RBAC model

**secuml.permission**
- enterBugDetails: Insert
- confirmBugDetails: Update

**secuml.permission**
- responsibleSpecialist
- report

**secuml.resource**
- ApplicationDevelopment
  - issue: String
  - task: String
  - revenue: Float
  - marketingplan: String
  + createIssue()
  + verifyIssue()
  + prioritizeTask()
  + calculateRevenue()
  + reviewMarketingplan()
  + developTask()
  + updateTask()
  + approveTask()

**secuml.permission**
- DeveloperPermission
  - writeCode: Insert
  - UpdateCode: Update

**secuml.permission**
- ManagerPermission
  - analyseTask: Select
  - StartDeployment: Update

**secuml.permission**
- SalesSpecialistPermission
  - checkRevenueDetails: Select
  - changeMarketingplan: Update

**secuml.permission**
- QASpecialistPermission
  - enterBugDetails: Insert
  - confirmBugDetails: Update

**secuml.permission**
- ManagerPermission
  - analyseTask: Select
  - StartDeployment: Update

**secuml.permission**
- SalesSpecialistPermission
  - checkRevenueDetails: Select
  - changeMarketingplan: Update

**secuml.permission**
- DeveloperPermission
  - writeCode: Insert
  - UpdateCode: Update

**secuml.permission**
- responsibleSpecialist
- report

**secuml.permission**
- responsibleManager
RBAC tasks

1. Choose the subject(s) of RBAC from above representation:

   a. ApplicationDevelopement
   b. Steve - Manager
   c. QASpecialistPermission
   d. David - Developer
   e. Sandy - Developer
   f. SalesSpecialistPermission
   g. DeveloperPermission
   h. Rene - SalesSpecialist
   i. ManagerPermission
   j. Arne - QA Specialist

2. Choose the permission(s) / policies of RBAC from above representation:

   a. ApplicationDevelopement
   b. Steve - Manager
   c. QASpecialistPermission
   d. David - Developer
   e. Sandy - Developer
   f. SalesSpecialistPermission
   g. DeveloperPermission
   h. Rene - SalesSpecialist
   i. ManagerPermission
   j. Arne - QA Specialist

3. Choose the Object(s) of RBAC from above representation:

   a. ApplicationDevelopement
   b. Steve - Manager
   c. QASpecialistPermission
   d. David - Developer
   e. Sandy - Developer
   f. SalesSpecialistPermission
   g. DeveloperPermission
   h. Rene - SalesSpecialist
   i. ManagerPermission
   j. Arne - QA Specialist

1.4 By considering the above RBAC model determine which user will able to run which operations to access the resource(s)?

   a. Arne - QASpecialist - enterBugDetails : Insert - createIssue()
   b. Arne - QASpecialist - analyseTask : Select - verifyIssue()
   c. Sandy - Developer - analyseTask : Select - prioritizeTask()
   d. Steve - Manager - analyseTask : Select - prioritizeTask()
   e. Rene – SalesSpecialist - checkRevenueDetails : Select - calculateRevenue()
   f. Rene - SalesSpecialist - changeMarketingplan : Update - reviewMarketingPlan()
   g. Sandy – Developer - writeCode : Insert - developTask()
   h. Sandy - Developer - UpdateCode : Update - updateTask()
   i. Steve - Manager - StartDeployment : Update - approveTask()
   j. David - Developer - writeCode : Insert - developTask()
   k. David - Developer - UpdateCode : Update - updateTask()
   l. David - Developer - analyseTask : Select - prioritizeTask()
   m. Arne - QASpecialist - confirmBugDetails : Update - verifyIssue()
## ABAC model

<table>
<thead>
<tr>
<th>User</th>
<th>Title</th>
<th>Project</th>
<th>Sensitivity</th>
<th>Classified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rene</td>
<td>Head of Sales</td>
<td>Alpha</td>
<td>Finance</td>
<td>Secret</td>
</tr>
<tr>
<td>Sandy</td>
<td>Developer</td>
<td>Beta</td>
<td></td>
<td>Restricted</td>
</tr>
<tr>
<td>Raigo</td>
<td>CEO</td>
<td>Alpha, Beta, Gamma</td>
<td>Finance, General</td>
<td>Top Secret</td>
</tr>
<tr>
<td>Arne</td>
<td>QA Specialist</td>
<td>Gamma</td>
<td></td>
<td>Protected</td>
</tr>
</tbody>
</table>

### Access Control Rules

- **Revenue Access**
  - Title AND Project = Grant

- **Billing Access**
  - Title OR Project = Grant

- **Progress Access**
  - Project OR Classified = Grant

- **Bug Access**
  - Title AND Classified = Grant

### Reports

- **RevenueReport**
  - Title: CEO
  - Project: Alpha

- **BillingReport**
  - Title: QA Specialist
  - Project: Alpha

- **ProgressReport**
  - Project: Beta
  - Classified: Confidential

- **BugReport**
  - Title: Developer
  - Classified: Protected
ABAC Task

1. Choose the subject(s) of ABAC from above representation:
   d. Arne           h. Rene      l. Bug Report

2. Choose the permission(s) / policies of ABAC from above representation:
   d. Arne           h. Rene      l. Bug Report

3. Choose the Object(s) of ABAC from above representation:
   d. Arne           h. Rene      l. Bug Report

2.4 By considering the above ABAC model determine which user(s) will able to access which resource(s)?

   a. Rene - can access – Revenue Report
   b. Raigo & Rene - can access – Revenue Report
   c. Sandy - can access – Bug Report
   d. Arne - can access – Progress Report
   e. Rene & Arne - can access - Bug Report
   f. Raigo & Sandy - can access – Progress Report
   g. Arne - can access - Bug Report
   h. Raigo, Sandy & Arne - can access – Billing Report
   i. Arne, Raigo & Rene - can access – Billing Report
   j. Sandy & Arne - can access – Bug Report
   k. No One - can access – Bug Report
   l. Raigo - can access – Revenue Report
RAdAC model

Access Request → Determine Security Risk

Check: If Security Risk is < 50%

Check: If Security Risk is < 30%
  True → Determine Operational Need
  False → False

Check: If Operational Need is > 70%
  True → Grant Access
  False → False

Determine Operational Need

Grant Access

Deny Access

Post Decision Processing

Access Granted

Application Development
Different Types of user with their quality measure

<table>
<thead>
<tr>
<th></th>
<th>ARNE</th>
<th>SANDY</th>
<th>DAVID</th>
<th>RENE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk:</td>
<td><strong>Very Low</strong></td>
<td><strong>Low</strong></td>
<td><strong>High</strong></td>
<td><strong>Very High</strong></td>
</tr>
<tr>
<td>Operational Need:</td>
<td>Low</td>
<td>High</td>
<td>Very High</td>
<td>High</td>
</tr>
</tbody>
</table>

**Security Risk Measure Table**

<table>
<thead>
<tr>
<th>Numerical Measure</th>
<th>Security Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>0% – 29.99%</td>
<td>Very Low</td>
</tr>
<tr>
<td>30% – 49.99%</td>
<td>Low</td>
</tr>
<tr>
<td>50% – 69.99%</td>
<td>High</td>
</tr>
<tr>
<td>70% – 100%</td>
<td>Very High</td>
</tr>
</tbody>
</table>

**Operational Need Measure**

<table>
<thead>
<tr>
<th>Numerical Measure</th>
<th>Operational Need</th>
</tr>
</thead>
<tbody>
<tr>
<td>0% – 49.99%</td>
<td>Low</td>
</tr>
<tr>
<td>50% – 69.99%</td>
<td>High</td>
</tr>
<tr>
<td>70% - 100%</td>
<td>Very High</td>
</tr>
</tbody>
</table>
RAdAC Task

1. Choose the subject(s) of RAdAC from its process representation:
   
   a. Check: If Security Risk is < 30%  
   b. Deny Access  
   c. Check: If Operational Need is > 70%  
   d. Determine Security Risk  
   e. Rene  
   f. Post Decision Processing  
   g. Grant Access  
   h. Arne  
   i. David  
   j. Sandy  
   k. Check: If Security Risk is < 50%  
   l. Application Development  
   m. Check: If Security Risk is < 70%  
   n. Access Request  
   o. Determine Operational Need  
   p. Permit Access

2. Choose the permission(s) / policies of RAdAC from its process representation:

   a. Check: If Security Risk is < 30%  
   b. Deny Access  
   c. Check: If Operational Need is > 70%  
   d. Determine Security Risk  
   e. Rene  
   f. Post Decision Processing  
   g. Grant Access  
   h. Arne  
   i. David  
   j. Sandy  
   k. Check: If Security Risk is < 50%  
   l. Application Development  
   m. Check: If Security Risk is < 70%  
   n. Access Request  
   o. Determine Operational Need  
   p. Permit Access

3. Choose the Object(s) of RAdAC from its process representation:

   a. Check: If Security Risk is < 30%  
   b. Deny Access  
   c. Check: If Operational Need is > 70%  
   d. Determine Security Risk  
   e. Rene  
   f. Post Decision Processing  
   g. Grant Access  
   h. Arne  
   i. David  
   j. Sandy  
   k. Check: If Security Risk is < 50%  
   l. Application Development  
   m. Check: If Security Risk is < 70%  
   n. Access Request  
   o. Determine Operational Need  
   p. Permit Access

4. By considering the above ABAC model determine which user(s) will able to access which resource(s) ?

   a. Rene - can access – Application Development  
   b. David - can access – Application Development  
   c. Sandy - can access – Application Development  
   d. Arne - can access – Application Development