

Roles

Fundamentals of IdentityIQ Implementation
IdentityIQ

Overview

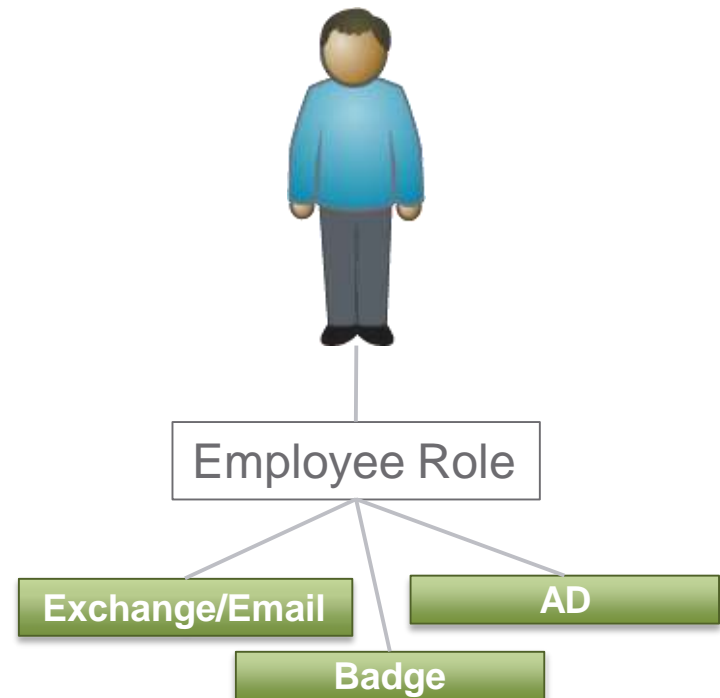
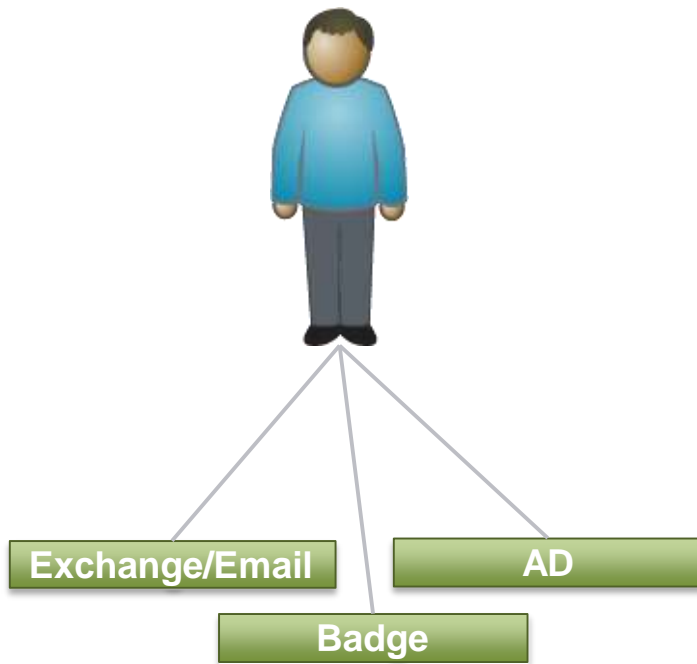
Roles

- Why Roles?
 - Role Definition
 - Role Management Benefits
- IdentityIQ Support for Roles
 - Common Role Management Models
 - Role Model Overview
 - Least Privilege
- Configuring and Managing Roles
 - Role Definition and Mining
 - Extending the Role Model
 - Role Assignment
 - Sunrise/Sunset of Roles
- Role Management Pointers

Role Management

Definition

- Manage user access by assigning a role
 - Regulate and provision access to resources based on the roles of the individual user



Why Roles?

- **Categorize and Manage users based on their job function**
 - Apply common functionality to groups of users based on Identity Attributes or other Assignment Rules
- **Provide a translation between the Business and IT functions within an organization**
 - Enforce least privilege
 - Provide user access to IT resources based on Business Roles
- **Improve Efficiency**
 - Encapsulate individual entitlements of IT Access
 - Simplify Access Review/Certification process
 - Ease request process for new access
 - Simplify Auditing

Why Roles?

Manage Access by Expertise

Business

- Expertise: *Specify what jobs need to be done and by whom*
- Simplifies *user* access certification
 - Should John have the Support role?
- Simplifies provisioning
 - Request a role

IT

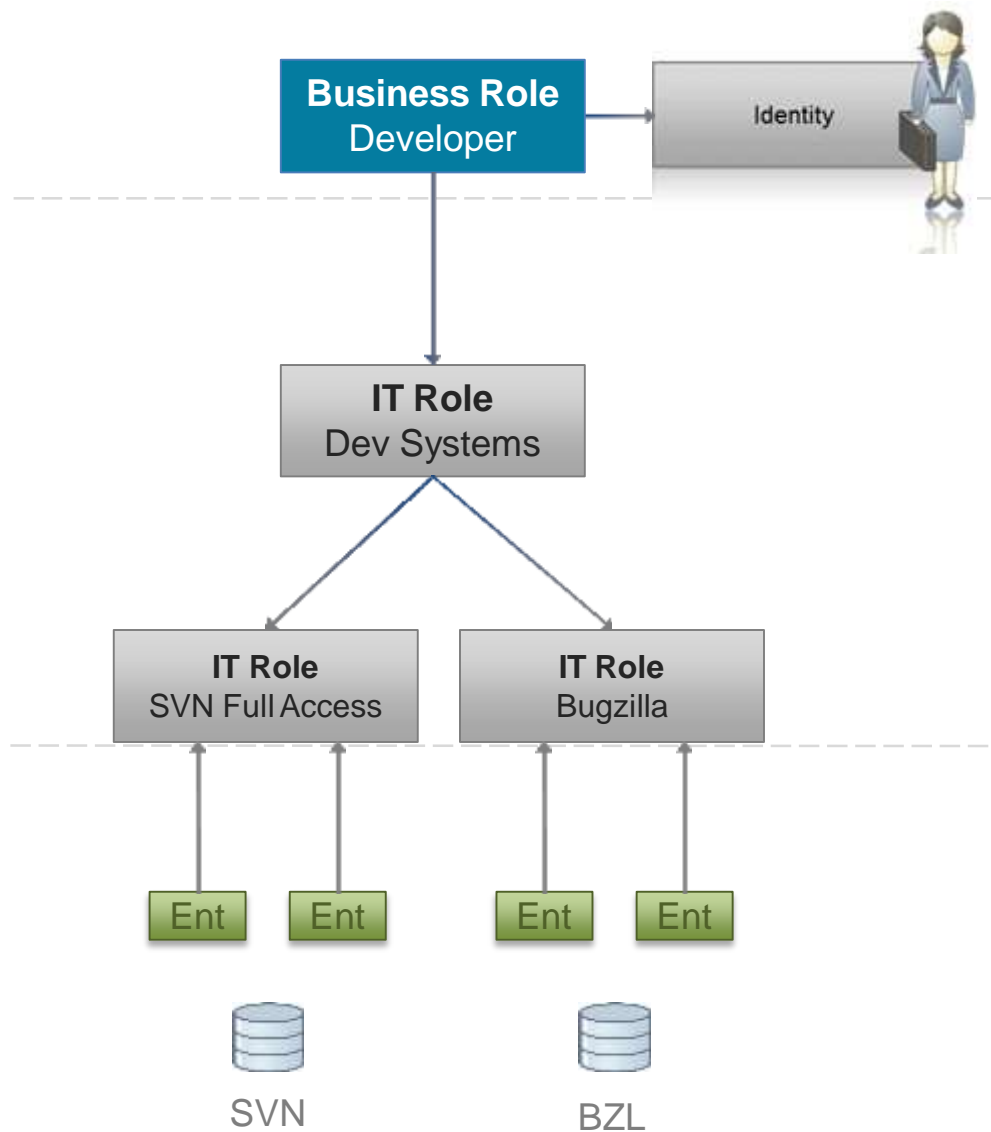
- Expertise: *What access is needed to do the job*
- Simplifies access certifications
 - Should the Support role have the AD-73 access?
- Simplifies provisioning
 - Automate the actual provisioning

IdentityIQ Support for Roles

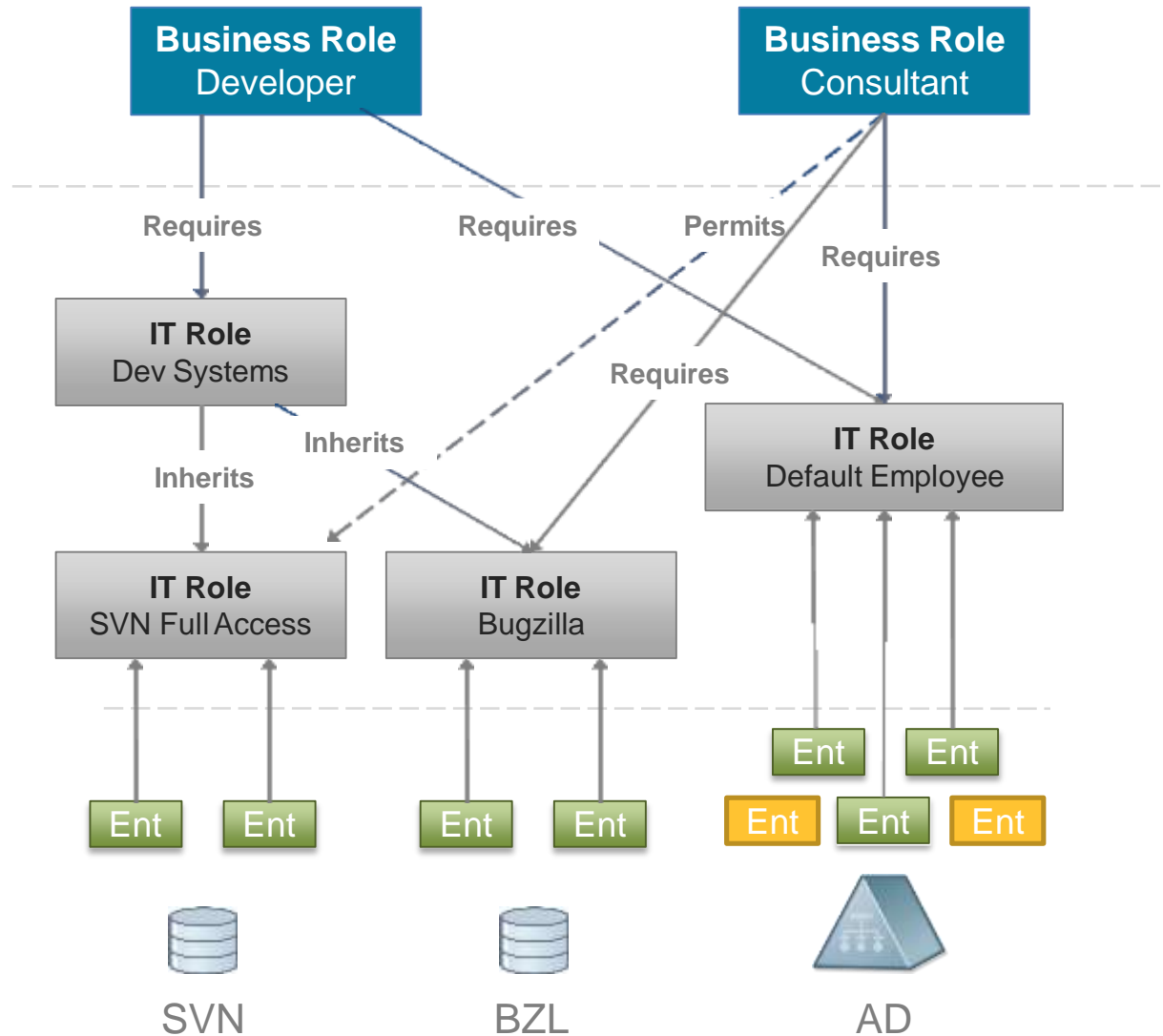
IdentityIQ Role Modeling

- Two-tier model (default)
- Supports
 - Discovery
 - Auto-assignment based on rule/logic
 - Self-service provisioning
 - Meaningful display names and descriptions
 - Extended attributes
 - Role mining
- Uses default workflows
 - Rules and metadata in role control workflow behavior
- Extensible
- Part of the identity governance framework
 - Access certification
 - Policy enforcement
 - Risk management

Two Tier Role Management Model

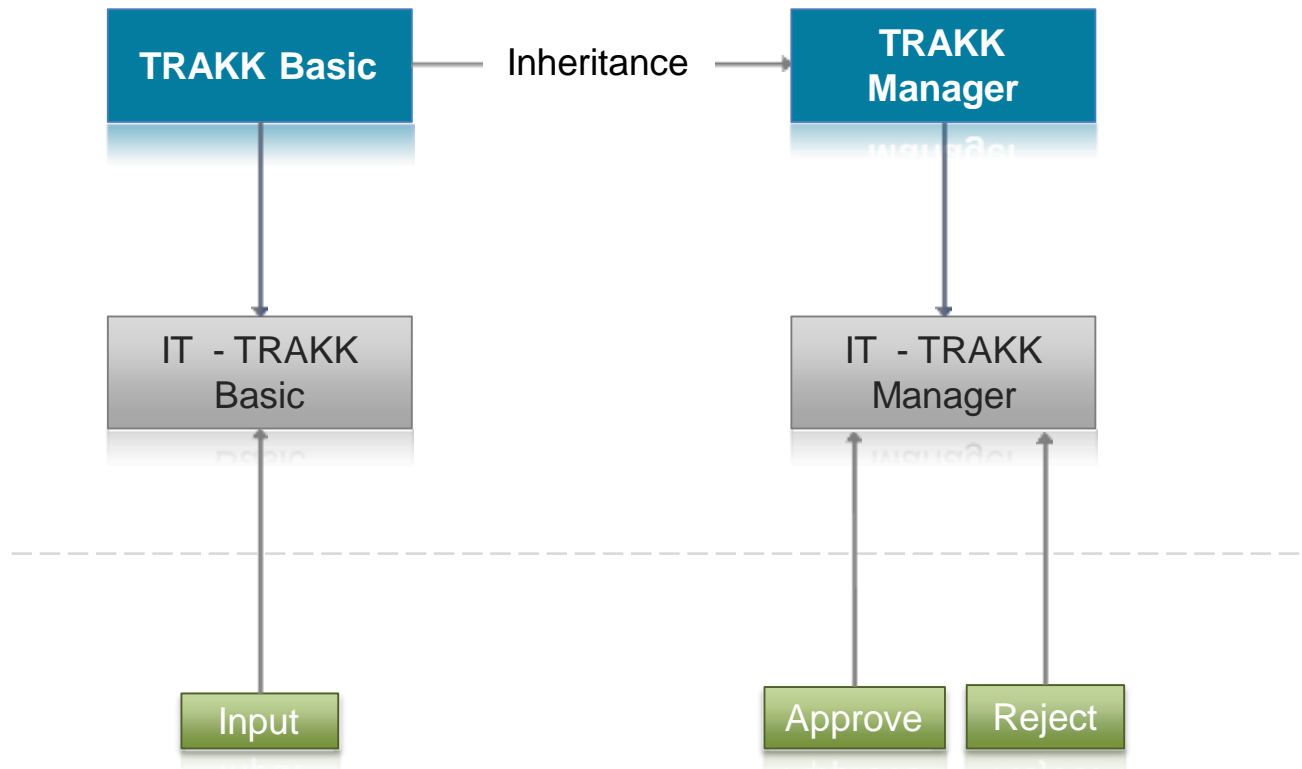


Role Relationships – Requires / Permits



Role Relationships – Inheritance

- Manager Role entitlements are additive
 - Input, Approve, & Reject
- Simpler model

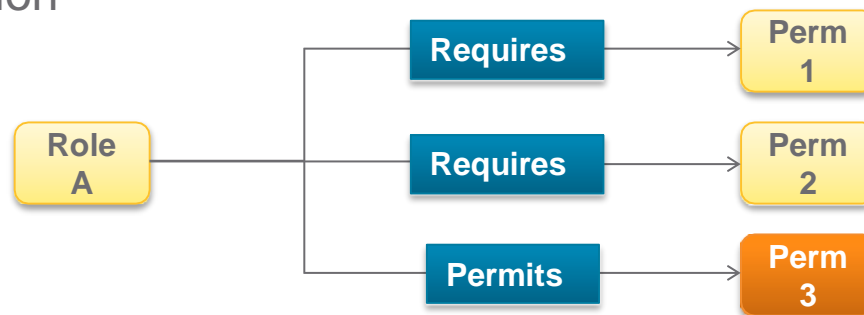


Least Privilege Without Role Explosion

- You want least privilege
 - Only award the entitlements needed for a given task
- But in some models that leads to role explosion
 - Normally functional decomposition means more roles...

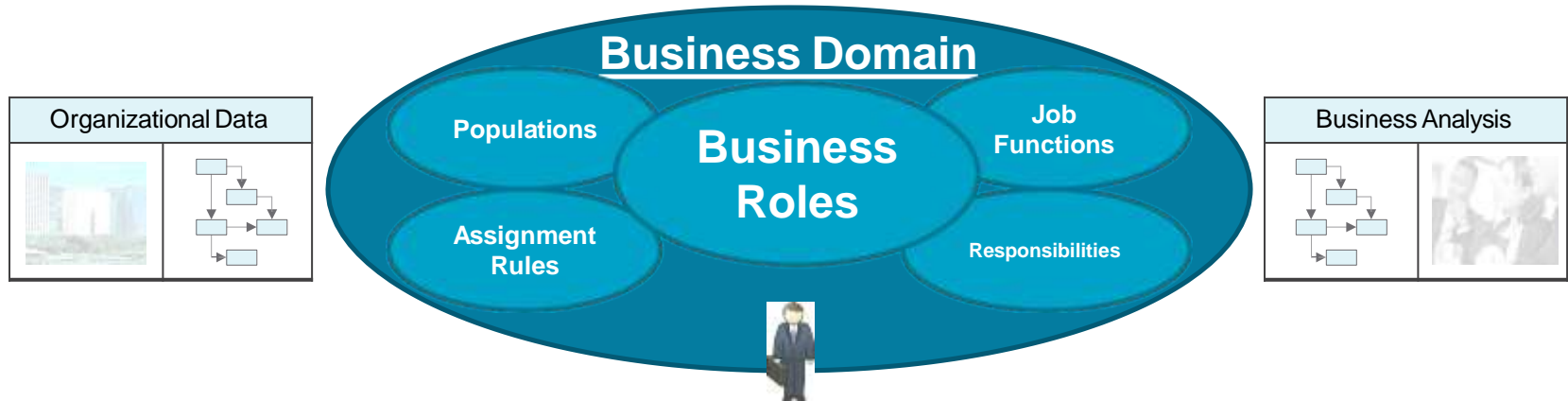


- Role association relationships capture least privilege
 - Producing simplified more manageable models with less role explosion



Two Tier Model

Business Roles

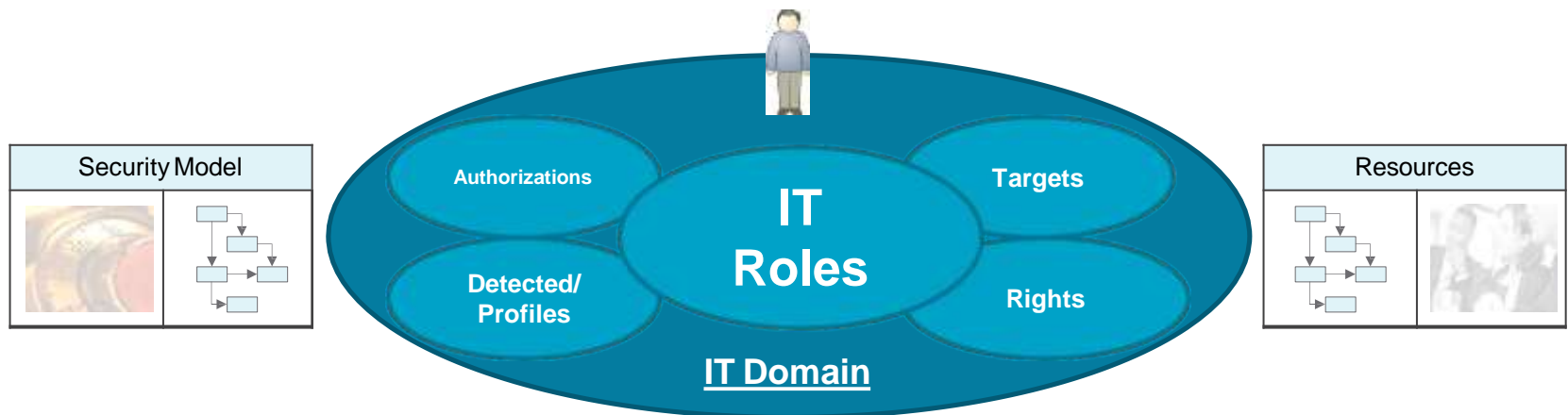


- Business Roles represent job functions, titles or responsibilities
- Needs determined by organizational structure or through business analysis
- Include metadata to increase understanding
- Can be assigned to users

Two Tier Model

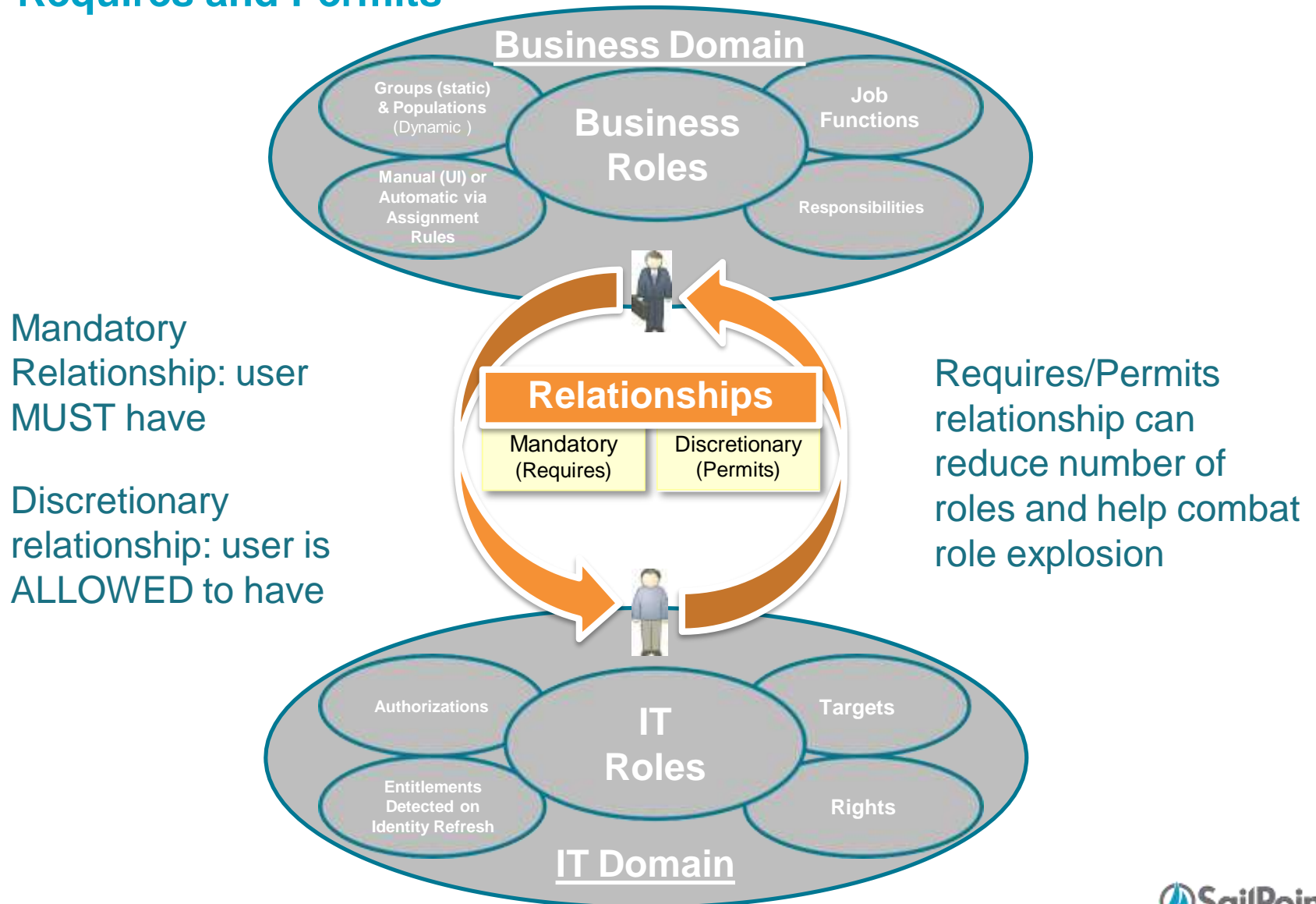
IT Roles

- Model the IT privileges required to perform a specific function within an application or other target system
- Represent a user's actual access
 - Accounts
 - Entitlements
 - Permissions
- Can be used to provision access



Relating Business and IT Roles

Requires and Permits



Acquiring a Role

Roles – Assigned or Detected

Dashboard **Define** Monitor Analyze Manage System Setup

Identities

Filter by Identity Name



User Nam	First Name	Last Name	Assigned Role Summary	Detected Role Summary	Risk
Debor...	Deborah	Collins	Region.Americas		● 0
Debra....	Debra	Wood	PRISM Manager, Region.Eu...	PRISM Manager-IT, PRI...	● 50
Denise...	Denise	Hunt	Region.Europe	TRAKK - Basic	● 50
Dennis...	Dennis	Barnes	Region.Europe, PRISM Man...	PRISM Manager-IT, PRI...	● 50
Diana....	Diana	Lawrence	Region.Asia-Pacific		● 0

Roles – Allowed By, Assigned By

View Identity Dennis.Barnes

- Attributes
- Entitlements
- Application Accounts
- Policy
- History
- Risk
- Activity
- User Rights

Dennis.Barnes was last refreshed on 6/11/14 at 8:15:49 AM CDT ?

Roles

Filter by role name



Advanced Search

Name	Description	Assigned By	Allowed By	Acquired	Application	Account
Region.Europe				Assigned		
TRAKK - Super User				Detected		
PRISM Manager				Assigned	PRISM	Dennis.B
PRISM Manager-IT			PRISM Manager	Detected	PRISM	Dennis.B
PRISM User-IT				Detected		

Obtaining Business Roles

- Requested manually through Lifecycle Manager (or, if configured, Identity→Entitlement page)
 - Prompts for allowed entitlements
- Automatically using assignment rules
 - Permits must be requested

The screenshot shows the 'Assignment Rule' configuration window. At the top, there are radio buttons for 'None', 'Match List' (selected), 'Filter', 'Script', 'Rule', and 'Population'. Below this is the 'IdentityIQ Items' section with an 'Add Identity Attribute' button. The 'Application Items' section has a dropdown menu for selecting an application, with 'Add Attribute' and 'Add Permission' buttons. The main area is a table with columns: Operation, Type, Application, Name, Value, and Is Null. A single row is visible with 'Or' in the Operation column, 'Attribute' in the Type column, 'IdentityIQ Identity' in the Application column, 'Region' in the Name column, 'Americas' in the Value column, and an empty checkbox in the Is Null column. At the bottom, there are buttons for 'Group Selected', 'Ungroup Selected', and 'Delete Selected'.

Operation	Type	Application	Name	Value	Is Null
Or	Attribute	IdentityIQ Identity	Region	Americas	<input type="checkbox"/>

Options

- Matching
- Filtering
- Scripts/rules (code snippets)
- Populations

Obtaining IT Roles

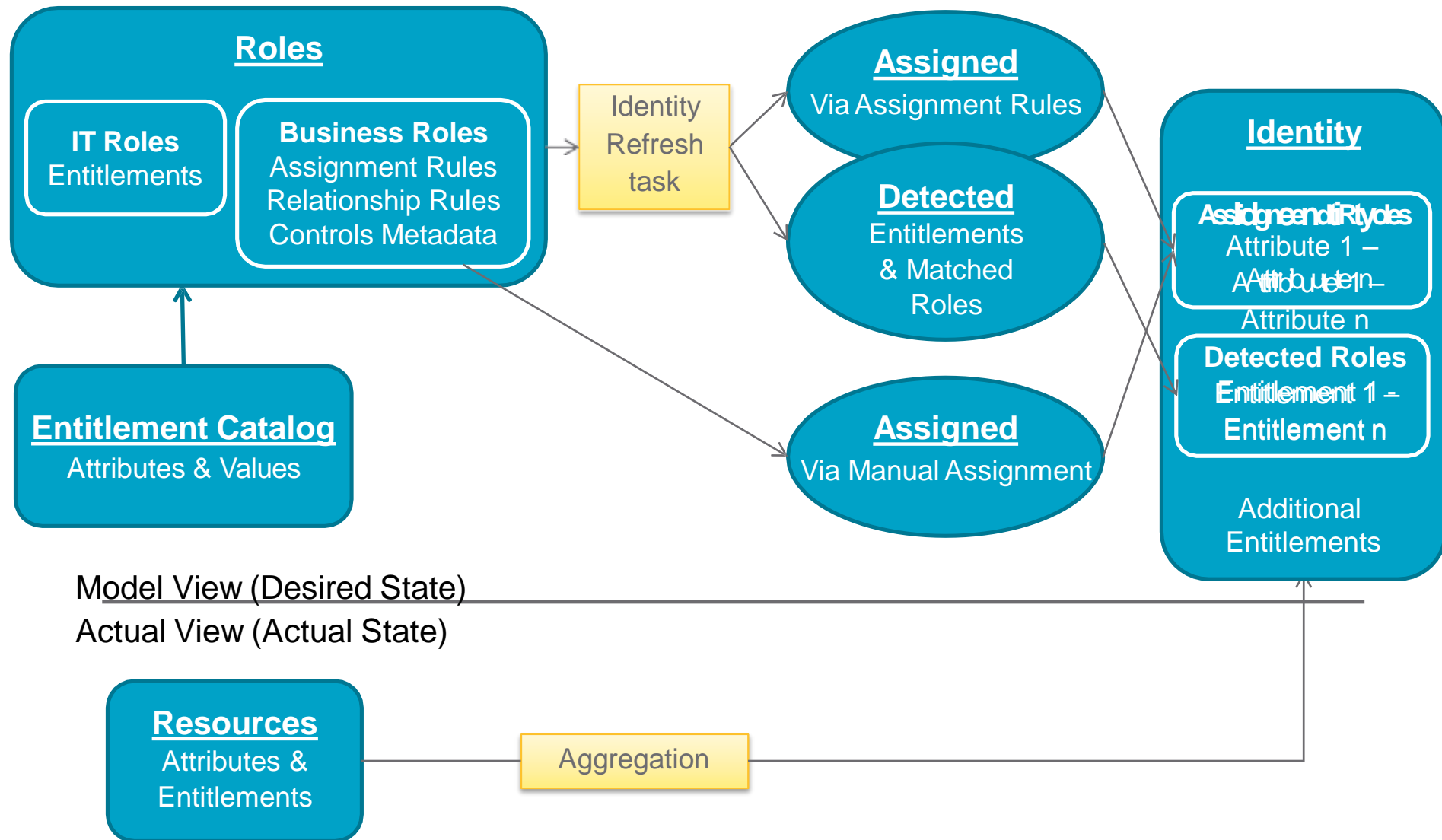
- Detected from environment on Identity Refresh
 - 'Refresh Assigned and Detected Roles' option selected
 - Detection is defined through a Role Profile
- Requested indirectly
 - Via LCM Access Request for a business role
 - Via business role assignment
 - During an Access Review (provisioning missing roles)

Assigning and Detecting Roles

- Monitor → Tasks
- Run “Identity Refresh” Task
 - “Refresh assigned, detected roles...” selected
 - Detection is defined through an IT Role Profile
- Optionally choose
 - “Provision assignments”
 - “Disable deprovisioning...”

Refresh assigned, detected roles and promote additional entitlements	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Provision assignments	<input type="checkbox"/>	<input type="checkbox"/>
Disable deprovisioning of deassigned roles	<input type="checkbox"/>	<input type="checkbox"/>

Assigned vs Detected Roles



Certification – Assigned vs Detected Roles

Access Review Details

Previous Identity

Certifying Ernest Lewis (3/6)

Next Identity

Decisions

Recent Changes

Employee Data

Risk Data

Approve All Revoke All Delegate All Clear Decisions

Legend: Approve Revoke Allow Exception Action Required

Roles

Decision	Role	Description
	Windows Administrator	Provides strategy setting, planning, supervision, technical, and administrative support for Windows 2003, 2008, 2012, x32 and x64 bit servers. Assists in the development of comprehensive information security procedures and practices and deployment.
	<div><div>Allowed Roles</div><div>Role Hierarchy</div></div>	
	<div><div>Role Hierarchy</div><div> Required Roles Break Glass Windows Administrator Access Permitted Roles Helpdesk Associate Access</div></div>	
	<div>Role Details</div> <div><p>Name: Windows Administrator</p><p>Type: Business</p><p>Owner: The Administrator</p><p>Description: Provides strategy setting, planning, supervision, technical, and administrative support for Windows 2003, 2008, 2012, x32 and x64 bit servers. Assists in the development of comprehensive information security procedures and practices and deployment.</p><p>Acquired: Assigned</p></div>	

Additional Entitlements

Decision	Application	Account Name	Attribute	Entitlements
	Active_Directory	Ernest Lewis	groupmbr	SecCompliance

Certification – Assigned vs Detected Roles

Access Review Details

[Previous Identity](#)

Certifying Daniel Wagner (2/6)

[Next Identity](#)[Decisions](#)[Recent Changes](#)[Employee Data](#)[Risk Data](#)[Approve All](#) [Revoke All](#) [Delegate All](#) [Clear Decisions](#)

Legend: Approve Revoke Allow Exception Action Required

Roles

Decision

Role

Description

Windows Administrator

Missing Required Roles

Provides strategy setting, planning, supervision, technical, and administrative support for Windows 2003, 2008, 2012, x32 and x64 bit servers. Assists in the development of comprehensive information security procedures and practices and deployment.

[Allowed Roles](#)[Role Hierarchy](#)

Role Hierarchy

Required Roles

Break Glass

Windows Administrator Access

Permitted Roles

No Matching Roles Found

Role Details

Name: Windows Administrator**Type:** Business**Owner:** The Administrator**Description:** Provides strategy setting, planning, supervision, technical, and administrative support for Windows 2003, 2008, 2012, x32 and x64 bit servers. Assists in the development of comprehensive information security procedures and practices and deployment.**Acquired:** Assigned

Page 1 of 1 Show 15 items

Displaying 1 - 1 of 1

Additional Entitlements

Decision

Application

Account Name

Attribute

Entitlements

23

Oracle_DB_oasis

Daniel Wagner

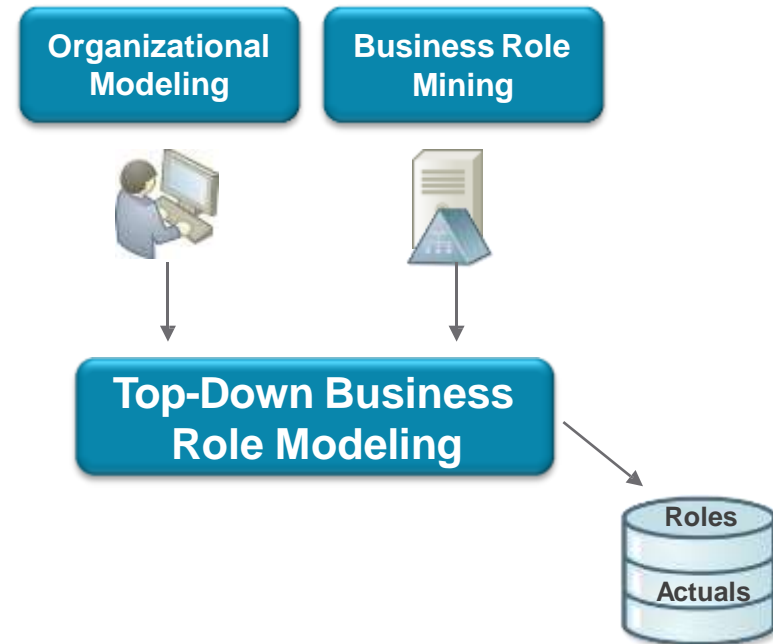
Allow Export

create

Configuring Roles

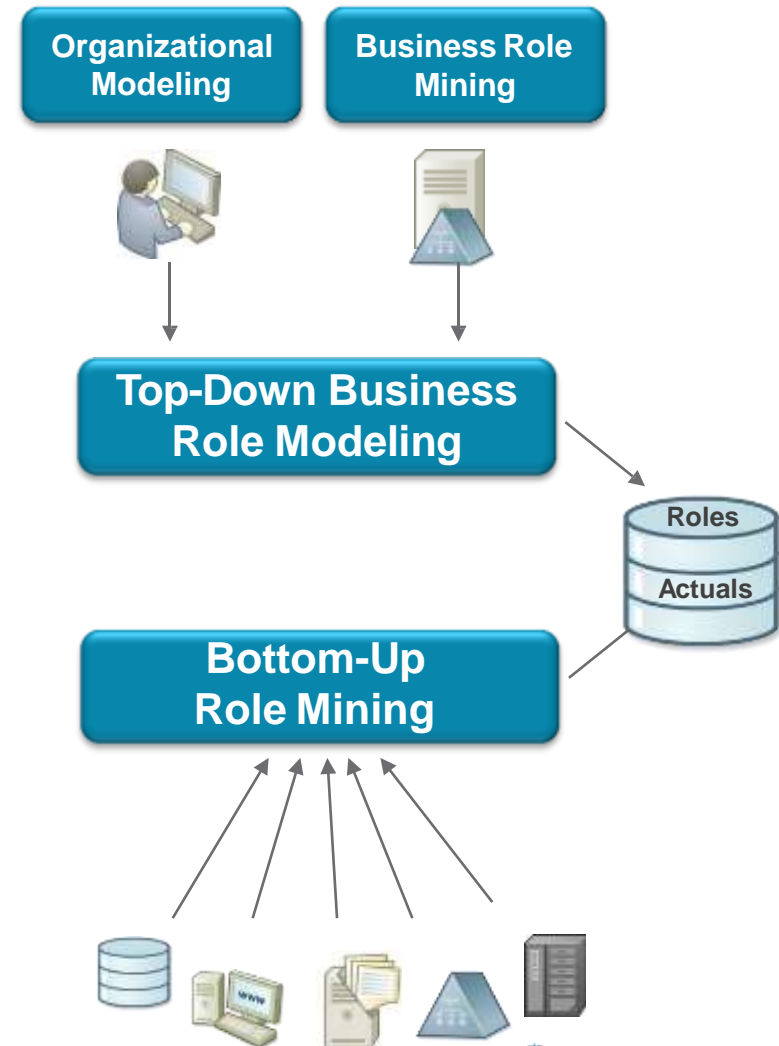
Role Definition and Mining

- **Top-Down Business Role Modeling**
 - Captured via business analysis and organizational modeling
 - Enhanced using automated analysis of identity data
 - Supported heavily by role membership certification



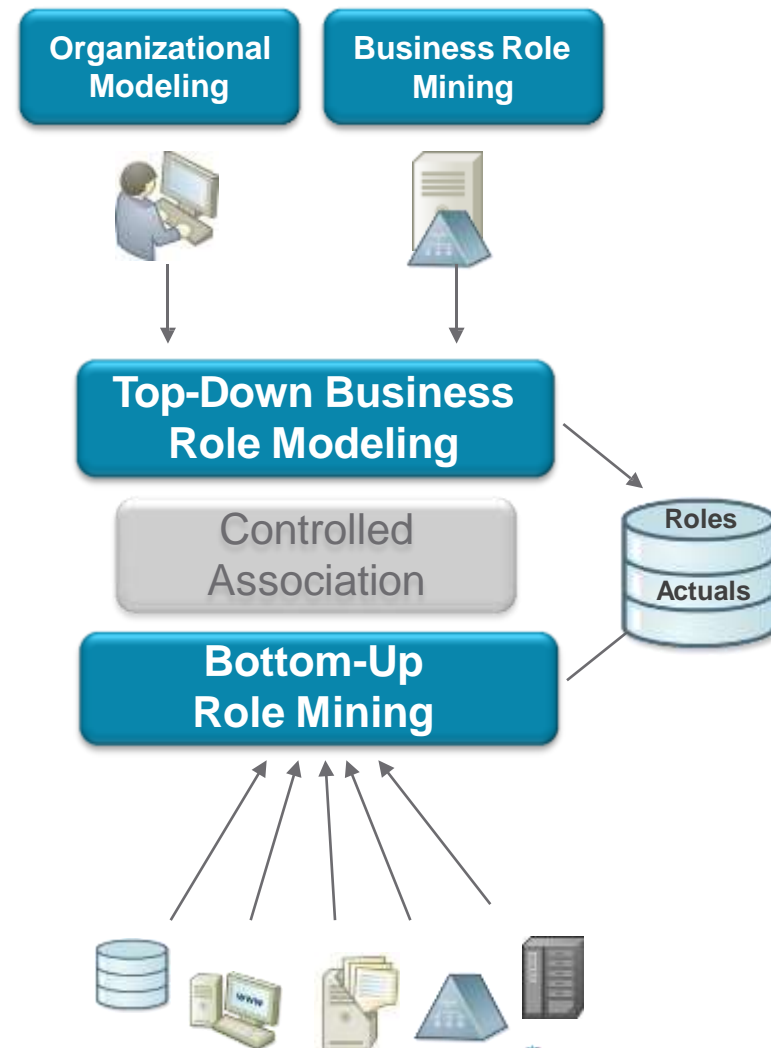
Role Definition and Mining

- **Top-Down Business Role Modeling**
 - Captured via business analysis and organizational modeling
 - Enhanced using automated analysis of identity data
 - Supported heavily by role membership certification
- **Bottom-Up IT Role Mining**
 - Driven by algorithmic analysis and analytics-focused mining processes
 - Derived from data pulled from the central repository or “actuals”
 - Supported heavily by role composition certification and analysis and “review” of those actuals



Role Definition and Mining

- **Top-Down Business Role Modeling**
 - Captured via business analysis and organizational modeling
 - Enhanced using automated analysis of identity data
 - Supported heavily by role membership certification
- **Bottom-Up IT Role Mining**
 - Driven by algorithmic analysis and analytics-focused mining processes
 - Derived from data pulled from the central repository or “actuals”
 - Supported heavily by role composition certification and analysis and “review” of those actuals
- **Collaborative Association**
 - Key to the hybrid approach
 - Join business & IT roles using the model
 - What if modeling & impact analysis
 - Population analysis
 - Assessment of actuals & policy evaluation
 - Controlled approvals & workflow



Role Mining

- Business role mining – “top down”
 - Model identities based on attributes and entitlements
 - Automatically creates roles (default)
- IT role mining – “bottom up”
 - Model IT privileges required to perform a specific function
 - Search for access patterns
 - Two methods
 - Create an IT Role Mining Task
 - Run an Entitlement Analysis
 - Analyze results and select roles for creation

Business Role Mining

- Create a Business Role Mining Task

- Define → Roles → Create New → Business Role Mining

- Input

- Select Identity Attributes to Mine
- Select entitlements (optional)
- Define assignment rule (optional)

- Execution creates roles (default)

- Must enable roles after creation

The screenshot shows the 'Role Mining' configuration window. At the top, there are tabs: 'Role Viewer', 'Role Search', 'Entitlement Analysis', 'Role Mining' (selected), and 'Role Mining'. Below the tabs is a 'View Mining Templates' button. The main area is divided into two sections. The top section, 'Ordered Identity Mining Attributes', has a red box around a 'Status' icon. The bottom section, 'Role Settings', contains several fields: 'Type of Business Roles to Generate' (set to 'Business'), 'Owner' (set to 'The Admin'), 'Minimum Number of Users per Role' (empty), 'Naming Algorithm' (set to 'Filter-Based'), and 'Prefix to Apply to Generated Role Names' (set to 'HR-'). A red box highlights the 'Save and Execute' button at the bottom left.

The screenshot shows the 'Role Navigation' window. At the top, there are tabs: 'Role Viewer', 'Role Search', 'Entitlement Analysis', and 'Role Navigation' (selected). Below the tabs are buttons for 'Top Down', 'Bottom Up', 'Grid', and 'Refresh'. There is an 'Enter a Role Name' input field with a 'Reset' button. A red box highlights a list of roles: 'Contractor', 'HR-Contractor', 'Employee', and 'HR-Employee'. The word 'Result' is written in red next to the list.

IT Role Mining

Each group represents access held by at least one identity

Role Viewer Role Search Entitlement Analysis **Role Mining** Role Mining Results *Result*

View Mining Templates

Identities to Mine

Search By Attributes ☒ Search By Population ☐

Identity Attributes

Manager

Is Manager

Inactive

Employee ID

Location

Region

Status

Applications to Mine *

☒ LDAP ☒ PAM ☒ PRISM ☒ TRAKK

Save Save and Execute Cancel

Identifier	Only these Ent	With these Ent	ACCOUNTING	ADMINISTRAT	FINANCE	HR	IT	TEST01
Group1	2 (33.33%)	5 (83.33%)	✓					✓
Group2	1 (16.67%)	1 (16.67%)	✓		✓			✓
Group3	1 (16.67%)	1 (16.67%)	✓	✓				✓
Group4	1 (16.67%)	1 (16.67%)	✓			✓	✓	✓
Group5	1 (16.67%)	1 (16.67%)			✓	✓	✓	✓

- Create an IT Role Mining Task

- Define → Roles → Create New → IT Role Mining

- Input

- Applications (required)
- Identity attributes or population (optional)
- Excluded entitlements (optional)

- Result is set of groups

- Create roles from groups

- Must enable roles after creation

IT Role Entitlement Analysis

- Perform an Entitlement Analysis search
 - Define → Roles → Create New → Entitlement Analysis
- Input: Applications; identity attributes or population (optional)
- Result is population per entitlement
- Group and analyze (optional)
- Create roles from checked entitlements
 - Enabled upon creation

Each entitlement is individually represented

Role Viewer Role Search Entitlement Analysis

Please choose an application from the list below to mine for entitlement search additional search fields.

Application:*

☐ PAM

☐ TRAKK

*Indicates a required field.

☒ Search By Attributes ☐ Search By Population

Identity Attributes

Standard Attributes

Role Viewer Role Search Entitlement Analysis Role Mining Role Mining

Result

PAM - Entitlement Attributes

<input type="checkbox"/>	Name	Value	Percent of Population
<input type="checkbox"/>	Database Name	TEST01	6/6 (100%)
<input type="checkbox"/>	Permission Group	ACCOUNTING	5/6 (83%)
<input type="checkbox"/>	Permission Group	FINANCE	2/6 (33%)
<input type="checkbox"/>	Permission Group	HR	2/6 (33%)
<input type="checkbox"/>	Permission Group	IT	2/6 (33%)
<input type="checkbox"/>	Permission Group	ADMINISTRATORS	1/6 (17%)

Displaying 1 - 6 of 6





TRAKK - Entitlement Attributes

<input type="checkbox"/>	Name	Value	Percent of Population
<input type="checkbox"/>	capability	input	6/6 (100%)
<input type="checkbox"/>	capability	approve	3/6 (50%)
<input type="checkbox"/>	capability	reject	3/6 (50%)
<input type="checkbox"/>	capability	super	3/6 (50%)

Displaying 1 - 4 of 4

Group and Analyze Search Again Create Role

Out of the Box Role Types

Type	Business 	IT 	Entitlement 	Organizational 
Allow Inheritance of other roles	Yes	Yes	Yes	Yes
Allow other roles inheriting this role	Yes	Yes	No	Yes
Auto Detection with Profiles	No	Yes	No	No
Entitlement Profiles	No	Yes	Yes	No
Automatic Assignment with Rule	Yes	No	No	No
Assignment Rule	Yes	No	No	No
Manual Assignment	Yes	No	Yes	No
Permitted Roles List	Yes	No	No	No
Allow being on permitted roles list	No	Yes	Yes	No
Required Roles list	Yes	No	No	No
Allow being on a Required Roles list	No	Yes	Yes	No
Allow granting of IIQ rights	No	No	No	No

Role Types

Name ▲

Business

Entitlement

IT

Organizational

New Type

Extensible Role Model

- System Setup → Role Configuration
 - Out of the Box
 - Business Roles (for assignment)
 - IT Roles (for detection/provisioning)
 - Organizational Roles (for containment)
 - Entitlement (legacy – use only for backwards compatibility)
 - Additional Roles?
 - Create New Types
 - New Icons
 - Example:
 - Roles for IIQ Capabilities
 - Roles for Compliance Purposes

Role Types	
Name ▲	
Business	
Entitlement	
IT	
Organizational	
New Type	

Sunrise/Sunset of Roles

- Global Configuration

- System Setup → IdentityIQ Configuration → Roles tab
 - Assignment configuration applies to both roles and entitlements
 - Default is enabled

Role Sunrise/Sunset Dates

Enable Sunrise/Sunset Dates on Role Assignment ☒

Enable Sunrise/Sunset Dates on Role Activation ☒

- Role Activation – Sunrise/Sunset Dates for Roles

- Define → Roles → Edit → Scheduled Events → Add Event
- Used for roles that have limited time usage or delayed activation

Add New Event

Date: 01/22/14

Action:

Activate

Deactivate

Sunrise/Sunset of Roles



■ Role Assignment






- Dashboard → Request Access → Select role/entitlement → Checkout
- Used to add or deactivate roles or entitlements for an individual user at a later date



Select Identity(s) > Select Access > Review & Submit

Summary of Requests for [Kevin.Phillips](#)

Please verify the changes you have requested below. To modify the activation or deactivation date of an individual item, click "Edit Details."

Request Options
Activation: 01/22/14  Deactivation: 

Action	Name	Type	Comments	Risk Score	Owner
  Edit Details	AcctsPayable  Activation: 1/22/14 • Attribute: groupmbr • Application: Financials	Entitlement		 1	FinanceEntitlementOwners

Page 1 of 1  Show 10  items

Displaying 1 - 1 of 1

Submit Cancel Make Additional Changes

Sunrise/Sunset of Roles

- Role Assignment – for Individual Identities
 - Define → Identities → Entitlements Tab → Add Role
 - Activate date
 - Deactivate date
 - Establish Date to
 - Add Role to User
 - Deactivate Role for User

The screenshot displays the 'View Identity Aaron.Nichols' interface. The 'Entitlements' tab is active, showing a table of assigned roles. The 'Add Role' button is highlighted with a red box. An 'Add New Role(s)' dialog is open, showing a list of roles with 'PRISM User' selected. The 'Activate' and 'Deactivate' date fields are also highlighted with a red box.

Name
<input type="checkbox"/> PRISM Manager
<input type="checkbox"/> Region.Asia-Pacific

Activate: 06/22/14

Deactivate:

Note: To enable role assignment through Define→Identity→Entitlements, set *enableAdminRoleChanges* in System Configuration to “true”: `<entry key="enableAdminRoleChanges" value="true"/>`

Role Project Pointers

Roles or Logical Applications?

Roles

- Good when thinking about access holistically
- Support governance
- Support provisioning
- Better scalability

Logicals

- Good when thinking about access in terms of an account
- Support governance
- Provisioning (including remediations) handled
 - Manually through work items
 - Automated through custom rules

Role Project Pointers



- **General**
 - Look for groupings of user types
 - Prevent role proliferation
 - Enforce least privilege
 - Define roles that are reusable
- **High turnover or high use roles are a good way to start**
 - Bank tellers, seasonal employees, employee vs. contractor
 - Don't attempt to "boil the ocean"
- **Know your scope**
 - Simplify certifications? Access requests?
 - Involve SME's who know the business

Role Project Pointers

- Build in Roles when the IdM Program is Mature
 - Because data is cleaner
- Every business approaches roles differently
- Roles are a program; not a project
 - Too big, too fast is how role projects fail
 - Roles have a lifecycle and should evolve
 - Start small and familiar
 - Can give key managers capability to create roles as needed; this still requires approvals
- Before inventing your own, consider the default IdentityIQ role model



Questions?

Exercise Preview

Section 3, Exercises 1, 2, 3

- Exercise 1: Defining a Role Model
- Exercise 2: Assign and Detect Business Roles
- Exercise 3: Using Roles to Provision Access to the PRISM Application