Role-Based Access Control (RBAC)

Tom Deaderick, PMP, CISSP, ITIL Expert, Scrum Master

Role-Based Access Control (RBAC)

- Current-State: Individual Access Control
  - Employees & Contractors (“Surrogate FTEs”) receive minimal (“birthright”) security provisions with a new account.
  - Managers request additional security provisions for staff accounts using paper forms.
  - Managers typically rely on “model users” as virtual provision collections.
  - Transferred Employees/Contractors typically retain provisions of prior roles (security risk).
- Future-State: RBAC
  - Employees & Contractors automatically receive provisions associated with their role upon assignment to a position.
  - Individually-appropriate provisions may be requested via form and excluded from RBAC inheritance at manager’s discretion.
  - Provisions associated with a role are automatically removed when transferred (except by manager’s request for a transition period).

Benefits

- Day-one provisioning (AD) of new hires and transfers.
- Individually-appropriate provisions may be excluded from roles at manager's discretion.
- Structured & streamlined manager oversight/recertification.
- Reduced processing by Identity & Access Management (IAM).
- Transfers strip prior role provisions, except by manager's request during a short transition.

Challenge

- 1,900 Unique positions
- 7,300 Active Users
- 5,360 Unique Security Groups

…with

- 391,000 ACE (Access Control Entry) individual combinations
- Converting to 81,500 role/individual ACEs

…without

- Users even noticing.

Moving parts

Initial AD structure

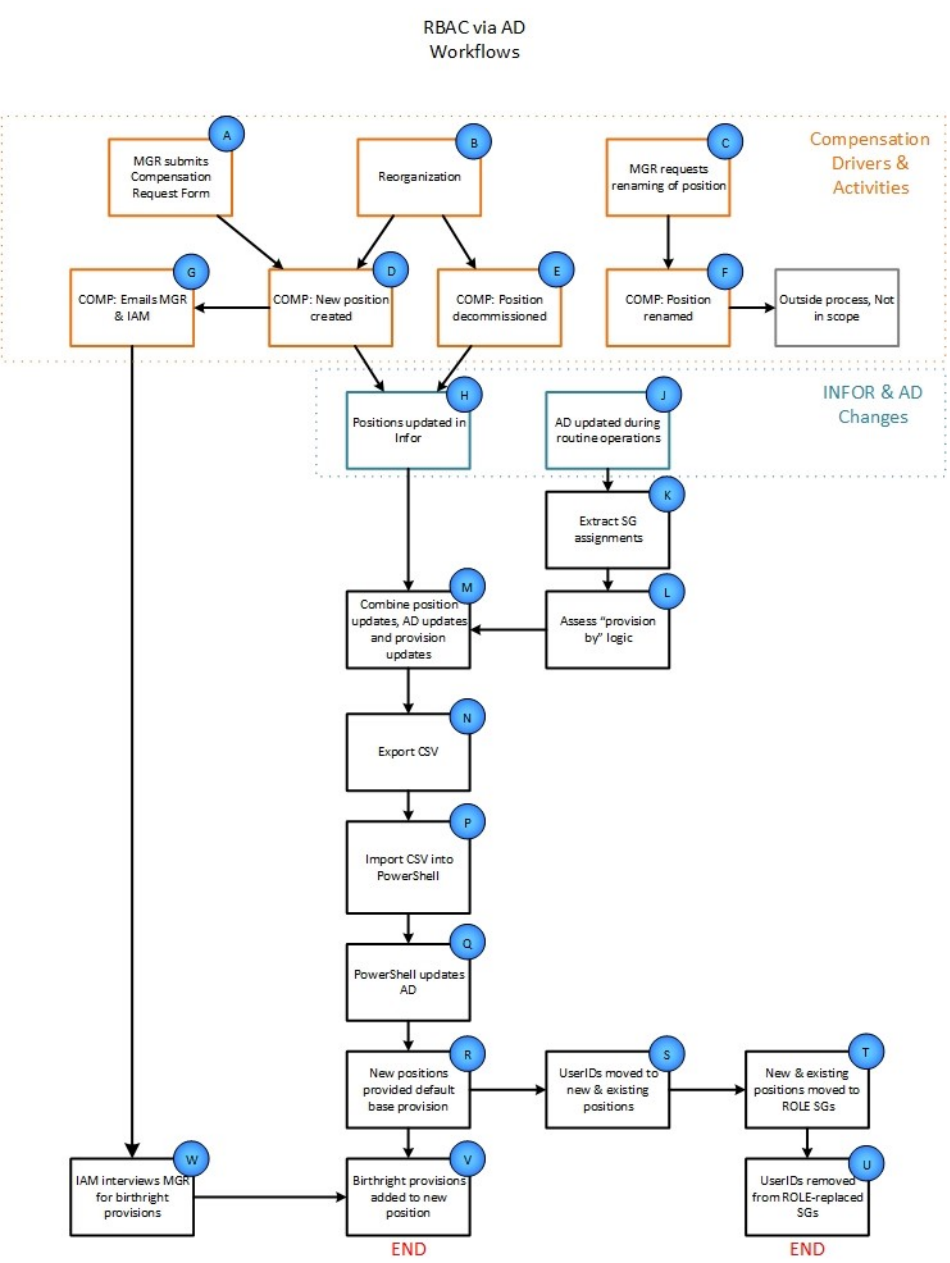
Company.ORG
... | Main_Groups
... |... | SecurityGroups
... | ... | ... | Location1_SecurityGroups
... | ... | ... | ... | DefaultBirthrightGroup1
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | ... | 12345111113
... | ... | ... | ... | SecurityGroup21
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | ... | 12345111113
... | ... | ... | Location2_SecurityGroups
... | ... | ... | ... | DefaultBirthrightGroup2
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | ... | 12345111113
... | ... | ... | ... | SecurityGroup1
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | SecurityGroup2
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | SecurityGroup3
... | ... | ... | ... | ... | User04
... | ... | ... | ... | SecurityGroup4
... | ... | ... | ... | ... | User02
... | ... | ... | ... | ... | User03
... | ... | ... | RBAC
... | ... | ... | ... | 12345111112
... | ... | ... | ... | ... | User01
... | ... | ... | ... | ... | User02
... | ... | ... | ... | 12345111113
... | ... | ... | ... | ... | User03
... | ... | ... | ... | ... | User04
... | Main_Users
... | ... | Location
... | ... | ... | User01
... | ... | ... | User02
... | ... | ... | User03
... | ... | ... | User04

Updated AD structure

Company.ORG
... | Main_Groups
... |... | SecurityGroups
... | ... | ... | Location1_SecurityGroups
... | ... | ... | ... | DefaultBirthrightGroup1
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | ... | 12345111113
... | ... | ... | ... | ... | 12345111114 (Added new position)
... | ... | ... | ... | SecurityGroup21
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | ... | 12345111113
... | ... | ... | Location2_SecurityGroups
... | ... | ... | ... | DefaultBirthrightGroup2
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | ... | 12345111113
... | ... | ... | ... | ... | 12345111114 (Added new position)
... | ... | ... | ... | SecurityGroup1
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | SecurityGroup2
... | ... | ... | ... | ... | 12345111112
... | ... | ... | ... | SecurityGroup3
... | ... | ... | ... | ... | User01
... | ... | ... | ... | ... | User04
... | ... | ... | ... | SecurityGroup4
... | ... | ... | ... | ... | ... | 12345111112 (Replaced individual with role priv.)
... | ... | ... | ... | ... | ... | 12345111114 (Replaced individual with role priv.)
... | ... | ... | RBAC
... | ... | ... | ... | 12345111112
... | ... | ... | ... | ... | ... | User01
... | ... | ... | ... | ... | ... | User03 (Moved to new position)
... | ... | ... | ... | 12345111113
... | ... | ... | ... | ... | User04
... | ... | ... | ... | ... | 12345111114 (Created new position)
... | ... | ... | ... | ... | ... | User02 (Moved to new position)
... | Main_Users
... | ... | Location
... | ... | ... | User01
... | ... | ... | User02
... | ... | ... | User03
... | ... | ... | User04

1. User04's initial individual membership in SecurityGroup4 is converted into a role and assigned to position 12345111112.
2. User02 was transferred from initial position (12345111112) to newly-created position (12345111114).

Process supports conversion of individual provisions to role provisions, and automatically provisions transferred employees & contractors nightly.



Process Overview

A, B & C

Compensation Department creates new positions for pay-grade reclassifications and organizational redesigns. Minor title changes do not require RBAC adjustment.

H & J

Infor and AD are the primary points-of-truth for position and security provisions respectively.

Positions are changed in Infor by processes A, B & C.

Security provisions are changed during daily provisioning/deprovisioning.

K to End

An SSIS package runs nightly, processing the departments and users identified for the proof-of-concept and metered production onboarding into RBAC provisioning.

Technical Components: RBAC_SSIS

- Purge prior day's data
- PS: Extract UserID, Group Membership from AD
- Load RBAC-AD Table
- Clean Data
- SQL Views: Assign SGs as ROLE or INDIVIDUAL provisions & manage exclusions
- Export CSV file of security assignments
- PS: Update AD positions and Security Groups
- SQL Views: Process Transition Exclusions
- PS: Update transitioning UserIDs to retain prior role's provisions in AD

* "PS" indicates "PowerShell.

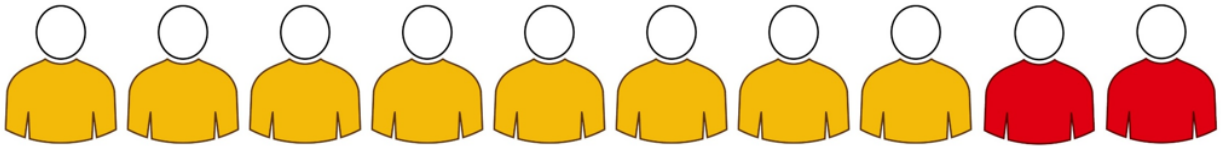
SSIS package runs after midnight (daily).

Primary decision logic, including:

- Departments included in project
- Positions included in project
- Security Groups excluded from Role assignments

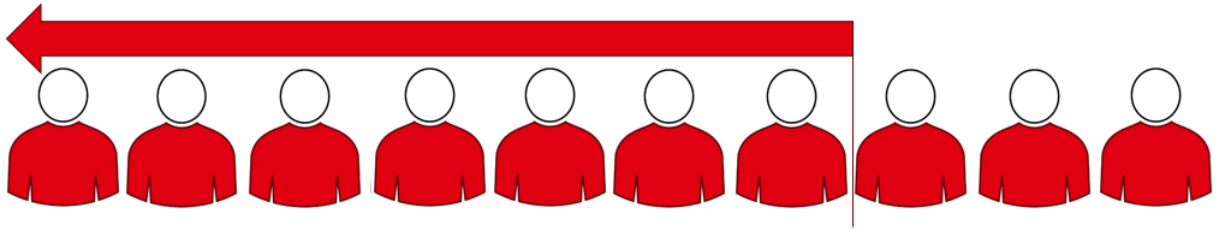
… are contained in SQL views (blue)

How are Roles Provisioned?



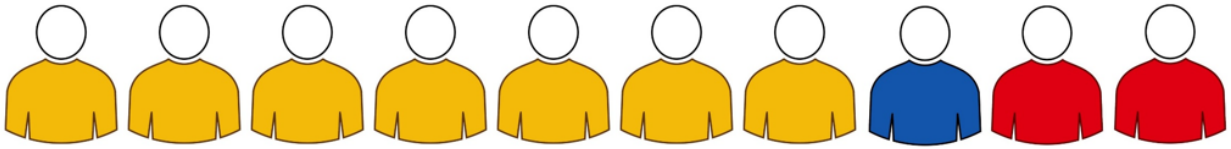
Warp drive engineers Two of ten are members of “Transporter fiddling” security group
Result: “Transporter fiddling” not added to warp drive engineer role & permissions are maintained

There are too few employees in the warp drive engineer” position with membership in “Transporter fiddling” security group to warrant adding this membership to the other eight employees.



Warp drive engineers Three of ten are members of “Impulse override” security group
Result: “Impulse override” added to warp drive engineer role & permissions extend to all in role.

Three of the "warp drive engineers" are members of the "Impulse override" security group, so this permission is added to their role, extending permission to the remaining seven employees in this position.



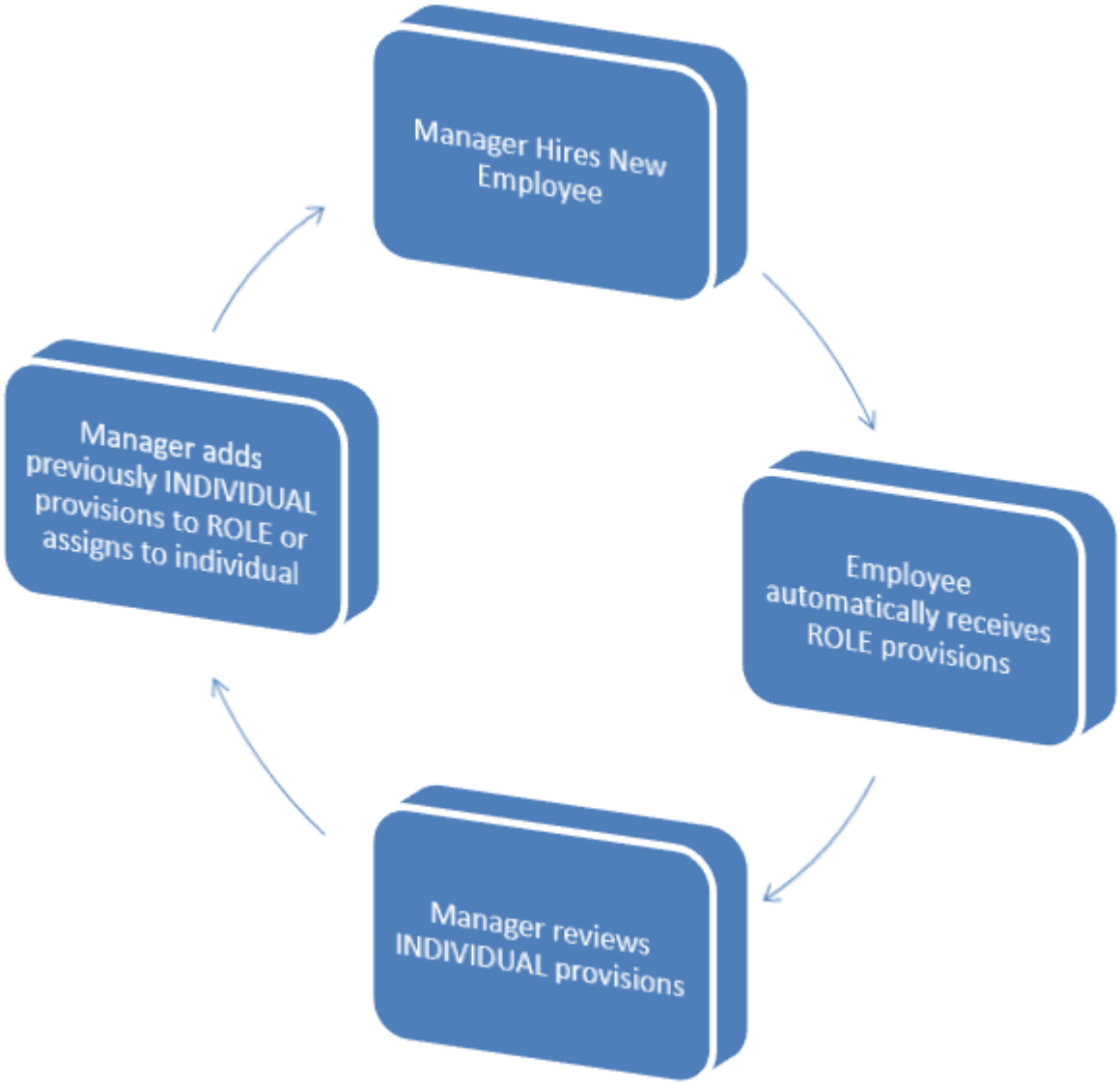
Warp drive engineers Transfer from Medical department
Manager may:

A) Individually provision new arrival with “Transporter fiddling”, or
B) Add “Transporter fiddling” to warp drive engineers role and add transferred employee into role.

As managers hire each new employee, they may continue provisioning the remaining user-level permissions by individual, or by assigning the permissions to the role.

This establishes a virtuous cycle.

Virtuous Cycle



As new staff are onboarded, managers that have perfectly-fitted role provisions require less additional efforts, or even none at all.

Managers of teams that rely on individual privileges must request provisions with each new hire.

During the manual provisioning process, the Identity & Access Management (IAM) team encourages managers to review individual and role provisions to maximize role-provisioning.

This creates a virtuous cycle, reinforcing the manager's perception of RBAC as a beneficial time-saving option and continually drawing newly-created individual privileges into roles where appropriate.

Conversion Plan

- Testing on test domain/test AD
- Testing in production with test users/test SGs
- Testing in production with live user/SGs
- Testing in production with small department
- Activating nightly execution for prior test subjects
- Expanding department by department



Role-Based Access Control (RBAC)

Tom Deaderick, PMP, CISSP, ITIL Expert, Scrum Master