



Create Certifications

Create Certification

1

General

* Certification Name

* Type

Incremental Enabled

Create Certification > Selection Strategy

2

Selection Strategy

Selected Business Structures

Selection Entries

 Add Business Structures  Remove Business Structures

<input type="checkbox"/>	Business Structure Name	Description
<input type="checkbox"/>	Investement Banking	Investement Banking Department


Create Certifications


Create Certification > Selection Strategy > Period and Certifier

3

Period and Certifier

* Certifier

Start Date 

End Date 

Configuration Details

Create Certification > Selection Strategy > Period and Certifier > Summary

4

Summary

Certification Name FY11_Investment_Banking

Type User Entitlement

Certifier User Manager

Start Date 10/25/2011

End Date 11/25/2011

Incremental



Business Structures Selected 1

Run Certification Now Later

Created Certifications

My Certifications

New certifications will require a complete review of the users, roles, or entitlements. Pending certifications have had some review but the process has not been complete. Expired certifications are past their allocated certification period but may be useful for review. Click on the information icon to view a summary of the certification.

 New Certification  Refresh

Show Me

	Status	Certification Name	Business Structure	Type	Start Date	End Date	Updated By	Created
<input type="checkbox"/>	 New	FY11_Investment_Banking_Birney_Allan 		User Entitlement	10/25/2011	11/25/2011		rbac
<input type="checkbox"/>	 New	FY11_Investment_Banking_Hannigan_Sandra 		User Entitlement	10/25/2011	11/25/2011		rbac
<input type="checkbox"/>	 New	FY11_Investment_Banking_Baker_Bob 		User Entitlement	10/25/2011	11/25/2011		rbac

Certification: Users

My Certifications > FY11_Investment_Banking_Birney_Allan

User Entitlement Certification [?](#)

Filter data by

Actions

<input type="checkbox"/>	User Name	First Name	Last Name	Primary Email	Status	Risk Summary	Accounts	Entitlements	Certification Comments
<input type="checkbox"/>	ad12715 ?	Aileen	Doyle	Aileen.Doyle@identric.com	<input type="text"/> 0%	■ ■ ■	9	40	
<input type="checkbox"/>	ad23073 ?	Alan	Doherty	Alan.Doherty@identric.com	Decline	■ ■	8	28	does not work for me
<input type="checkbox"/>	bs38009 ?	Brian	Smith	Brian.Smith@identric.com	<input type="text"/> 0%	■ ■ ■	8	29	
<input type="checkbox"/>	cg31835 ?	Conor	Geary	Conor.Geary@identric.com	<input type="text"/> 0%	■ ■ ■	10	26	
<input type="checkbox"/>	dl67518 ?	David	Lock	David.Lock@identric.com	<input type="text"/> 0%	■ ■	8	25	
<input type="checkbox"/>	dw39309 ?	Deirdre	Worthington	Deirdre.Worthington@identric.com	Decline	■ ■	8	27	retired 4 weeks ago
<input type="checkbox"/>	el14716 ?	Emma	Leahy	Emma.Leahy@identric.com	<input type="text"/> 0%	■ ■	8	23	
<input type="checkbox"/>	eo58821 ?	Edward	O'Toole	Edward.O'Toole@identric.com	<input type="text"/> 0%	■ ■	8	24	
<input type="checkbox"/>	ew58570 ?	Edward	Ward	Edward.Ward@identric.com	<input type="text"/> 0%	■ ■	9	45	
<input type="checkbox"/>	hm63573 ?	Hannah	Mulhall	Hannah.Mulhall@identric.com	<input type="text"/> 0%	■ ■	8	27	

Certification: Entitlements

My Certifications > FY11_Investment_Banking_Birney_Allan

User Detail Doyle, Aileen

<< First < Previous | Next

(1 of 26) -

Doyle, Aileen Research Analyst II
Phone 303-863-8451 **E-Mail** Aileen.Doyle@identric.com **EID** 12715

Filter data by

Risk Levels High Me

Entitlements

Actions

Value X

Actual Value CN=BAND_2,ou=Groups,dc=identric,dc=com
Glossary Translation BAND_2
Description

<input type="checkbox"/>	UNIX	Red Hat Linux	ad12715	Primary group	gwleil			Low	No	Unknown	
<input type="checkbox"/>	LDAP	LDAP	ad12715	LDAP Groups	Translation BAND_2			Low	No	Unknown	
<input type="checkbox"/>	LDAP	LDAP	ad12715	LDAP Groups	CN=ROLE_79111,ou=Groups,dc=identric,dc=com			Low	No	Unknown	
<input type="checkbox"/>	LDAP	LDAP	ad12715	LDAP Groups	CN=DEPT_INVB,ou=Groups,dc=identric,dc=com			Low	No	Unknown	
<input type="checkbox"/>	RACF	RACF	ad12715	Group	OAU1AUD2			Low	No	Unknown	not required any more
<input type="checkbox"/>	RACF	RACF	ad12715	Group	OAU2ARR			Low	No	Unknown	
<input type="checkbox"/>	RACF	RACF	ad12715	Group	ARR1128			Low	No	Unknown	
<input type="checkbox"/>	RACF	RACF	ad12715	Dataset	IDSX00S.GB.EWDWECRW.SETRRVW.*			Low	No	Unknown	
<input type="checkbox"/>	AD	Windows Active Directory	ad12715	AD Groups	CN=Domain Admin,CN=Users,DC=identric,dc=com			High	No	Unknown	
<input type="checkbox"/>	AD	Windows Active Directory	ad12715	AD Groups	CN=HR_User,OU=Applications,OU=Corporate,DC=identric,DC=com			Low	No	Unknown	
<input type="checkbox"/>	AD	Windows Active Directory	ad12715	AD Groups	CN=Paycheck_User,OU=Applications,OU=Corporate,DC=identric,DC=com			Low	No	Unknown	
<input type="checkbox"/>	AD	Windows Active Directory	ad12715	AD Groups	CN=Remote Desktop Users,CN=Builtin,DC=identric,DC=com			Low	No	Unknown	

Page 1

1 - 49 of 49 Records - Display 50

Certification: Reports

Home > My Certifications > FY11_Investment_Banking_Birney_Allan > Reports > Revoked

Certification Report [X]

Select Certification Report

- Revoked Access Report
- Certified Access Report
- Decline Report
- Complete Certification Report
- Abstain Access Report
- Certify Conditionally Access Report

[X Cancel] [✓ OK]

Revoked Access Report

Certification Name: FY11_Investment_Banking_Birney_Allan
Business Structure:
Signed Off By: rbacadmin
Signed Off On: 10/25/11 3:43 PM

Doyle, Aileen- [ad12715]

Account Name	Resource	Comments	De-provisioning Steps	Last Update Date
RACF				
ad12715	RACF			
Attribute Name	Attribute Value	Comments	Last Update Date	Update
Group	OAU1AUD2	not required any more	10/25/11 3:41 PM	rbacadmin

Certification: Reports

Certification Report [X]

Select Certification Report

- Revoked Access Report
- Certified Access Report
- Decline Report
- Complete Certification Report
- Abstain Access Report
- Certify Conditionally Access Report

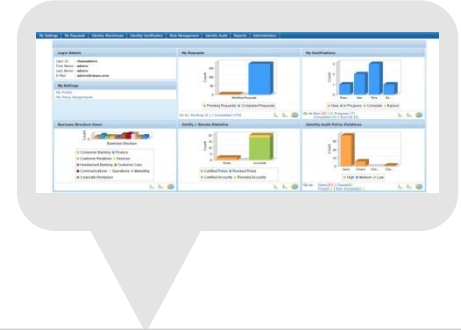
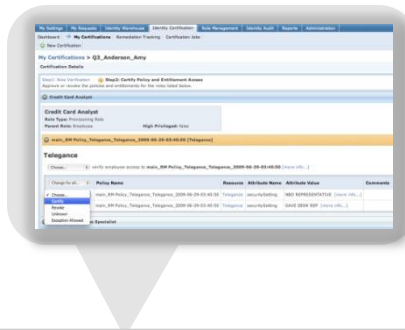
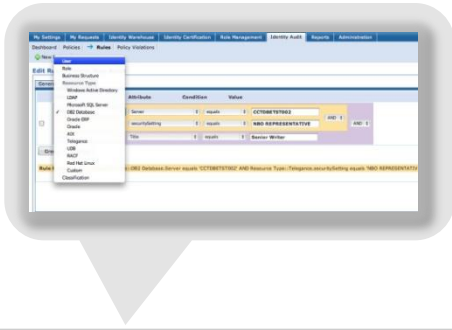
[X Cancel] [✓ OK]

ort

Declined Users Report						10/25/11 3:45 PM
Certification:		FY11_Investment_Banking_Birney_Allan				
Business Structure:						
Signed Off By:		rbacxadmin				
Signed Off On:		10/25/11 3:43 PM				
User ID	Last Name	First Name	Title	Email	Status	Comments
ad23073	Doherty	Alan	Research Analyst I	Alan.Doherty@identric.com	Declined	does not work for me
dw39309	Worthington	Deirdre	Research Analyst I	Deirdre.Worthington@identric.com	Declined	retired 4 weeks ago

Identity-based Controls Audit Policy

IT Audit Policy Monitoring



IT Audit Policies

- Across Entitlements & Roles
- Within Application or Cross-Applications
- Preventative & Detective Remediation

Role Exceptions

- Roles Vs. Actuals
- Entitlements Outside Roles
- Mitigating Controls
- Manager Signoff for Audit Exceptions

Monitoring

- 50+ Reports
- Compliance Dashboards
- Compliance Metrics Monitoring
- Historical Trend Analysis
- Remediation Tracking

IT Audit Policy Monitoring

The screenshot shows the Oracle Identity Audit console interface. The top navigation bar includes tabs for My Settings, My Requests, Identity Warehouse, Identity Certification, Role Management, Identity Audit, Reports, and Administration. The main content area is titled "Edit Rule > Create New Asset" and has two tabs: "General" and "Conditions". The "Conditions" tab is active, displaying a table with columns for Object, Attribute, Condition, Value, and Operation. Three conditions are listed:

Object	Attribute	Condition	Value	Operation
DB2 Database	Server	equals	CCTDBETST002	
Telegance	securitySetting	equals	NBO REPRESENTATIVE	AND
User	Title	equals	Senior Writer	AND

Below the table, a "Rule Condition" is displayed as a logical expression: `(((Resource Type::DB2 Database.Server equals 'CCTDBETST002' AND Resource Type::Telegance.securitySetting equals 'NBO REPRESENTATIVE') AND User.Title equals 'Senior Writer'))`. Buttons for "Group", "Ungroup", "Add Condition", "Remove", "Cancel", and "Save" are visible.

Complex Audit Rule Conditions

Enterprise wide Rule Objects

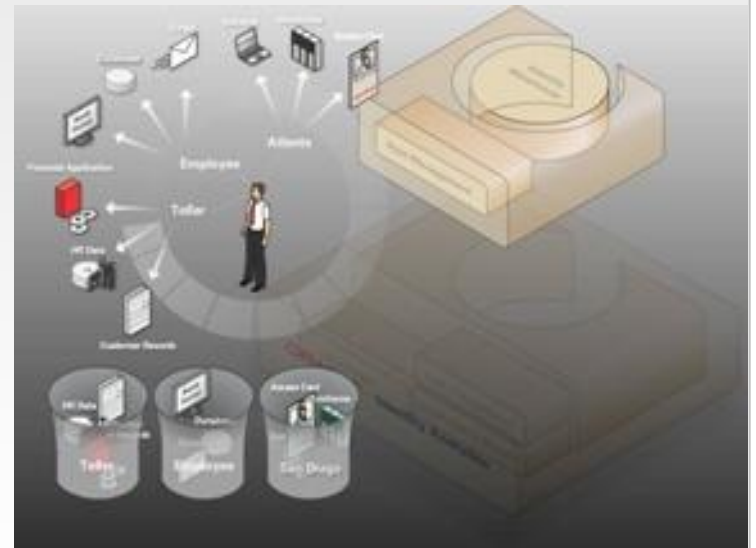
This screenshot shows the same Oracle Identity Audit console interface, but with a dropdown menu open over the "Object" column of the conditions table. The dropdown menu lists various system objects, including "User", "Role", "Business Structure", "Resource Type", "Windows Active Directory", "LDAP", "Microsoft SQL Server", "DB2 Database", "Oracle ERP", "Oracle", "ADX", "Telegance", "UDB", "RACF", "Red Hat Linux", "Custom", and "Classification". The "User" option is currently selected. The background shows the same rule configuration as the top screenshot.

Role Management & Governance

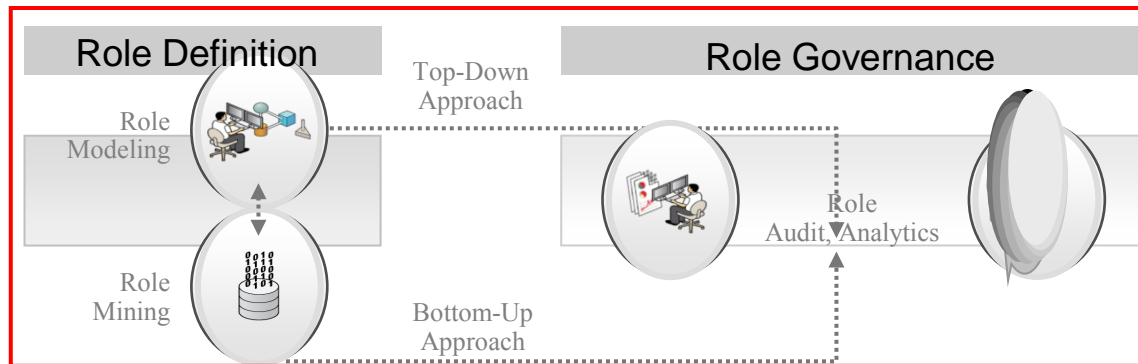
Role Mining

Intelligent Role Discovery Engine

- Comprehensive Role Discovery using Hybrid Approach:
 - Bottom Up (User Entitlements)
 - Top Down (User HR Attributes)
- Flexible User Population Selection
- Mining Results Dashboard
 - Statistics & Analytics
 - Graphical Representations
- Incremental Role Mining
 - Role Entitlement Discovery to mine new applications based on existing roles



Define and Govern User Roles



Change Mgmt

- Role Change Approvals
- Role Versioning
- Rollbacks & Comparison
- Role Change Impact Analysis
- Rule Management

Role Audit

- Role –Entitlement Mapping History
- Role Membership History
- Approvals History
- Role Ownership History

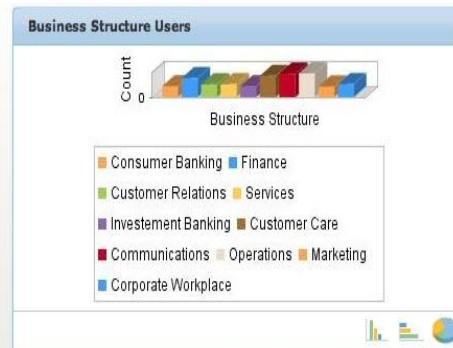
Governance

- Role Definition Attestation
- Role Membership Attestation
- Role Consolidation
- Role Mining

Compliance Command Console

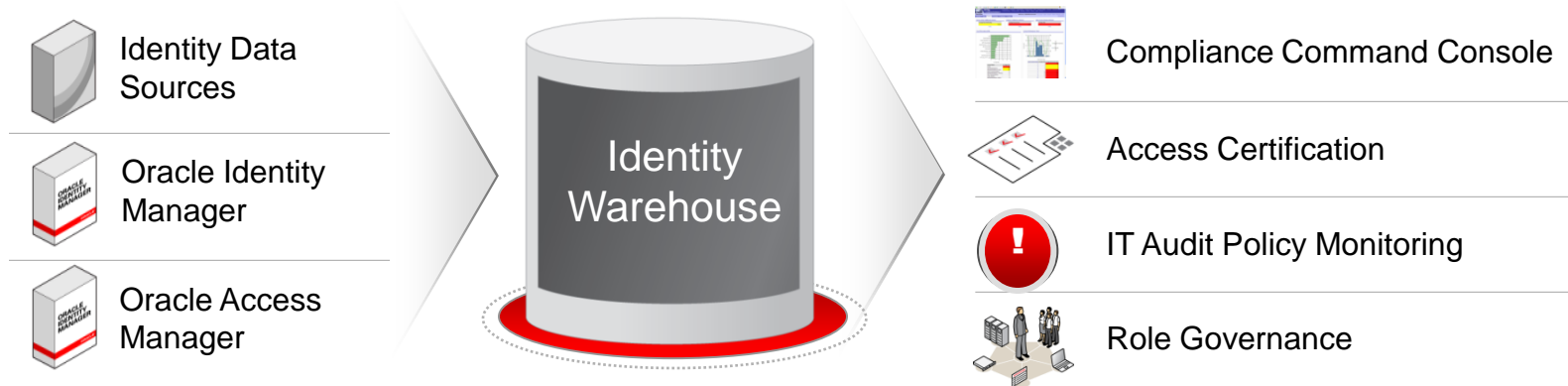
Presentation of Identity Data in Business-Friendly Format

- Actionable dashboards
 - Reliable risk analysis
 - Compliance Dashboards
- 50+ OOTB Reports
- Publicly available schema
- Comprehensive cross-referenced presentable data
 - Enable complete Identity Governance
- Advanced analytics



Summary

Oracle Identity Analytics 11g



- **Compliance Command Console**
 - Actionable Dashboards, Business Reports & Comprehensive Analytics
- **Accelerated and Sustainable Compliance Automation**
 - Access Certification, IT Audit Policy Monitoring, Closed-loop Remediation, Risk based
- **Intelligent Role Governance**
 - Change Management, Attestation, Consolidation & Audit, Role Mining
- **Rich Identity Warehouse**
 - Optimized for Analysis, Mining, Correlation, Reporting on Identity, Access and Policy Data

Summary



- **Oracle Identity Analytics**
 - Is comprehensive and proven
 - Offers rich set of identity governance features including risk based attestation, continuous SoD monitoring, role governance, dashboards & reporting
 - Is available for download today
- **For More Information**
 - www.oracle.com/identity
 - www.identigov.wordpress.com



ORA



ORACLE IS THE INFORMATION COMPANY