Building RBAC in Heterogeneous environment – A Methodical Approach

Rony Hay

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.0

July 25, 2004

Table of Contents

1. Introduction

1.1. Abstract

Role Based Access Control (RBAC) is a way to provide access privileges to computer resources. It is known to be the best way to provide the least access privileges to users so they will be able to accomplish their day-to-day job functions. Over the years many vendors have used various techniques to implement RBAC either on their products or Operating Systems. Companies with heterogeneous environments needed to learn and adopt several disciplines of RBAC implementation. The challenge is therefore to develop a common RBAC method which is based on a recognized RBAC model that can be simultaneously platform independent. Before reading this document, be familiar with the definitions found in the Glossary on page 39 which are frequently used throughout this document.

This document explores and discusses several methods that were developed to build and implement Business Roles. Only one method proved to be successful. The selected method unifies the different types of RBAC models implemented in various Platforms into one database. It also provides a seamless process through a consistent technique that converts Function Roles into Business Roles across multiple platforms. This document also includes a detailed description of the Access Control Processes that are required to maintain the newly developed Business Roles. The implementation of Business Roles is the main subject of this document. Also included is a short description of the all the other components required for the Business Role implementation. Each component is a stand-alone, independent of the other, but at the same time, constitutes an essential part in the RBAC building blocks

1.2. Background

The Environment

The current environment is in full operation 24/7 year-round. This makes the process of building and implementing new roles a very complicated and challenging task. Providing new access privileges to a User via a new role may cause the User to be idle for an unknown period of time. To prevent this from occurring, there is a need to take the following precaution:

1. The new Business Role should not interfere with the current User's access.
2. Access Administration will be able to revert the User's access instantly in case the new access privileges, provided via the Business Roles, are not sufficient and cause the User to be idle.

Access Administration

In a heterogeneous environment, the Access Administration's responsibilities are based on the type of platform. This means that each Platform Administrator works and manages User's Access privileges detached from other Access Privileges for the same user in other platforms. The distributed responsibilities of the Access Administration seriously undermined the current security model. The immediate results of this on RBAC implementation are:

1. A user may have different identities on each platform. This makes the User Termination Process very complicated and in many cases difficult or impractical to achieve.

2. The Platform-Groups that were created on a particular platform by Access Administration represent Function Roles and not Business Roles which are defined as platform independent.

3. Difficulty to produce a consolidated report that shows "who has access to what" based on business needs across multiple platforms.
   This kind of report is needed to justify an access base on the User Business Role. (*for example: why a User that has a Business Role of "Pharmacist" needs access to "Monthly Cash flow report").*

The lack of a unified Access Administration group that controls and monitors access to the company's assets based on business needs produced a number of issues:

1. Access Administration has difficulty in assessing the business exposure risks when adding a new resource to an existing group.

2. Access Administration does not have either the business knowledge or the means to compare the Pattern of Access of the existing Group to identify which Group is the best fit for a new resource. Therefore, an Administrator would prefer to create a new Platform-Group in which, as a result, the number of groups on a given platform tends to grow over time to an unmanageable number.

3. Providing access to users becomes a complicated task that forces Access Administration to use the "model after" technique *(provides access to a User based on his/her manager's access).*

2. Objective

The purpose of this effort is to build Business Roles (as opposed to Function Roles that are platform dependent). Business Roles should be defined based on business requirements. This means working with Business Users to define roles and role privileges based on the Users' day-to-day job function. A Business Role should be useful for more than one Application or System that could be used across multiple platforms. A driving force behind this study is The HIPAA Privacy and Security requirements. The main objectives are:

1. Build and maintain Business Roles based on the users' job functions

2. Comply with the following HIPAA privacy regulations to protect health information:

   - Use and disclosure of Protected Health Information
     Any use or disclosure of Protected Health Information (PHI) should be based on "the minimum necessary to accomplish the intended purpose."

   - Segregation of duties
     It is a security control that divides Business activities of one Business Transaction between several individuals, so one individual will not be able to complete one Business Transaction. (e.g. the pharmacist that dispense controlled drugs will not be the same pharmacist that approve the dispensing)

3. Provide access to users via the auto-provisioning tool.

The benefits of implementing the Business Roles concept are: reducing the current number of relationships (authorizations and permissions), reducing management costs, improving the accuracy of Access Control information (metadata), making scaling easier, increasing security and confidentiality by allowing the enforcement of Separation of Duties.

3. Audience

The audiences for this study are: Business Users, RBAC developers, Security Custodians, Security Architects, Security Developers and Managers who are familiar with HIPAA security and privacy requirements.

4. Scope

The following describes the current environment where User information and access privileges are stored and maintained. This information is the basis for the new Business Roles Model.

4.1. User

The universe of users includes:
Employees, Consultants and the Clients and Vendors workforce.

4.2. Platforms

The current environment includes the following platforms:
IBM mainframe, UNIX (several flavor), PC.

4.3. Operating System

MVS, UNIX, Linux, MS window

4.4. Database

RACF *(IBM Mainframe user dB)*, Oracle, Sybase, Informix, Teradata
SQL Server

5. Current Status

Currently the company maintains separate Function Roles on each platform based on Platform-Groups. Eighty percent of the applications are considered to be a legacy system that runs on IBM mainframe. This means that the Permissions (ACL) are solely maintained on the platform. The names of Groups and Resources that are maintained in RACF (Users' and Resources' dB) have a maximum of eight characters because of the operating systems' limitation.

5.1. Problems

1. The names of the Groups are too short to help identify their function.

2. The names of the Resources are too short and not meaningful therefore making the Resource identification process an impossible task.

3. Access Administration provides access privileges to users based on the "Model After" technique. This means that a user obtains access privileges based on his/her manager profile. By following this technique, the user inherits all access privileges from the manager. For an administrator, it is a fast and easy technique for providing access to an individual but it is considered to be a security disaster. Over time, users may acquire access privileges to almost every resource. This is true especially in a dynamic environment where users are transferred often to a new position, obtaining new access privileges without relinquishing any of the access privileges of the old job function. A sample test that was taken demonstrates that 80%-95% of all access privileges that a user has are not needed to fulfill his/her day-to-day job function.

4. Users cannot be identified uniquely across multiple platforms.

5. Users who have more than one User-id make auto-provisioning difficult to achieve.

6. Access Administration failed to remove all access privileges from former employees. (the reason is shown in #4)

5.2. Metrics

The following statistics represent collective information extracted from all platforms. Implementing Business Roles may significantly reduce the number of Groups, Authorizations and Permissions links if RBAC processes are implemented properly.

1	Number of users	10k
2	Number of User-ids managed on the platforms	40k
3	Number of Platform-groups	7k
4	Number of Resources	70k
5	Number of authorization (links between users-to-groups)	325k
6	Number of permissions (links between resources-to-groups)	525k

Careful analysis of the data shown above raises a number of fundamental problems that undermine the current security model:

- The Number of users (1) versus the number of User-ids on the platforms (2)

  This fact points out that there are many User-ids that belong to former employees with active access privileges.

- The Number of Platform-groups (3)

  7k Platform-Groups is more than anyone can manage in order to effectively maintain an adequate Access Control.

- Number of permissions (6)

  Careful analysis of the Permission shows that there are almost 325K unique patterns of access (PoA). This means that there are about 325K unique "roles".

  Further analysis shows that more than 95% of the Permissions can be merged into a small number of Platform-Groups.

The ultimate conclusion is that the best and most sophisticated Access Control Model cannot provide sufficient long term security control without additional means that exercise the RBAC rules.

6. RBAC building blocks

In order to support company-wide Business Roles Model that enable the building and the maintenance of a strong Access Control on the company's Electronic information Assets, there are several security related components which are the necessary building blocks for any RBAC implementation. The following describes in short the required components for building and maintaining Business Roles:

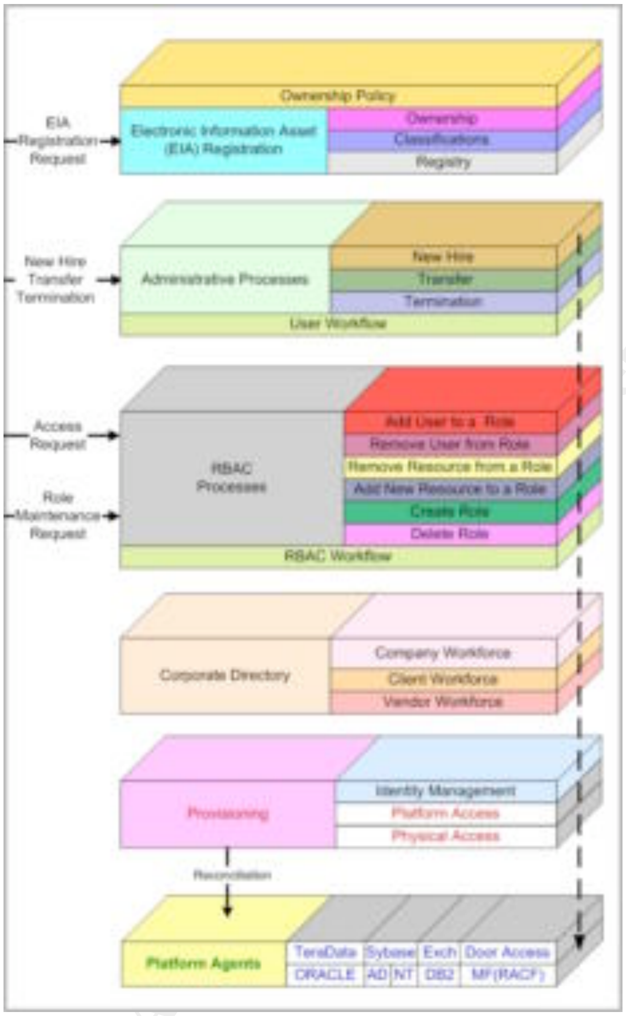
Module Name	Description
People Information	The People Information Module is responsible for the quality, the completeness and accuracy of the information about people who may need access to the Company's Network. It is also the component that is responsible to identify the authoritative source for each type of information related to People. This Module is an essential input for the creation of the Corporate Directory.
Identity Management and Reconciliation	Identity Management is the module that manages all the aspects of a user's identity on all platforms. It also points to the underlying business problem of managing multiple user identity information across systems and platforms. The main responsibilities of this module are: a) To resolve and consolidate information about users into one authoritative reference of user information. b) To prevent unauthorized individuals from gaining access to the company's resources. (e.g. Platform Administrator bypasses the RBAC processes, opens an account, and provides access to an EIA for an unauthorized User using the Operating System tool).
Corporate Directory	The Corporate Directory module is the authoritative reference Repository for People Information. The Corporate Directory is a database where user information is stored and managed. It is an essential component in the Identity Management & Reconciliation Process and a vital part for the automation of RBAC *(The technology used to build the Corporate Directory is LDAP- Light Directory Access Protocol).*

Directory Integrator	The Directory Integrator (IDI) is a tool that enables performance of unattended synchronization of People Information between the authoritative sources and the Corporate Directory. Using this tool will enable the consolidation of all People information into one database using the same method and the same set of rules. It is an essential tool for the implementation of the Corporate Directory and a fundamental infrastructure for the implementation of RBAC system.
Electronic Information Asset (EIA) Ownership	The EIA ownership module is a concept that provides a roadmap for ownership which facilitates in identifying and assigning owners for each object that was categorized as Electronic Information Asset (EIA). The EIA ownership module also lists the tasks and responsibilities relevant to the EIA owners and Security Custodians. The EIA ownership module is a vital component for supporting the automation of RBAC.
EIA ownership & custody Policy	The EIA policy is the tool which enforces the EIA ownership requirements making sure that Owners and Security Custodians are assigned and fulfill their respective tasks. The EIA policy is a required component for disseminating the EIA ownership concept in the corporate culture.
EIA Registry	The registry module is the component responsible for tracking inventory information about EIAs, utilizing built-in processes to keep the inventory information current including the EIA owner, Security custodians and their responsibilities.
Administrative Processes/Workflow	The current administrative processes are partially automated and ignore the integration of human touch points with system-based processes. The main processes are: New Hire, Transfer and Termination. Streamlining these processes is necessary to deliver business value to the enterprise by allowing a business process or series of processes to function in an uninterrupted fashion from the time they are triggered until they fulfill their purpose. Aligning these processes is a very important for the implementation of Business Roles Model and is vital to its success.

RBAC Workflow	The RBAC workflow Module is the process by which a Access Request to an EIA is approved, rejected, or sent for completion. A workflow process is when (e.g.) the Immediate Manager places a request for a User to have additional access rights to an EIA. The request must be approved by the Role owner before the Access rights are granted.
Provisioning Tool	The provisioning Module translates the RBAC instructions into a specific platform language. The Provisioning Agent is the program that implements the RBAC instructions on the target platform. It acts as a Platform Administrator and works on its behalf to grant or revoke access to a resource on the target platform.

6.1. Building Blocks Model Diagram

The diagram below illustrates the complexity of implementing Business Roles. The RBAC model deals with data and its links (Authorizations and Permissions). The RBAC processes are the means to enforce the RBAC rules which make sure that the RBAC model's integrity will not be violated. The RBAC processes are the building blocks required for the success of RBAC's implementation.



6.2. Triggers

As illustrated in the above diagram, the RBAC processes are initiated by triggers. A trigger is a Request Form filled by a User or a transaction generated by the program. The triggers are translated into specific instructions, then processed by the primary layer and are finally passed downstream to the next intermediate layer for additional processing. The only exception to the above statement is the EIA Registration Request. The Request is processed by the EIA Registration layer but does not pass the results to the next layer.

6.2.1. Trigger Description

The RBAC processes are triggered by initiation of a Request. Below is a short description of all the triggers that are involved in the RBAC implementation. The Access control Requests will be described in more detail in the next paragraphs.

EIA Registration Request - The EIA Registration is the foundation for RBAC and it is a prerequisite for RBAC's implementation. This process collects many details. Among them is security related information that is relevant for RBAC such as:

- EIA Name
- EIA Description
- EIA owner
- EIA Classification
- Security Custodians for:
  - Access Control
  - Backup and Restore
  - Disaster Recovery/Business Continuity

New Hire, Transfer, Termination Transactions - These transactions are RBAC related transactions that require an action:

New Hire - provides basic Access privileges (via Role) for a new hire based on the employee's job function (determined by Human Resources)

Transfer - Provides new Access privileges (via Role) and Revoke old access

Termination - Revokes Access privileges from all platforms.

Role Maintenance Request - See detail in Role Maintenance Process Page 29

Access Request - See detail in Role Access Process Page 35

Reconciliation - This Transaction is generated by the Provisioning tool based on a pre-defined schedule. It is a process that identifies unauthorized Users' Accounts created on any given platform. Unauthorized accounts are accounts that were created without getting the appropriate approvals (via RBAC workflows).

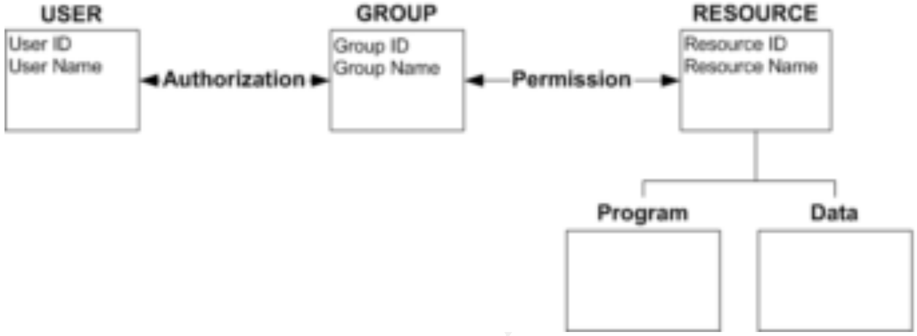
7. RBAC Logical Architecture

The basic model that will be used to discuss RBAC is depicted in the following diagram. Resources are either Programs or Data. Authorization is defined as the relationship between Users to Groups. Permission is defined as the relationship between groups and resources.

7.1. Group Model

This model is a Group Model being implemented on several platforms. The Authorization and the Permission reflect the access privileges on only one platform.

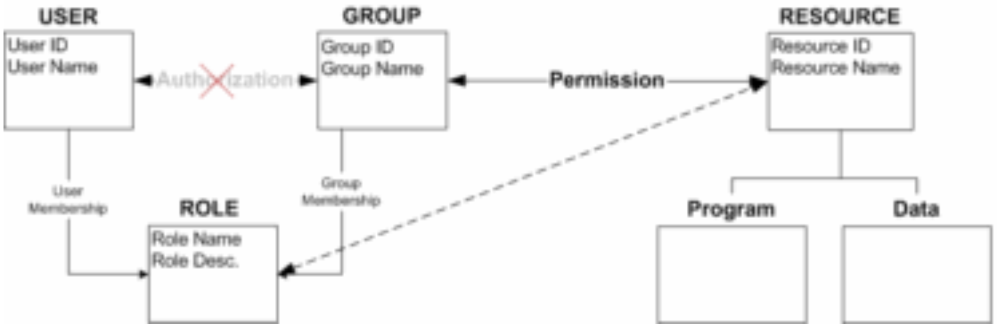
- A Group may have Permissions to one or more Resources
- A User may have Authorization to one or more Groups



7.2. Business Role Model

The Business Role is the model that will utilize the Platform-Group Model that is used by several platforms. It adds an additional layer that represents Business Roles.

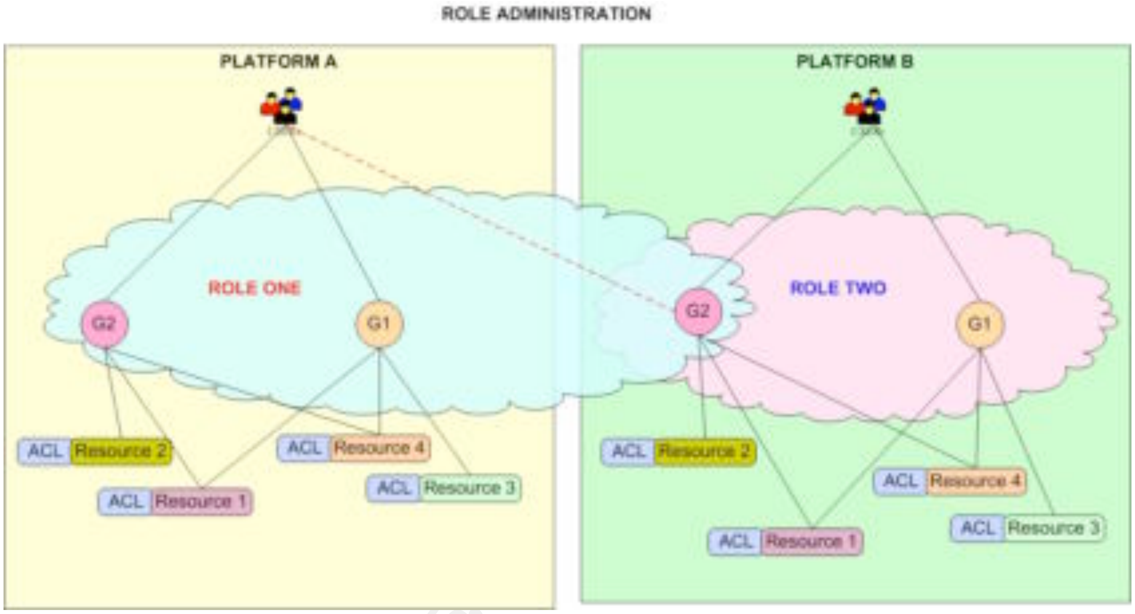
- A Role is a collection of Groups
- A User may be assigned to one or more Roles



NOTE: The relationship indicated by the dotted line represents a logical relationship. The physical implementation will still use the standard RBAC model which is a Platform-Group to Resources relationship.

7.3. Business Role Model Diagram

The diagram below illustrates how a Business Role is used across multiple platforms. In this example, ROLE ONE includes Group1, Group2 on Platform A and Group2 on platform B. Users on Platform A are members in ROLE ONE. ROLE ONE is defined as a cross platform Business Role.



The solid lines depict the physical links between Users to Groups on the platform. When a Business Role is applied, an addition links between Users to Groups on the platform that needs to be applied (indicated by the dotted lines).

7.4. Preparing the Groundwork

Applying Business Roles in a production environment is a complex task. It involves adding and removing access privileges while users are fully active. Therefore, the task of migrating or converting Function Roles into Business Roles should be planned efficiently and effectively so it will not have a negative impact on the day-to-day work (Zero downtime).

7.4.1. Role Identification Process

<u>Identifying Business Roles guidelines</u>

When identifying Roles, there are several rules that need to be followed. The following are the guidelines that help the Business User define and identify the Business Roles for their area of responsibilities:

1. Trade-off between the number of Roles and the cost of administering them

   There is a trade off between the number of Roles and the administrative cost. The more Roles there are, the more costly it is to administer them. There is also a trade-off between the number of Roles and the actual level of security.

   a) *The more Roles there are, the harder it is to ensure that the memberships to a Role remain correct and it is harder to ensure that the security control <u>remains</u> as intended.*

   b) *The fewer Roles there are the broader is the access granted to each member of the Role, but it is more likely that the <u>desired</u> security level will be achieved.*

2. Number of Business Roles should be between 300 to 400 Roles which is an optimum number for a company of this size.
3. Be acquainted with the organization’s structure.
4. Cluster Organization Groups into Business Groups.
5. Identify and associate potential Users to Business Groups.
6. Identify and create Roles’-names for each identified Business Group *(The name of the Role should be a self-explanatory and clear name).*
7. Flag all Roles that potentially may have access to PHI Resources
8. Identify and associate potential User to a Role.

Other privacy criteria to consider when defining Business Roles are:

9. Disclosure of PHI data to a User should be based on the minimum amount required to perform a function.
10. Segregation of Duties & Level of authority

7.4.2. Building Access Privileges Repository

RBAC Repository

In order to have a company-wide view of the current access for each User across all platforms, there is a need to collect information about Users, Resources and Access Privileges from all platforms. This information needs to be stored uniformly in a common repository. This storage will be the sole dB where user's Authorization and Permissions will be reviewed and analyzed. Building this Repository requires an in-depth understanding of the current Authorizations and Permissions method used in various platforms so that a common Logical Data Model (LDM) can be developed to consistently accommodate the collected information extracted from the targeted platforms.

7.5. Building Business Roles

The following work streams represent the work required to build Business Roles. The work is divided into a number of steps that must be followed in the order presented and are organized in several phases as follows:

7.5.1. Phase I – Building and Populating the RBAC Repository

The purpose of this phase is mainly to validate the feasibility of the Business Role model as described. This is accomplished by populating the Repository with Users and Access information, making sure that the RBAC model applied to each targeted platform fits into the logical concept implemented in the RBAC Repository.

Phase I consists of the following steps:

- Building the RBAC repository based on LDM.
- Building the interface between the various platforms and RBAC Repository.
- Extracting Access data from the various platforms (based on a pre-define format).
- Populating the RBAC Repository with the current Users information, Users' Authorization and Permissions to Resources extracted from the target platforms.
- Producing various reports to validate whether the concept stands on solid ground.

NOTE: The RBAC repository needs to be refreshed frequently to reflect the changes made by the Platform Administrator on the various platforms.

7.5.2. Phase II – Validate Inventory and Enhance Metadata

This phase is dedicated to collecting the raw information from the various platforms and augmenting it with additional information (metadata). Importing the information from the various platforms into the RBAC repository is an important step forward but it is not enough. Why? Because the name of the Resource defined on the platform, is limited to a maximum of eight characters. For example a name such as *$$MCAPPL* does not provide any indication about the nature of the program, its behavior, activities or which system is using it. It would be a difficult task for a Business User to make a decision based on a vague and unclear name. A name like *Internal Message Processing* is clearer and more indicative of the type of program it is. Therefore, a Business User can easily recognize the name of the Resource and be more willing to participate in the Role Building and Role Assignment Process. As a result, the Business User will be able to make an educated decision. This information is most valuable and critical to the success of the project. It provides essential information about Resources as it paves the way for the next phases. In order to achieve the goal of this phase, a process needs to be developed which includes the following steps:

- Develop survey forms
- Interview Business Analysts
- Identify, collect, and apply meaningful, self explanatory names for Resources.
- Identify collect, and apply meaningful, self-explanatory names for Systems.
- Link identified Resources to the identified System (EIA).
- Classify identified Resources based on PHI exposure.
- Periodically Refresh RBAC Repository with new data extracted from the various platforms. *(This activity is a necessary step to make certain that the RBAC repository contains the most recent information).*

The completed Inventory and data enrichment provides a complete view of the current Users' access privileges to Resources of all the Users across all platforms. This will allow the preparation of a strategy and a detailed work plan for the Building Business Roles and a roadmap for its implementation. Guidelines and tools such as procedures, forms, and reports will be developed to be used in the phases to follow.

7.5.3. Phase III – The Principles of Building Roles

The basic principles of building roles are fairly straightforward. This encompasses the following key steps:

1. Assign Roles to Users (User Membership).
2. Assign Roles to Resources (Role Membership).
3. Export Business Roles, User Membership (Authorizations), Role Membership (Permissions) to the Provisioning tool.

This appears to be an easy task to achieve but results in a very complex process. The following describes three pilot-methods that were developed to identify the best way to implement Business Roles. This is a high-level key principle and does not intend to describe a detailed process.

Method One: Clean-Up Platform

This is the initial method considered for use. It is based on the assumption that the Administrators and Subject Matter Experts on each platform will be able to perform a platform's clean-up. The key principles of the Platform method are as follows:

1. Remove Resources' links to Groups that are not needed.
2. Delete entire Groups (if not used).
3. Merge Groups with identical Permissions.
4. Create new Groups and link the appropriate Resources based on Role requirements.
5. Split existing Groups (for Segregation of Duties).

This method proved to be unrealistic and never materialized. The main reasons were:

1. There are thousands of Platforms' Groups and it would be almost impossible to manage the categorization of so many groups.

2. Deleting, merging or splitting Platforms' Groups is problematic because of the massive impact on the operation of business.

3. Allocating business Subject Matter Experts for an undetermined or unpredicted amount of time was not possible.

Method Two: Role-Member Method

The Role-Member Method is a method that relies heavily on the knowledge of Users about their current access and their knowledge of the day-to-day job function *(these users are potential candidates to be members in the Role).*

The key principles of the Role-Member method are as follows:

1. Aggregate the current access of all users who are candidates to be members in the Role.
2. Work with the potential members in a Role to identify and justify each resource that is currently part of their access.
3. Remove any unjustified access to a Resource.

The Role-Member method proved to be unsuccessful and never materialized. The main reasons were:

1. The RBAC Repository contained thousands of Resources and additional informative descriptions about Users, Roles, Systems and Resources. Despite this fact, the potential members in the Roles were unable to categorically state whether the Resource(s) should or should not be included in the Role.

2. No person or a group within the company is neither able nor has the time or resources to help scan thousands of Resources and make a decision about the access privileges for each identified Role.

3. Potential members in the Role could not allocate adequate time to identify and justify every resource currently included in their access privileges.

4. The teams that were part of this process did not have sufficient means to deal with the volume of Resources that needed to be analyzed before a Role could be implemented.

Method Three: SPE Method (Recommended method)

The SPE method *(System-Platform-Environment)* is a less aggressive method than the previously described methods. The previous methods failed primarily because of the numerous number of Resources. This method taks a different approach which allows the building of Roles with broader access at first and then refines, tunes or reduces access to the appropriate level at a later time. The main idea of this method is to shift the focus from a Resource level to a System-Platform-Environment (SPE) level. This means Users would not need to identify specific resources but would need to identify the Systems *(Billing, Inventory, etc.),* the Platform *(Mainframe, Informix, Oracle or Sybase)* and the Environment *(Production, QA, etc.)* to which they need access.

The key principles of the SPE method are as follows:

1. Identify the selected Role

2. Identify one or more Users *(Pilot-User)* for whom their current pattern of access may serve as a model for the selected Role *(as opposed to all access of all potential users for the Role in the previous method).*

3. Identify the appropriate SPE for the selected Role.

4. Define a new platform Group for the selected Role *(the new Group name will be used on every target-Platform to link all the Resources of the Role).*

5. Extract all the resources that the Pilot User currently has access to which conforms to the selected SPE and links it to the new Group on the target platforms.

6. Revoke old access of the Pilot-User (Remove old Authorizations)

7. Grant the Pilot-User access to the new Group.

8. Verify that the Pilot-User is able to do his/her day-to-day job without any violation.

9. Once the Pilot-User is satisfied, add the next user to be a member in the Role *(perform Activities 6-9).* In case of access violation, identify and analyze the missing SPE that caused the violation to occur and add only those SPE resource(s) that are part of the User's current access to the new Group which was created for the Role.

10. Delete old access of all the Users who are part of the new Business Role.

This method demonstrated that the technique used is a workable technique based on the following reasons:

1. Users can easily relate to the SPEs technique and are able to provide the needed information *(which in method two they were unable to do).*

2. Based on the identified SPEs, the needed Resources can be automatically identified, using the information in RBAC Repository, to establish the required access privileges of a Role.

3. This method requires Users to spend a limited amount of time to justify SPEs for the Role. Therefore, Users were more willing to assist in this particular process than in the previous process (User cooperation is essential to the success of RBAC implementation).

4. This method allows a gradual enhancement of the Role's membership and provides enough time for a more in-depth analysis of each Role without impacting the operation of the business.

<u>Conclusion</u>

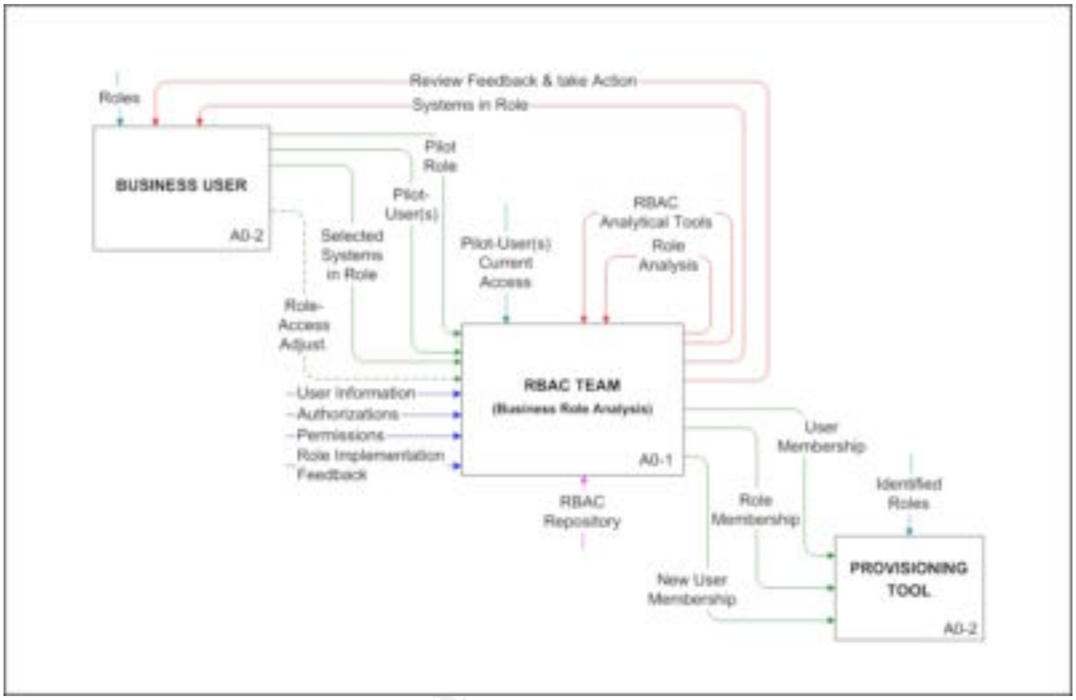
By following the SPE method, the statistics demonstrated the elimination of 85%-90% of the current access of Users who are members in the Role.

The only disadvantage of this method is that the technique used carried some of the Pilot-User's Resources (included in the selected SPE) as part of the Role, when it is known that at least some of the Resources that were carried-over may not have been necessary. Therefore, tuning, reducing or adjusting the Role's Pattern of Access (PoA) can be done at a later time, after completing the first phase of rolling-out the Business Role.

<u>Phase IV – Refine Roles</u>

As described above, the newly created Roles have a broader access than the individual User needs. Therefore, individuals who are members of a Role may inherit access that they did not have in the past *(Still the Users have significantly less access privileges than they had prior to joining the new Role).* This phase is dedicated to tuning, reducing or adjusting the Role's Pattern of Access (PoA).

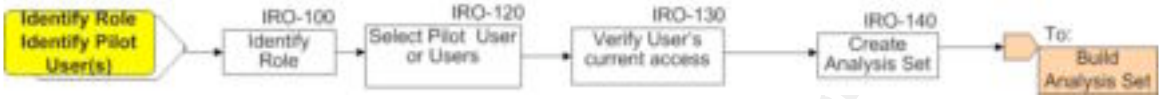
Building Roles Process – High Level View



7.6. Role Assembly

The following steps describe the process of rolling out Roles:

7.6.1. Identify Role & User



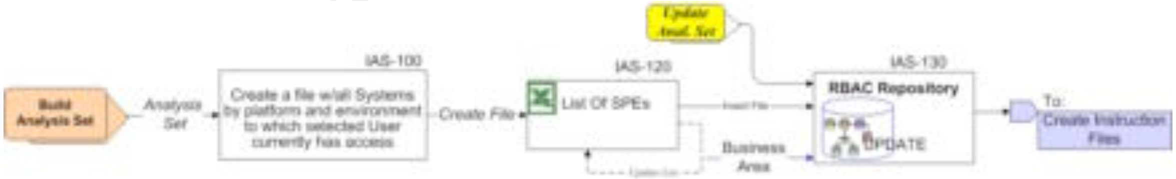
IRO-100 - The Business Area representative identifies a Business Role to be rolled-out.

IRO-120 - The Business Area representative *(BA)* selects a candidate User or Users whose current access best represents the functionality of the selected Role.

IRO-130 - The BA with the RBAC analyst helps to verify if the current access of the selected User(s) fit the need(s) of the selected Role.

IRO-140 - The RBAC analyst creates an Analysis Set Number associated with the selected Business Role and the selected user *(The analysis Set is an identifier that links the select Role with its groups and resources).*

7.6.2. Build Analysis Set.

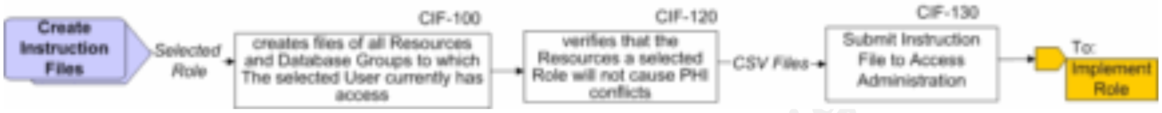


IAS-100 - The RBAC Analyst creates the list of Resources to which the User currently has access according to Systems, Environment and Platform that were determined to be included in the Role.

IAS-120 - The list of Resources is used to create the proposed access for the Role. The BA identifies job functions that need to be validated against the proposed access for the Business Role. The BA Rep Enters "Yes" or "No" on each SPE line in the Excel spreadsheet to indicate if the Role should have access to each System-Platform-Environment.

IAS-130 - Import the updated Excel spreadsheet to be stored in the RBAC repository. This information will serve as a base for extracting the required Resources based on the selected SPEs for the Role which appears on the Excel spreadsheet.

7.6.3. Create Instruction Files


Create Instruction Files
Selected Role
CIF-100
creates files of all Resources and Database Groups to which The selected User currently has access
CIF-120
verifies that the Resources a selected Role will not cause PHI conflicts
CSV Files
CIF-130
Submit Instruction File to Access Administration
To:
Implement Role

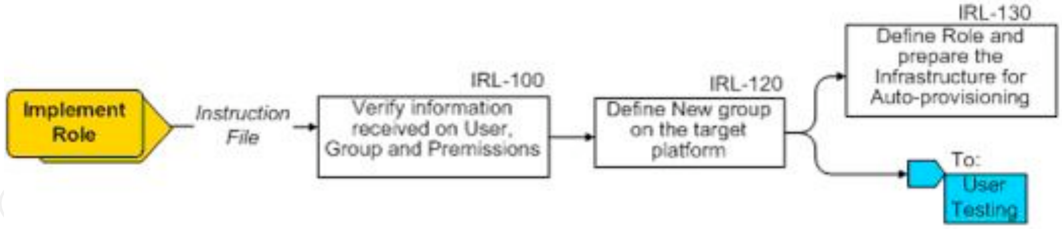
CIF-100 - Creates an Instruction File containing all Groups and Resources that the selected User currently has access to, based on all the System-Platform-Environments in which the BA Representative has indicated "Yes" for the selected Role.

CIF-120 - Verifies that the Resources selected in the Role will not cause an access conflict *(Non-PHI Role having access to a PHI Resource)*.

CIF-120 - The RBAC Analyst submits the created Instruction Files based on the BA selected SPEs to Access Administration in order to be implemented on the target platforms (Permissions) and update the provisioning tool with Roles and Authorization information:

- User(s) in the Role
- Groups in Role (Authorizations)
- Resources to the new Group (Permissions)

7.6.4. Implement Role


Implement Role
Instruction File
IRL-100
Verify information received on User, Group and Premissions
IRL-120
Define New group on the target platform
IRL-130
Define Role and prepare the Infrastructure for Auto-provisioning
To:
User Testing

IRL-100 – IRL-120 Access Administration receives the Instruction Files and verifies the accuracy of the information. It then implements the necessary changes on the target platforms as follows:

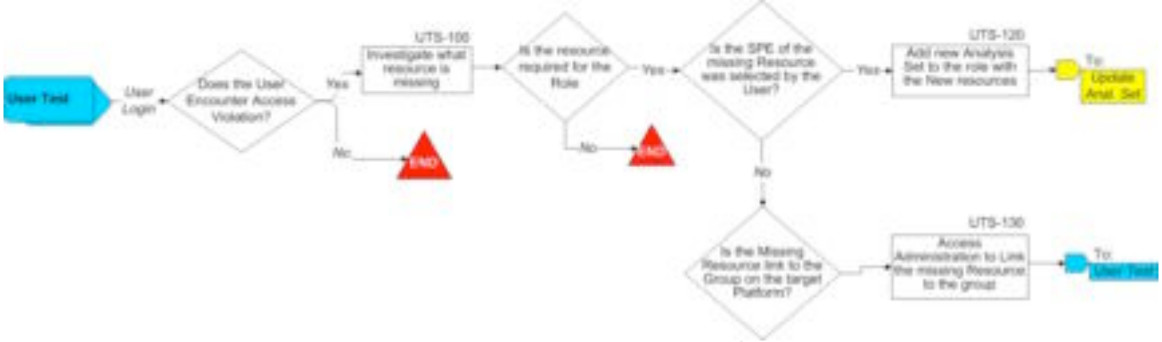
- Create a new Group on the target platform for the Business Role

- Grant new Group Permissions to Resources included in the Instruction File
- Remove all current access of the Selected User
- Grant access to the Selected User(s) to the newly created Group on the target platform

IRL-130 Implement the Business Role instructions on the target platforms (Permissions) and update the provisioning tool with Roles and Authorization information. Once completed, the new Business Role is ready for testing by the User.

7.6.5. User Testing

The Selected User logs-in using his/her User-id and performs all the activities related to his/her job function. If the User does not encounter any access violations he/she may continue to work and fulfill the job function duties based on the new Role.


User Test
User Login
Does the User Encounter Access Violation?
Yes
No
END
UTS-100
Investigate what resource is missing
Is the resource required for the Role
Yes
No
END
Is the SPE of the missing Resource was selected by the User?
Yes
No
UTS-120
Add new Analysis Set to the role with the New resources
To: Update Anal. Set
Is the Missing Resource link to the Group on the target Platform?
UTS-130
Access Administration to Link the missing Resource to the group
To: User Test

If the User encounters access violation:

UTS-100 - RBAC Analysts investigate the problem using the same techniques used to create the Role. Below are some of the questions the RBAC Analyst needs to ask:

- Is the missing Resource needed for the Role?
- Is the Missing Resource linked to the new Group on the target Platform?
- Was the SPE of the missing Resource selected by the User?

UTS-120 - If the SPE was missing, create a new Analysis set for the Role. For more details see paragraph Build Analysis Set, Page 25

UTS-130 - Access Administration to make sure that the resource is linked to the appropriate Group on the platform.

NOTE: If the Selected User cannot access one or more resources, and it is not possible to remediate the problem within the acceptable time, the RBAC Analyst will instruct Access Administration to restore the previous access of the Selected User so that the RBAC Analyst may have more time to assess the problem without impacting the User.

7.7. Role Maintenance Process

The Role Maintenance is an automated business processes workflows. It is a required workflow to make sure that the security rules will not be violated. The workflows are initiated by Requests. Every Request passed from one Actor in the process to the next Actor is based on pre-defined rules. Each activity in the workflow can proceed only after the previous activity has completed its duties.

7.7.1. Current workflow and responsibilities

In the current process, the Platform Administrator is solely responsible for defining Authorization and Permissions. The Platform Administrator may link Resources to a Platform-Group based on a request sent by a user via e-mail without analyzing the consequences or the risks associated with these links. For example, linking a PHI Resource to a Platform-Group may expose restricted information to all the members in the Platform-Group when the intention was to give access to this Resource only to a handful of Users within the same Platform-Group.

The current workflow requires the involvement of two contributors:

Access & Administration	Verify request. Implement Requests on the requested platform.
Approver	Approve the request (without in-depth analysis).

7.7.2. Recommended workflow and responsibilities

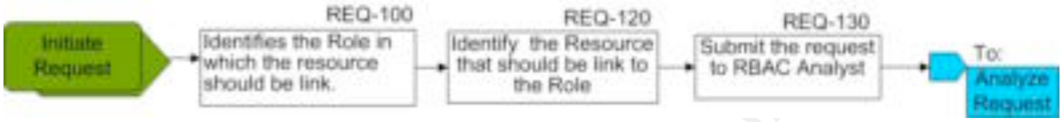
After rolling-out the initial Business Roles, there is a need for a more stringent workflow in order to make sure that the implemented Business Roles will not be "infected" with Resources that are not needed or do not naturally fit into the Role. The recommended workflow is an automated workflow, introducing new contributors (Actors) while keeping the Access Administration role with limited responsibilities:

EIA Owner	The Owner of the EIA who approves Requests that change the relationship between Role and Resources *(Permissions).*
Role Owner	• Initiate, approve or reject requests to add or remove Resources from the Role. • Approve or reject requests to add Users to the Role *(EIA owners that participating in the Business Role must delegates power of Granting or Revoking access to the Role Owner).*
RBAC Analyst	The individual who analyzed RBAC requests.
Privacy Officer	Notified about new access to PHI Resource.
Access & Administration	Implementer only.

7.7.3. Add New Resource to Existing Role

The following describes the steps required in the process of adding a new Resource to an existing Role:

Initiate Request

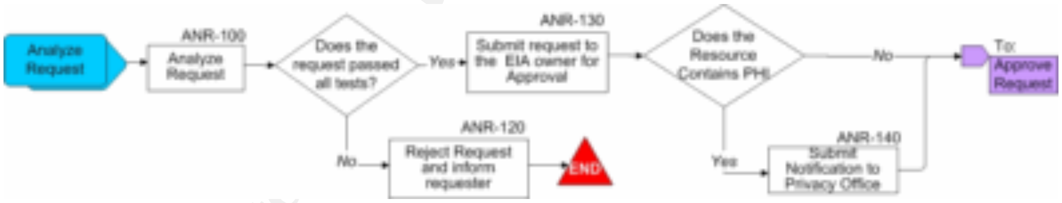

Initiate Request
REQ-100
Identifies the Role in which the resource should be link.
REQ-120
Identify the Resource that should be link to the Role
REQ-130
Submit the request to RBAC Analyst
To:
Analyze Request

REQ-100 - The Requester (User or Role Owner) Identifies the Role to which the resource should be linked.

REQ-120 - The Requester/Role Owner identifies the Resources that are candidates to be linked to the identified Role.

REQ-130 - Submit the request to the RBAC Analyst for further analysis.

Analyze Request


Analyze Request
ANR-100
Analyze Request
Does the request passed all tests?
Yes
No
ANR-120
Reject Request and inform requester
END
ANR-130
Submit request to the EIA owner for Approval
Does the Resource Contains PHI
No
Yes
ANR-140
Submit Notification to Privacy Office
To:
Approve Request

ANR-100 - The RBAC Analyst receives the request and analyzes it based on one or more of the following considerations:

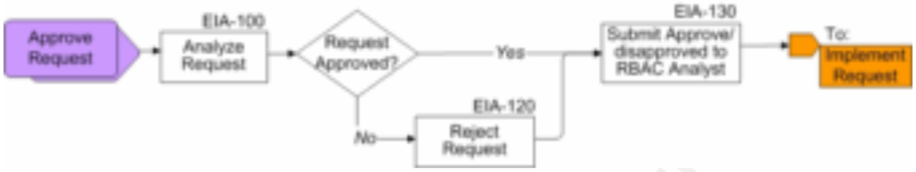
- Does the Resource naturally fit into the Role function?
- How many users in the Role need access to the Resource?
- Can the Users get access to the Resource through another existing Role?
- Is the Resource considered to be PHI Resource?
- How is the Resource being used? Online/Batch

ANR-120 - If the analysis did not pass the above tests, the request will be rejected and notification will be issued to the requester with the specific reason for its rejection.

ANR-130 - If the analysis passed the above test, the request will be submitted to the EIA owner for approval.

ANR-140 - If the Resource is a PHI Resource, a notification will be submitted to the privacy officer. In this case, no further action is required.

Approve Request

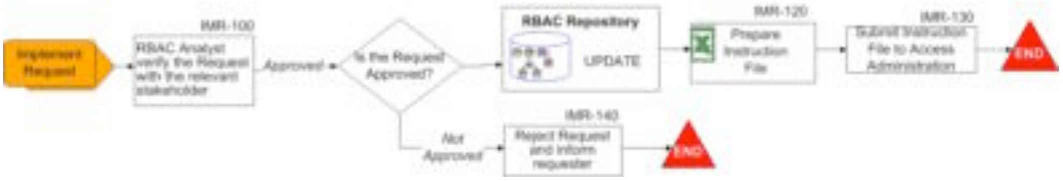


EIA-100 - The EIA Owner receives the request and analyzes it based on one or more of the following considerations:

- Is the Resource being used for View or Update?
- Were the users trained on how to use the Resource?
- How often will the Resource be used (frequency of access)?
- Would adding the Resource to the Role impact Performance?

EIA-120
EIA-130 - The EIA Owner sends the decision (approved or disapproved) back to the RBAC Analyst for further action.

Implement Request


Implement Request
IMR-100
RBAC Analyst verify the Request with the relevant stakeholder
Approved
Is the Request Approved?
RBAC Repository
UPDATE
IMR-120
Prepare Instruction File
IMR-130
Submit Instruction File to Access Administration
END
Not Approved
IMR-140
Reject Request and inform requester
END

IMR-100 - The RBAC Analyst verifies the Request with one of the following stakeholders *(where applicable and depending on the type of request)*: EIA Owner, Role Owner, Human Resource.

If the request was not approved, the RBAC Analyst submits the request back to the Requester with the exact reason for its rejection.

If the request was approved, the RBAC Analyst performs one of the following actions:

- Add the new Resource to the Role
- Add User to a Role
- Revoke User access from a Role
- Remove existing Resource from the Role
- Remove user(s) from a Role

IMR-120 - • The RBAC Analyst prepares an instruction file

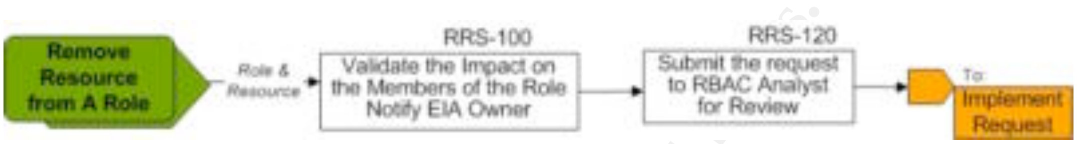
IMR-130 - • The RBAC Analyst submits the instruction file to Access Administration for implantation on the various platforms and informs the requester when completed.

IMR-140 If the EIA owner rejects the request

- The RBAC Analyst Informs the requester and specifies the reason for the rejection of the request

7.7.4. Remove Resource form Existing Role

Removing a resource from a Role may have a significant impact on the Members of the Role. But a request coming from the Role Owner is sufficient enough to remove the Resource from the Role. The RBAC Analyst is not required to analyze the request but needs to verify/notify the EIA owner before sending the instruction to the Platform Administrator for implementation.


Remove Resource from A Role
Role & Resource
RRS-100
Validate the Impact on the Members of the Role Notify EIA Owner
RRS-120
Submit the request to RBAC Analyst for Review
To:
Implement Request

RRS-100 - The Role owner validates with the EIA owner the impact of removing the Resource from the Role on the Role Members.

RRS-120 - The Role Owner submits the request to the RBAC Analyst for review.

7.7.5. Add New Role

Adding a new Role requires the RBAC Analyst to perform an in-depth assessment of the request. Usually it means that none of the current Roles provide adequate access to the potential Members of the new Role. The process of creating a new Role is identical to the Role Assembly described on page 25. In addition, the RBAC Analyst needs to perform a task using the RBAC Repository that compares the Pattern of Access (PoA) of the new Role with the PoA of all the existing Roles. This task is required to validate that the PoA of the new Role is unique across all the existing Roles. This task may raise serious questions that the RBAC Analyst or higher level management need to answer:

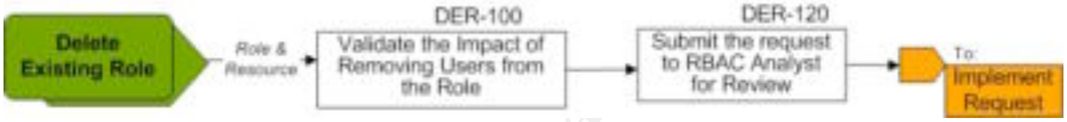
1. If an identical PoA is found linked to an existing Role, can the potential Users of the new Role be added to the existing Role?
    a. If the answer is Yes, it may eliminate the need for a new Role.

2. If 90% of the Resources needed for the new Role are found to be linked to an existing Role, can the potential Users of the new Role be added to the existing Role?
    a. If the answer is Yes, it may eliminate the need for a new Role but the new added users may have excessive access to Resources which they don't need (potential Risk).

3. If 100% of the Resources needed for the new Role are found to be linked to an existing Role but the existing Role has additional Resources which the new Role does not need, can the potential Users of the new Role be added to the existing Role?
    a. If the answer is Yes, it may eliminate the need for a new Role but the new added users may have excessive access to resources which they don't need (potential Risk).

7.7.6. Delete Existing Role

Delete Role requires first to remove Users from the Role and then remove the Resources from the Role. Once this has been completed, the Role can be deleted.

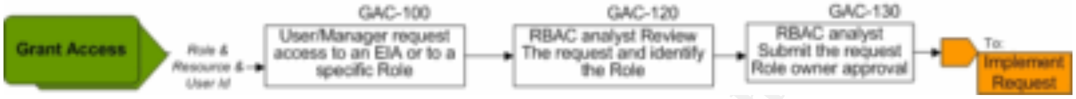

Delete Existing Role
Role & Resource
DER-100
Validate the Impact of Removing Users from the Role
DER-120
Submit the request to RBAC Analyst for Review
To:
Implement Request

DER-100	-	The Role owner validates with the EIA owner the impact of removing the Users from the Role.
DER-120	-	The Role Owner submits a request to delete the Role (remove Users and Resources from the Role) to the RBAC Analyst for review.

7.8. Role Access Process

7.8.1. Grant User Access to a Resource (or a Role)

In general, Users are not familiar with the Role structure *(at least at the beginning of the Business Role Roll-out)*. What they know is the specific name of the Resource for which they need access.


Grant Access
Role & Resource & User Id
GAC-100
User/Manager request access to an EIA or to a specific Role
GAC-120
RBAC analyst Review The request and identify the Role
GAC-130
RBAC analyst Submit the request Role owner approval
To:
Implement Request

GAC-100 - The user fills the “Request for Access” Form, including the specific name of the Resource or the name of Role and submits the request to the RBAC Analyst.

GAC-120 - The RBAC Analyst analyzes the request based on the following criteria:

a. If The Requester indicates the Role Name, the RBAC Analyst submits the request to the Role Owner for approval.
b. If The Requester indicates the Resource, the RBAC Analyst analyzes the request based on one or more of the following considerations:

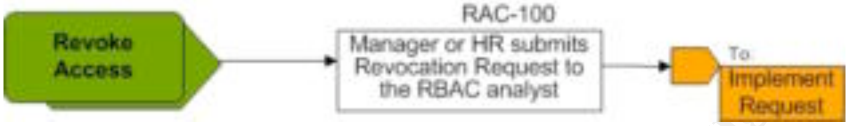
    1. Can the Resource be added to the requester’s Role?
    2. Does the Resource naturally fit into the requester’s Role?
    3. How many users in the requester’s Role also need access to the same Resource?
    4. Can the Users get access to the Resource through another existing Role? If yes, what are the risks?
    5. Is the Resource considered to be a PHI Resource?

GAC-120 - The RBAC Analyst sends the decision with the analysis results to the Role Owner for approval.

7.8.2. Revoke User Access From a Role

Revocation of Access workflow is triggered by one of the following events:

1. A temporary Access that was granted to a User has been expired
2. Employee was transferred to a new position
3. Employee was terminated


Revoke Access
RAC-100
Manager or HR submits Revocation Request to the RBAC analyst
To
Implement Request

RAC-100 - The Revocation Request can come from one of the following sources:

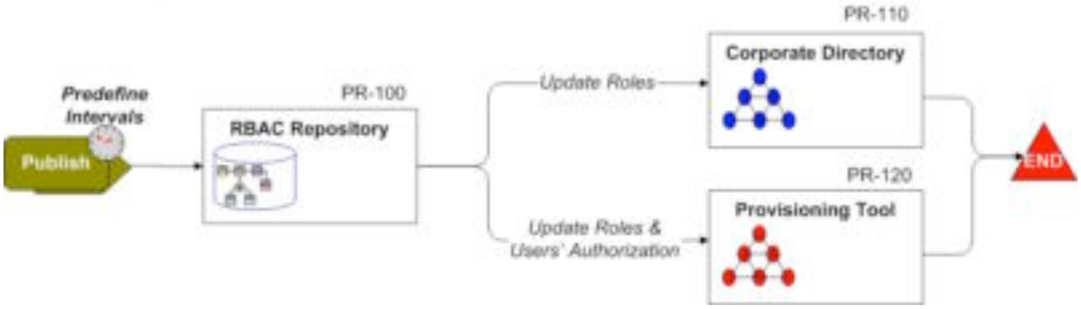
User's Manger - A Revoke Request submitted by the User's Manager usually is an Emergency Request.

Human Resources - A Termination Request *(notification)* submitted by Human Resources, triggers a Request for Revoking Access.

7.9. Role Publishing Process

The RBAC Repository process publishes the Users' Business Roles on the Corporate Directory periodically based on pre-defined intervals. Any EIA that maintains internal roles within the application (in cases where the authorizations are maintained and provided by the application based on the User's role) may interact with the Corporate Directory to retrieve the User's Roles.

The Provisioning tool also needs to interact with the RBAC Repository in order to update the User Roles and its Authorizations.



8. Summary

In a dynamic environment the number of Function Roles on each platform tends to grow over time to an unmanageable number. Managing multiple repositories of User information contribute to the proliferation of different user's identities across many platforms. These facts create a significant gap between what was initially perceived to be a good security control versus the actual security control achieved. As a result, security breach is imminent. Therefore, the implementation of Business Roles becomes a necessity.

The migration from Function Roles to Business Roles has a wider impact on the company's working culture than was initially thought. This requires changes in several key areas including Security Policy, EIA Ownership & Custody, and Identity Management. The most important impact is on several of the company's strategic processes that have direct or indirect correlation to security. This includes the New Hire, Transfer, Termination Processes, and the Access Control Processes.

Another area that will be impacted is the area of responsibilities of the EIA's Access Control. At the present time, the Platform Administrator is the sole gate keeper for all accesses to the company's EIAs. Based on this document's recommendation the Access Control responsibilities will be split between the Platform Administrator and the RBAC Analyst. The RBAC Analyst is a new position that takes on many of the current responsibilities of the Platform Administrators. The RBAC Analyst is an individual who has an overwhelming knowledge of business, an understanding of the RBAC concept and Business Roles in particular. He/she must understand the impact of any decision related to Security and Confidentiality and is familiar with the regulatory requirements. This position serves as the liaison between the EIA & Role Owners and the Platform Administrator. The Platform Administrator role will be limited to the technical issues on the platform and will carry-out the Access Control Requests after they pass all the necessary approvals.

The implementation of the Business Roles is a gradual process and could be spread over a number of years. However, its success depends both on senior management's acceptance and the resources allocated for this effort. Senior management's engagement in this process is critical for RBAC's implementation. Senior management may not have the knowledge and experience necessary to develop a strategy. Therefore, they may not be aware of the problem or implications of the project. It is imperative to put together a strategy. A good strategy always starts with a good preparation. The strategy must be very well thought-out and be able to foresee the end results. It should demonstrate and explain to senior management the benefits of Business Roles, the underlying issues, risks, challenges and how this plan provides significantly better security control on the company's EIAs. Therefore, obtaining the support of senior management is critical for the success of RBAC's implementation. Below is a summary of the recommended strategy needed to implement Business Roles:

1. Learn and understand the environment and method used for Access Control across all platforms.
2. Reconcile and consolidate all Users' information and their current access privileges to one Repository for analysis.
3. Define good Business Roles based on the business needs while adhering to the Privacy and Security requirements.
4. Analyze, build, and refine the recommended Business Roles based on the current access privileges of the users in all platforms.
5. Identify and implement the necessary components required for building and maintaining Business Roles.
6. Provide Access to Users via an Auto-provisioning tool utilizing consistent and rigorous workflows so that security control will not be violated.

An important factor for the success of RBAC's implementation is the human factor. Creating Roles in a heterogeneous environment is a very complex process and it affects many areas in the enterprise. For example, there are issues that need to be identified, underlying issues that need to be clarified, and there is knowledge that needs to be shared. This requires the involvement of many individual in this process such as Business Users, Developers and Platform Administrators. Their involvement is crucial and fundamental to the process and their contribution is indispensable. Maintaining a good working relationship and building a consensus between all the participants is vital for sustainable results.

Gaining senior management's support, employing a good strategy, and building a consensus with the user community are the key success factors which will provide the enterprise with a better and robust security model. It will improve the accuracy of the information about Users, Users' Access to EIAs. It will also make scaling easier, will increase the security and the confidentiality while significantly reducing management cost.

* * *

9. Glossary

Authorization The relationship between a User and a Platform-Group which allows the User access to the Resources associated with the Platform-Group.

BA A short for Business Area. The BA is a representative of a business area that helps with the initial efforts to define Business Role and User membership.

Business Role A Role-based method used to provide access to users on all platforms based on the user's Job Function. A Business Role is platform independent and it represents a consolidation of all the users' access across all platforms into one Role that has a unique business context.

EIA Electronic Information Asset – All the electronic information and the computer hardware, and software which stores, transfers or processes it.

EIA Owner An officer who classifies the EIA and ensures that all security responsibilities related to the EIA are assigned to Security Custodians. The EIA owner also involve in the permission workflow Add New Resource to Existing Role Page 30

Function Role A Platform-Group method that is currently used to provide access to users on a given platform.

LDAP Light Directory Access Protocol. LDAP is based on the standards contained within the X.500 standard, but it is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite.

Permission A relationship between a Resource and Platform-Group which provides certain access rights to User who are associated with the Platform-Group. Allows the Platform-Group to access a Resource in one or more specific ways.

PHI Patient Health Information

RACF RACF (Resource Access Control Facility) is the IBM security management product for its mainframe (large server) operating system, OS/390 (MVS) as well as for its VM operating system. RACF identifies and authenticates a user, determines the resources to which the user is authorized, and logs and reports attempts to get access to protected resources by unauthorized users.

RBAC Short for Role-Based Access Control. A system of controlling which users have access to resources based on the role of the user. Access rights are grouped by Role Name and access to Resources is restricted to Users who have been authorized to assume the associated role.

RBAC Analyst An individual who understands the impacts of any decision related to Security and Confidentiality and is familiar with the regulatory requirements. This individual serves as the liaison between the EIA & Role Owners and the Platform Administrator.

Resource A program, data or thing to which access must be controlled.

Role A collection of Permissions to one or more Resources. In order to be cost-effective, more than one User and more than one Resource should be associated with the Role at any one time.

Role Owner An individual, who is a member of the company's workforce. The Role Owner responsibilities are:

- Provides prior approval to a Request to grant a User membership in a Role. (see Role Access Process Page 35)
- Approves or rejects a Request to grant, modify or revoke access by a Role to a Resource of an EIA *(Through consultation with the EIA Owner)*. See Add New Resource to Existing Role Page 30
- Periodically reviews and approves Role Access reports.

User An individual who is part of the company's workforce and has a need to access an EIA.

User ID A string of characters that identifies the User for access control purposes.

10. References

- National Standard of Technology (NIST) Role Based Access Control American
  http://csrc.nist.gov/rbac/rbac-std-ncits.pdf

- International Standard ISO/IEC 17799 Information technology – Code of Practice for Information Security Management

- Webopedia - The online Dictionary
  http://www.webopedia.com

- HIPAA Security Standard
  http://www.hipaadvisory.com/regs/Regs_in_PDF/finalsecurity.pdf

- Standards for Privacy of Individually Identifiable Health Information
  http://www.hipaadvisory.com/regs/Regs_in_PDF/Final%20Privacy%20Rule.pdf