HL7 Role Based Access Control (RBAC) Role Engineering Process Applied Example

Version 1.0

HL7 Security Technical Committee

13 July 2005

Table of Contents

Section **Page**

List of Figures

Figure **Page**

List of Tables

Table **Page**

1 Applied Example

The following sample storyboard, “Lab Frequency Order with Results,” was obtained from an HL7 Orders/Observations Technical Committee. The storyboard depicts an Emergency Room Physician who evaluates a patient with complaints of chest pains and orders frequency laboratory tests whose results provide confirmation of the admitting diagnosis.

Portions of the sample storyboard will create UML sequence diagrams with structured text (steps) to represent the activity.

For ease of reference, the sections that follow are titled the same as the corresponding sub sections of the *HL7 Role-Based Access Control (RBAC) Role Engineering Process* “Process Steps” section.

2 Identify and Model Usage Scenarios

STEP 1 ➨ Gather an initial list of healthcare scenarios using HL7 storyboards and actual system access patterns.

Purpose: the purpose of this storyboard is to illustrate the order and result messaging related to lab frequency orders that report both preliminary and final results.

<|>**Presentation**</|>
Dr. Eric Emergency, an emergency room physician, sees a 45-year old male patient Adam Everyman, for chest pains. Myocardial infarction is suspected and the patient is admitted.

<|>**Activate Order**</|>
To determine whether the Adam Everyman has had a heart attack, Dr. Emergency orders a CPK with MB fractionation battery to be collected immediately and then every 8 hours for the next 2 days. The order is sent from the ordering system to the laboratory system.

<|>**Intent to Perform Order**</|>
A phlebotomist, Boris Bleeder, from the laboratory arrives to collect the first specimen shortly after the order is entered. Boris labels the specimen with labels printed on the STAT printer in the laboratory and then transports the labeled specimen back to the lab. Once the specimen arrives at the specimen processing section of the laboratory, lab tech Bill Beaker spins the tube of blood down in a centrifuge and delivers an aliquot of serum to the appropriate workstation. The laboratory system notifies the ordering system that the specimen has been received and that it intends to perform the requested series of tests.

<|>**Notify Laboratory Results**</|>
The total CPK test is performed and the result is transmitted from the laboratory system to the results reporting system. Because the MB fractionation will not be performed until the next run of isoenzymes, the partially resulted battery is reported as preliminary. Two hours later, the MB

fractionation test is performed. The MB result is entered, the battery is marked as final and the results are sent to the results reporting system.

<|>**Intent to Perform Occurrence**</|>
At the next designated time 8 hours after the first specimen was obtained, the laboratory arrives to collect the next specimen in the series. Once the specimen arrives in the laboratory it is processed, delivered to the workstation and a notice is sent to the ordering system that the specimen has been received and that the lab intends to perform the requested tests on the current specimen.

<|>**Notify Laboratory Results**</|>
The total CPK test is performed and the result is transmitted from the laboratory system to the results reporting system. Because the MB fractionation will not be performed until the next run of isoenzymes, the partially resulted battery is reported as preliminary. After the MB fractionation test is performed, the battery is marked as final and the results are sent to the results reporting system.

The <|>**Intent to Perform Occurrence**</|> and the <|>**Notify Laboratory Results**</|> repeat for each requested specimen collection. Based on the series of results, Dr. Emergency concludes that his preliminary diagnosis of myocardial infarction was correct. Because the MB fraction peaks approximately 12-24 hours after heart attack, Dr. Emergency presumes Adam Everyman most likely infarcted very close to the time of admission and that no further myocardial damage occurred during this episode of care.

STEP 2 ➨Assign each scenario a name using the HL7 nomenclature. Create structured text (steps) and a sequence diagram for each scenario.

Storyboard Name: Frequency Lab Order with Results

For purposes of this example, two scenarios from the above “Frequency Lab Order with Results” complex storyboard are depicted in the following Sequence Diagrams: “Intent to Perform Order – Collect Specimen”, “Intent to Perform Order – Process Specimen,” and “Intent to Perform Occurrence” in Figures 1-3. Each diagram in the scenario modeling sub-process is provided with a unique name to identify the scenario and to facilitate search operations within the scenario model. [Neumann/Strembeck]

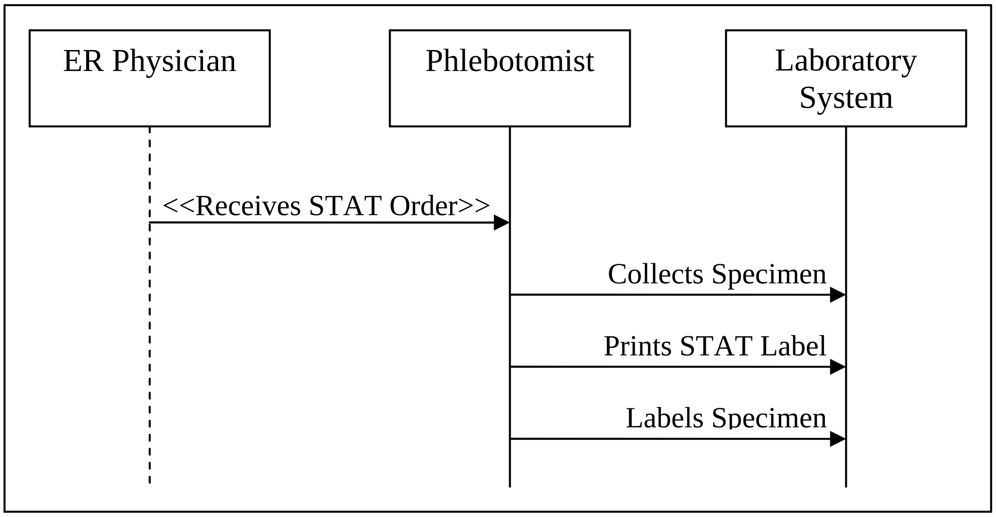

Figure 1: Intent to Perform Order – Collect Specimen Scenario

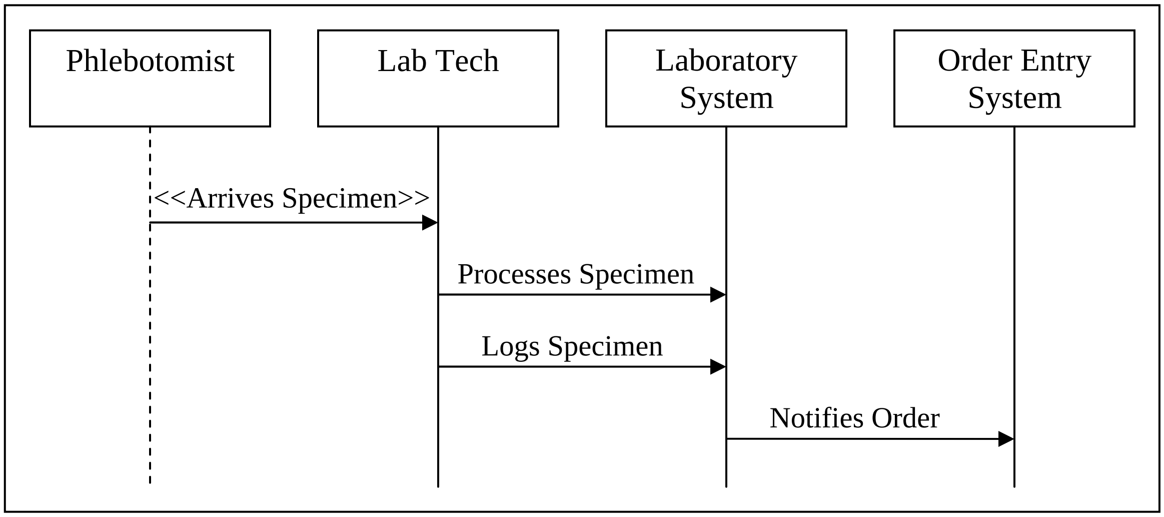

Figure 2: Intent to Perform Order – Process Specimen Scenario

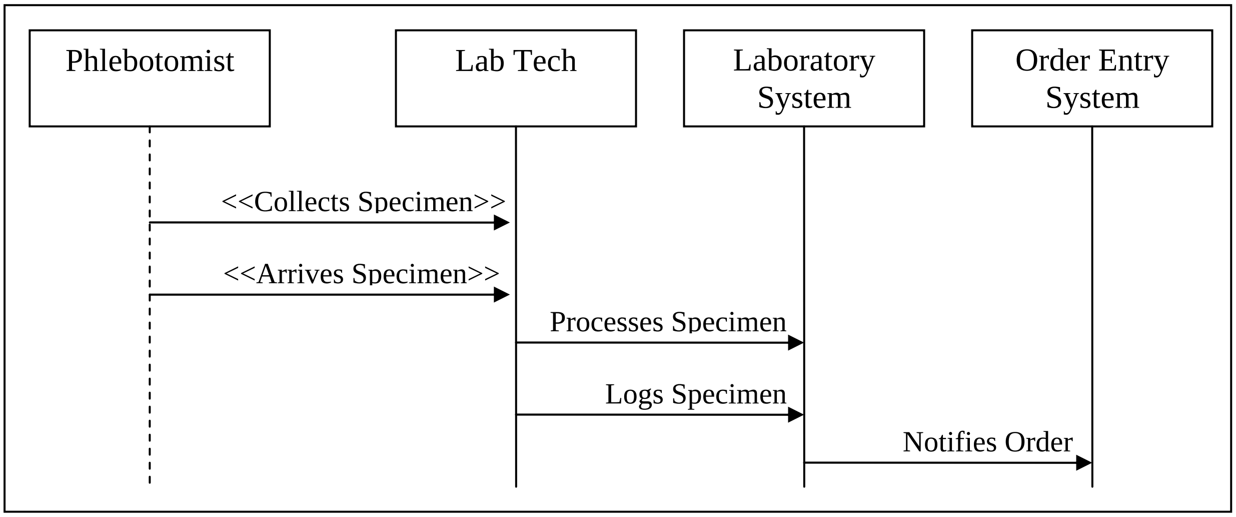

Figure 3: Intent to Perform Occurrence Scenario

STEP 3 ➡ Validate and complete scenarios with input from healthcare domain experts.

At this point, the scenarios would be reviewed and validated by other domain experts.

STEP 4 ➡ Record consolidated list of scenarios. This is the Scenario Model.

The storyboard or workflow name "Frequency Lab Order with Results" and its sub-scenarios are recorded as shown in Table 1. (New items in the tables that follow will be identified using italicized text.)

Table 1: Scenario Recordation

Workflow	Scenario
Frequency Lab Order with Results	*Intent to Perform Order - Collect Specimen*
Frequency Lab Order with Results	*Intent to Perform Order - Process Specimen*
Frequency Lab Order with Results	*Intent to Perform Occurrence*

3 Permission Derivation from Scenarios

The second major activity in the process is to derive permissions that correspond with the step-sequence. The operation that a subject (e.g., user) performs to complete a step is identified and stored as {operation, object} pairs in the permission catalogue. [Neumann/Strembeck]

STEP 1 ➨ Review scenario and identify the actors and steps in the scenario.

In this part of the process, each scenario is reviewed and the actors and steps are identified. Table 2 contains the actor-to-step mapping.

Table 2: Identification of Actors and Steps

Workflow	Scenario	Actor	Step
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	*Phlebotomist*	*Receives STAT Order*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	*Phlebotomist*	*Collects Specimen*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	*Phlebotomist*	*Prints STAT Label*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	*Phlebotomist*	*Labels Specimen*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	*Phlebotomist*	*Arrives Specimen*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	*Lab Tech*	*Processes Specimen*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	*Lab Tech*	*Logs Specimen*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	*Laboratory System*	*Notifies Order*
Frequency Lab Order with Results	Intent to Perform Occurrence	*Phlebotomist*	*Collects Specimen*
Frequency Lab Order with Results	Intent to Perform Occurrence	*Phlebotomist*	*Arrives Specimen*
Frequency Lab Order with Results	Intent to Perform Occurrence	*Lab Tech*	*Processes Specimen*

Table 2: Identification of Actors and Steps

Workflow	Scenario	Actor	Step
Frequency Lab Order with Results	Intent to Perform Occurrence	*Lab Tech*	*Logs Specimen*
Frequency Lab Order with Results	Intent to Perform Occurrence	*Laboratory System*	*Notifies Order*

STEP 2 ➨ Identify the operations and objects required to perform each step.

In the review, identify the objects associated with the steps from the scenarios. Table 3 contains the step to operation and object mapping. The system operations are defined as “C, R, U, D, E”, or create, read, update, delete, and execute, respectively.

Table 3: Identification of Operations and Objects

Workflow	Scenario	Actor	Step	Operation	Object
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	Phlebotomist	Receives STAT Order	*R*	*Order*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	Phlebotomist	Collects Specimen	*C,* *U,* *R*	*Observation,* *Order,* *WorkList*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	Phlebotomist	Prints STAT Label	*C*	*Device*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	Phlebotomist	Labels Specimen	*C*	*Container*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	Phlebotomist	Arrives Specimen	*U,* *U*	*Observation,* *Order*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	Lab Tech	Processes Specimen	*U*	*Observation*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	Lab Tech	Logs Specimen	*U*	*Observation*

Table 3: Identification of Operations and Objects

Workflow	Scenario	Actor	Step	Operation	Object
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	Laboratory System	Notifies Order	*U*	*Order*
Frequency Lab Order with Results	Intent to Perform Occurrence	Phlebotomist	Collects Specimen	*C,* *U,* *R*	*Observation,* *Order,* *WorkList*
Frequency Lab Order with Results	Intent to Perform Occurrence	Phlebotomist	Arrives Specimen	*U,* *U*	*Observation,* *Order*
Frequency Lab Order with Results	Intent to Perform Occurrence	Lab Tech	Processes Specimen	*U*	*Observation*
Frequency Lab Order with Results	Intent to Perform Occurrence	Lab Tech	Logs Specimen	*U*	*Observation*
Frequency Lab Order with Results	Intent to Perform Occurrence	Laboratory System	Notifies Order	*U*	*Order*

STEP 3 ➨ For each scenario step, record the associated {operation, object} pairs.

In this step, the operations and objects from the last table are merged into an associated pair. The associated pairs for this scenario are listed in Table 4.

Table 4: Identification of Associated {Operation, Object} Pairs

Workflow	Scenario	Actor	Step	{Operation, Object}
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	Phlebotomist	Receives STAT Order	*{R, Order}*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	Phlebotomist	Collects Specimen	*{C, Observation},* *{U, Order},* *{R, WorkList}*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	Phlebotomist	Prints STAT Label	*{C, Device}*
Frequency Lab Order with Results	Intent to Perform Order - Collect Specimen	Phlebotomist	Labels Specimen	*{C, Container}*

Table 4: Identification of Associated {Operation, Object} Pairs

Workflow	Scenario	Actor	Step	{Operation, Object}
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	Phlebotomist	Arrives Specimen	*{U, Observation},* *{U, Order}*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	Lab Tech	Processes Specimen	*{U, Observation}*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	Lab Tech	Logs Specimen	*{U, Observation}*
Frequency Lab Order with Results	Intent to Perform Order - Process Specimen	Laboratory System	Notifies Order	*{U, Order}*
Frequency Lab Order with Results	Intent to Perform Occurrence	Phlebotomist	Collects Specimen	*{C, Observation},* *{U, Order},* *{R, WorkList}*
Frequency Lab Order with Results	Intent to Perform Occurrence	Phlebotomist	Arrives Specimen	*{U, Observation},* *{U, Order}*
Frequency Lab Order with Results	Intent to Perform Occurrence	Lab Tech	Processes Specimen	*{U, Observation}*
Frequency Lab Order with Results	Intent to Perform Occurrence	Lab Tech	Logs Specimen	*{U, Observation}*
Frequency Lab Order with Results	Intent to Perform Occurrence	Laboratory System	Notifies Order	*{U, Order}*

Basic steps, such as “Notifies Order,” will likely be included in many different scenarios. These steps will be normalized as shown in the next section. Each permission is registered only once in the permission catalogue.

3.1 Identification of Permission Constraints

Permission Constraints are currently not used in the HL7 permission definition process.

3.2 Scenario Model Refinement

The Scenario Model Refinement process activity involves reviewing the initial scenario model to ensure that it contains complexity details (Concretion). The scenario is then compared against other similar scenarios to possibly define an abstract type (Generalization). [Neumann/Strembeck]

Concretion:

STEP 1 ➨For each complex scenario, define sub-scenarios, as necessary.

The storyboard used for this example was already deemed complex and decomposed into multiple scenarios in the "Identify and Model Scenarios" section.

STEP 2 ➨Update the scenario model.

The scenario model for this storyboard was updated in the "Identify and Model Scenarios" section.

Generalization:

Our example storyboard represents the ordering, collecting, processing, and resulting of frequency STAT laboratory orders. For generalization purposes, an example of a similar storyboard for comparison and possible abstract definition could include one-time laboratory orders, non-panel laboratory orders, and laboratory tests to be collected and resulted with ASAP, routine, pre-op, etc., timing.

STEP 1 ➨ Search the scenario model for similar {operation, object} pairs.

In this step, search the complete list of {operation, object} pairs for duplicates. Duplicates are color coded in Table 5. (Note: rows without colors are not duplicates.)

Table 5: {Operation, Object} Pairs – Duplicates

Scenario	Actor	Step	{Operation, Object}
Intent to Perform Order - Collect Specimen	Phlebotomist	Receives STAT Order	{R, Order}
Intent to Perform Order - Collect Specimen	Phlebotomist	Collects Specimen	{C Observation}, {U, Order}, {R, WorkList}
Intent to Perform Order - Collect Specimen	Phlebotomist	Prints STAT Label	{C, Device}
Intent to Perform Order - Collect Specimen	Phlebotomist	Labels Specimen	{C, Container}
Intent to Perform Order - Process Specimen	Phlebotomist	Arrives Specimen	{U, Observation}, {U, Order}
Intent to Perform Order - Process Specimen	Lab Tech	Processes Specimen	{U, Observation}
Intent to Perform Order - Process Specimen	Lab Tech	Logs Specimen	{U, Observation}
Intent to Perform Order – Process Specimen	Laboratory System	Notifies Order	{U, Order}

Table 5: {Operation, Object} Pairs – Duplicates

Scenario	Actor	Step	{Operation, Object}
Intent to Perform Occurrence	Phlebotomist	Collects Specimen	{C, Observation}, {U, Order}, {R, WorkList}
Intent to Perform Occurrence	Phlebotomist	Arrives Specimen	{U, Observation}, {U, Order}
Intent to Perform Occurrence	Lab Tech	Processes Specimen	{U, Observation}
Intent to Perform Occurrence	Lab Tech	Logs Specimen	{U, Observation}
Intent to Perform Occurrence	Laboratory System	Notifies Order	{U, Order}

STEP 2 ➨ Consolidate the list of similar steps and {operation, object} pairs, eliminating duplicates.

Normalize the list of actors, steps, and {operation, object} pairs by grouping similar steps and identical {operation, object} pairs. Duplicates will be eliminated, as shown in Table 6. Isolated pairs (no color) are recorded but not grouped.

Table 6: Associated Pairs – Normalized

Scenario	Actor	Step	{Operation, Object}
Intent to Perform Order - Collect Specimen	Phlebotomist	Receives STAT Order	*{R, Order}*
Intent to Perform Order - Collect Specimen	Phlebotomist	Collects Specimen	*{C, Observation},* *{U, Order},* *{R, WorkList}*
Intent to Perform Occurrence	Phlebotomist	Collects Specimen	
Intent to Perform Order - Collect Specimen	Phlebotomist	Prints STAT Label	*{C, Device}*
Intent to Perform Order - Collect Specimen	Phlebotomist	Labels Specimen	*{C, Container}*
Intent to Perform Order - Process Specimen	Phlebotomist	Arrives Specimen	*{U, Observation},* *{U, Order}*
Intent to Perform Occurrence	Phlebotomist	Arrives Specimen	
Intent to Perform Order - Process Specimen	Lab Tech	Processes Specimen	*{U, Observation}*
Intent to Perform Occurrence	Lab Tech	Processes Specimen	
Intent to Perform Order - Process Specimen	Lab Tech	Logs Specimen	*{U, Observation}*
Intent to Perform Occurrence	Lab Tech	Logs Specimen	

Table 6: Associated Pairs – Normalized

Scenario	Actor	Step	{Operation, Object}
Intent to Perform Order – Process Specimen	Laboratory System	Notifies Order	*{U, Order}*
Intent to Perform Occurrence	Laboratory System	Notifies Order	

STEP 3 ➡ Define an abstract type for the scenario, if necessary.

Not applicable to example.

STEP 4 ➡ Group the similar scenarios and derive a common abstract type.

Steps are then labeled as 'permissions' and given unique permission identifications within a Permission Catalogue. Table 7 contains the abstract and basic permissions derived from the set of scenario steps from Table 6 above and the associated {Operation, Object} pairs. The Scenario ID and Unique Permission ID will be name-spaced (i.e., OR_Adm might represent "Order, Admission Type") so that the scenarios and permissions being performed are easily identifiable.

Table 7: Permission Catalogue

Scenario ID	Unique Permission ID	Abstract Permission Name	Basic Permission Name
Scen_1	*Perm_1*	*Receives STAT Order*	{R, Order}
Scen_2	*Perm_2*	*Collects Specimen*	{C, Observation}, {U, Order}, {R, WorkList}
Scen_3	*Perm_3*	*Prints STAT Label*	{C, Device}
Scen_4	*Perm_4*	*Labels Specimen*	{C, Container}
Scen_5	*Perm_5*	*Arrives Specimen*	{U, Observation}, {U, Order}
Scen_6	*Perm_6*	*Processes Specimen*	{U, Observation}
Scen_7	*Perm_7*	*Logs Specimen*	{U, Observation}
Scen_8	*Perm_8*	*Notifies Order*	{U, Order}

STEP 5 ➨ For each entity and permission, record a corresponding "x" or "o" in the roadmap.

The roadmap is populated with the data that has been derived in the previous steps; an "x" is entered to indicate the entity performs the step and an "o" is entered to indicate the entity does not perform the step. Table 8 illustrates a sample roadmap.

Table 8: Roadmap

Permission ID	Scenario ID	Basic Permission Name	Step	Phlebotomist	Lab Tech	Laboratory System
Perm_1	*Scen_1*	*{R, Order}*	*Receives STAT Order*	*x*	*o*	*o*
Perm_2	*Scen_2*	*{C, Observation},* *{U, Order},* *{R, WorkList}*	*Collects Specimen*	*x*	*o*	*o*
Perm_3	*Scen_3*	*{C, Device}*	*Prints STAT Label*	*x*	*o*	*o*
Perm_4	*Scen_4*	*{C, Container}*	*Labels Specimen*	*x*	*o*	*o*
Perm_5	*Scen_5*	*{U, Observation},* *{U, Order}*	*Arrives Specimen*	*x*	*o*	*o*
Perm_6	*Scen_6*	*{U, Observation}*	*Processes Specimen*	*o*	*x*	*o*
Perm_7	*Scen_7*	*{U, Observation}*	*Logs Specimen*	*o*	*x*	*o*
Perm_8	*Scen_8*	*{U, Order}*	*Notifies Order*	*o*	*o*	*x*

3.3 Remaining Process Activities

The remaining process activities, "Definition of Tasks and Work Profiles" and "Derivation of a Preliminary Role-hierarchy/RBAC Model Definition," cannot be represented until more scenarios are defined and normalization of the collected data occurs.