GRC TRAINING:

BUSINESS SYSTEMS ANALYSTS (IS&T)

Massachusetts
Institute of
Technology

Table of Contents

GRC Roles & Responsibilities – Business System Analysts

Business System Analysts (BSAs) will carry out the following tasks as part of their GRC-related responsibilities:

- Assist the Role Owner and Risk Owner with:
    - Analysis of changes to risks due to changes in roles or user/role assignments
    - Redesign of Roles in terms of business-relevant information and Single vs Composite role design
    - Understanding the Risk – i.e. what the SAP access allows and if there are any additional technical features which are being used , or can be used, to reduce / mitigate the risk – this includes configuration settings, MIT enhancements, additional access security.
- When there are new "Z" transactions, the BSA will assist in categorizing to the closest standard SAP action. The GRC Admin group will add these to the ruleset in the same place as that standard SAP action.
- Assist the BA to document the new / changed role design and communicate it to the SAP R/3 Security Admin group. Potentially assist in the initial role testing.
- Assist the BA with documenting any technical Mitigation Controls
- Prepare mini-specs for any new mitigation controls which require technical work (configuration settings, MIT enhancements, additional access security, and new SAP control reports).

Responsibilities Reference

TASKS	PROCESS & STEP
Analysis of Risks related to user access	1.2, 1.3, 2.1
User role redesign and test plan	1.4
Review for SOD issues from periodic ARA review	5 Q.2
Definition of Mitigation controls	2.2, 2.3
Assist with testing new or changed roles	1.7, 1.11

REPORTS	PROCESS
05 Roles by Role Name	1
06 User to Role Relationship	1
07 Role Relationship with User - User Group	1
08 Users by User ID	1
09 Count Authorizations for Users	1
10 Action Usage by User Role and Profile	1
11 Mitigation Control Report	2
12 User Level	1, 2
13 User Level Simulation	1, 2

FORMS	PROCESS & STEP
None	None

WORKFLOW OR EMAIL-TRIGGERED ACTIONS	PROCESS & STEP
None	None

SAP Security and Governance Procedures

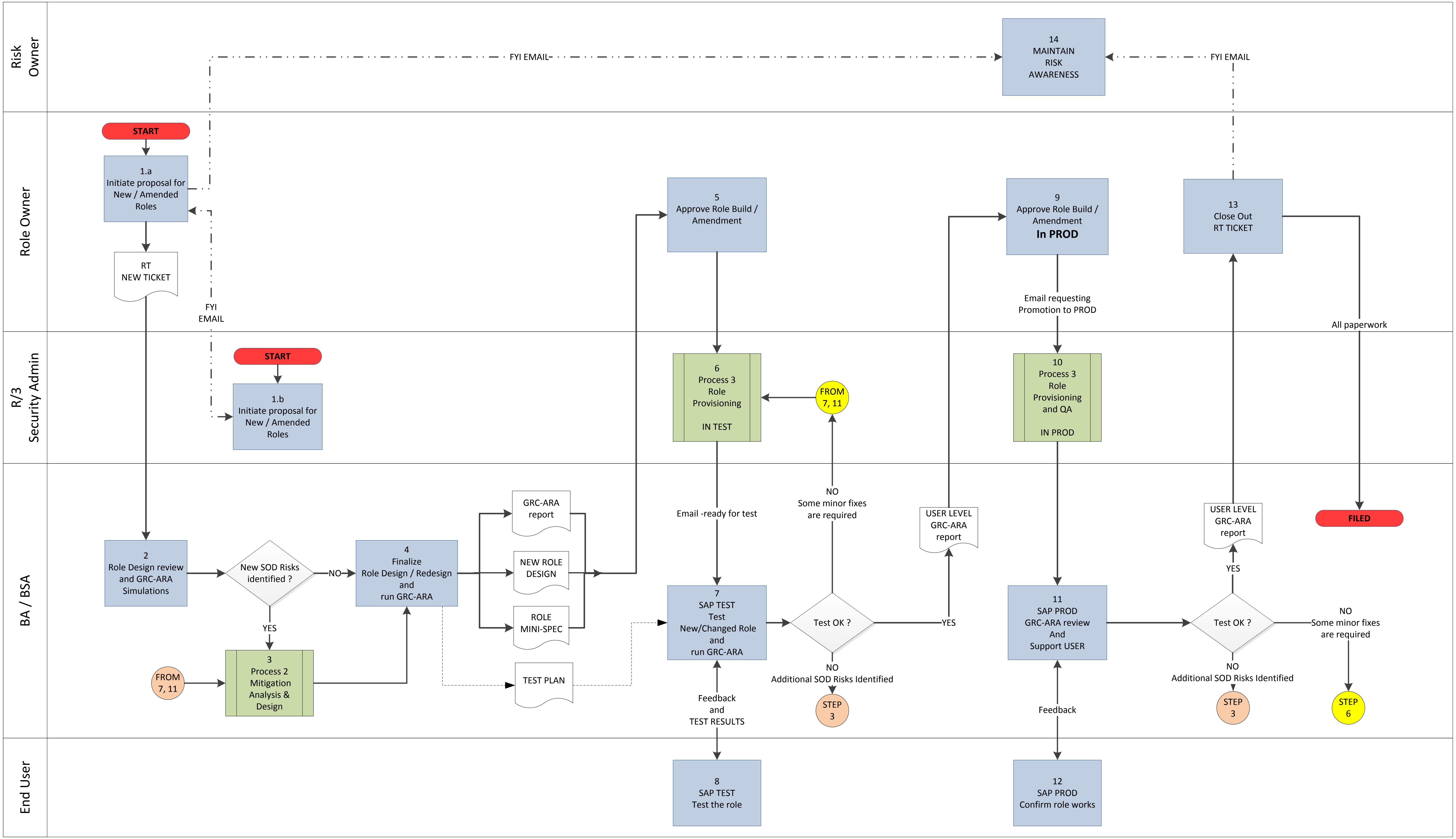
PURPOSE OF THIS DOCUMENT

The SAP Security and Governance Procedures are documented in five flowcharts.   The sections in this document describe the details of each step.

CONTENTS

Process 1: New or Amended Roles

MIT SAP Security & GRC Process : 1. New or Amended Roles



Risk Owner

FYI EMAIL

14 MAINTAIN RISK AWARENESS

FYI EMAIL

Role Owner

START

1.a Initiate proposal for New / Amended Roles

RT NEW TICKET

FYI EMAIL

5 Approve Role Build / Amendment

9 Approve Role Build / Amendment **In PROD**

Email requesting Promotion to PROD

13 Close Out RT TICKET

All paperwork

R/3 Security Admin

START

1.b Initiate proposal for New / Amended Roles

6 Process 3 Role Provisioning IN TEST

FROM 7, 11

10 Process 3 Role Provisioning and QA IN PROD

BA / BSA

2 Role Design review and GRC-ARA Simulations

New SOD Risks identified ?

NO

YES

FROM 7, 11

3 Process 2 Mitigation Analysis & Design

4 Finalize Role Design / Redesign and run GRC-ARA

GRC-ARA report

NEW ROLE DESIGN

ROLE MINI-SPEC

TEST PLAN

Email -ready for test

7 SAP TEST Test New/Changed Role and run GRC-ARA

Feedback and TEST RESULTS

Test OK ?

NO Some minor fixes are required

NO Additional SOD Risks Identified

STEP 3

YES

USER LEVEL GRC-ARA report

11 SAP PROD GRC-ARA review And Support USER

Feedback

Test OK ?

YES

USER LEVEL GRC-ARA report

NO Additional SOD Risks Identified

STEP 3

NO Some minor fixes are required

STEP 6

FILED

End User

8 SAP TEST Test the role

12 SAP PROD Confirm role works

Process 1: New or Amended Roles

The “New or Amended Role” process is for the scenario where a new or amended business role is needed, and includes the high-level steps for initial investigation, design, development and GRC Access Risk assessment.

The requirement SAP Access Role maintenance can be identified during the following business events, with the first two being the most frequent and represented in the flowchart. The process for the other triggering events is almost the same, with any differences documented in the text.

1. Departmental reorganization.
2. New or changed job duties within a department.
3. New SAP functionality which is not expected to be included in common roles but is needed for several users with different access and does fit into an existing role. This may be :
   - Small changes, for extra functionality in existing applications
   - Larger, project-related changes where a whole new application is rolled-out, and probably multiple SAP Access roles.
4. Audits, Compliance and other reviews – this would be less common.
5. SAP Access role redesign / tidy-up (triggered from technical reviews).
6. Removal of functionality from roles – (no SOD risk issues).

Roles & Responsibilities for Process 1:

- **Risk Owner :** Maintains awareness of role changes and potential for new risks
- **Role Owner :** Initiates proposals for role changes, approved role changes, closes out role change process
- **BA / BSA :** **Involvement in several steps**
  - Performs preliminary role change analysis
  - Creates role design / redesign documentation and test plan
  - Tests new roles in TEST – including GRC-ARA simulation
  - Supports end-user in Production.

- **R/3 Security Admin:** Builds roles and provisions role (see process 3).
- **SOD Coordinator:** Indirectly involved if there is any Mitigation requirements – see Process 2.
- **GRC Admin:** Indirectly involved if there is any Mitigation requirements – see Process 2.
- **End User:** Test their User in SAP Production.

Reports available to support the Process 1:

Rept. 5	R/3 SUIM	Roles by Role Name
Rept. 6	GRC	User to Role relationship
Rept. 7	GRC	Role relationship with User
Rept. 8	R/3 SUIM	Users by User ID
Rept. 9	GRC	Count of Authorizations
Rept. 10	GRC	Action Usage by User, Role, Profile
Rept. 12	GRC	User Level access analysis
Rept. 13	GRC	User Level access analysis – simulation with added / removed actions, roles, profiles.
Rept. 14	GRC	Role Level access analysis
Rept. 15	GRC	Role Level access analysis – simulation with added / removed actions, roles, profiles.

TCODE SU01D   Display User information – with Roles and Profiles tab

The following report are also available, but will be less frequently used in the MIT environment:

Rept. 16	GRC	Profile Level access analysis
Rept. 17	GRC	Profile Level access analysis – simulation with added / removed actions.

Process 1: New or Amended Roles - Detailed Steps

P.1 STEP	Business Role	Responsibility / Action	Output	Details
1	Role Owner	Initiate proposal for New/Amended Roles.	• Email to BA/BSA and Risk Owner, SAP Security Admin and MIT Audit • RT Queue – new task	a. Role Owner identifies a potential need for a new role due to : • Departmental Reorganization – new roles are needed to reflect completely new, permanent job duties, and old roles probably can be deactivated. • New or changed job duties – may be combined roles or split role or just completely new. This is less likely where provisioning is managed with Composite roles which can have existing roles added / removed without the need for a new role. • New SAP functionality which does not easily fit into an existing role. b. Role Owner communicates (email) potential need to BA/BSA and Risk Owner. c. The requirement may be triggered from a technical role redesign proposed by SAP Security Admin. **Note** that MIT's has made more use of "**composite roles**" in the redesigned VPF access. The composite role is where several roles are linked together to represent a job position or a specific user's duties. • So some minor User access changes can be managed by adding or removing roles from the composite role. • This would be identified by the Role Owner in simpler cases, or by the BA/BSA for more complicated cases – see step 2.

P.1 STEP	Business Role	Responsibility / Action	Output	Details
2	BA/BSA	Role Design review and GRC-ARA simulations	• GRC-ARA Risk simulation reports • For existing risks, assessment of existing Mitigation Controls to new tcode combination. • If new Risks, kick-off a full risk assessment (see next step = Process 2).	a. For major changes, e.g. complete business reorganization or new major multi-role applications being rolled out, there will always be a need for everyone to be involved, like the SOD project had. b. For minor changes, the BA/BSA will **review the current role design (GRC and SUIM reports)** and decide if any new Roles are necessary to achieve the business changes. Where there are any new action tcodes (create, change, post etc.), or new combinations of tcodes due to composite role changes, a GRC-ARA SOD analysis is required for : • The proposed new / changed role • The users for whom the change will be made • The GRC-ARA simulation can use the current user in PROD, plus any tcodes (entered) or existing roles (in DEV, TEST/QA or PROD). • SAP R/3 Security Admin may need to advise on additional authorizations (permission level) which may reduce the risk. • The BSA may need to advise on alternative tcodes (actions) and standard SAP equivalents of custom “Z” transactions. • The proposed design can be workshopped, including bringing up any SOD issues and recommendations for mitigation. (See details in **Process 2: Mitigation Analysis**). c. In defining design requirements for the request, the BA/BSA works with the Role Owner and Risk Owner. • to mitigate risks and SODs wherever possible, • reaching out to the GRC Analysis Team when input is required d. Check any existing Mitigation Controls related to the current role, and check the detail of the new tcode combinations. It is possible the existing Mitigation Control does not fully cover the new tcodes.

P.1 STEP	Business Role	Responsibility / Action	Output	Details
3	BA/BSA Risk Owner Role Owner SOD Coordinator	Mitigation Analysis	See Process 2 Flowchart for details	**Also, see Flowchart for Process 2 for more details.** a. Mitigation analysis is required where : • New SOD Risks are reported • Existing SOD Risks remain, but are changed due to the new tcodes • New “Critical” transactions (actions) are reported. b. Detailed SOD Risk analysis will confirm if : • risk is low level and is acceptable, or • existing mitigation could apply / still applies, or • a new mitigation control can be defined, or • a new mitigation process may need to be developed ○ new report ○ system enhancement ○ system configuration change ○ additional SAP Access restrictions – permission level ○ new manual process. c. The output of this step will be one or more role redesigns and potentially a new Mitigation Control if the Risk remains after the role redesigns. Note the Risk may have been avoided due to “Remediation” : • Several roles and related user assignments were changed • The tcode causing the issue was put in a “FireFighter” role.

P.1 STEP	Business Role	Responsibility / Action	Output	Details
4	BA/BSA	Finalize role Design / Redesign ad run GRC-ARA simulation	• Role Mini-Spec • New Role Design spreadsheet • GRC-ARA Simulation reports • Test plan and test cases	a. Prepare Role Design / Redesign documentation – including : • Composite Role changes ○ Existing Composite Role: roles to be added or removed ○ New Composite Role to be created and its roles ○ Changes in assignment of Composite Roles to User • Single Role changes ○ New Single Roles ○ Transaction Codes (Actions) to be added or removed ○ Authorizations (Permissions) to be added, removed or changed • FireFighter roles for back-up of new/amended role – ○ New FireFighter roles ○ Existing FireFighter roles - changes to tcodes and other authorizations. ○ Assignment of new FireFighter Roles to Users (see Process 4) • Mitigation documentation (part of Process 2: Mitigation Analysis). • **GRC-ARA SOD Risk Analysis Role and/or User simulation Report 13 and 15**, where possible. b. For major redesigns or new complex applications, the supporting documentation must include full GRC-ARA analysis – probably on the new Roles built in DEV. This step is not included in the flowchart.

P.1 **STEP**	**Business Role**	**Responsibility / Action**	**Output**	**Details**
5	Role Owner	Approve Role Built / Amendment	a. Email SAP Security Admin b. SAP Mini-Spec for Access Change request	a. Give the initial go ahead for new/amended role. • Check GRC-ARA simulation results (printed report) • Review detailed Mini-Spec / SAP Access Change request • Email SAP R/3 Security Admin ○ Give approval to proceed and RT # ○ Include New Role Design document (for new roles) ○ Include Role Mini-Spec (for new / amended roles)
6	SAP Security Admin	Process 3 : New Users and User Role Provisioning In TEST system	• Email to BA/BSA when complete • Amended Role • Saved copy of current role • Update RT Ticket	a. IS&T have a process for managing RT tickets, their prioritization and execution, including a QA review prior to approval of transports going into Production. The details of this process are not documented here. b. Here are the action steps specific to the Role Change requests : • Review all supporting documentation for completeness and for correspondence with the RT ticket description. • **Determine if this request involves the already redesigned roles, or the old roles. For amending original roles, proceed with the old provisioning process.** • Identify any potential overlap with the RoleDB • For any new roles, determine naming convention and check the proposed assignment to composite roles (and related users) or users. • Build or amend the role in SAP Development, move it to TEST/QA, and then assign to a test user, alias or to a composite role. ○ Take a safety copy of any existing role being amended ○ This can be iterative where role design is incomplete or incorrect. • Perform basic unit testing. • Advise BA/BSA the new / amended role is ready for testing

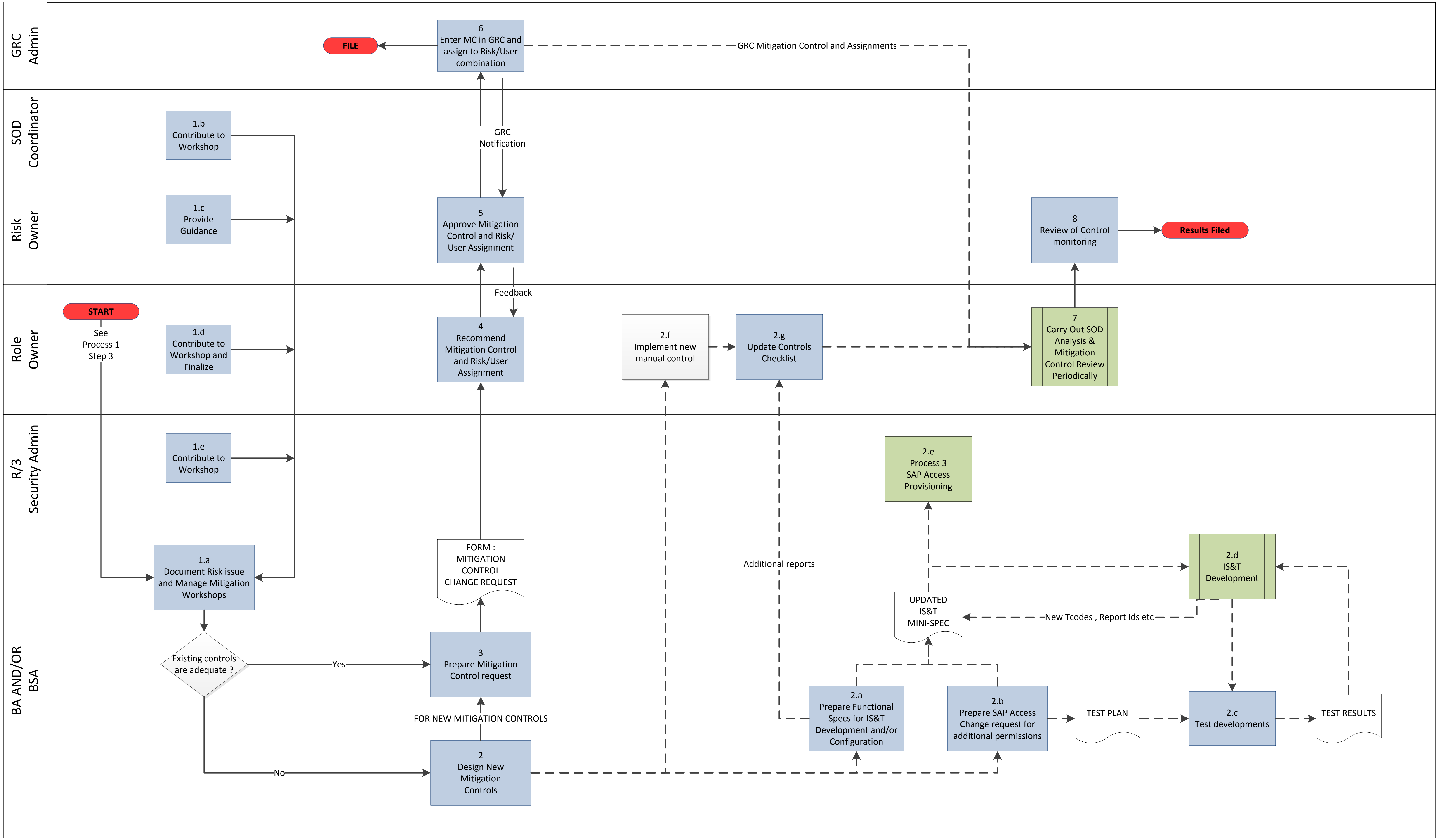
P.1 STEP	Business Role	Responsibility / Action	Output	Details
7	BA/BSA	Check role build, GRC-ARA and assist user with testing	• GRC-ARA simulation reports • Functionality test results • Updated RT-related documentation	a. Check role build / amendments in TEST/QA system • **SUIM report** b. Run GRC-ARA SOD Risk simulation Report 15 on the Role & Report 13 on all Users to be assigned the role. • Use the new/amended Role from TEST/QA system, User from PROD system. • If any new risks are reported, check the reason and revisit the Mitigation process (Step 3). c. Assist the business User with testing the role functionality in SAP TEST/QA system (see Step 8.) d. Update RT-related documentation with test results. e. Email Role owner when business user has accepted the changes.
8	End user and/or BA		• Functionality test results	a. Test the new/amended role functionality in TEST/QA system b. If there are any issues : • Go back to Step 6 for minor changes (e.g. a previously unidentified permission is required for a new tcode). • Go back to Step 4 for any major changes – e.g. additional or alternative tcodes are required. [Not shown on flowchart].
9	Role Owner	Review simulations - if no issues, approve move to SAP Production.	• Email to SAP Security Admin • Updated SAP Access Change request form • Update RT Ticket	a. Review all the paperwork, including Simulation reports. b. Follow-up any issues. c. If all is good, send email to SAP R/3 Security Admin to request promotion to PROD. • Include any special requests – e.g. staggered roll-out to several users at a time, which is more difficult when using Composite Roles.

P.1 STEP	**Business Role**	**Responsibility / Action**	**Output**	**Details**
10	SAP Security Admin	Role provisioning and Transport QA review	• Email to BA/BSA and Role Owner when complete • Update RT Ticket	a. IS&T have a process for managing RT tickets, their prioritization and execution, including a QA review prior to approval of transports going into Production. The all the details of this process are not documented here, just the ones relating to the roles. ○ Ensure roles in DEV and TEST/QA are matching ○ Ensure existing role to be amended in PROD is backed up ○ Check all paperwork for release is complete, coordinate with BSA as appropriate. ○ Request Transport QA review and promotion to PROD ○ Check transports were imported and briefly review roles. b. Email status to Role Owner • **NOTE:** It is also possible there is a need to tweak the RolesDataBase interface with SAP Production – i.e. stop a profile coming over for the users affected by the role changes.
11	BA/BSA	Run User level GRC simulation for all users expected to be assigned the new role. Potential risk that RolesDB profiles causes an issue see Step 17.	• GRC-ARA simulation reports.	Repeat of step 7 – except BA/BSA does not have access in PROD so cannot confirm anything is working.
12	End user	Test role functionality in Production	• Functionality test results	Repeat of Step 8.

P.1 STEP	**Business Role**	**Responsibility / Action**	**Output**	**Details**
13	Role Owner	If no issues, close out the change request	• Email to SAP Security Admin • Updated RT • Signed off SAP Access request?	a. RT ticket can be closed out b. Courtesy email to all involved c. Paperwork check (or confirm with BA/BSA) – all is filed d. Mitigation: additional coordination required if new / amended Mitigations were required – see **Process 2: Mitigation Analysis.**
14	Risk Owner	Maintains awareness of role changes and their implementation.		Maintains general awareness of SAP access within business area. Look out for any new issues at next SOD Review.

Process 2: Mitigation Analysis

MIT SAP Security & GRC Process : 2. Mitigation Analysis


GRC Admin
SOD Coordinator
Risk Owner
Role Owner
R/3 Security Admin
BA AND/OR BSA
FILE
6 Enter MC in GRC and assign to Risk/User combination
GRC Mitigation Control and Assignments
1.b Contribute to Workshop
GRC Notification
1.c Provide Guidance
5 Approve Mitigation Control and Risk/ User Assignment
8 Review of Control monitoring
Results Filed
Feedback
START
See Process 1 Step 3
1.d Contribute to Workshop and Finalize
4 Recommend Mitigation Control and Risk/User Assignment
2.f Implement new manual control
2.g Update Controls Checklist
7 Carry Out SOD Analysis & Mitigation Control Review Periodically
1.e Contribute to Workshop
2.e Process 3 SAP Access Provisioning
FORM : MITIGATION CONTROL CHANGE REQUEST
Additional reports
2.d IS&T Development
1.a Document Risk issue and Manage Mitigation Workshops
UPDATED IS&T MINI-SPEC
New Tcodes , Report Ids etc
Existing controls are adequate ?
Yes
3 Prepare Mitigation Control request
FOR NEW MITIGATION CONTROLS
2.a Prepare Functional Specs for IS&T Development and/or Configuration
2.b Prepare SAP Access Change request for additional permissions
TEST PLAN
2.c Test developments
TEST RESULTS
No
2 Design New Mitigation Controls

Process 2: Mitigation Analysis

The "Mitigation" process described in this flowchart is for the scenario where a new or amended business role is needed, and a new GRC SOD Risk is identified and cannot be avoided.

- See Process 1: New or Amended Roles - which described when role changes occur and where the SOD Risk Analysis and then this Mitigation step fits in.

When a new SOD Risk is identified, there can be several outcomes:

a. **Mitigation is not required :**
    a. Role change is not made – risk cannot be mitigated
    b. Functionality is added to a different user, creating no new Risk – require some additional role redesign, to move tasks between several end-users.
    c. Functionality is added to Emergency Access – Firefighter Role

b. **Mitigation is required**
    a. There is an existing Mitigation Control which applied to the Risk (and to the exact combination of tcodes creating the risk).
    b. A new Mitigation Control definition is required – based on :
        - existing business and/or system control processes
        - new control processes
            - new / amended Mitigation Control reports
            - new manual procedures
            - amended system configuration or enhancements providing additional restrictions
    c. additional Authorization (Permission Level) restrictions to be added to the SAP User security role

c. **Where mitigation is required, the GRC system needs to be updated**
    a. A new GRC Mitigation Control definition
    b. Assignment of existing or new Mitigation Controls to the Risk/User combination

Note: this process is initiated when a potential SOD risk has been identified and is seems like it cannot be avoided and so needs to be "mitigated".   It may also be that a "critical transaction" is assigned and so is being reported as a risk.   This implies a "remediation" process has already been gone through, with the following steps, but none of which are acceptable or possible:

- Consider assigning the transaction code to a different user where there will not be an SOD issue
- If the specific user really needs the new transaction code assignment, then consider removing the assigned tcodes which are triggering the SOD.
- Investigate using any alternative transaction codes which deliver the functionality but do not trigger the SOD issue.
- For "critical transactions", it may be that they are acceptable within a specific business area, but not outside that.   It is proposed that MIT will have a GRC report to monitor this situation.

Roles & Responsibilities for Process 2:

- **Risk Owner:** Provide guidance for level of MIT risk acceptance and formally approve Mitigation Controls.
- **Role Owner:** Assist BA/BSA with Mitigation Control definition; propose final Mitigation Controls and User Assignments to Risk Owner.
- **BA / BSA :** **Involvement in several steps**
    - Manage Mitigation workshops / meetings
    - Assist in design of any new Mitigation Controls
    - Document existing and new Mitigation controls – prepare GRC MC Change Request for Role Owner
- **SOD Coordinator :** Contribute to Mitigation workshops / meetings
- **R/3 Security Admin :** Contribute to Mitigation workshops / meetings , and provision access to any new Mitigation Control reports
- **GRC Admin :** Update GRC Mitigation Controls and Risk/User assignments

Reports available to support the Process 2:

Rept. 11a	GRC	Mitigation Control report – lists Mitigation Controls
Rept. 11b	GRC	Mitigated Object report - lists assignment of Mitigation Controls to Risk/User combinations
Rept. 12	GRC	User Level access analysis
Rept. 13	GRC	User Level access analysis – simulation with added / removed actions, roles, profiles.
Rept. 14	GRC	Role Level access analysis
Rept. 15	GRC	Role Level access analysis – simulation with added / removed actions, roles, profiles.

The following report are also available, but will be less frequently used in the MIT environment:

Rept. 16	GRC	Profile Level access analysis
Rept. 17	GRC	Profile Level access analysis – simulation with added / removed actions.

Some important GRC concepts relevant to SOD Risk identification:

1. In SAP Access control and related GRC risk analysis, there can be two levels of access to review :

   i. SAP Transaction Code (GRC Activity) level, like :
      - FB01 : Post a financial document
      - ME22 : Change a Purchase Order
      - FS00 : Create, change, display a GL Account master records

   ii. SAP Authorization (GRC Permission) – like a RolesDB “qualifier”, but can be more than that.
      - Financial Document Posting : Company Codes allowed
      - Financial Document Posting : Customer usage restriction (e.g. not allowed to post to Sponsored Accounting customers)
      - Purchase Order Type : only allowed to access “NB” purchase orders
      - GL Account Master Maintenance: only allowed Display, not Create or Change – no matter what tcode is provisioned (like FS00).

   iii. Note that one SAP transaction usually checks many different SAP authorizations – e.g. checking that a financial posting is allowed to specific objects like: a Company Code, FI Document Type, Customer account, GL Account, Prior Posting Period, Profit Center, Fund, etc.

Not all of the standard SAP authorization checks are being used at MIT – and the SAP R/3 Security Analyst is able to identify what is called up by standard SAP and what is used at MIT.

2. The way the GRC system identifies an SOD issue is by having a "rule set" of pre-defined data :
   i. "SOD Risks" – with an id like X099 and a description like "Create a fictitious Vendor and post a fictitious Vendor invoice".
   ii. Combination of Functions which create the risk: e.g. ZAP01 = Create Vendor master WITH ZAP02 Post a Vendor Invoice.
   iii. Activities (transaction codes) which the Function contains, e.g. :
      - Function ZAP01 may have 4 transaction codes like; FK01, FK02, XK01, XK02.
      - Function ZAP02 may have many transaction codes like : FB60, FB65, FB01, FB02, F-xx
      - So there are 4 x 5 = 20 possible combinations of transaction codes triggering the SOD issue.

3. There is no way of avoiding looking into the reported combinations of transaction codes which the user actually has and were reported. In most cases the pre-defined is reporting a clear and specific issue no matter what the combination of transaction codes. In that case an existing Mitigation Control for the same risk (by for another User) should apply to this user being reviewed.   However :
   i. In the example above, say that User 1 had transaction codes FK02 + FB02 and so Risk X099 was reported. Neither of these transaction codes is create/post, and the business risk for these may be lower than having FK01 + FB60. So any Mitigating Control assigned to User 1 for risk X099 may not apply to User 2 who has FK01 + FB60 for the same Risk = X099 .
   ii. Additionally, User 2 may have additional restrictions – only creating Sponsor Vendors, or only posting to non-Sponsor vendors. So any Mitigating Control description will be different and so will need a new GRC mitigating Control definition.

4. In GRC risk analysis, always report at the Permission level.   If some Activities (transaction codes) are not additionally defined with a Permission (authorization) level, they will still be shown in the "Permission level" report.

5. The GRC system manages "Mitigating Controls" in two steps :
   i. Define a "Mitigating Control", with a unique id and description
   ii. Assign the Mitigating Control to a <u>combination</u> of Risk + User(s).   So the GRC system can report to the Risk Owner any new users with the Risk who have not yet been assigned to the Mitigating Control.

Process 2: Mitigation Analysis - Detailed Steps

P.2 STEP	Role	Responsibility / Action	Output	Responsibility / Action
1.a	BA/BSA	Document the risk issue and manage the Mitigation Workshops / Process	• Documentation of risk issue and existing possible mitigations • Work plan and potential workshop agenda • Workshop results – i.e. decision on what to do • Workshop results sent to Audit - for their information.	a. Describe the Risk and the exact combination of tcodes causing the risk. b. If possible, quantify / evaluate the risk in the MIT business environment – see also 1.c Risk Owner contribution. c. Review existing Mitigation Controls for the SOD Risk or similar SOD Risks – evaluate if they might apply. d. Also, the risk may already be subject to a Mitigation Control, but that may not apply to a new combination of tcodes reported for the same GRC Risk. e. Identify other business system controls (manual or automated) relevant to the risk. f. Prepare and manage a brief “workshop” meeting to review the information gathered and make a recommendation. g. Document the results of the workshop.
1.b	SOD Coordinator	Contribute to workshop	None	a. Contribute to the understanding of the risk and possible mitigations
1.c	Risk Owner	Provide Guidance	None	a. Provide guidance on the significance of the risk and the relative importance of mitigation – and therefore level of resource that can be justified to mitigate the risk. b. Potential suggestions for end-user role redesign or organizational adjustments, to eliminate or minimize risks.
1.d	Role Owner	Contribute to Workshop and Finalize Workshop results	• Email to BA/BSA formally summarizing the workshop’s outcome / decision.	a. Contributes to workshop b. Finalizes the workshop – ensures preliminary design is acceptable.
1.e	SAP Security Admin	Contribute to Workshop	None	a. Provide any technical assistance – information on addition permissions, RolesDB interactions.

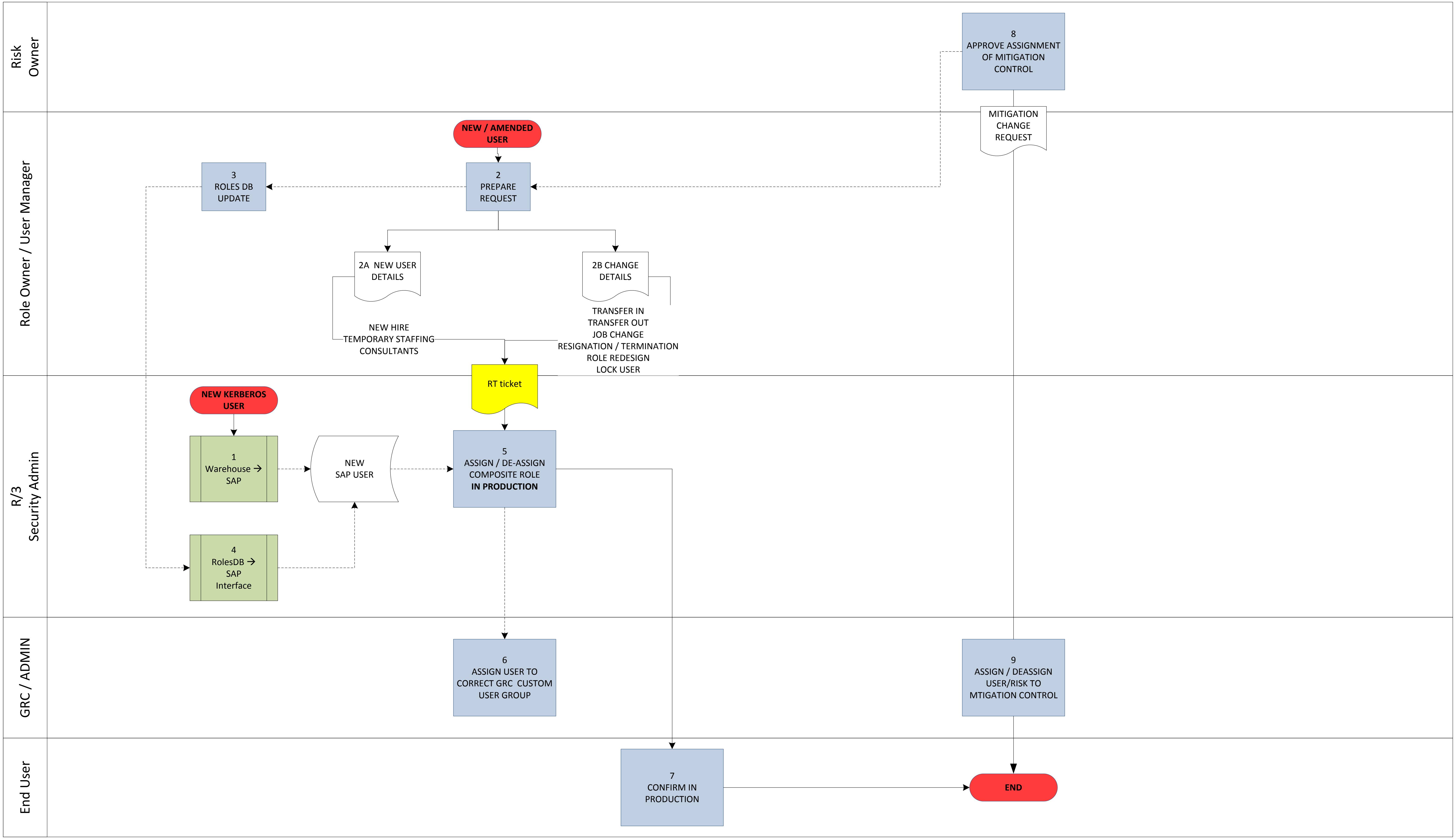
P.2 STEP	**Role**	**Responsibility / Action**	**Output**	**Responsibility / Action**
2	BA/BSA	Design new Mitigation Controls	• Detailed Workshop results with all proposed action items listed and reasons for rejecting alternatives.	**Design** the proposed Mitigation approach and detailed activities required to implement the additional controls : a. New manual processes b. New/amended mitigation control reports c. New/amended SAP enhancements d. Changes to SAP configuration e. Additional Permission-level restrictions
2.a-g	***BA/BSA***	***Mitigation Control development***	• ***New manual process*** • ***New mitigation report with new tcode*** • ***System enhancements*** • ***Changed SAP configuration*** • ***Additional SAP Security permissions***	***See details in following 2.a – g steps***
2.a.i	BA/BSA	SAP Development - Prepare Mini-Spec	• Functional Specification • Test plan	Prepare Functional Mini-Specification for SAP Development : a. new / amended report b. new / amended enhancement. Create or amend a test plan.
2.a.ii	BA/BSA	IMG configuration change - Prepare Mini-Spec	• Functional Specification • Test plan	Prepare Functional Mini-Specification for SAP IMG configuration change Create or amend a test plan.
2.b	BA/BSA	SAP Access Change Request – additional permissions	• FORM : SAP Access Change Request	Prepare SAP Access Change Request – additional permissions Create or amend a test plan.
2.c	BA/BSA	Test configuration and reports	• Test results	Test new / amended configuration and reports

P.2 STEP	**Role**	**Responsibility / Action**	**Output**	**Responsibility / Action**
2.d	IS&T Development or BSA	Develop reports, enhancements and make config changes	• New/amended report • New/amended enhancement • Changed configuration	There are no additional processes here. The standard IS&T processes apply to these.
2.e	SAP Security Admin	• Amend permissions • Add tcodes	• Updated • See Process 3. New Users and User Role Provisioning	For Mitigation-related activities : • Amend permission-level data to restrict existing end users • Add new tcodes for Mitigation reports to user roles
2.f	Role Owner	Implement and document new manual control	• Manual Process documentation • Updated Controls Checklist	Implement and document new manual control. Ensure all new controls which require periodic review are added to any Controls Checklist which may be managed for the business area.
3	BA/BSA	Prepare Mitigation Control (MC) request	• FORM : Mitigation Control Request : MC Definition and/or Assignments	Prepare Mitigation Control (MC) request : a. New / Amended MC definition – with details from Step 2 above. b. New / Amended MC assignments - MC : Risk/User combinations
4	Role Owner	Recommend Mitigation Controls	• Send MC Request – as it should have all the details. • Risk Owner may provide feedback.	Inform Risk Owner of workshop final outcome – confirming the proposed mitigation approach is still valid.
5	Risk Owner	Approve Mitigation Control and Risk/User assignment	Request to add/amend in GRC • Mitigation Control definition • Mitigation Control assignment to Risk/User combination	a. Check final result was as advised from workshop results, review MC definition and assignment. b. Request GRC Administrator to update the GRC system with the new / amended MC definition and new/amended assignments to users.
6	GRC Admin	Enter approved Mitigation Control definition and/or Risk/User assignments.	• Updated MC definition and/or assignments • Automated email for assignment changes	Update GRC system : • Mitigation Control definition and/or • MC assignments to Risk / User combinations

P.2 STEP	Role	Responsibility / Action	Output	Responsibility / Action
7	Role Owner	Periodic : Carry out SOD analysis and Mitigation Control review	• Signed off Checklist and supporting documentation (reports, screen prints etc.)	Role Owner or delegate carry out periodically : a. Where specifically mentioned in Mitigation Controls, confirm that general business control processes– e.g. Bank Reconciliations – are still in place. b. Specific Mitigation Control processes (manual or supported by reports).
8	Risk Owner	Review results of mitigation control processes and signs off checklist.	• Completed and filed checklist and supporting documentation.	a. Review results of mitigation control processes and b. If there is a period review checklist, signs off checklist has been completed for the period under review. c. Additionally, check that any “exceptions” reported were adequately followed up.

Process 3: New Users and User Role Provisioning

MIT SAP Security & GRC Process : 3. New Users & User Role Provisioning



Risk Owner

8 APPROVE ASSIGNMENT OF MITIGATION CONTROL

MITIGATION CHANGE REQUEST

Role Owner / User Manager

NEW / AMENDED USER

2 PREPARE REQUEST

3 ROLES DB UPDATE

2A NEW USER DETAILS

2B CHANGE DETAILS

NEW HIRE
TEMPORARY STAFFING
CONSULTANTS

TRANSFER IN
TRANSFER OUT
JOB CHANGE
RESIGNATION / TERMINATION
ROLE REDESIGN
LOCK USER

R/3 Security Admin

RT ticket

NEW KERBEROS USER

1 Warehouse → SAP

NEW SAP USER

4 RolesDB → SAP Interface

5 ASSIGN / DE-ASSIGN COMPOSITE ROLE **IN PRODUCTION**

GRC / ADMIN

6 ASSIGN USER TO CORRECT GRC CUSTOM USER GROUP

9 ASSIGN / DEASSIGN USER/RISK TO MTIGATION CONTROL

End User

7 CONFIRM IN PRODUCTION

END

Process 3: New Users and User Role Provisioning

The “Role Provisioning” process described here is primarily for the scenario where SAP User access is assigned or amended, within the current role definitions. Of course there can be new roles (see process 1) which would require assignment. Secondarily, for completeness, some additional SAP User administration is briefly included here, and often has to precede the role assignments. Also, the MIT Roles Database is referred to in places, but its detailed administration is not included in this flowchart, nor is Kerberos Id assignment for new hires etc.

The requirement for SAP Role provisioning changes are most often identified during the following business events:

1 Departmental reorganization
2 New or changed job duties for a user – including transfers to different departments / business areas.
3 New hire
4 Temporary Staffing, where SAP access is required.
5 Resignation / termination / semi-permanent leave

Less common situations are:

6 New roles have been defined (see Process 1) - e.g. for new Functionality - which need to be assigned to users
7 Audits, Compliance and other reviews require changes (usually removal of access, which may also require role redesign)
8 General role redesign / tidy-up - triggered from technical reviews or MIT RolesDatabase redesign.
9 Removal of functionality from roles (so usually no SOD risk issues) so they can be assigned more widely.

Additional User provisioning requirements which are not specifically role related:

- New and existing users – new / changed administrative data: name, address, defaults/PIDs, account number, validity period etc.
- Changes to User Group (SAP core) and Custom User Group (in GRC only)
- Lock / unlock user
- Reset password

Note the following points relating to the VPF business areas which have affected the process of SAP access management:

- Typically each person has a unique set of job duties, and a “Composite Roles” is created for this.
  - The Composite Role has a number of “Single Roles” assigned to it.
  - So each VPF business area has a number of single roles – between 5 and 10 – which are combined in different combinations into Composite Roles to reflect the different job duties.
  - Additional “common roles’ can be included in the Composite Role.
  - Where access is provisioned from the MIT Roles database, this access is added to the SAP User as an additional “Profile” and is not adjusting the single or composite roles definitions as such.
- In the cases where there are users with identical access requirements, they have been assigned the same Composite Role.
- There are some VPF User “FireFighter” roles – see **Process 4** – which are used for emergency back-up requirements, rather than building the access into the regular user’s role or amending a user.
- In general, the process of making minor changes to individual user access has been eliminated. There are tested and complete business roles, and these are assigned through Composite Roles. So any requested minor access change would be a role change – see process 1 – unless it was complete assignment or de-assignment of a role in a Composite role.

Roles & Responsibilities for Process 3:

- **Risk Owner** Requests assignment / deassignment of User in GRC Mitigation Control
- **Role Owner / User Manager** Requests new SAP user, assignment / deassignment of roles
  - This includes VPF Roles and IS&T Support roles.
  - Assignment of Users to GRC EAM FireFighter roles is covered in Process 4.
- **SAP R/3 Security Admin** Several tasks :
  - Assignment of roles to composite roles and Composite Roles to Users
  - Performs the maintenance of SAP User admin data
  - Manages MIT custom RolesDatabase interface to SAP User security.
- **GRC Admin** Manager user-related GRC data at the request of the Risk Owner – assignment of Users to MCs

Process 3: New Users and User Role Provisioning - Detailed Steps

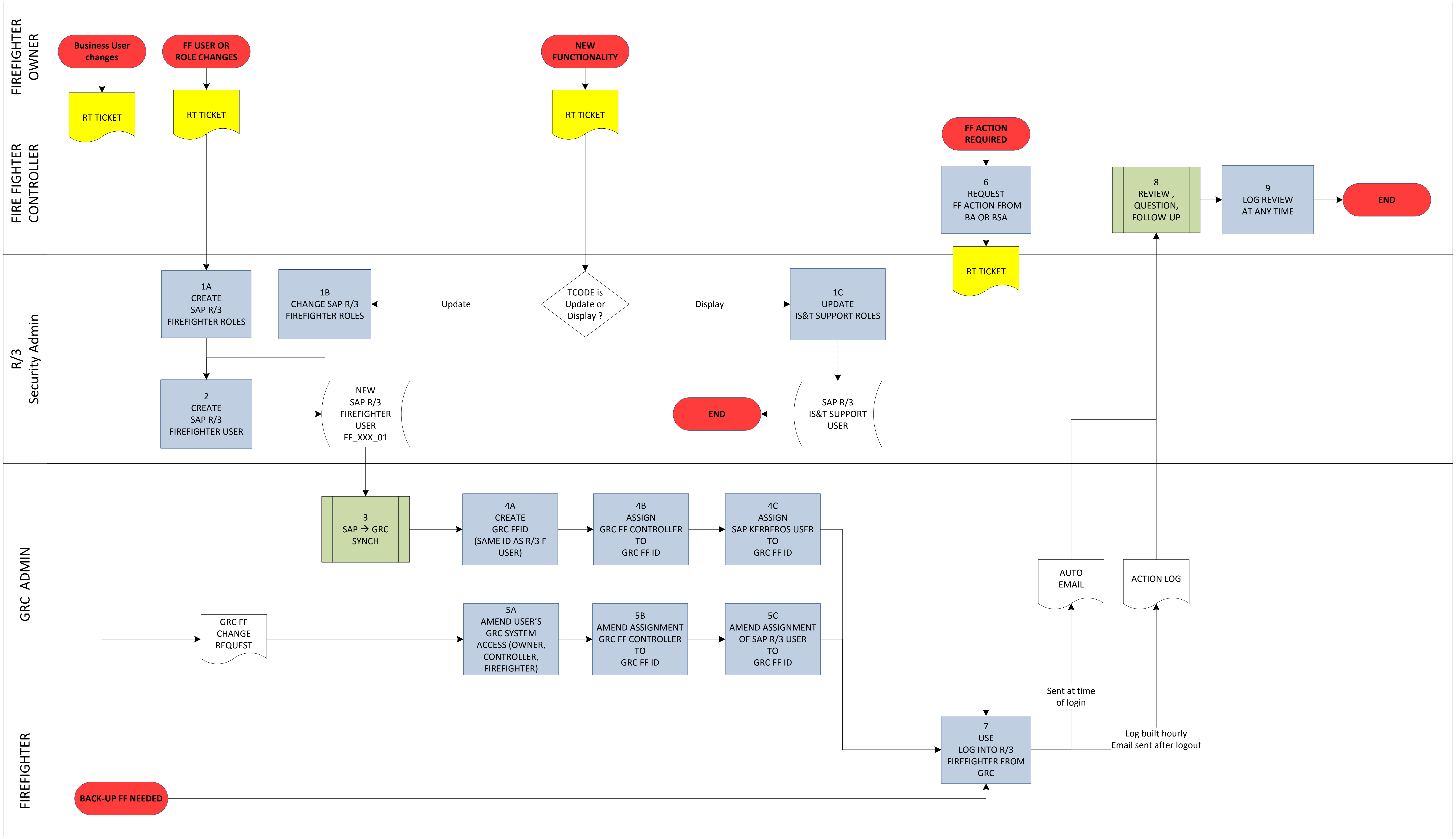
P.3 STEP	Business Role	Responsibility / Action	Output	Details
1a	AUTOMATED	KERBEROS /WAREHOUSE	• New SAP User	• New SAP User automatically created from various sources, including Warehouse. Basic admin information and some basic ESS etc. access profiles are assigned.
2a	Role Owner / User manager	Request new user	• Email / Form with details	• Provide Admin details: Kerberos Id, Name, MIT address, validity period etc. • Provide Role Assignment information: Composite Role or variation of role combinations required. Note: if any role changes were required, this would have gone through Process 1 and 2 first to define the new role, with any SOD analysis as required. • **TEMPORARY STAFFING – may need 2 composite roles – potential SOD.**
2b	Role Owner / User manager	Request user role change	• Email / Form with details	• Provide Role Assignment information: Composite Role or variation of role combinations required. Note: if any role changes were required, this would have gone through Process 1 and 2 first to define the new role, with any SOD analysis as required.
2c	Role Owner / User manager	Request user admin data change	• Email / Form with details	• Provide changes to User Admin data information – rare.
3	User manager	RolesDB provisioning	• Updated RolesDB	• Update RolesDB with required information
4	R/3 Security Admin	RolesDB → SAP interface	• Updated User access	• Any SAP-relevant RolesDB provisioning will result in the SAP User having additional “profiles” assigned, in addition to the profiles generated from the assigned SAP Security roles.

P.3 STEP	**Business Role**	**Responsibility / Action**	**Output**	**Details**
5	R/3 Security Admin	Maintain business-related roles to user	•	• Assign Roles – for VPF, this is now a "Composite Role" which has a number of roles relating to the VPF business area. In some cases, a VPF user is unique and so effectively has a job or user specific composite role. ○ New User : add composite role ○ Transfer In : add composite role (confirm removal of ld composite role) ○ Transfer Out : remove composite role ○ Job Change : remove old Composite / add new Composite ○ Consultants : validity period – ***approval for PRODUCTION access (several IS&T approvers required)*** ○ ***Temporary Staff: potential SOD if two composite roles assigned.*** ○ Termination with Prejudice : Lock immediately
6	GRC Admin	Assign user to GRC Custom User Group	• Updated user assignment	• Assign user to GRC Custom User Group
7	End User	Confirm access	• Email	• Confirm changed access in Production
8	Risk Owner	Approve assignment of GRC MC	• MC change form	• Request assignment of Mitigation Control to Risk User combination.
9	GRC Admin	Update User/Risk -> MC	• GRC updated	• Update assignment of Mitigation Control to Risk User combination.

Process 4: FireFighter Users and Roles

Massachusetts Institute of Technology

MIT SAP Security & GRC Process : 4. FireFighter Users and Roles



FIREFIGHTER OWNER

Business User changes

FF USER OR ROLE CHANGES

NEW FUNCTIONALITY

RT TICKET

RT TICKET

RT TICKET

FIRE FIGHTER CONTROLLER

FF ACTION REQUIRED

6 REQUEST FF ACTION FROM BA OR BSA

8 REVIEW , QUESTION, FOLLOW-UP

9 LOG REVIEW AT ANY TIME

END

R/3 Security Admin

1A CREATE SAP R/3 FIREFIGHTER ROLES

1B CHANGE SAP R/3 FIREFIGHTER ROLES

Update

TCODE is Update or Display ?

Display

1C UPDATE IS&T SUPPORT ROLES

RT TICKET

2 CREATE SAP R/3 FIREFIGHTER USER

NEW SAP R/3 FIREFIGHTER USER FF_XXX_01

END

SAP R/3 IS&T SUPPORT USER

GRC ADMIN

3 SAP → GRC SYNCH

4A CREATE GRC FFID (SAME ID AS R/3 F USER)

4B ASSIGN GRC FF CONTROLLER TO GRC FF ID

4C ASSIGN SAP KERBEROS USER TO GRC FF ID

AUTO EMAIL

ACTION LOG

GRC FF CHANGE REQUEST

5A AMEND USER'S GRC SYSTEM ACCESS (OWNER, CONTROLLER, FIREFIGHTER)

5B AMEND ASSIGNMENT GRC FF CONTROLLER TO GRC FF ID

5C AMEND ASSIGNMENT OF SAP R/3 USER TO GRC FF ID

Sent at time of login

FIREFIGHTER

7 USE LOG INTO R/3 FIREFIGHTER FROM GRC

Log built hourly Email sent after logout

BACK-UP FF NEEDED

Process 4: FireFighter Users and Roles

This section covers the special circumstances where users and roles are created for emergency "FireFighter" use *and for changes to IS&T Support roles*. Where the term "FireFighter" is used here, it relates to the use of the GRC-EAM (Emergency Access Management) functions which have some special features which require administration and monitoring.

The features in use at MIT are:

- Special SAP R/3 FireFighter Users and Roles – typically with limited update functionality. Access rights to the R/3 FF Users are pre-assigned in GRC-EAM to specific business users who need occasional or emergency access to functions which would otherwise create SOD issues if permanently assigned. Some Firefighter Users have roles with more access than others - see the various FFID types described below.
- The firefighter logs into the GRC-EAM system with their SAP Kerberos User ID run the transaction /n GRAC_SPM; they will see the Firefighter launch pad, with the pre-assigned FireFighter user. The firefighter "logs in" to the pre-assigned Firefighter user, which allows them to access SAP R/3 to perform the emergency or back-up business functions. When finished, they log out of their SAP R/3 session, and then log out of SAP GRC.
    - A FFID can be shared, but can only one person can log into it at a time.
    - The FireFighter ID Owner determines the appropriate assignment for the Firefighter ID.
    - The FireFighter Controller for that FFID is notified when it is used
    - The FireFighter User actions are logged and reviewed by FireFighter Controller or Delegate when the Firefighter logs out.
- All SAP Users which are set up for FireFighter usage will be named like "FF_XXX_NN" where XXX = the business area letters (can be a few more characters if needed) and NN is a sequential number. User Type = SERVICE and special role assigned to identify it as a GRC FireFighter (see step 2A). The R/3 GRC Repository Synch job synchronizes R/3 user assignment data with production GRC. The GRC Admin creates a FFID in the NWBC (NetWeaver Business Client) interface with the same id as the R/3 User. All Firefighter users must have their own personal SAP IDs manually created in GRC. The different

FFID types have different roles in R/3:

- **Business User FFID:** has limited update transactions, specific to the business areas or job duties for the users being backed-up. This would have SODs when combined with business user's standard role.
- **Business Analyst FFID:** has update transactions with broad business access – roles are either Finance/Logistics or HR/Payroll focused. Will always have SODs are they are broad access to deal with any issues. At MIT these are Composite Roles combining all the standard business roles for the business area.

  - ○ **IS&T BSA FFID and BSA Manager FFID:** has update transactions with broad business access – roles are either Finance/Logistics or HR/Payroll focused.   Will always have SODs are they are broad access to deal with any issues.
  - ○ **IS&T Basis Admin FFID:** has *some special access over and above what they already have.*
  - ○ **IS&T Developer FFID and Developer Manager FFID:** has update transactions with broad business access to deal with any issues – and these will always have SODs.   The roles are either Finance/Logistics or HR/Payroll focused and some Developer FFIDs and the Developer Manager FFID include EDI and Workflow support access,
- **Note: Support User in IS&T BSA:** has display only transactions with broad business access, so should never have an SOD for these.
- **Note: Regular BA users:** display only transactions with broad business access, so should never have an SOD for these.

After the initial FireFighter process set-up, the ongoing administration consists of:

- **More frequently**
  - Creation of SAP Kerberos ID in GRC for Firefighters
  - GRC Assignment of SAP Users to FireFighter Ids (adding and removing assignment)
  - SAP R/3 FireFighter Role maintenance – new functionality for the business needs to be added, and discontinued functionality removed.
- **Less frequently**
  - GRC Assignment / de-assignment of FireFighter Ids to FFID Controllers
  - New SAP R/3 FireFighter Users when there are additional FFID Controllers

Some additional MIT-specific background points related to FireFighter design:

- The FireFighter SAP R/3 users do not have Kerberos ids, so they are created by SAP R/3 Security Admin, and no profiles are provisioned through Warehouse or RolesDB.
- So that automated monitoring of BA and BSA FireFighter Id usage can go to the appropriate business manager, separate FireFighter Users have been set up for each business area manager (the FFID Controller). Typically the same role is assigned to several FF R/3 Users, as the BA/BSA needs the same access no matter which manager requested the FireFighter usage.
- Use of FF will require an RT Ticket to be created and justification and details of its usage are documented there.

GRC FireFighter terminology

- **R/3 FireFighter User:** - the R/3 User called up by GRC when the FireFighter requests access via GRC – it cannot be accessed in SAP R/3 directly.
- **FireFighter** - the business user, BA or BSA or BSA Manager or IS&T Developer or IS&T Developer Manager, SAPADM user or SAPADM manager who needs access to the R/3 FireFighter User in Production.
- **FireFighter Id** - the GRC object used to control access to the R/3 FireFighter User – it links the R/3 FireFighter User to the FireFighter.
- **FireFighter's R/3 Role Owner** - like the standard R/3 Security Role Owner – will usually be the same as the FireFighter ID Owner.
- **FireFighter ID Owner** - requests/approves GRC assignment of Users to FF Ids. *GRC functionality for FFID Owner is not being used.*
- **FireFighter ID Controller** - informed of FF usage at start and end of session and reviews logs. Typically the Business Role Owner.
- ***FireFighter ID Controller's Delegate*** *Not currently being used at MIT.*

Roles & Responsibilities for Process 4:

- **SAP R/3 Security Admin** Maintain FireFighter and Support Users in SAP, and their assignment to MIT personnel
- **GRC Admin** Maintain FFIDs and assignments - also can maintain R/3 Users.
- **FFID Owner** Requests user assignment to FFIDs and any new FFIDs
  - For VPF, this varies per business area. May be Risk Owner or Role Owner.
  - For IS&T, these are Frank and Siobhan
- **FFID Controller** Review FFID actions.
  - For VPF, this is Controller or Director level. May be Role Owner or Business Area manager.
  - For IS&T this is Bart
- **FireFighter**

Process 4: FireFighter Users and Roles - Detailed Steps

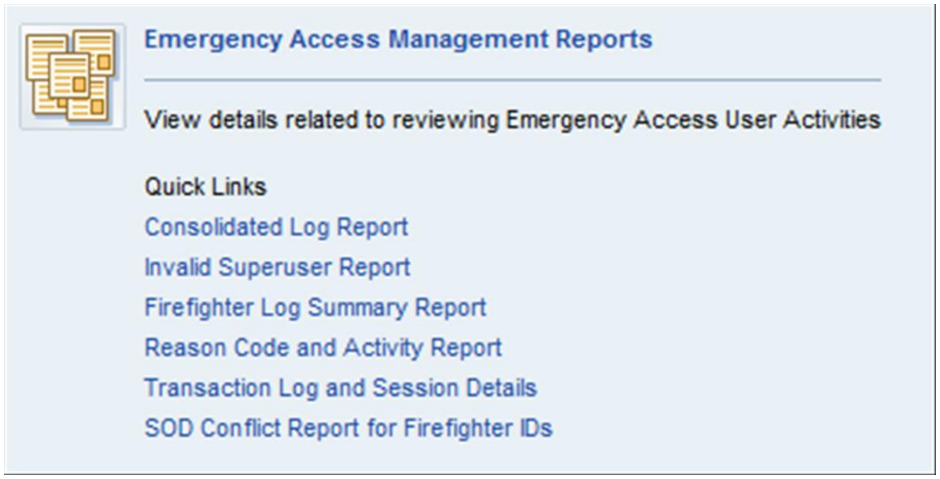
P.4 STEP	Business Role	Responsibility / Action	Output	Details
1a	R/3 Security Admin	Create FireFighter Roles	• Roles	There are several types of FF roles : • Business Analysts (BA) • IS&T Business System Analysts (BSA) • IS&T Basis Role • IS&T Developers • IS&T Managers • Business users – limited and specific to each requirement (mostly for back-up) The Role Provisioning process (requesting, approving, auctioning, and testing) is no different to any other role – except that SOD issues are not relevant.
1b	R/3 Security Admin	Maintain FireFighter Roles	• Roles updated	Changes should be infrequent, once the system matures : • Add new Functionality • Remove The Role Provisioning process (requesting, approving, auctioning, and testing) is no different to any other role – except that SOD issues are not relevant. There are special designated approvers for changes to FF roles : • *FFID Owner for BAs* • *FFID Owner for IS&T FireFighters* • *FFID Owner for Business FF = Risk Owner of the business area?*
1c	R/3 Security Admin	Maintain IS&T Support Roles	• Roles updated	IS&T Support Roles • These are Display only roles and are in daily use. • They are not part of the “FireFighter” control process. The Role Provisioning process (requesting, approving, auctioning, and testing) is no different to any other role. There must be NO SOD ISSUES in these roles.

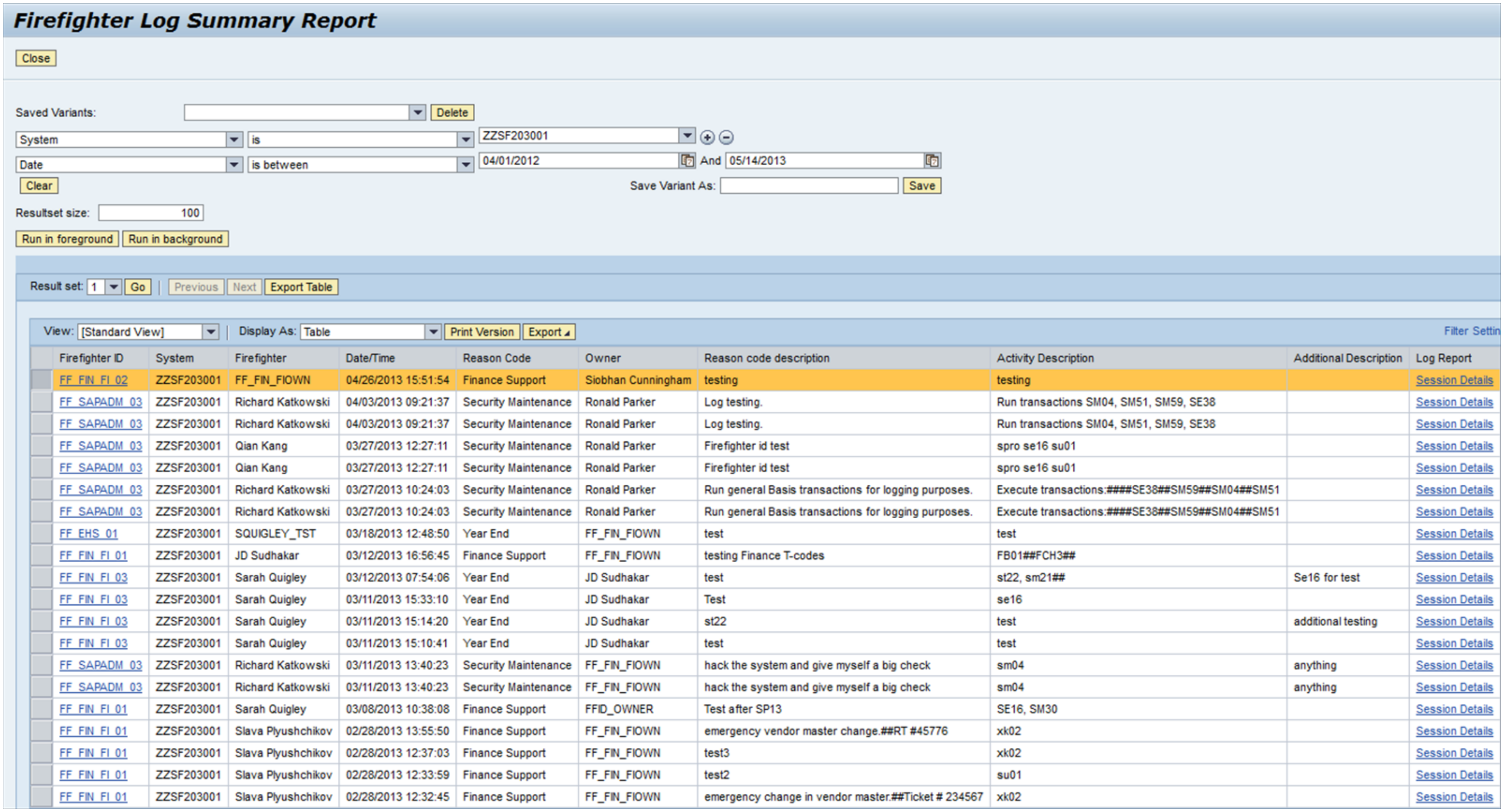
P.4 STEP	Business Role	Responsibility / Action	Output	Details
2A	R/3 Security Admin	Maintain FireFighter Users	• Users updated • Business Roles assigned • FireFighter role assigned	The R/3 FireFighter Users are generic in that they are assigned to anyone / more than one person via the GRC system. See Step 4.c New R/3 FireFighter Users will be infrequent - perhaps if there is a whole new area of SAP implemented. • Creation of R/3 FF Users is a manual process (cf. regular Kerberos R/3 users are automatically created during MIT on-boarding.) • The R/3 FireFighter User is assigned the special FireFighter role with some RFC access privileges (identified in the GRC system parameter 4010 as Z_SAP_GRAC_EAM_FFID). This identifies the FireFighter R/3 User to GRC as a FireFighter. • Also the User Type = SERVICE, as the login is activated/controlled by a call from the GRC system when the user logs into the FF ID from GRC.
2B	*R/3 Security Admin*	*Lock/Unlock R/3 Users*	• *R/3 User locked or unlocked*	*Like any other R/3 User, the R/3 FireFighter user can have validity periods (not used much at MIT) or can be locked / unlocked to control access.* • *Users are created in Production – so may be locked until needed.*
3	Basis / GRC	Synch systems : SAP to GRC Repository	• GRC = ECC	An automated process makes sure that the GRC system has up-to-date information from SAP R/3 about roles and users. In this case, specific to FireFighters : • The FireFighter R/3 User needed for step 4.A • The Business R/3 Users are needed for step 4A, 4B and 4C • Any new FireFighter roles – in case GRC-ARA analysis is needed (not at MIT).

P.4 STEP	**Business Role**	**Responsibility / Action**	**Output**	**Details**
4A	GRC Admin	Maintain FFIDs	- FF Ids in GRC-EAM	The GRC FFID attribute settings are central to the control and usage of the FireFighter roles in R/3 - In this step the following updates are made in the GRC-EAM system : ○ The FFID is created– with the same naming convention as the SAP R/3 FireFighter user - like FF_FAR_01. ○ The FFID is assigned to the matching SAP R/3 FireFighter User. ○ The FFID is assigned to an FFID Owner – at MIT this is mostly for information only, as the FFID Owner will not be logging in to GRC to maintain user assignment. ○ Additional information for the FFID can be added if required. The GRC FFIDs are mostly set up during the initial phase of the GRC project, and is related to the business organization, so additions will be less frequent.
4B	GRC Admin	Assign FFID Controllers NOTE : FFID Controller "Delegates" not currently used at MIT	- FF Id assigned to FFID Controller (SAP R/3 User)	In this step an FFID is assigned an FFID Controller (which is another R/3 User) : - The FFID Controller is emailed when the FFID user logs in and logs out – with a link to the FFID detailed usage logs after logging out. - For the VPF business areas, the VPF business managers are the FFID Controllers – for the Business FF, BA FF and BSA FF. - For non-VPF areas, there are FFID Controllers in IS&T so that the BSA FFID usage can be monitored.
4C	GRC Admin	Assign FFID to SAP Users	- FF Id assigned to SAP R/3 Users	In this step an FFID is assigned the R/3 User who is the actual FF person - and this is a different R/3 user than the FFID's Controller. - An FFID can be assigned to several R/3 users - An R/3 User can be assigned to several FFIDs - The assignment can be for a limited period.

P.4 STEP	Business Role	Responsibility / Action	Output	Details
5A	GRC Admin	Grant appropriate access to the GRC system	• Assign GRC access rights to R/3 Users	There are several types of GRC users who need specific access privileges in GRC – predefined in GRC access roles : a. FFID Owners (although MIT is not really using this feature) – GRC Role = Z_FFID_OWNER b. FFID Controllers GRC Role = Z_FF_CONTROLLER c. FFID Users – those who have to log in to the FFID. GRC Role = Z_FF_ENDUSER d. Other MIT users who may want to run FF-related reports. This data will typically need updating as users change their job positions or when they join / leave the MIT workforce.
5B	GRC Admin	Amend FFID / Controller assignment	• FF Id assigned to different Controller	This assignment will typically need updating where the FFID Controller changes jobs, leaves MIT or if there is a Departmental Reorganization. ○ Change the assignment (an FFID has only one Controller) An RT Ticket is required, plus a new Form – GRC FireFighter ID Assignment Change request. *Note: if this reassignment is made after the event, the FFID logs can still be reviewed through FRC-EAM reporting.*
5C	GRC Admin	Amend FFID / SAP User assignment	• FF Id assigned to different SAP Users	This assignment in GRC will need updating when the R/3 User changes jobs, leaves MIT or perhaps if there is a Departmental Reorganization. ○ Add an assignment – with a future “Valid From” date if known in advance. ○ Remove an assignment ad amend the “Valid To” date if move is know in advance? An RT Ticket is required, plus a new Form – GRC FireFighter ID Assignment Change request.

P.4 STEP	Business Role	Responsibility / Action	Output	Details
6	FireFighter Controller / Business Manager	Request FF usage	• RT ticket	An RT Ticket is required where the business manager has requested support from BA/BSA etc. - with justification and details of expected usage.
7a	SAP User	Log into the FFID	• RT ticket, if not already created • Email to FFID Controller	The Business FireFighters performing back-up / unusual work do not need a ticket. Otherwise there is an RT Ticket either from step 6. or created by the BA or BSA based on email from the Business Manager (FireFighter Controller). Also, a "Reason Code" is selected when logging in to the FFID, and additional information can be entered by the FireFighter. When the FFID is used, • an email is sent immediately to the FFID Controller • an activity log is started and is updated hourly
7b	SAP User	Log out of the FFID		Where there is an RT Ticket, any additional / unexpected FireFighter usage will be noted on the RT ticket by the FireFighter. When the user logs out of the FFID, within the hour the activity log is updated and an email is sent to the FFID Controller with a link to the Activity Log for that FFID and time period it was used.

P.4 STEP	Business Role	Responsibility / Action	Output	Details
8	FFID Controller	Review, Question, Follow-up	• Approval or action list	• The email from GRC to the FFID Controller is a request for approval and a link to the details action log. • Action logs are reviewed – looking for unusual activities in general, and activities inconsistent with the ○ Business FireFighters have limited, pre-approved access, so it is unlikely that anything will result from review of the logs alone. ○ For the other FireFighters, any master data changes or financial postings need to be reviewed and approved – a common technique for this is printing the log and initialing each line that was verified. In SAP the master data change history and financial documents are available for review at any point afterwards. • The reviewer's options are to : ○ Request the FireFighter to provide more details ○ Approve the whole log. ○ "Hold" the log – i.e. not approve it yet. The work item will stay in their GRC inbox for subsequent processing. • Additional notes can be made on the log for any action to be taken.
9	Reporting Actions	Review FFID usage and Activity Logs at any time	• Reports – some of the standard reports will be used – Log Summary and Consolidated Log (see next two pages)	 Emergency Access Management Reports View details related to reviewing Emergency Access User Activities Quick Links Consolidated Log Report Invalid Superuser Report Firefighter Log Summary Report Reason Code and Activity Report Transaction Log and Session Details SOD Conflict Report for Firefighter IDs



Firefighter Log Summary Report

Saved Variants:

System | is | ZZSF203001

Date | is between | 04/01/2012 And 05/14/2013

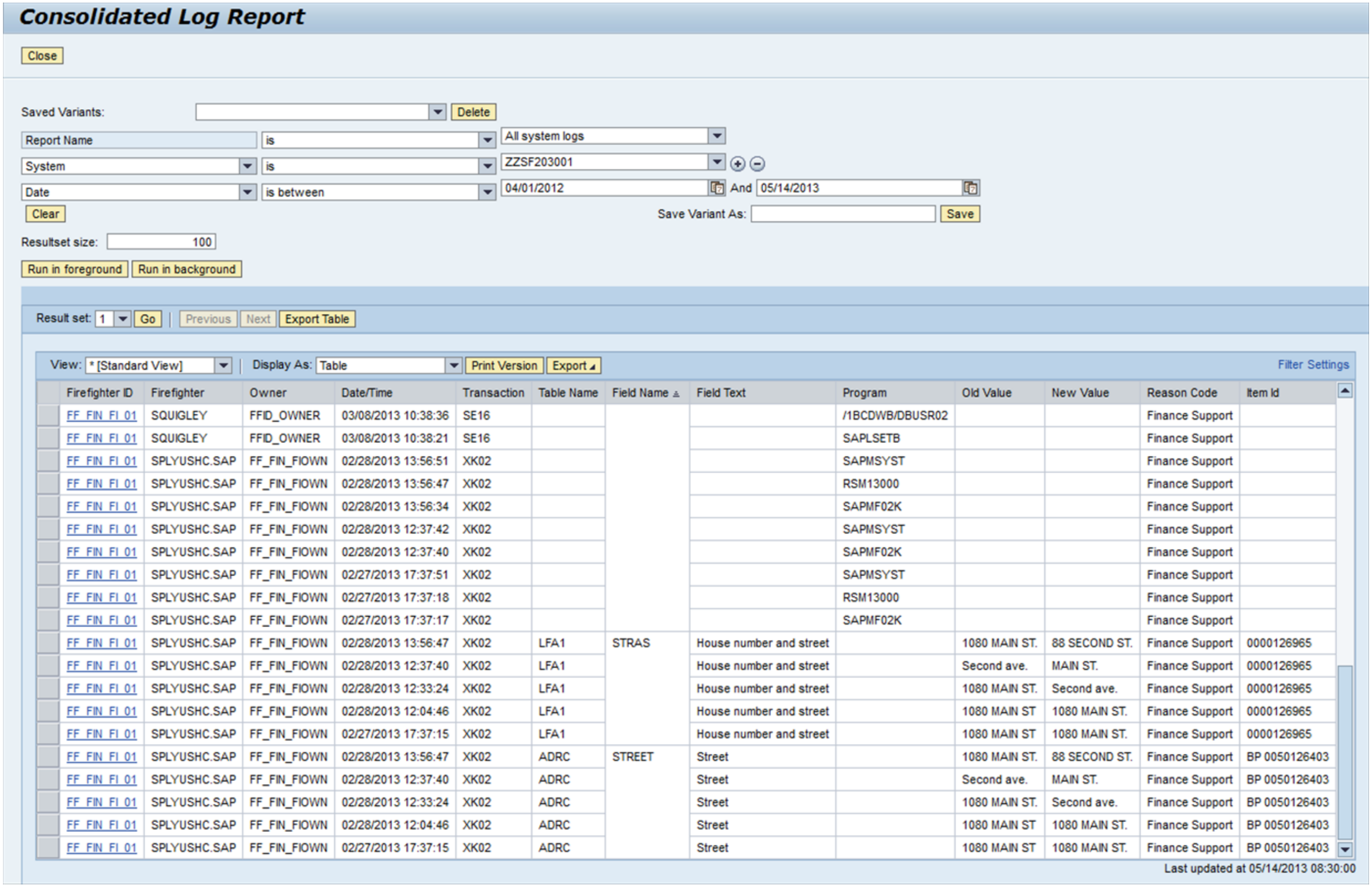
Save Variant As:

Resultset size: 100

Result set: 1

View: [Standard View] | Display As: Table

Firefighter ID	System	Firefighter	Date/Time	Reason Code	Owner	Reason code description	Activity Description	Additional Description	Log Report
FF_FIN_FI_02	ZZSF203001	FF_FIN_FIOWN	04/26/2013 15:51:54	Finance Support	Siobhan Cunningham	testing	testing		Session Details
FF_SAPADM_03	ZZSF203001	Richard Katkowski	04/03/2013 09:21:37	Security Maintenance	Ronald Parker	Log testing.	Run transactions SM04, SM51, SM59, SE38		Session Details
FF_SAPADM_03	ZZSF203001	Richard Katkowski	04/03/2013 09:21:37	Security Maintenance	Ronald Parker	Log testing.	Run transactions SM04, SM51, SM59, SE38		Session Details
FF_SAPADM_03	ZZSF203001	Qian Kang	03/27/2013 12:27:11	Security Maintenance	Ronald Parker	Firefighter id test	spro se16 su01		Session Details
FF_SAPADM_03	ZZSF203001	Qian Kang	03/27/2013 12:27:11	Security Maintenance	Ronald Parker	Firefighter id test	spro se16 su01		Session Details
FF_SAPADM_03	ZZSF203001	Richard Katkowski	03/27/2013 10:24:03	Security Maintenance	Ronald Parker	Run general Basis transactions for logging purposes.	Execute transactions:####SE38##SM59##SM04##SM51		Session Details
FF_SAPADM_03	ZZSF203001	Richard Katkowski	03/27/2013 10:24:03	Security Maintenance	Ronald Parker	Run general Basis transactions for logging purposes.	Execute transactions:####SE38##SM59##SM04##SM51		Session Details
FF_EHS_01	ZZSF203001	SQUIGLEY_TST	03/18/2013 12:48:50	Year End	FF_FIN_FIOWN	test	test		Session Details
FF_FIN_FI_01	ZZSF203001	JD Sudhakar	03/12/2013 16:56:45	Finance Support	FF_FIN_FIOWN	testing Finance T-codes	FB01##FCH3##		Session Details
FF_FIN_FI_03	ZZSF203001	Sarah Quigley	03/12/2013 07:54:06	Year End	JD Sudhakar	test	st22, sm21##	Se16 for test	Session Details
FF_FIN_FI_03	ZZSF203001	Sarah Quigley	03/11/2013 15:33:10	Year End	JD Sudhakar	Test	se16		Session Details
FF_FIN_FI_03	ZZSF203001	Sarah Quigley	03/11/2013 15:14:20	Year End	JD Sudhakar	st22	test	additional testing	Session Details
FF_FIN_FI_03	ZZSF203001	Sarah Quigley	03/11/2013 15:10:41	Year End	JD Sudhakar	test	test		Session Details
FF_SAPADM_03	ZZSF203001	Richard Katkowski	03/11/2013 13:40:23	Security Maintenance	FF_FIN_FIOWN	hack the system and give myself a big check	sm04	anything	Session Details
FF_SAPADM_03	ZZSF203001	Richard Katkowski	03/11/2013 13:40:23	Security Maintenance	FF_FIN_FIOWN	hack the system and give myself a big check	sm04	anything	Session Details
FF_FIN_FI_01	ZZSF203001	Sarah Quigley	03/08/2013 10:38:08	Finance Support	FFID_OWNER	Test after SP13	SE16, SM30		Session Details
FF_FIN_FI_01	ZZSF203001	Slava Plyushchikov	02/28/2013 13:55:50	Finance Support	FF_FIN_FIOWN	emergency vendor master change.##RT #45776	xk02		Session Details
FF_FIN_FI_01	ZZSF203001	Slava Plyushchikov	02/28/2013 12:37:03	Finance Support	FF_FIN_FIOWN	test3	xk02		Session Details
FF_FIN_FI_01	ZZSF203001	Slava Plyushchikov	02/28/2013 12:33:59	Finance Support	FF_FIN_FIOWN	test2	su01		Session Details
FF_FIN_FI_01	ZZSF203001	Slava Plyushchikov	02/28/2013 12:32:45	Finance Support	FF_FIN_FIOWN	emergency change in vendor master.##Ticket # 234567	xk02		Session Details



Consolidated Log Report

Saved Variants:

Report Name	is	All system logs
System	is	ZZSF203001
Date	is between	04/01/2012 And 05/14/2013

Resultset size: 100

Result set: 1

View: * [Standard View]

Display As: Table

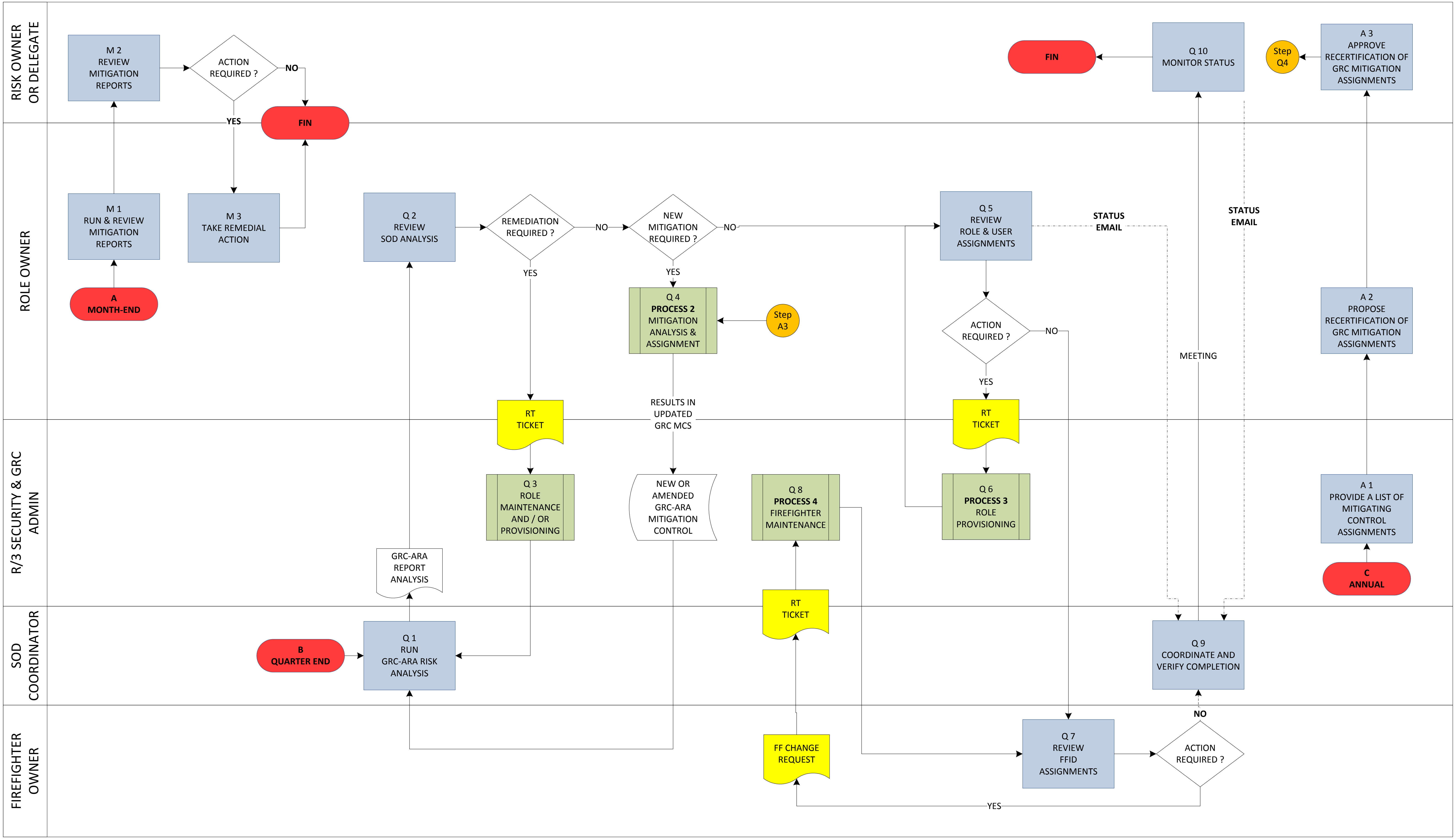
Firefighter ID	Firefighter	Owner	Date/Time	Transaction	Table Name	Field Name	Field Text	Program	Old Value	New Value	Reason Code	Item Id
FF_FIN_FI_01	SQUIGLEY	FFID_OWNER	03/08/2013 10:38:36	SE16				/1BCDWB/DBUSR02			Finance Support	
FF_FIN_FI_01	SQUIGLEY	FFID_OWNER	03/08/2013 10:38:21	SE16				SAPLSETB			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 13:56:51	XK02				SAPMSYST			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 13:56:47	XK02				RSM13000			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 13:56:34	XK02				SAPMF02K			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 12:37:42	XK02				SAPMSYST			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 12:37:40	XK02				SAPMF02K			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/27/2013 17:37:51	XK02				SAPMSYST			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/27/2013 17:37:18	XK02				RSM13000			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/27/2013 17:37:17	XK02				SAPMF02K			Finance Support	
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 13:56:47	XK02	LFA1	STRAS	House number and street		1080 MAIN ST.	88 SECOND ST.	Finance Support	0000126965
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 12:37:40	XK02	LFA1		House number and street		Second ave.	MAIN ST.	Finance Support	0000126965
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 12:33:24	XK02	LFA1		House number and street		1080 MAIN ST.	Second ave.	Finance Support	0000126965
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 12:04:46	XK02	LFA1		House number and street		1080 MAIN ST	1080 MAIN ST.	Finance Support	0000126965
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/27/2013 17:37:15	XK02	LFA1		House number and street		1080 MAIN ST	1080 MAIN ST.	Finance Support	0000126965
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 13:56:47	XK02	ADRC	STREET	Street		1080 MAIN ST.	88 SECOND ST.	Finance Support	BP 0050126403
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 12:37:40	XK02	ADRC		Street		Second ave.	MAIN ST.	Finance Support	BP 0050126403
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 12:33:24	XK02	ADRC		Street		1080 MAIN ST.	Second ave.	Finance Support	BP 0050126403
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/28/2013 12:04:46	XK02	ADRC		Street		1080 MAIN ST	1080 MAIN ST.	Finance Support	BP 0050126403
FF_FIN_FI_01	SPLYUSHC.SAP	FF_FIN_FIOWN	02/27/2013 17:37:15	XK02	ADRC		Street		1080 MAIN ST	1080 MAIN ST.	Finance Support	BP 0050126403

Last updated at 05/14/2013 08:30:00

Process 5: Periodic Compliance Reviews

Massachusetts Institute of Technology

MIT SAP Security & GRC Process : 5. Periodic Compliance Reviews



RISK OWNER OR DELEGATE

M 2 REVIEW MITIGATION REPORTS

ACTION REQUIRED ?

NO

YES

FIN

FIN

Q 10 MONITOR STATUS

Step Q4

A 3 APPROVE RECERTIFICATION OF GRC MITIGATION ASSIGNMENTS

ROLE OWNER

M 1 RUN & REVIEW MITIGATION REPORTS

A MONTH-END

M 3 TAKE REMEDIAL ACTION

Q 2 REVIEW SOD ANALYSIS

REMEDIATION REQUIRED ?

NO

YES

NEW MITIGATION REQUIRED ?

NO

YES

Q 4 PROCESS 2 MITIGATION ANALYSIS & ASSIGNMENT

Step A3

RESULTS IN UPDATED GRC MCS

Q 5 REVIEW ROLE & USER ASSIGNMENTS

STATUS EMAIL

STATUS EMAIL

ACTION REQUIRED ?

NO

YES

MEETING

A 2 PROPOSE RECERTIFICATION OF GRC MITIGATION ASSIGNMENTS

RT TICKET

RT TICKET

R/3 SECURITY & GRC ADMIN

Q 3 ROLE MAINTENANCE AND / OR PROVISIONING

NEW OR AMENDED GRC-ARA MITIGATION CONTROL

Q 8 PROCESS 4 FIREFIGHTER MAINTENANCE

Q 6 PROCESS 3 ROLE PROVISIONING

A 1 PROVIDE A LIST OF MITIGATING CONTROL ASSIGNMENTS

C ANNUAL

GRC-ARA REPORT ANALYSIS

RT TICKET

SOD COORDINATOR

B QUARTER END

Q 1 RUN GRC-ARA RISK ANALYSIS

Q 9 COORDINATE AND VERIFY COMPLETION

NO

FIREFIGHTER OWNER

FF CHANGE REQUEST

Q 7 REVIEW FFID ASSIGNMENTS

ACTION REQUIRED ?

YES

Process 5: Periodic Compliance Reviews

This section covers the different activities which are periodically carried out to ensure the mitigation controls are in place and the various access-related and mitigation-related user assignments are still valid.

1. **Monthly** : **Operation and verification of Mitigation Controls,** including **:**

   1.1. Reports specifically designed to provide mitigation control for SOD issues or monitoring Critical Actions

   1.2. Other general business controls (typically reports) which were incorporated in the Mitigation Control definition.

2. **Quarterly** : **Access Analysis ,** including **:**

   2.1. GRC-ARA - reviewing Access Risk Analysis (SOD and Critical Action) reports

   2.2. GRC & R/3 - checking User / Role and Role / User assignments and Single Role / Composite Role assignments

   2.3. GRC-ARA - checking User / Risk to Mitigation Control assignments

   2.4. GRC-EAM - checking FireFighter and FireFighter Controller assignments

3. **Annual** : recertification of GRC Mitigation Controls

   3.1. GRC-ARA **-** recertification of GRC Mitigation Controls definitions

Roles & Responsibilities for Process 5:

- **SAP R/3 Security Admin** Maintain FireFighter and Support Users in SAP, and their assignment to MIT personnel
- **GRC Admin** Assist in the review of FFIDs assignments and Mitigating Control Assignments.
- **FFID Owner** Ensure all FFIDs are correctly assigned to Controllers and to FireFighters (Business, BA, BSA, IS&T Manager, etc.)
- **Role Owner** Ensure all “owned” roles assignments are valid, and all users for that business area have appropriate roles
- **Risk Owner** Check that mitigation controls are in place and operating effectively.
- **SOD Coordinator** Execute GRC-ARA reports and provide interpretation to Role Owner and Risk Owner.

Process 5: Periodic Compliance Reviews - Detailed Steps

P.5 STEP	**Business Role**	**Responsibility / Action**	**Output**	**Details**
M	**MONTHLY**			
M1	ROLE OWNER	Review mitigation reports	• Mitigation reports	• Mitigation reports may be specific for GRC issues or general (existing for the business). • The reports may be executed by different people, but the Role Owner / Business Area manager brings them all together and checks for explanations and follow-up actions. • The assumption is that the Mitigation Control report identified some unusual activity (master data creation/changes and/or financial postings). This would be followed up by Role owner to determine if it was ○ unusual but not an issue ○ a mistake which may or may not need correcting / reversing / reposting ○ a deliberate attempt
M2	RISK OWNER	Ensure all mitigation controls are in place and functioning	• Signed-off checklist • Email to SOD Coordinator	• Role owner (usually a business area manager) or delegates run the Mitigation Control reports for the SAP users in their business area. These list out, per user, any unusual activity related to the specific SOD risk.

P.5 STEP	**Business Role**	**Responsibility / Action**	**Output**	**Details**
M3	ROLE OWNER	Take remedial action	Depends on the issue	• Role owner and Risk Owner decide on any remedial action. This may include : ○ Correcting / reversing / reposting data ○ Better training / job aids ○ Amending the Mitigation Control report to filter out the exact item if it is "not so unusual". ○ Worst case : investigate the historical posting activity of the user
Q	**QUARTERLY**			
Q1	SOD COORDINATOR	Execute and interpret the GRC-ARA risk analysis reports	• GRC-ARA report • Analysis interpretation	• Execute **GRC-ARA Report 12** - **Risk Analysis – User level** for each User Group or for each Custom User Group – to show any unmitigated risks ○ Note: use option "Show All Objects" to ensure all users are listed – with or without violation. • Prepare a summary document providing interpretation of any SOD or Critical Risk results. • If this is a new issue, also determine what has changed in the user's access to trigger this. • Assist Risk Owner with interpretation of the four recommended Access Dashboard Reports: ○ GRC Report 1 – Risk Violations ○ GRC Report 2 – User Analysis ○ GRC Report 3 – Violations Comparisons ○ GRC Report 4 – Access Rule library

P.5 STEP	Business Role	Responsibility / Action	Output	Details
Q2	ROLE OWNER	Review analysis and initiate action	• Sign-off • Request for action where required • Email final status to SOD Coordinator	• Provide a sign-off where there were no unmitigated risks (i.e. a nil report) • Assist the SOD Coordinator to review any new issues which would have occurred because of deliberate or accidental changes : ○ User has new roles assigned (e.g. their composite role has a new role assigned) ○ One of the user's roles has new actions or permissions ○ User has new profiles from RolesDatabase • Initiate any request for : ○ Role amendments ○ Role provisioning amendments ○ Mitigation Control creation and assignment to Risk/User.
Q3	R/3 SECURITY ADMIN	Role Maintenance Role Provisioning	• Amended roles or composite roles • Amended user/role assignments	See GRC Process 3 for details.
Q4	ROLE OWNER RISK OWBER BA AND BSA GRC ADMIN	GRC Mitigation Control definition , approval, maintenance and assignment	• New or existing Mitigation Controls defined and assigned in GRC	See GRC Process 2 for details, including : • Definition, review and approval (business side) • Creating a new GRC Mitigation Control definition in GRC • Assigning the Mitigation Control to the Risk / User combination.
Q 5	ROLE OWNER	Validate role and user assignments	• GRC reports • If required, request for role provisioning change	• NOTE : MONTHLY FOR NEW SYSTEM – MOVE TO QUARTERLY • Several GRC and R/3 SUIM reports will be used for this: ○ Roles for a User ○ Users for a Role
Q 6	R/3 SECURITY ADMIN	Amend role provisioning to user	• Amended user access	See details of Process 3: New Users and User Role Provisioning

P.5 STEP	**Business Role**	**Responsibility / Action**	**Output**	**Details**
Q 7	FIRE FIGHTER ID OWNER	Confirm FFID assignments to Controllers and FireFighters	• Confirmation of assignments • If required, request to amend assignments	• GRC-EAM Reports ○ FFID – controller assignment (business manager) ○ FFID – user assignment (business user, BA, BSA, BSA manager, Developer etc.) • A change request will be need for any changes : ○ FFID Controllers may have transferred / resigned / retired ○ Firefighters may have transferred / resigned / retired
Q 8	GRC ADMIN	Amend FFID assignments	• Report showing updated, correct assignments	• See GRC Process 4: FireFighter Users and Roles.
Q9	SOD COORDINATOR	Quarterly GRC Review Status & Closure	• Email to Risk Owners	• Summary of results and action items (closed or still open) for the review – per risk owner.
Q10	RISK OWNER	Status monitoring	N/A	• Maintain awareness of status of the review. • Monitor the overall situation with the four recommended Access Dashboard Reports (assisted by SOD Coordinator) : ○ GRC Report 1 – Risk Violations ○ GRC Report 2 – User Analysis ○ GRC Report 3 – Violations Comparisons ○ GRC Report 4 – Access Rule library
A	**ANNUAL**			
A1	GRC ADMIN	Provide information on MC assignments	• Risk / User → Mitigation Control report	• Generate the Risk / User → Mitigation Control report – per Risk Owner ○ GRC-ARA Report 11a Mitigation Control Report = List ○ *GRC-ARA Report 11b Mitigated Object Report* ▪ *Report by User / User Group* ○ GRC-ARA Report 12 Risk Analysis – User level ▪ Run with option showing Invalid users assignments (MC assigned but no longer have the risk).

P.5 STEP	**Business Role**	**Responsibility / Action**	**Output**	**Details**
A2	ROLE OWNER	Review and propose recertification	•	• Identify any MCs that are no longer in place - rare • Identify any assignments that are no longer valid – these will not be recertified – should be unusual, but could be due to job transfers / resignations not fully processed. • Propose the recertification list to the Risk Owner
A3	RISK OWNER		•	• Review and approve recertification list. • Advise GRC Admin to recertify the MCs

GRC Reporting

Job Aids

PURPOSE OF THIS DOCUMENT

Procedures on execution of each of the GRC Reports in scope for Business Analysts are documented in reporting Job Aids. The Job Aid for each report provides details on execution for each step of the report. For some reports, multiple report execution scenarios have been identified.

CONTENTS

Job Aid 01 Risk Violations

USE

This report can be used to gain insight into MIT’s overall exposure to risk. The report provides an overview of risk violations across all MIT ECC systems.

INFORMATION

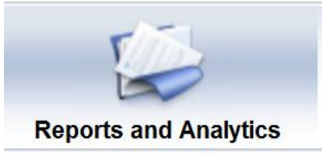
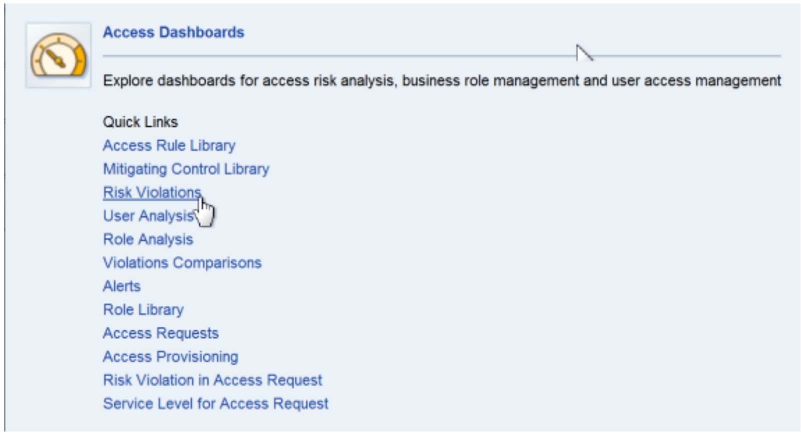
Risk count by risk level and process.

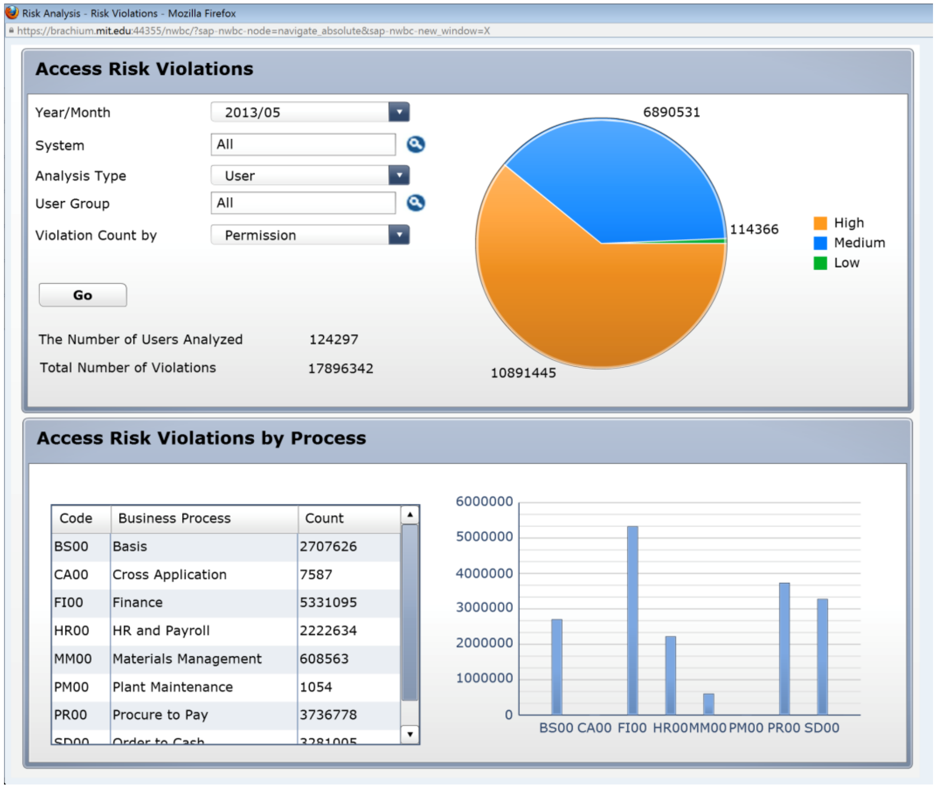
RELATED PROCESSES

- Process 5: Periodic Compliance Reviews

SPECIFIC SCENARIOS

- Step 14A: Analyze report data by Risk Level. (Pie Chart)
- Step 14B: Analyze report data by Business Process. (Table)
- Step 14C: Analyze report data by Business Process. (Bar Graph)

Step	Description	Screenshot
1	Navigate to the ‘Reports and Analytics’ tab.	
2	Click on the ‘Risk Violations’ report located in the ‘Access Dashboards’ section.	 Access Dashboards Explore dashboards for access risk analysis, business role management and user access management Quick Links Access Rule Library Mitigating Control Library Risk Violations User Analysis Role Analysis Violations Comparisons Alerts Role Library Access Requests Access Provisioning Risk Violation in Access Request Service Level for Access Request

3	The report will show risk violations information for the latest period, across all systems (to which GRC is connected) and user groups, at the user level. The count will be given by permission (i.e. each instance of a violation will be counted, even if it is a repeated violation for a user). The report data must be appropriately filtered to provide information that can be of use to MIT.	

Risk Analysis - Risk Violations - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Access Risk Violations

Year/Month 2013/05

System All

Analysis Type User

User Group All

Violation Count by Permission

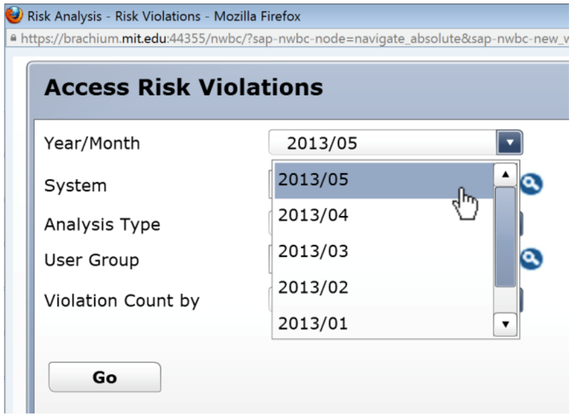
Go

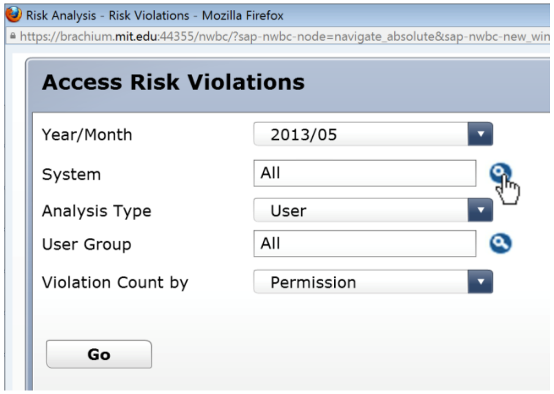
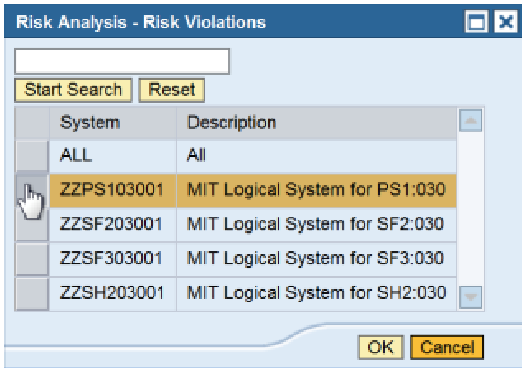
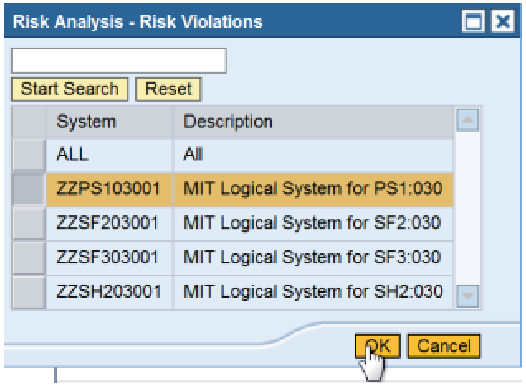
The Number of Users Analyzed 124297

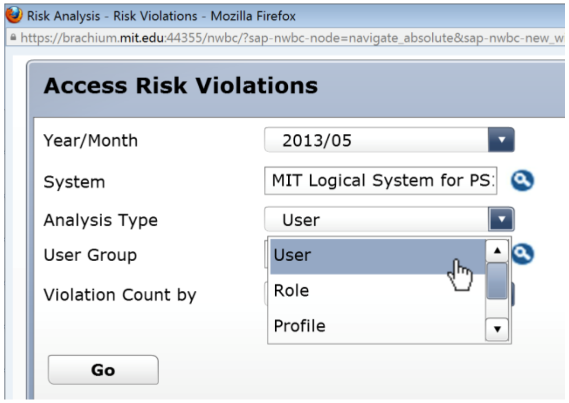
Total Number of Violations 17896342

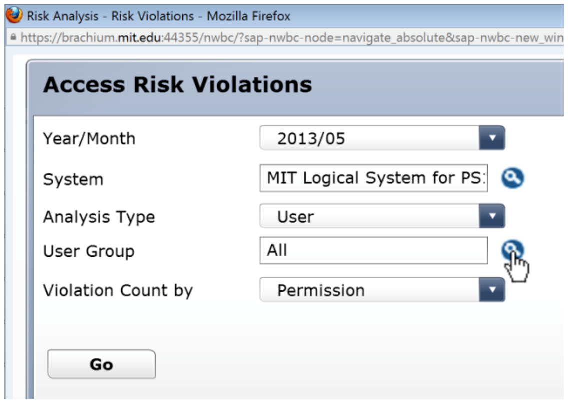
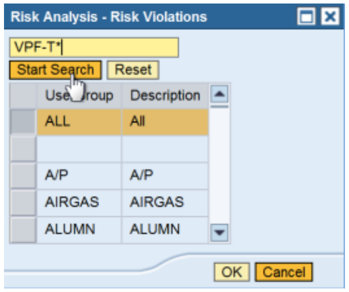
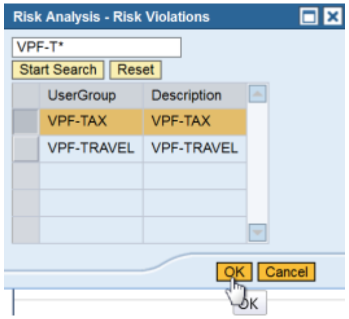
Access Risk Violations by Process

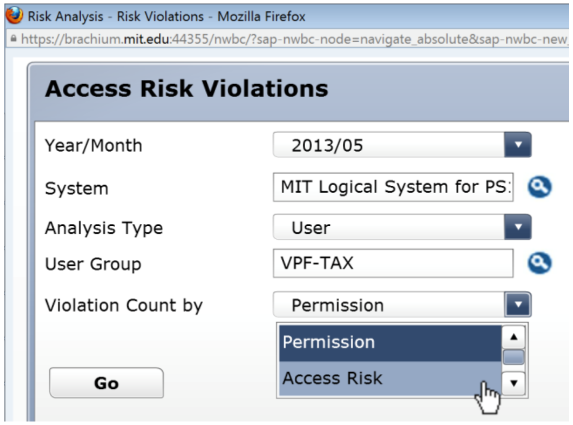
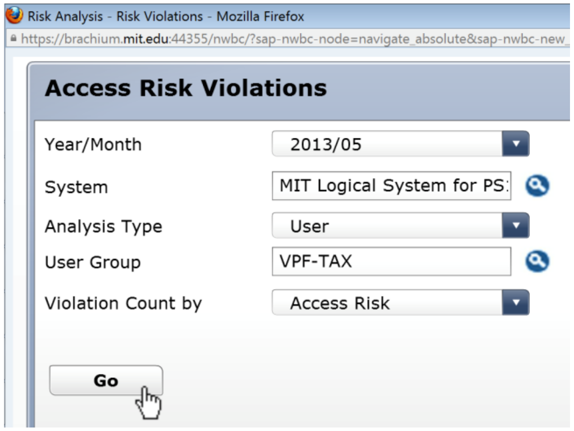
Code	Business Process	Count
BS00	Basis	2707626
CA00	Cross Application	7587
FI00	Finance	5331095
HR00	HR and Payroll	2222634
MM00	Materials Management	608563
PM00	Plant Maintenance	1054
PR00	Procure to Pay	3736778
SD00	Order to Cash	3281005

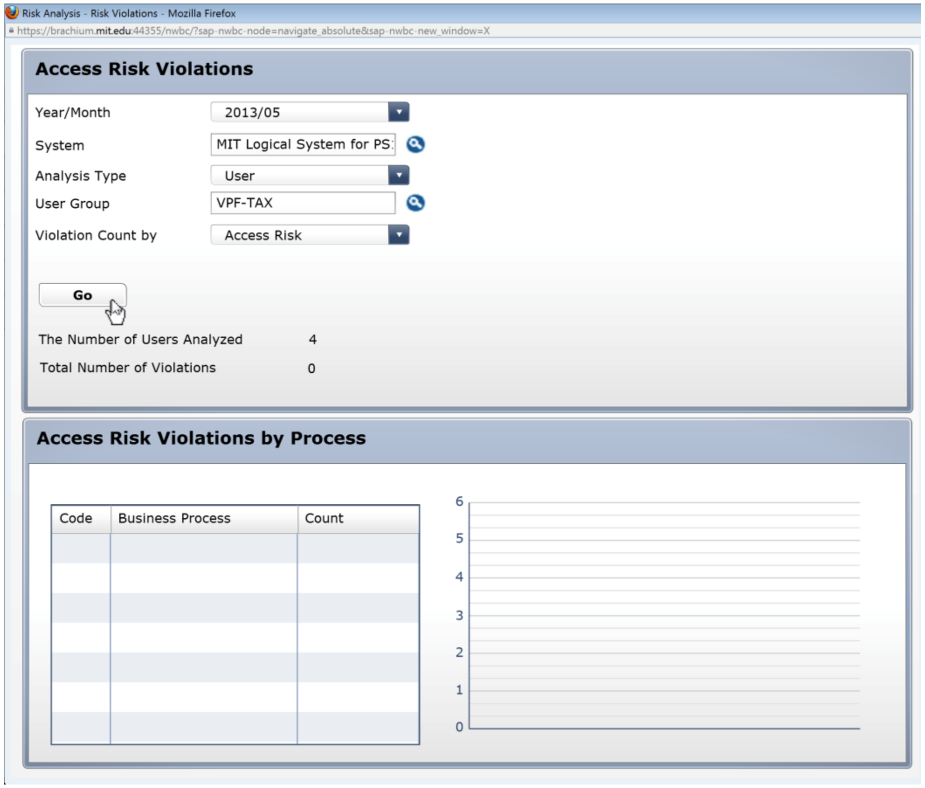
4	In the report filters section, click on the drop down for ‘Year/Month’ to select the time period for which data is required. In this case, ‘2013/05’ is selected.	 Risk Analysis - Risk Violations - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_v Access Risk Violations Year/Month 2013/05 System Analysis Type User Group Violation Count by 2013/05 2013/04 2013/03 2013/02 2013/01 Go

5	In the report filters section, select the system for which information is required. Click on the search icon next to 'System'. Since the desired selection is PS1 (Production), select the connector for PS1. Click on 'OK'.	 Risk Analysis - Risk Violations - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_win Access Risk Violations Year/Month 2013/05 System All Analysis Type User User Group All Violation Count by Permission  Risk Analysis - Risk Violations System — Description ALL — All ZZPS103001 — MIT Logical System for PS1:030 ZZSF203001 — MIT Logical System for SF2:030 ZZSF303001 — MIT Logical System for SF3:030 ZZSH203001 — MIT Logical System for SH2:030  Risk Analysis - Risk Violations System — Description ALL — All ZZPS103001 — MIT Logical System for PS1:030 ZZSF203001 — MIT Logical System for SF2:030 ZZSF303001 — MIT Logical System for SF3:030 ZZSH203001 — MIT Logical System for SH2:030

6	In the report filters section, click on the drop down for 'Analysis Type' to select the security object (user, role or profile) for which data is required. In this case, 'User' is selected.	 Risk Analysis - Risk Violations - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_w Access Risk Violations Year/Month 2013/05 System MIT Logical System for PS: Analysis Type User User Group Violation Count by User Role Profile Go

7	In the report filters section, select the user group for which information is required. Click on the search icon next to ‘User Group’. Enter search criteria to search for the desired user group. In this case, ‘VPF-T*’ is entered to search for all VPF user groups starting with ‘T’. Click on ‘Start Search’. Select the desired user group from the search results. In this case, ‘VPF-TAX’ is selected. Click on ‘OK’.	 Risk Analysis - Risk Violations - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_win Access Risk Violations Year/Month 2013/05 System MIT Logical System for PS: Analysis Type User User Group All Violation Count by Permission  Risk Analysis - Risk Violations VPF-T* UserGroup Description ALL All A/P A/P AIRGAS AIRGAS ALUMN ALUMN  Risk Analysis - Risk Violations VPF-T* UserGroup Description VPF-TAX VPF-TAX VPF-TRAVEL VPF-TRAVEL

8	In the report filters section, click on the drop down for ‘Violation Count by’ to select the count methodology required for the report. In this case, ‘Access Risk’ is selected to count unique violations per user.	 Risk Analysis - Risk Violations - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new Access Risk Violations Year/Month: 2013/05 System: MIT Logical System for PS: Analysis Type: User User Group: VPF-TAX Violation Count by: Permission Permission Access Risk
9	Click on ‘Go’ to execute the report based on the criteria that have been defined.	 Risk Analysis - Risk Violations - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new Access Risk Violations Year/Month: 2013/05 System: MIT Logical System for PS: Analysis Type: User User Group: VPF-TAX Violation Count by: Access Risk

10	The report shows that there are a total of 4 users in the 'VPF-TAX' user group. The report also shows that these 4 users have 0 unmitigated violations. No pie chart, business process table, or business process bar graph are shown due to the fact that the violation count is 0.	

Risk Analysis - Risk Violations - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

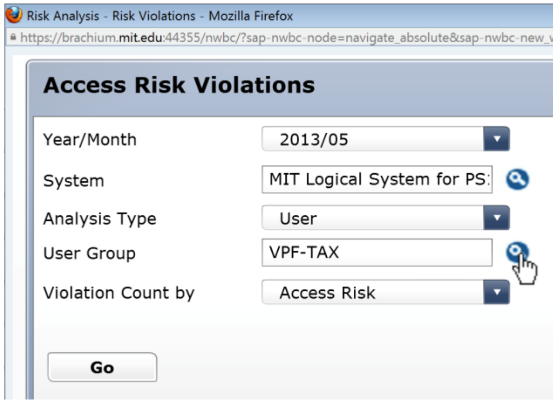
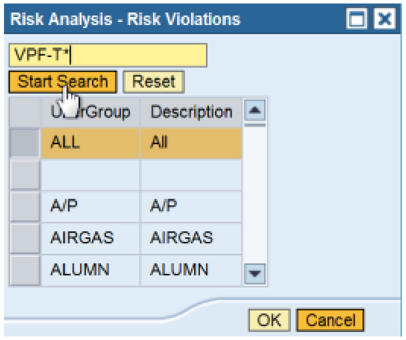
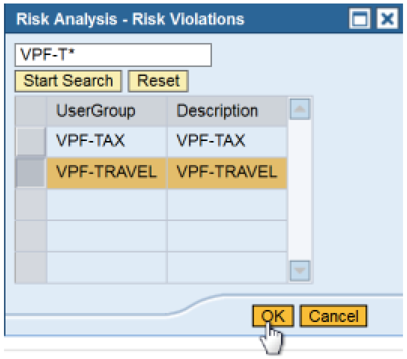
Access Risk Violations

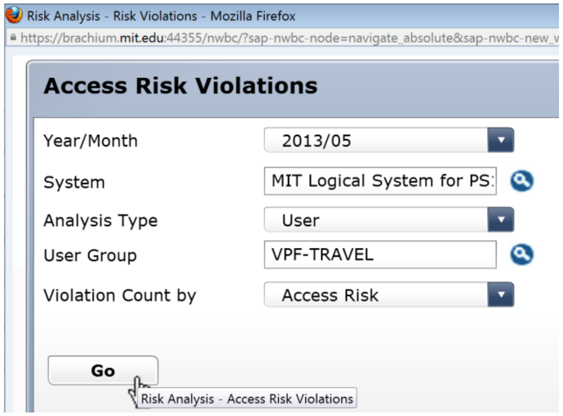
Year/Month	2013/05
System	MIT Logical System for PS
Analysis Type	User
User Group	VPF-TAX
Violation Count by	Access Risk

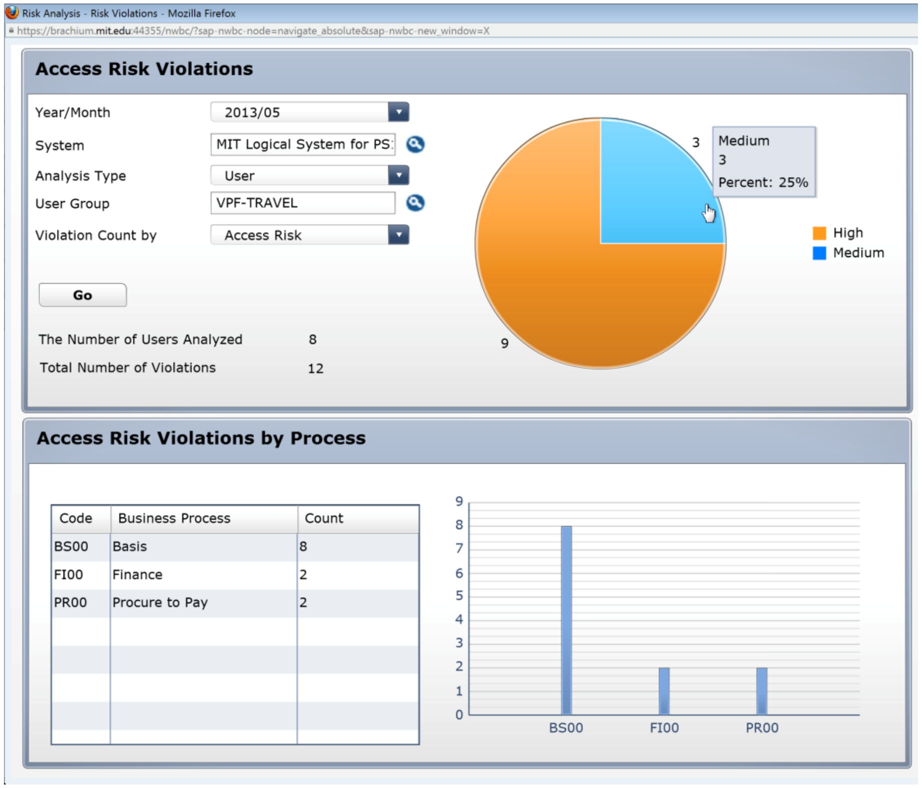
The Number of Users Analyzed	4
Total Number of Violations	0

Access Risk Violations by Process

Code	Business Process	Count

11	In the report filters section, select another user group for which information is required. Click on the search icon next to ‘User Group’. Enter search criteria to search for the desired user group. In this case, ‘VPF-T*’ is entered to search for all VPF user groups starting with ‘T’. Click on ‘Start Search’. Select the desired user group from the search results. In this case, ‘VPF-TRAVEL’ is selected. Click on ‘OK’.	 Risk Analysis - Risk Violations - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_v Access Risk Violations Year/Month: 2013/05 System: MIT Logical System for PS: Analysis Type: User User Group: VPF-TAX Violation Count by: Access Risk Go  Risk Analysis - Risk Violations VPF-T* Start Search Reset UserGroup / Description: ALL / All; A/P / A/P; AIRGAS / AIRGAS; ALUMN / ALUMN OK Cancel  Risk Analysis - Risk Violations VPF-T* Start Search Reset UserGroup / Description: VPF-TAX / VPF-TAX; VPF-TRAVEL / VPF-TRAVEL OK Cancel

12	Click on 'Go' to execute the report based on the updated criteria that have been defined.	 Risk Analysis - Risk Violations - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_v **Access Risk Violations** Year/Month: 2013/05 System: MIT Logical System for PS: Analysis Type: User User Group: VPF-TRAVEL Violation Count by: Access Risk

13	The report shows that there are a total of 8 users in the 'VPF-TRAVEL' user group. The report also shows that these 8 users have 12 unmitigated violations. The graphic displays are populated based on information regarding the 12 unmitigated violations. The User Level analysis report (12), reports that: • 8 users have unimitigated Basis Critical Transactions • 2 users have unmitigated Finance SODs • 2 users have unmitigated Procure to Pay SODs	

Risk Analysis - Risk Violations - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Access Risk Violations

Year/Month: 2013/05

System: MIT Logical System for PS:

Analysis Type: User

User Group: VPF-TRAVEL

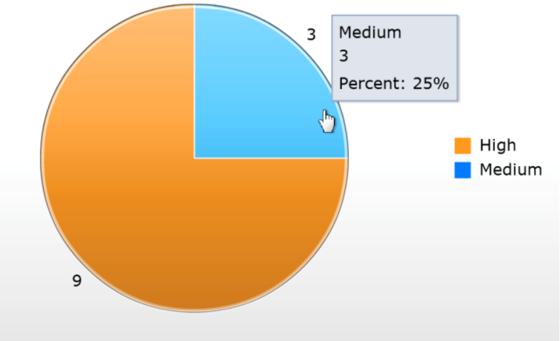
Violation Count by: Access Risk

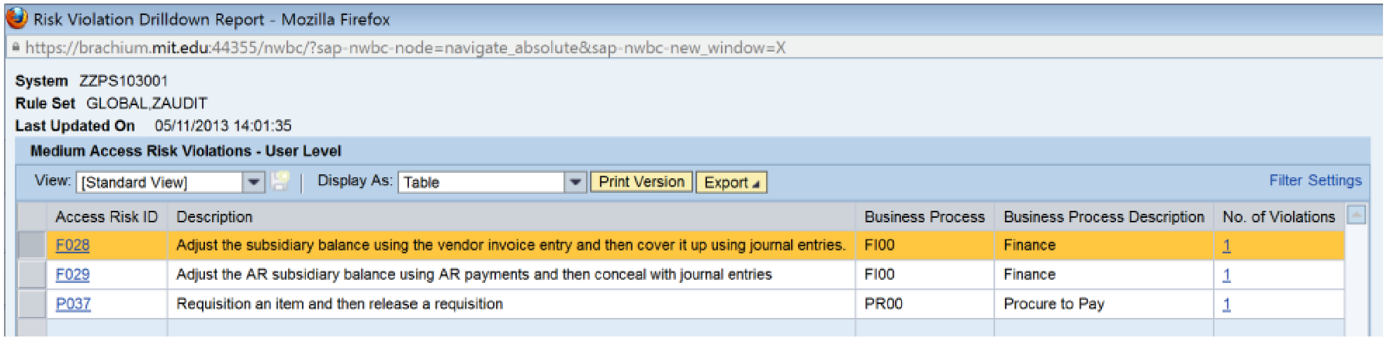
The Number of Users Analyzed: 8

Total Number of Violations: 12

Access Risk Violations by Process

Code	Business Process	Count
BS00	Basis	8
FI00	Finance	2
PR00	Procure to Pay	2

14A-1	Analyze report data by risk level. Scroll over the different pieces of the pie chart to see information about unmitigated violations at each risk level. Click on the 'Medium' risk level piece of the pie chart for more information about medium risks.	

14A-2	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. Access Risk: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist Description: Business description of the Access Risk Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set No. of Violations: The number of violations for each Access Risk that exist	

Risk Violation Drilldown Report - Mozilla Firefox

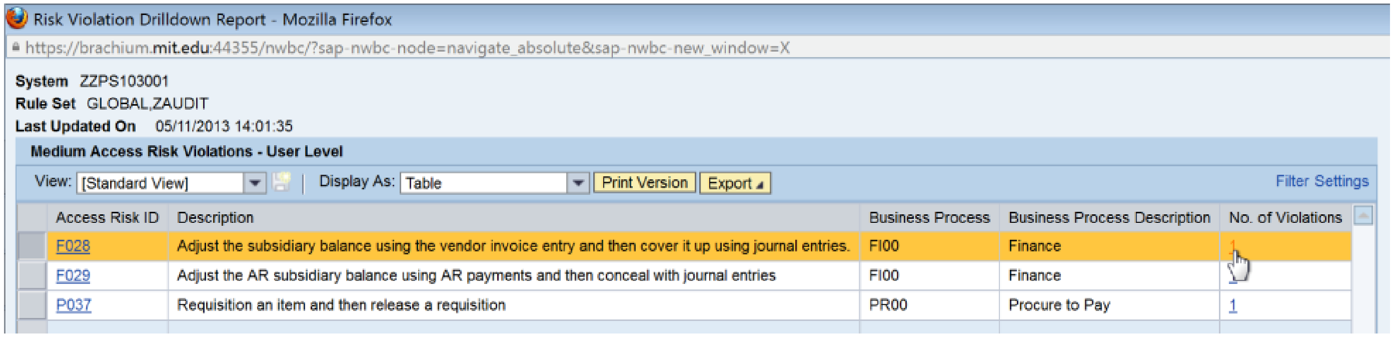
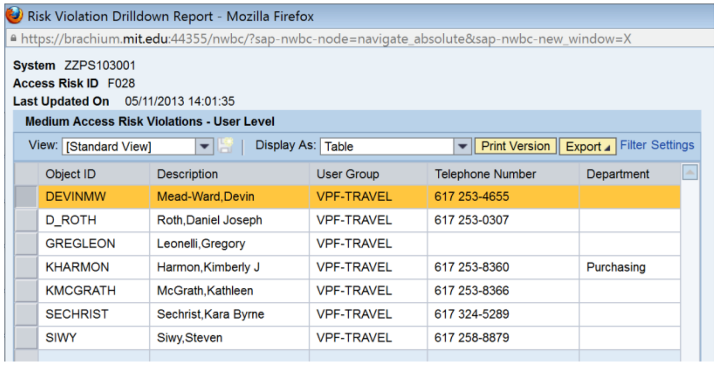
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

System ZZPS103001
Rule Set GLOBAL,ZAUDIT
Last Updated On 05/11/2013 14:01:35

Medium Access Risk Violations - User Level

View: [Standard View] Display As: Table

Access Risk ID	Description	Business Process	Business Process Description	No. of Violations
F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	FI00	Finance	1
F029	Adjust the AR subsidiary balance using AR payments and then conceal with journal entries	FI00	Finance	1
P037	Requisition an item and then release a requisition	PR00	Procure to Pay	1

14A-3	Click on the ‘No. of Violations’ link for each Access Risk to view the Users that have violations for that Risk. In this case, clicking on ‘1’ for Access Risk ‘F028’ shows the 7 VPF-TRAVEL Users that have related violations.	 

Risk Violation Drilldown Report - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

System ZZPS103001
Rule Set GLOBAL,ZAUDIT
Last Updated On 05/11/2013 14:01:35

Medium Access Risk Violations - User Level

View: [Standard View] Display As: Table Print Version Export Filter Settings

Access Risk ID	Description	Business Process	Business Process Description	No. of Violations
F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	FI00	Finance	1
F029	Adjust the AR subsidiary balance using AR payments and then conceal with journal entries	FI00	Finance	1
P037	Requisition an item and then release a requisition	PR00	Procure to Pay	1

Risk Violation Drilldown Report - Mozilla Firefox

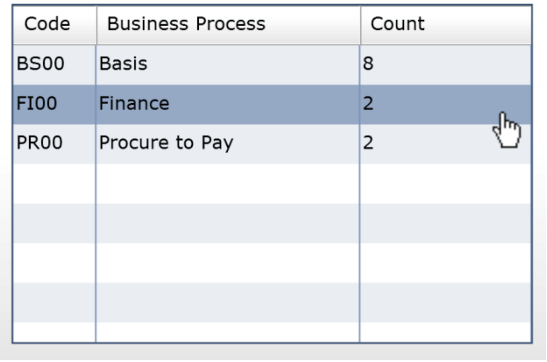
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

System ZZPS103001
Access Risk ID F028
Last Updated On 05/11/2013 14:01:35

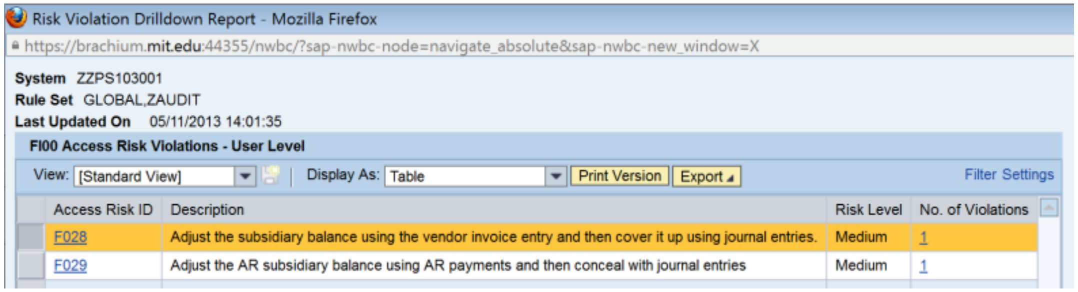
Medium Access Risk Violations - User Level

View: [Standard View] Display As: Table Print Version Export Filter Settings

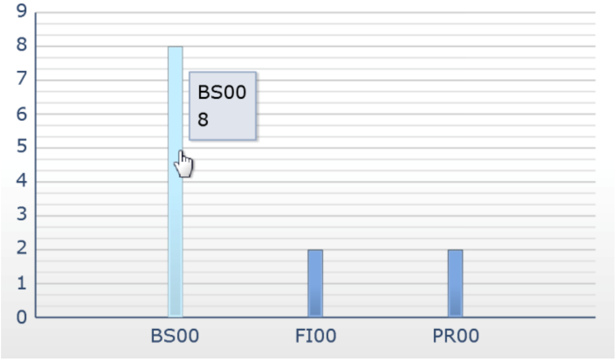
Object ID	Description	User Group	Telephone Number	Department
DEVINMW	Mead-Ward,Devin	VPF-TRAVEL	617 253-4655	
D_ROTH	Roth,Daniel Joseph	VPF-TRAVEL	617 253-0307	
GREGLEON	Leonelli,Gregory	VPF-TRAVEL		
KHARMON	Harmon,Kimberly J	VPF-TRAVEL	617 253-8360	Purchasing
KMCGRATH	McGrath,Kathleen	VPF-TRAVEL	617 253-8366	
SECHRIST	Sechrist,Kara Byrne	VPF-TRAVEL	617 324-5289	
SIWY	Siwy,Steven	VPF-TRAVEL	617 258-8879	

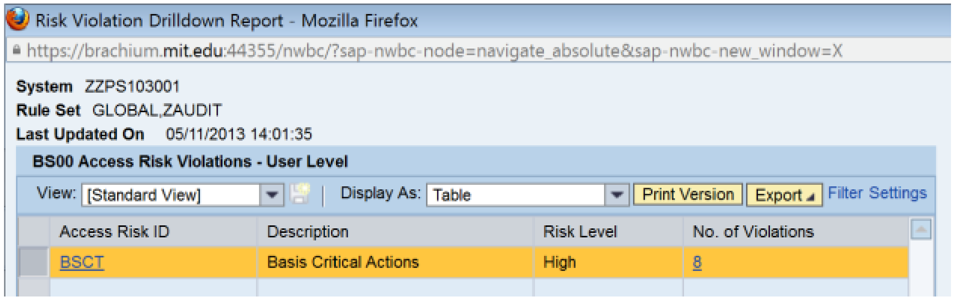
14B-1	Analyze report data by Business Process. Scroll over the different line items of the Business Process Table to see information about unmitigated violations for each Business Process. Click on the ‘Finance’ risk level row of the Table for more information about Finance Risks.	

Code	Business Process	Count
BS00	Basis	8
FI00	Finance	2
PR00	Procure to Pay	2

<table>
<tr>
<td>14B-2</td>
<td>Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.
Access Risk: The 4-digit ID representing each Finance-Risk (as defined in the standard rule set) for which violations exist
Description: Business description of the Access Risk
Risk Level: The risk level defined for each Access Risk in the standard rule set
No. of Violations: The number of violations for each Access Risk that exist</td>
<td>
Risk Violation Drilldown Report - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

System ZZPS103001
Rule Set GLOBAL,ZAUDIT
Last Updated On 05/11/2013 14:01:35
FI00 Access Risk Violations - User Level
View: [Standard View] Display As: Table
Print Version
Export
Filter Settings
<table>
<tr><th>Access Risk ID</th><th>Description</th><th>Risk Level</th><th>No. of Violations</th></tr>
<tr><td>F028</td><td>Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.</td><td>Medium</td><td>1</td></tr>
<tr><td>F029</td><td>Adjust the AR subsidiary balance using AR payments and then conceal with journal entries</td><td>Medium</td><td>1</td></tr>
</table>
</td>
</tr>
</table>

14C-1	Analyze report data by Business Process. Scroll over the different bars of the Business Process Bar Graph to see information about unmitigated violations for each Business Process. Click on the 'BS00' Risk bar of the Graph for more information about Basis Risks.	

14C-2	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. Access Risk: The 4-digit ID representing each Basis-Risk (as defined in the standard rule set) for which violations exist Description: Business description of the Access Risk Risk Level: The risk level defined for each Access Risk in the standard rule set No. of Violations: The number of violations for each Access Risk that exist	

Risk Violation Drilldown Report - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

System ZZPS103001
Rule Set GLOBAL,ZAUDIT
Last Updated On 05/11/2013 14:01:35

BS00 Access Risk Violations - User Level

View: [Standard View] Display As: Table

Access Risk ID	Description	Risk Level	No. of Violations
BSCT	Basis Critical Actions	High	8

Job Aid 02 User Analysis

USE

This report can be used to gain insight into MIT's overall exposure to risk. The report provides an overview of user violations across all MIT ECC systems.

INFORMATION

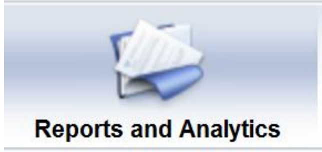
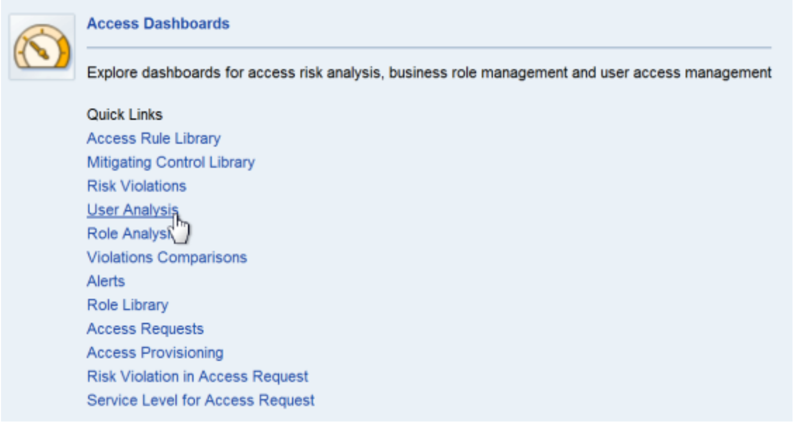
Risk count by risk type and user.

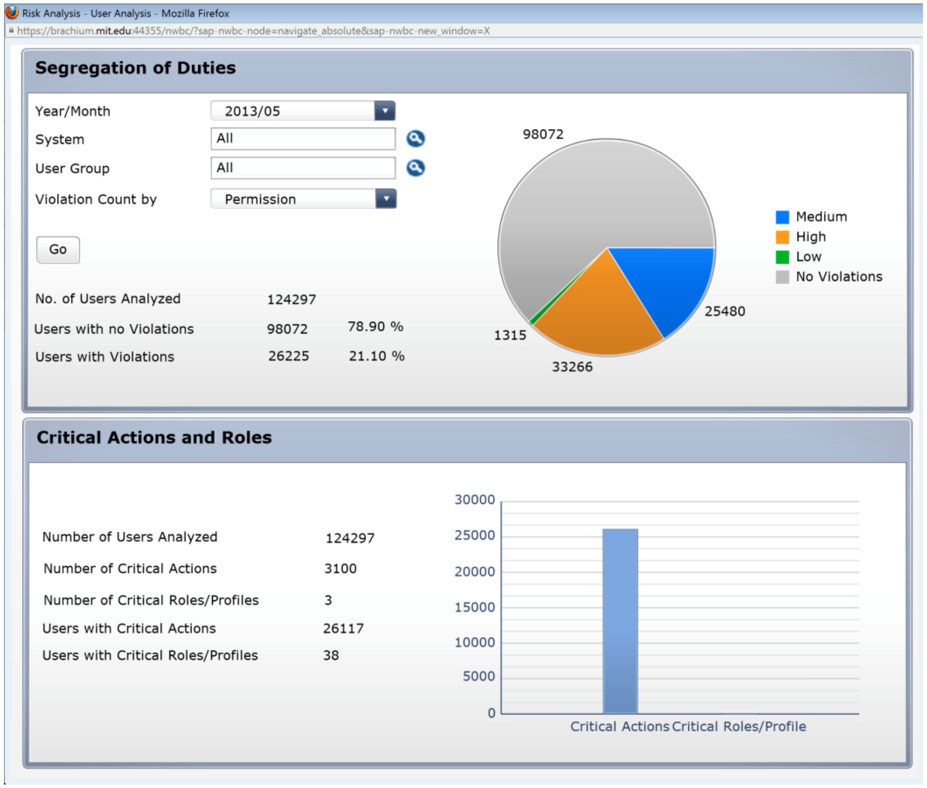
RELATED PROCESSES

- Process 5: Periodic Compliance Reviews

SPECIFIC SCENARIOS

- Step 13A: Analyze report data by Mitigated Users. (Pie Chart)
- Step 13B: Analyze report data by Risk Level. (Pie Chart)
- Step 13C: Analyze report data by Critical Actions, Roles and Profiles. (Bar Graph)

Step	Description	Screenshot
1	Navigate to the ‘Reports and Analytics’ tab.	
2	Click on the ‘User Analysis’ report located in the ‘Access Dashboards’ section.	 Access Dashboards Explore dashboards for access risk analysis, business role management and user access management Quick Links Access Rule Library Mitigating Control Library Risk Violations User Analysis Role Analysis Violations Comparisons Alerts Role Library Access Requests Access Provisioning Risk Violation in Access Request Service Level for Access Request

3	The report will show risk violations and critical actions, roles and profiles information for the latest period, across all systems (to which GRC is connected) and user groups, at the user level. The violation count will be given by permission (i.e. each instance of a violation will be counted, even if it is a repeated violation for a user). The 'Critical Actions and Roles' section will state the number of each that were evaluated for the selected user group. The report data must be appropriately filtered to provide information that can be of use to MIT.	

Risk Analysis - User Analysis - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Segregation of Duties

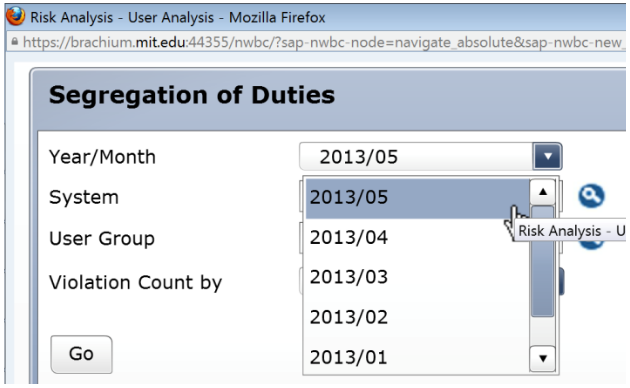
Year/Month	2013/05
System	All
User Group	All
Violation Count by	Permission

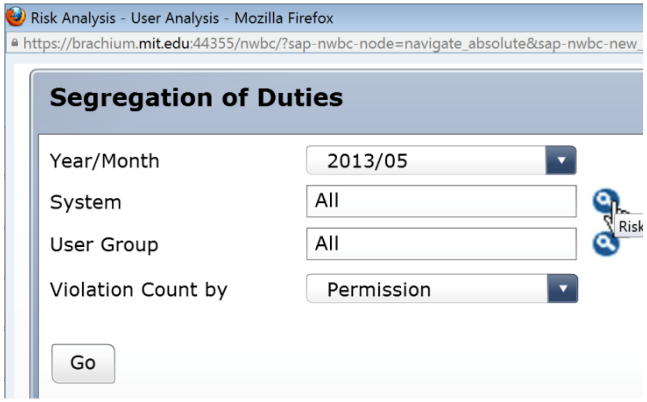
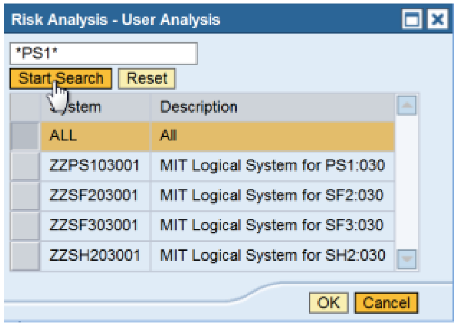
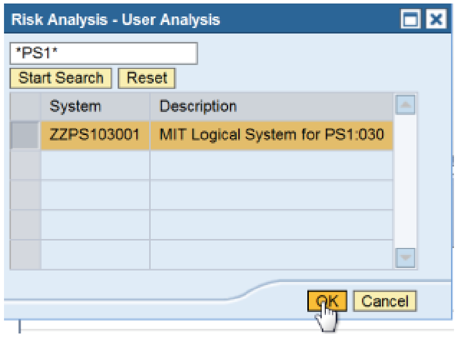
Go

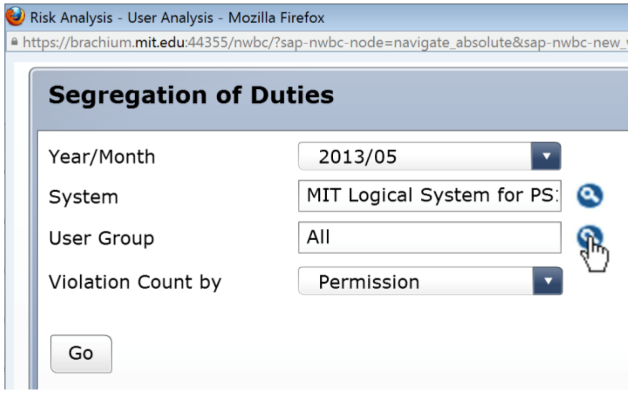
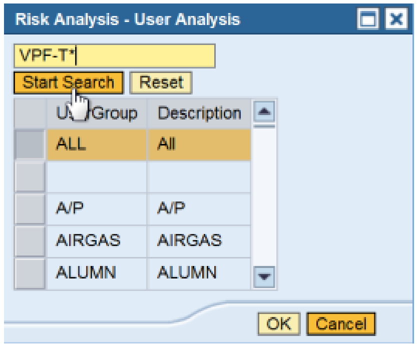
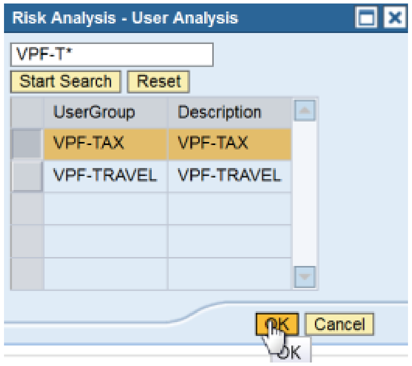
No. of Users Analyzed	124297	
Users with no Violations	98072	78.90 %
Users with Violations	26225	21.10 %

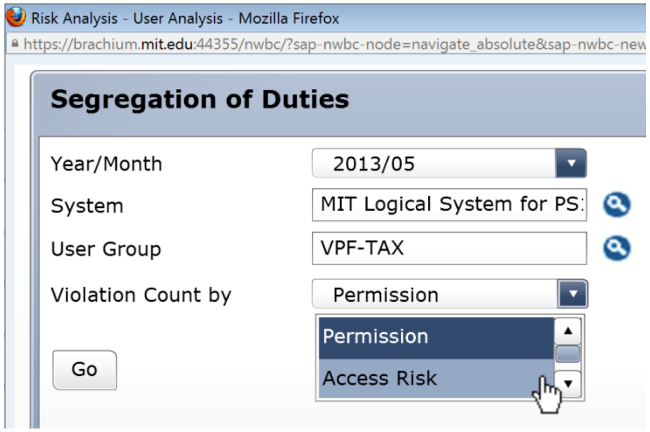
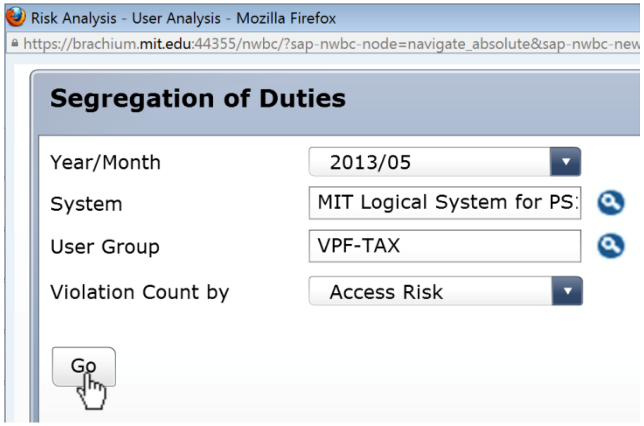
Critical Actions and Roles

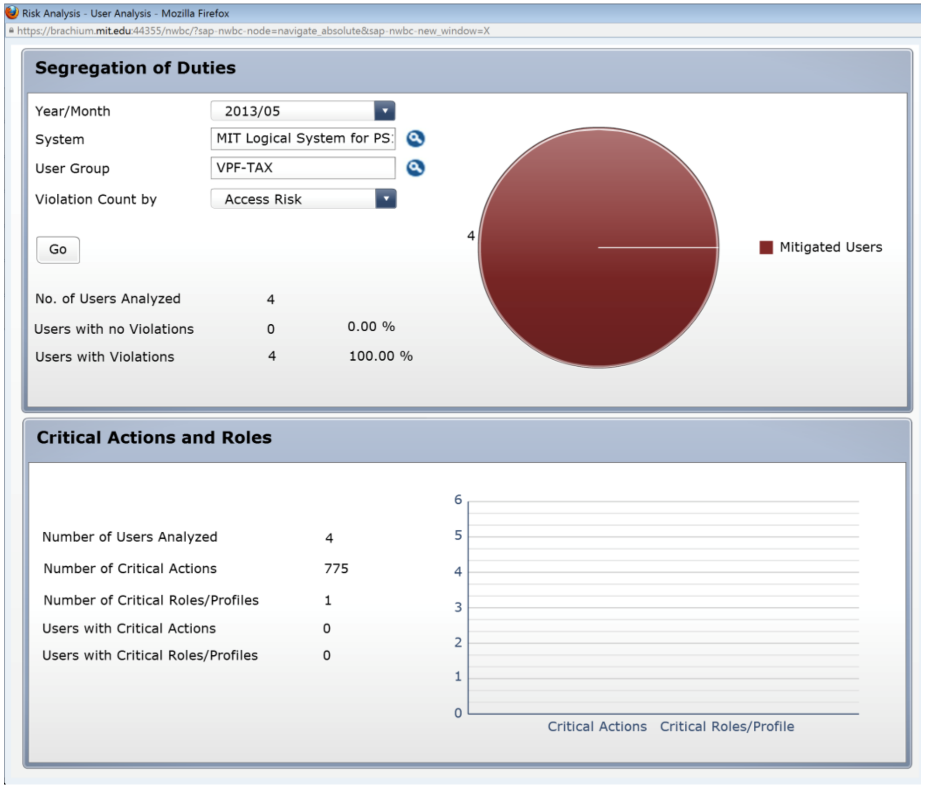
Number of Users Analyzed	124297
Number of Critical Actions	3100
Number of Critical Roles/Profiles	3
Users with Critical Actions	26117
Users with Critical Roles/Profiles	38

4	In the report filters section, click on the drop down for 'Year/Month' to select the time period for which data is required. In this case, '2013/05' is selected.	 Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_ Segregation of Duties Year/Month 2013/05 System User Group Violation Count by 2013/05 2013/04 2013/03 2013/02 2013/01 Risk Analysis - U Go

5	In the report filters section, select the System for which information is required. Click on the Search icon next to 'System'. Since the desired selection is PS1 (Production), select the Connector for PS1; if necessary, '*PS1*' can be used as search criteria to find the correct connector for PS1. Click on 'OK'.	 Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_ Segregation of Duties Year/Month: 2013/05 System: All User Group: All Violation Count by: Permission Go  Risk Analysis - User Analysis *PS1* Start Search Reset System | Description ALL | All ZZPS103001 | MIT Logical System for PS1:030 ZZSF203001 | MIT Logical System for SF2:030 ZZSF303001 | MIT Logical System for SF3:030 ZZSH203001 | MIT Logical System for SH2:030 OK Cancel  Risk Analysis - User Analysis *PS1* Start Search Reset System | Description ZZPS103001 | MIT Logical System for PS1:030 OK Cancel

6	In the report filters section, select the user group for which information is required. Click on the Search icon next to 'User Group'. Enter search criteria to search for the desired user group. In this case, 'VPF-T*' is entered to search for all VPF user groups starting with 'T'. Click on 'Start Search'. Select the desired user group from the search results. In this case, 'VPF-TAX' is selected. Click on 'OK'.	 Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_ Segregation of Duties Year/Month 2013/05 System MIT Logical System for PS: User Group All Violation Count by Permission Go  Risk Analysis - User Analysis VPF-T* Start Search Reset UserGroup Description ALL All A/P A/P AIRGAS AIRGAS ALUMN ALUMN OK Cancel  Risk Analysis - User Analysis VPF-T* Start Search Reset UserGroup Description VPF-TAX VPF-TAX VPF-TRAVEL VPF-TRAVEL OK Cancel

7	In the report filters section, click on the drop down for 'Violation Count by' to select the count methodology required for the report. In this case, 'Access Risk' is selected to count unique violations per User.	 Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new Segregation of Duties Year/Month 2013/05 System MIT Logical System for PS: User Group VPF-TAX Violation Count by Permission Permission Access Risk Go
8	Click on 'Go' to execute the report based on the criteria that have been defined.	 Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new Segregation of Duties Year/Month 2013/05 System MIT Logical System for PS: User Group VPF-TAX Violation Count by Access Risk Go

9	The report shows that there are a total of 4 Users in the 'VPF-TAX' user group. The report also shows that these 4 Users all have mitigated violations. In the 'Critical Actions and Roles' section, the report shows: • 4 Users were analyzed • The users were evaluated for violations against 775 Critical Actions and 1 Critical Role/Profile • 0 VPF-TAX Users have Critical Actions • 0 VPF-TAX Users have Critical Roles/Profiles	

Risk Analysis - User Analysis - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Segregation of Duties

Year/Month: 2013/05

System: MIT Logical System for PS:

User Group: VPF-TAX

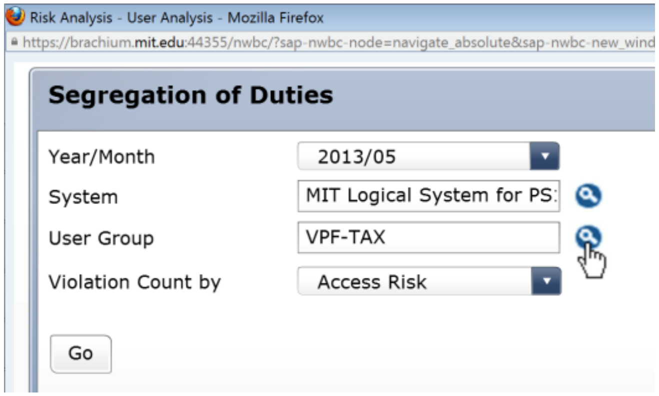
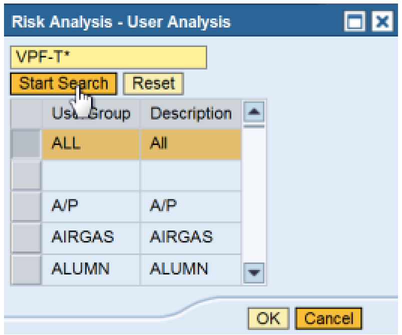
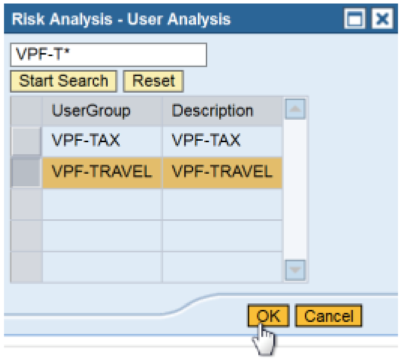
Violation Count by: Access Risk

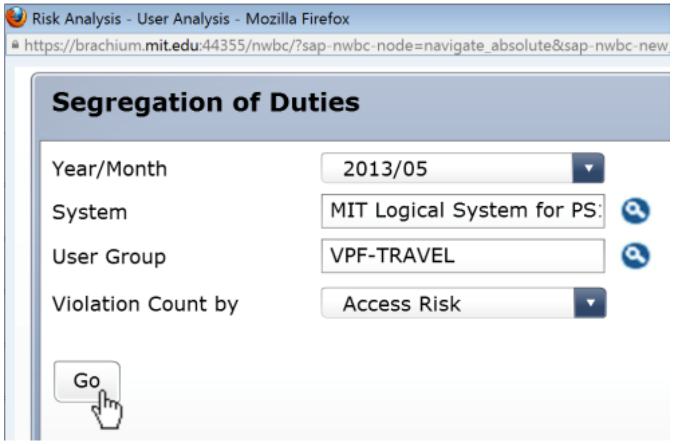
Go

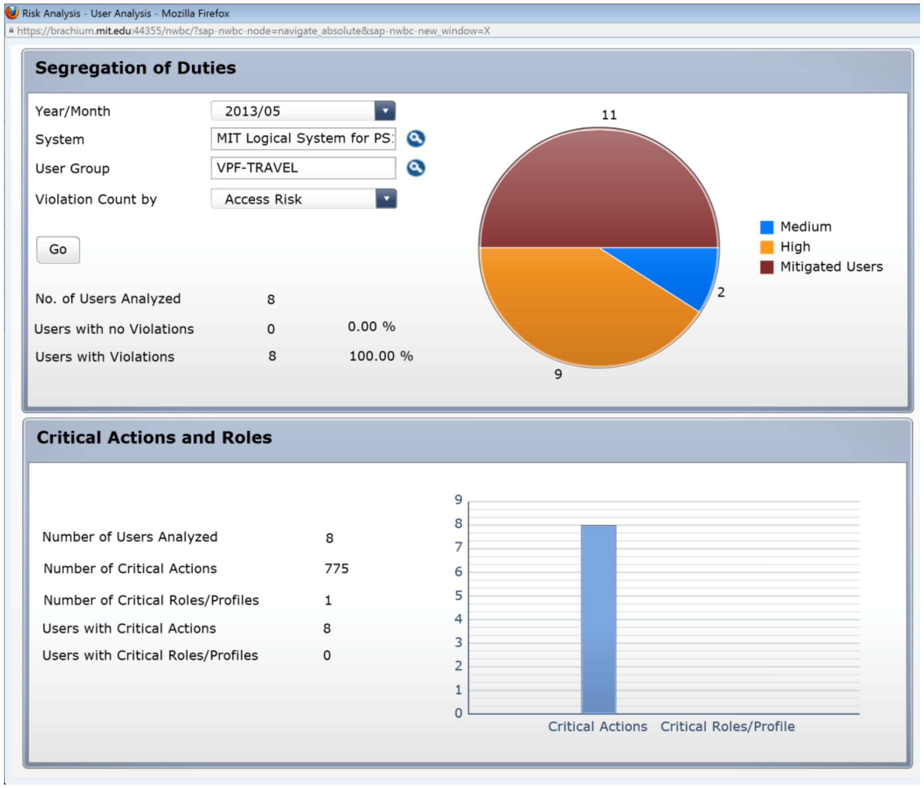
No. of Users Analyzed	4	
Users with no Violations	0	0.00 %
Users with Violations	4	100.00 %

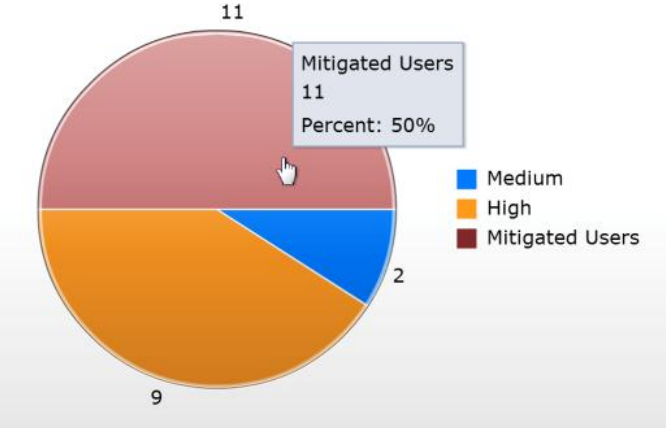
Critical Actions and Roles

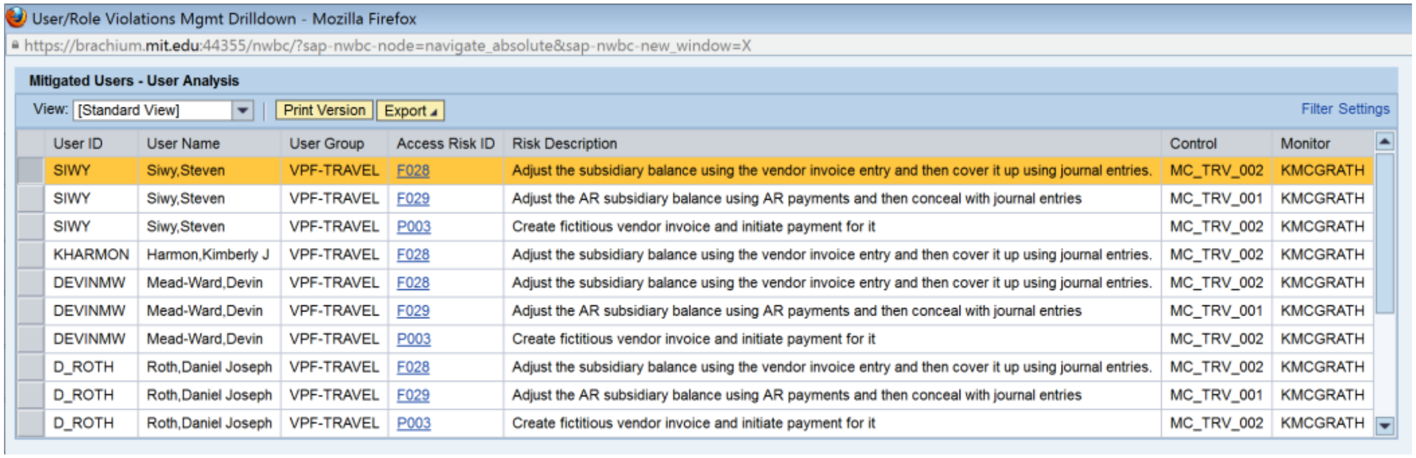
Number of Users Analyzed	4
Number of Critical Actions	775
Number of Critical Roles/Profiles	1
Users with Critical Actions	0
Users with Critical Roles/Profiles	0

10	In the report filters section, select another user group for which information is required. Click on the Search icon next to 'User Group'. Enter search criteria to search for the desired user group. In this case, 'VPF-T*' is entered to search for all VPF user groups starting with 'T'. Click on 'Start Search'. Select the desired user group from the search results. In this case, 'VPF-TRAVEL' is selected. Click on 'OK'.	 Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_wind **Segregation of Duties** Year/Month: 2013/05 System: MIT Logical System for PS: User Group: VPF-TAX Violation Count by: Access Risk Go  Risk Analysis - User Analysis VPF-T* Start Search Reset UserGroup | Description ALL | All A/P | A/P AIRGAS | AIRGAS ALUMN | ALUMN OK Cancel  Risk Analysis - User Analysis VPF-T* Start Search Reset UserGroup | Description VPF-TAX | VPF-TAX VPF-TRAVEL | VPF-TRAVEL OK Cancel

11	Click on 'Go' to execute the report based on the updated criteria that have been defined.	 Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new Segregation of Duties Year/Month: 2013/05 System: MIT Logical System for PS: User Group: VPF-TRAVEL Violation Count by: Access Risk Go

12	The report shows that there are a total of 8 Users in the ‘VPF-TRAVEL’ user group. The report also shows that these 8 Users have 11 mitigations, as well as 11 instances (9 High Risk + 2 Medium Risk) of Users with unmitigated violations. NOTE: Each type of Violation – SOD, Critical Transaction, etc. – is counted only once per User. Thus, a User with only 2 SOD, contributes 1 to the violation count. And a User with 1 SOD and 1 Critical Action, contributes 2 to the violation count. In the ‘Critical Actions and Roles’ section, the report shows: • 8 users were analyzed • The users were evaluated for violations against 775 Critical Actions and 1 Critical Role/Profile • 8 VPF-TRAVEL users have Critical Actions • 0 VPF-TRAVEL users have Critical Roles/Profiles	Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Segregation of Duties** Year/Month 2013/05 System MIT Logical System for PS: User Group VPF-TRAVEL Violation Count by Access Risk Go No. of Users Analyzed 8 Users with no Violations 0 0.00 % Users with Violations 8 100.00 % **Critical Actions and Roles** Number of Users Analyzed 8 Number of Critical Actions 775 Number of Critical Roles/Profiles 1 Users with Critical Actions 8 Users with Critical Roles/Profiles 0 9 8 7 6 5 4 3 2 1 0 Critical Actions Critical Roles/Profile

13A-1	Analyze report data by mitigated users. Scroll over the different pieces of the pie chart to see information about mitigated violations as well as unmitigated violations at different risk levels. Click on the 'Mitigated Users' piece of the pie chart for more information about VPF-TRAVEL users that have Mitigated Risks.	

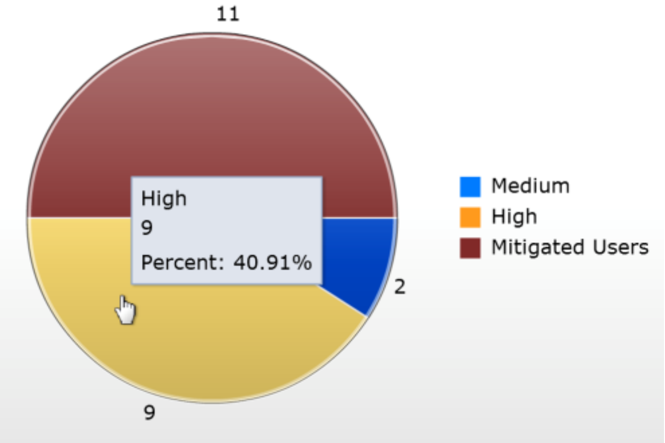
13A-2	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. User ID: User ID of the user with a Risk that has been mitigated User Name: User name associated with the user ID User Group: User group code Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist Risk Description: Business description of the Access Risk Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk Monitor: The user ID of the Monitor responsible for the Mitigating Control	

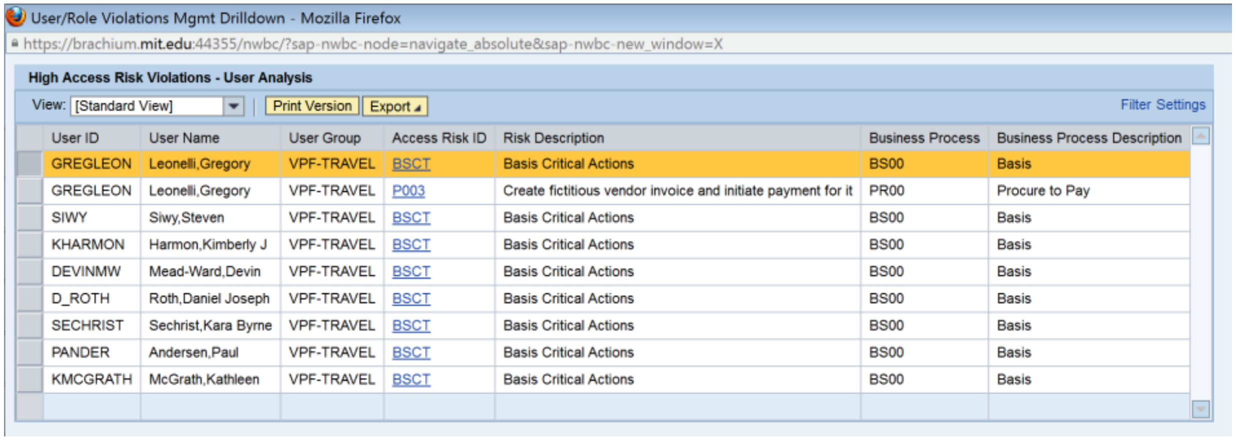
User/Role Violations Mgmt Drilldown - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Mitigated Users - User Analysis

User ID	User Name	User Group	Access Risk ID	Risk Description	Control	Monitor
SIWY	Siwy,Steven	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	MC_TRV_002	KMCGRATH
SIWY	Siwy,Steven	VPF-TRAVEL	F029	Adjust the AR subsidiary balance using AR payments and then conceal with journal entries	MC_TRV_001	KMCGRATH
SIWY	Siwy,Steven	VPF-TRAVEL	P003	Create fictitious vendor invoice and initiate payment for it	MC_TRV_002	KMCGRATH
KHARMON	Harmon,Kimberly J	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	MC_TRV_002	KMCGRATH
DEVINMW	Mead-Ward,Devin	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	MC_TRV_002	KMCGRATH
DEVINMW	Mead-Ward,Devin	VPF-TRAVEL	F029	Adjust the AR subsidiary balance using AR payments and then conceal with journal entries	MC_TRV_001	KMCGRATH
DEVINMW	Mead-Ward,Devin	VPF-TRAVEL	P003	Create fictitious vendor invoice and initiate payment for it	MC_TRV_002	KMCGRATH
D_ROTH	Roth,Daniel Joseph	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	MC_TRV_002	KMCGRATH
D_ROTH	Roth,Daniel Joseph	VPF-TRAVEL	F029	Adjust the AR subsidiary balance using AR payments and then conceal with journal entries	MC_TRV_001	KMCGRATH
D_ROTH	Roth,Daniel Joseph	VPF-TRAVEL	P003	Create fictitious vendor invoice and initiate payment for it	MC_TRV_002	KMCGRATH

13B-1	Analyze report data by risk level. Click on the ‘High’ risks piece of the pie chart for more information about VPF-TRAVEL Users that have high risk level risks.	

13B-2	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. User ID: User ID of the user with a Risk that has been mitigated User Name: User name associated with the user ID User Group: User group code Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist Risk Description: Business description of the Access Risk Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set	

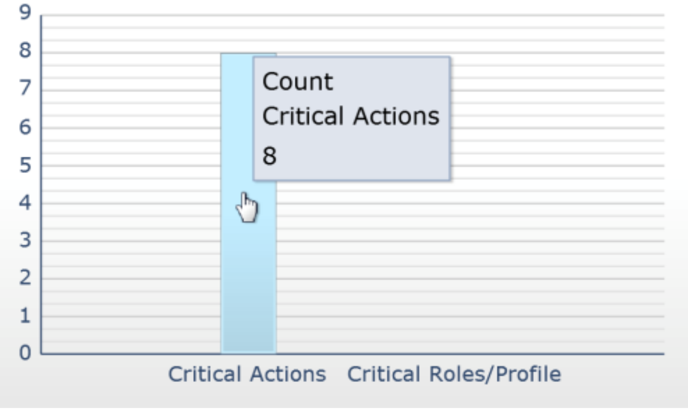
User/Role Violations Mgmt Drilldown - Mozilla Firefox

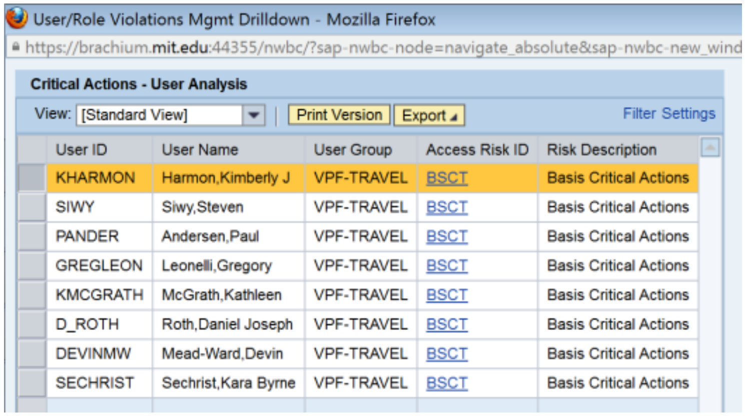
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

High Access Risk Violations - User Analysis

View: [Standard View] | Print Version | Export | Filter Settings

User ID	User Name	User Group	Access Risk ID	Risk Description	Business Process	Business Process Description
GREGLEON	Leonelli,Gregory	VPF-TRAVEL	BSCT	Basis Critical Actions	BS00	Basis
GREGLEON	Leonelli,Gregory	VPF-TRAVEL	P003	Create fictitious vendor invoice and initiate payment for it	PR00	Procure to Pay
SIWY	Siwy,Steven	VPF-TRAVEL	BSCT	Basis Critical Actions	BS00	Basis
KHARMON	Harmon,Kimberly J	VPF-TRAVEL	BSCT	Basis Critical Actions	BS00	Basis
DEVINMW	Mead-Ward,Devin	VPF-TRAVEL	BSCT	Basis Critical Actions	BS00	Basis
D_ROTH	Roth,Daniel Joseph	VPF-TRAVEL	BSCT	Basis Critical Actions	BS00	Basis
SECHRIST	Sechrist,Kara Byrne	VPF-TRAVEL	BSCT	Basis Critical Actions	BS00	Basis
PANDER	Andersen,Paul	VPF-TRAVEL	BSCT	Basis Critical Actions	BS00	Basis
KMCGRATH	McGrath,Kathleen	VPF-TRAVEL	BSCT	Basis Critical Actions	BS00	Basis

13C-1	Analyze report data by Critical Actions, Roles and Profiles. Scroll over the different bars of the Bar Graph to see information about Critical Actions and Critical Roles/Profiles. Click on the ‘Critical Actions’ bar of the Graph for more information about Critical Actions violations.	

13C-2	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. User ID: User ID of the user with a Risk that has been mitigated User Name: User name associated with the user ID User Group: User group code Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist Risk Description: Business description of the Access Risk	

User/Role Violations Mgmt Drilldown - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_wind

Critical Actions - User Analysis

View: [Standard View]

User ID	User Name	User Group	Access Risk ID	Risk Description
KHARMON	Harmon,Kimberly J	VPF-TRAVEL	BSCT	Basis Critical Actions
SIWY	Siwy,Steven	VPF-TRAVEL	BSCT	Basis Critical Actions
PANDER	Andersen,Paul	VPF-TRAVEL	BSCT	Basis Critical Actions
GREGLEON	Leonelli,Gregory	VPF-TRAVEL	BSCT	Basis Critical Actions
KMCGRATH	McGrath,Kathleen	VPF-TRAVEL	BSCT	Basis Critical Actions
D_ROTH	Roth,Daniel Joseph	VPF-TRAVEL	BSCT	Basis Critical Actions
DEVINMW	Mead-Ward,Devin	VPF-TRAVEL	BSCT	Basis Critical Actions
SECHRIST	Sechrist,Kara Byrne	VPF-TRAVEL	BSCT	Basis Critical Actions

Job Aid 03 Violations Comparisons

USE

This report can be used to gain insight into the progress MIT is making with respect to reducing and mitigating risk exposure. The report provides an overview of violations remediation/mitigation progress.

INFORMATION

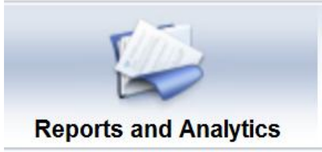
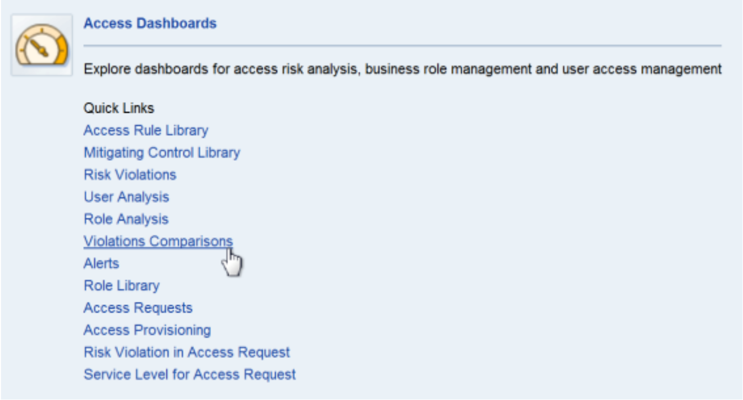
Violation count and comparison over time.

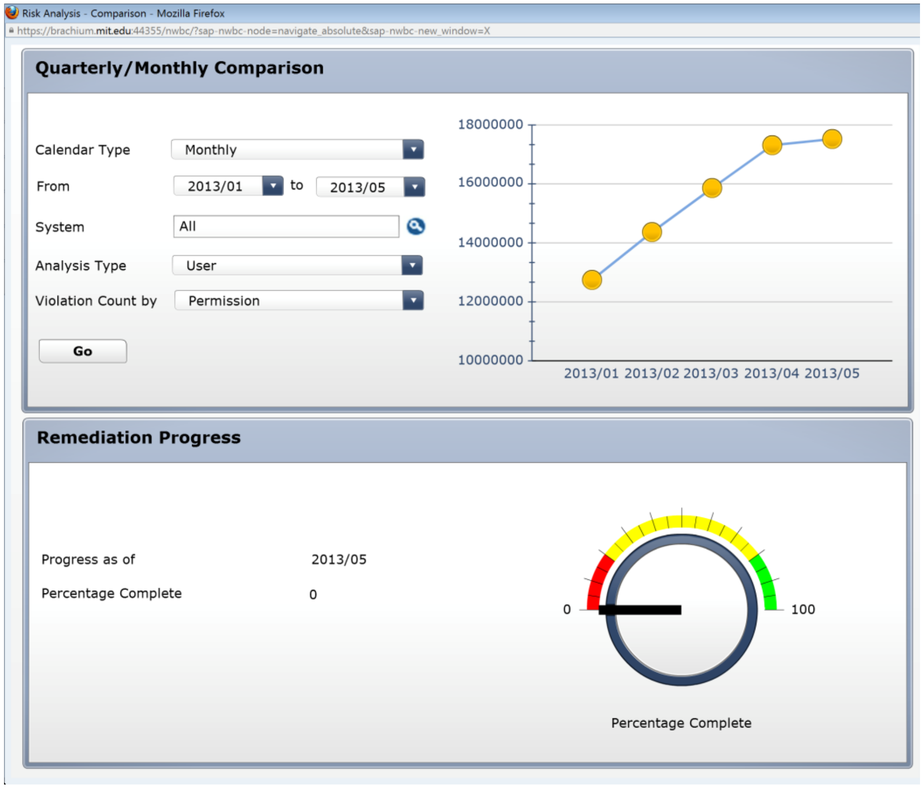
RELATED PROCESSES

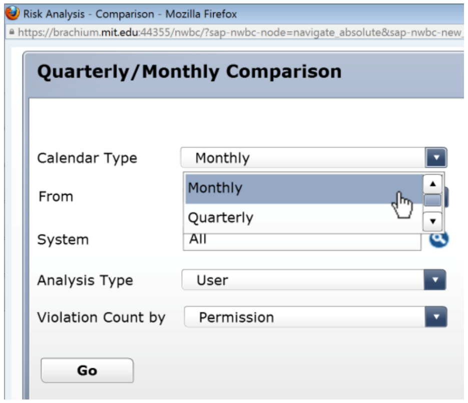
- Process 5: Periodic Compliance Reviews

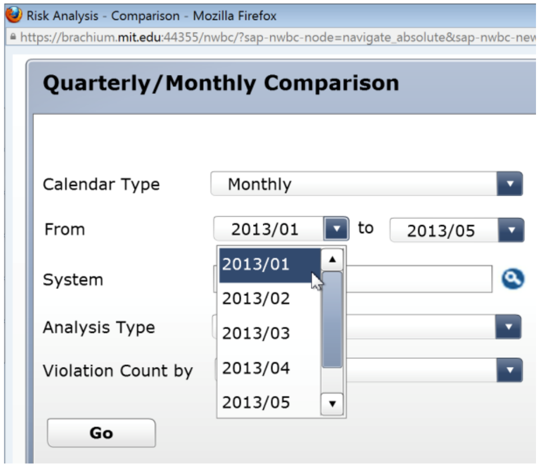
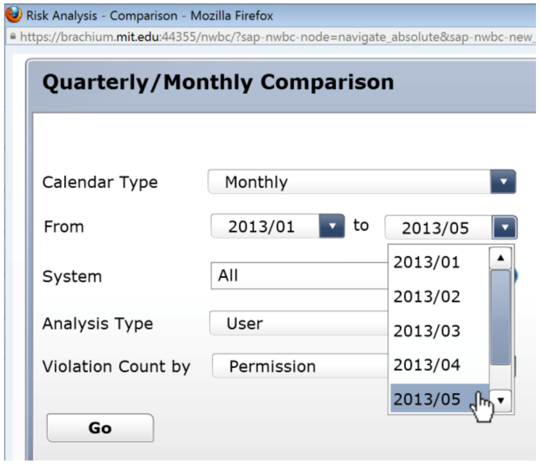
SPECIFIC SCENARIOS

- N/A

Step	Description	Screenshot
1	Navigate to the 'Reports and Analytics' tab.	 Reports and Analytics
2	Click on the 'Violations Comparisons' report located in the 'Access Dashboards' section.	 Access Dashboards Explore dashboards for access risk analysis, business role management and user access management Quick Links Access Rule Library Mitigating Control Library Risk Violations User Analysis Role Analysis Violations Comparisons Alerts Role Library Access Requests Access Provisioning Risk Violation in Access Request Service Level for Access Request

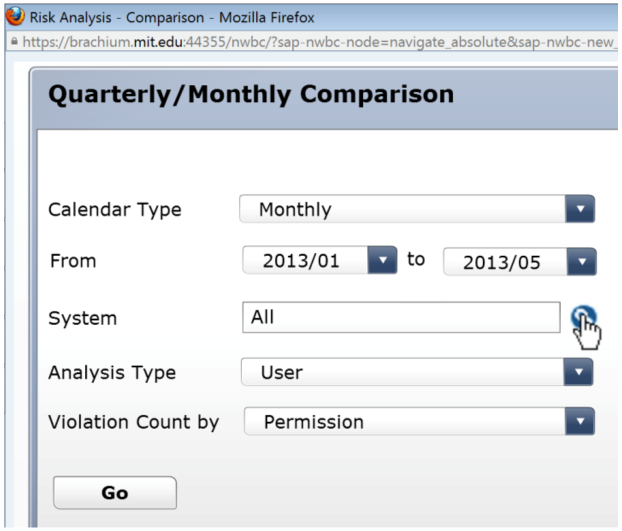
3	The report will show risk violations information over time, across all systems (to which GRC is connected) on a monthly basis, at the user level. The count will be given by permission (i.e. each instance of a violation will be counted, even if it is a repeated violation for a user). The report data must be appropriately filtered to provide information that can be of use to MIT.	 Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Quarterly/Monthly Comparison** Calendar Type: Monthly From: 2013/01 to 2013/05 System: All Analysis Type: User Violation Count by: Permission Go 18000000 16000000 14000000 12000000 10000000 2013/01 2013/02 2013/03 2013/04 2013/05 **Remediation Progress** Progress as of: 2013/05 Percentage Complete: 0 0 100 Percentage Complete

4	In the report filters section, click on the drop down for ‘Calendar Type’ to select the reporting periods by which data will be reported. In this case, ‘Monthly’ is selected.	 Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_ Quarterly/Monthly Comparison Calendar Type: Monthly From System: All Analysis Type: User Violation Count by: Permission

5	In the report filters section, click on the drop down for ‘From’ to select the start of the time period for which data is required. In this case, ‘2013/01’ is selected. Next, click on the drop down for ‘to’ to select the end of the time period for which data is required. In this case, ‘2013/05’ is selected.	 Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new Quarterly/Monthly Comparison Calendar Type: Monthly From: 2013/01 to 2013/05 System Analysis Type Violation Count by 2013/01 2013/02 2013/03 2013/04 2013/05 Go  Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_ Quarterly/Monthly Comparison Calendar Type: Monthly From: 2013/01 to 2013/05 System: All Analysis Type: User Violation Count by: Permission 2013/01 2013/02 2013/03 2013/04 2013/05 Go

6

In the report filters section, select the System for which information is required. Click on the Search icon next to 'System'. Since the desired selection is PS1 (Production), select the Connector for PS1; if necessary, '*PS1*' can be used as search criteria to find the correct connector for PS1. Click on 'OK'.


Risk Analysis - Comparison - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_

Quarterly/Monthly Comparison

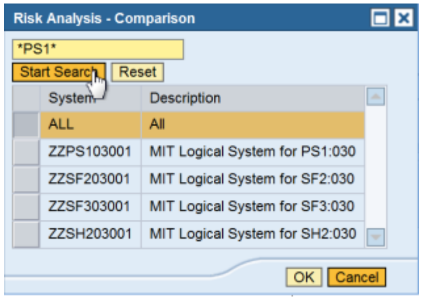
Calendar Type Monthly

From 2013/01 to 2013/05

System All

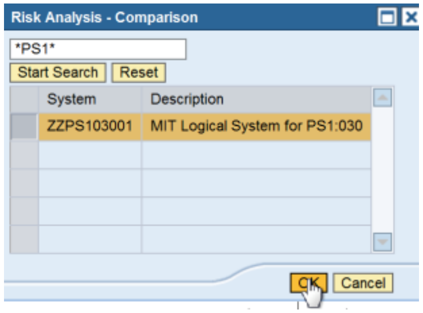
Analysis Type User

Violation Count by Permission



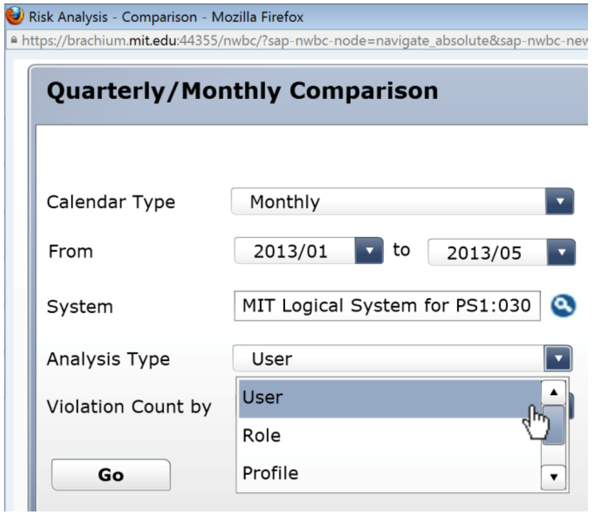
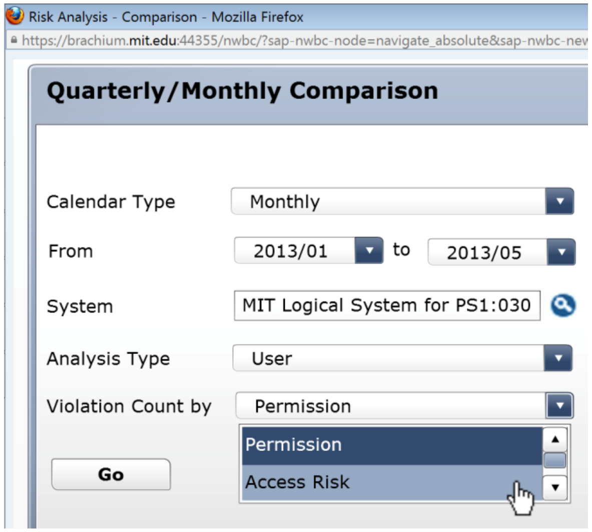
PS1

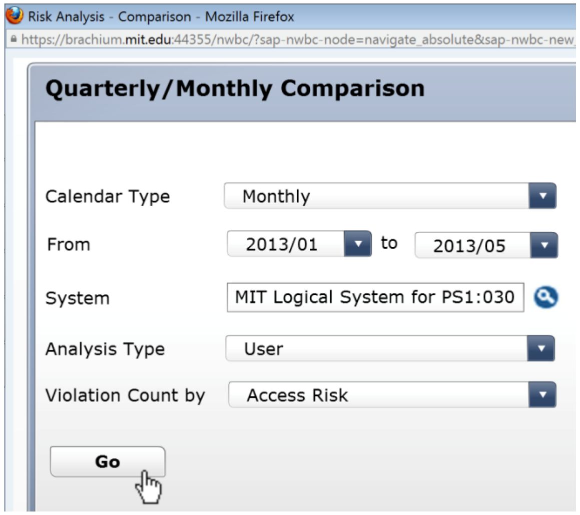
System	Description
ALL	All
ZZPS103001	MIT Logical System for PS1:030
ZZSF203001	MIT Logical System for SF2:030
ZZSF303001	MIT Logical System for SF3:030
ZZSH203001	MIT Logical System for SH2:030

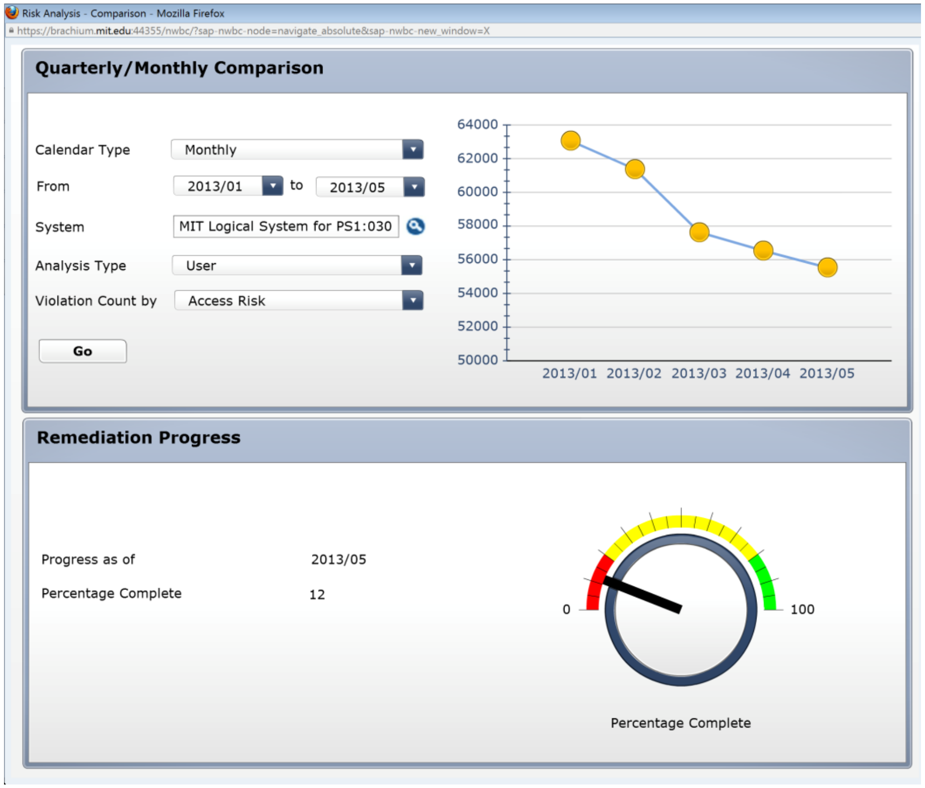


PS1

System	Description
ZZPS103001	MIT Logical System for PS1:030

7	In the report filters section, click on the drop down for ‘Analysis Type’ to select the Security Object (User, Role or Profile) for which data is required. In this case, ‘User’ is selected.	 Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-nev Quarterly/Monthly Comparison Calendar Type: Monthly From: 2013/01 to 2013/05 System: MIT Logical System for PS1:030 Analysis Type: User Violation Count by
8	In the report filters section, click on the drop down for ‘Violation Count by’ to select the count methodology required for the report. In this case, ‘Access Risk’ is selected to count unique violations per User.	 Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-nev Quarterly/Monthly Comparison Calendar Type: Monthly From: 2013/01 to 2013/05 System: MIT Logical System for PS1:030 Analysis Type: User Violation Count by: Permission

9	Click on 'Go' to execute the report based on the criteria that have been defined.	 Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new Quarterly/Monthly Comparison Calendar Type: Monthly From: 2013/01 to 2013/05 System: MIT Logical System for PS1:030 Analysis Type: User Violation Count by: Access Risk Go

10	The report shows the steady decrease in Access Risk violations in MIT’s Production System since the start of the SOD/GRC initiative. A cleanup of the majority of the VPF Areas has yeilded a cleanup of 12% of the PS1 system.	 Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Quarterly/Monthly Comparison** Calendar Type: Monthly From: 2013/01 to 2013/05 System: MIT Logical System for PS1:030 Analysis Type: User Violation Count by: Access Risk Go 64000 62000 60000 58000 56000 54000 52000 50000 2013/01 2013/02 2013/03 2013/04 2013/05 **Remediation Progress** Progress as of: 2013/05 Percentage Complete: 12

Job Aid 04 Access Rule Library

USE

This report can be used to understand MIT's GRC rule set. The report provides an overview of risk rules in GRC.

INFORMATION

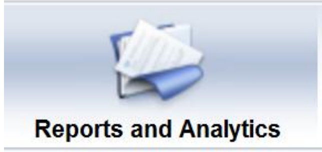
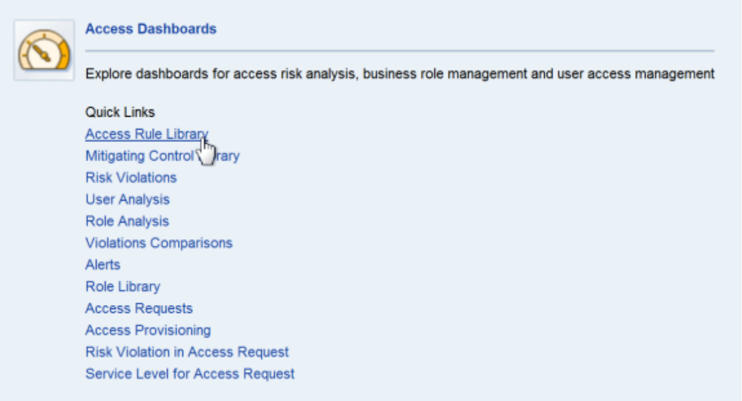
Rule count by risk level and process.

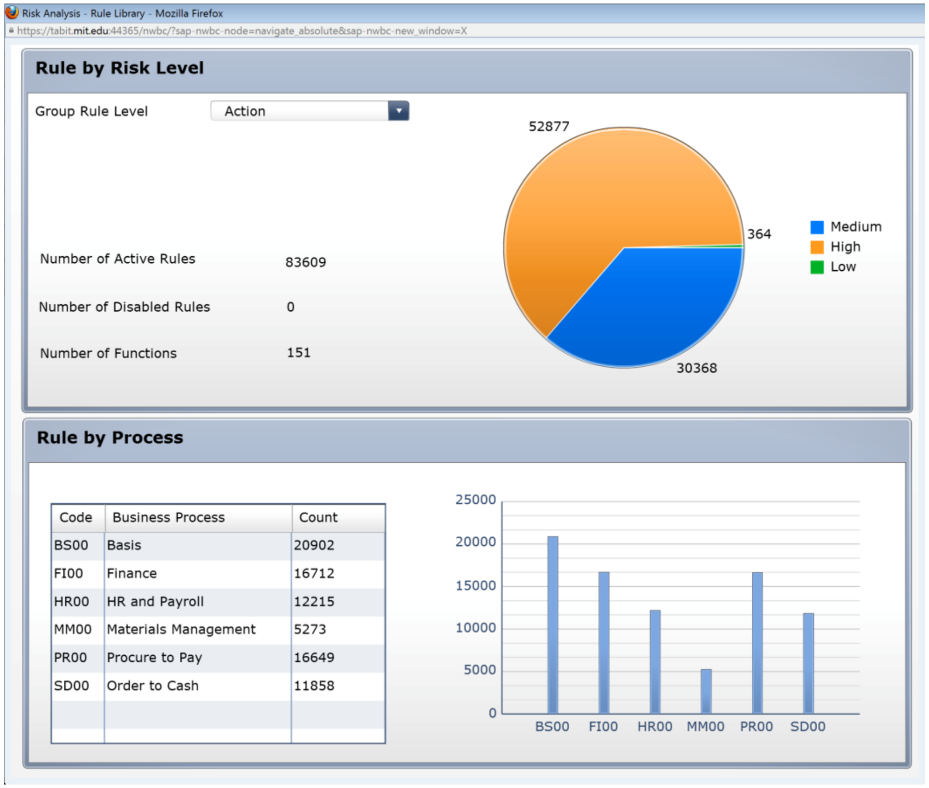
RELATED PROCESSES

- Process 5: Periodic Compliance Reviews

SPECIFIC SCENARIOS

- Step 5A: Analyze report data by Risk Level. (Pie Chart)
- Step 5B: Analyze Access Rules by Business Process. (Table)
- Step 5C: Analyze report data by Business Process. (Bar Graph)

Step	Description	Screenshot
1	Navigate to the 'Reports and Analytics' tab.	
2	Click on the 'Access Rule Library' report located in the 'Access Dashboards' section.	Access Dashboards Explore dashboards for access risk analysis, business role management and user access management Quick Links Access Rule Library Mitigating Control Library Risk Violations User Analysis Role Analysis Violations Comparisons Alerts Role Library Access Requests Access Provisioning Risk Violation in Access Request Service Level for Access Request

3	The report will show information on rules that are defined within all rule sets within the GRC environment.	

Risk Analysis - Rule Library - Mozilla Firefox

https://tabit.mit.edu:44365/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Rule by Risk Level

Group Rule Level: Action

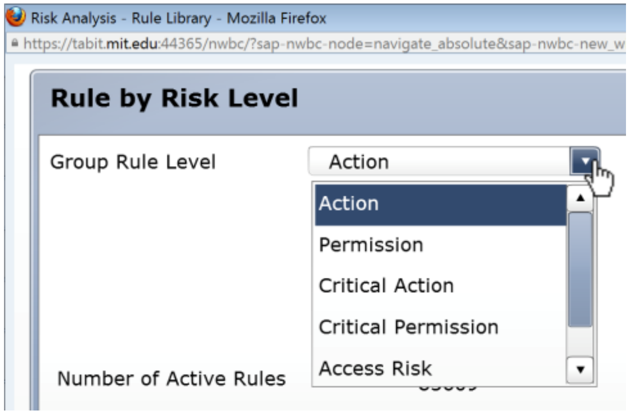
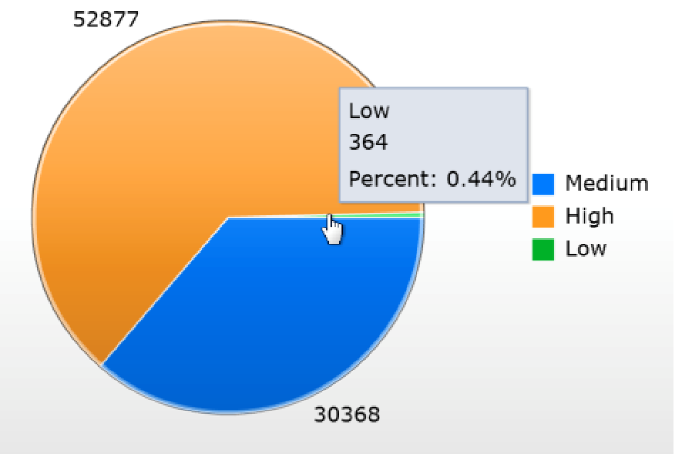
Number of Active Rules 83609

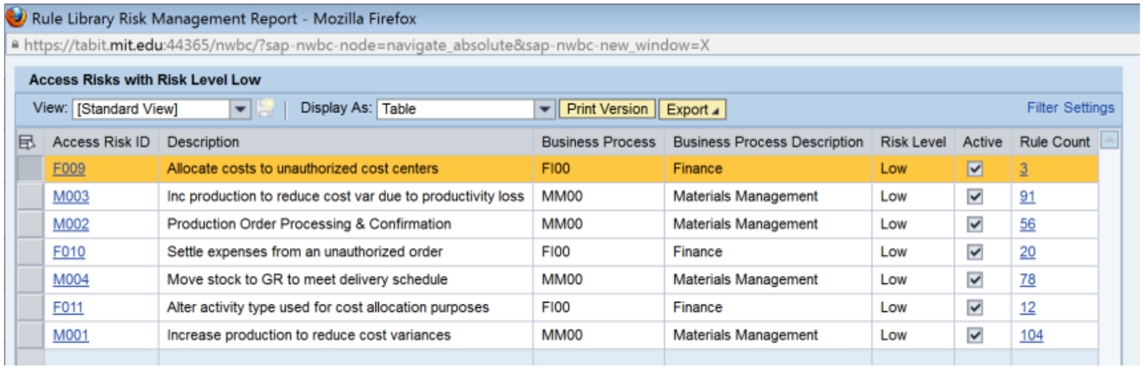
Number of Disabled Rules 0

Number of Functions 151

Rule by Process

Code	Business Process	Count
BS00	Basis	20902
FI00	Finance	16712
HR00	HR and Payroll	12215
MM00	Materials Management	5273
PR00	Procure to Pay	16649
SD00	Order to Cash	11858

4	The report data can be filtered to provide information pertaining to rules that are specific to Actions and Permissions. The report can also be filtered to provide information on Critical Actions, Critical Permissions, and Access Risks, including how many of each exist. In this case, 'Actions' is selected.	 Risk Analysis - Rule Library - Mozilla Firefox https://tabit.mit.edu:44365/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_w Rule by Risk Level Group Rule Level: Action Number of Active Rules Action Permission Critical Action Critical Permission Access Risk
5A-1	Analyze report data by risk level. Scroll over the different pieces of the pie chart to see information about unmitigated violations at each risk level. Click on the 'Low' risk level piece of the pie chart for more information about rules that pertain to Low Level Risks.	

5A-2	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. Access Risk ID: The 4-digit ID representing each Low Risk (as defined in the standard rule set) for which violations exist Description: Business description of the Access Risk Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set Risk Level: The risk level defined for each Access Risk in the standard rule set Active: Whether the rule is active Rule Count: The number of rules for each Access Risk that exist	

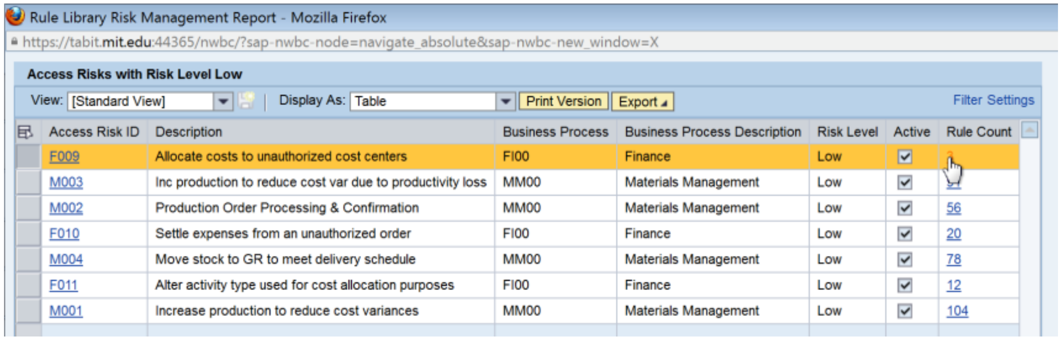
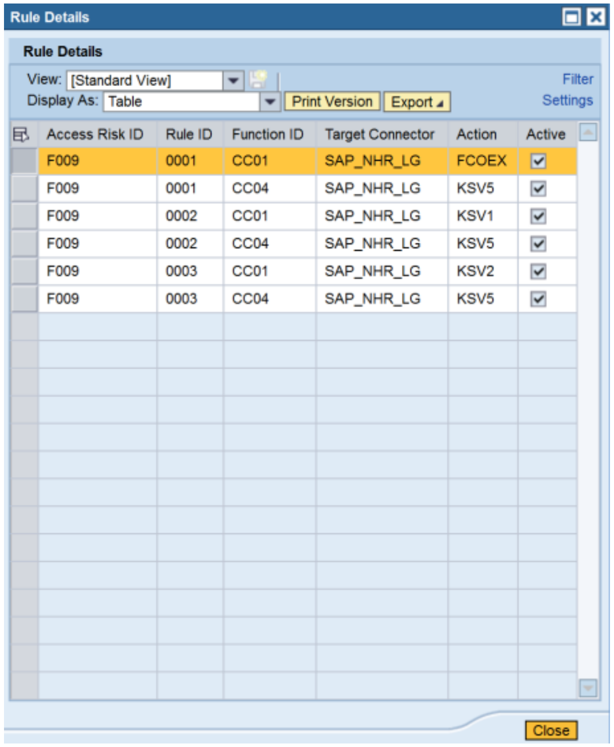
Rule Library Risk Management Report - Mozilla Firefox

https://tabit.mit.edu:44365/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Access Risks with Risk Level Low

View: [Standard View] Display As: Table

Access Risk ID	Description	Business Process	Business Process Description	Risk Level	Active	Rule Count
F009	Allocate costs to unauthorized cost centers	FI00	Finance	Low	☑	3
M003	Inc production to reduce cost var due to productivity loss	MM00	Materials Management	Low	☑	91
M002	Production Order Processing & Confirmation	MM00	Materials Management	Low	☑	56
F010	Settle expenses from an unauthorized order	FI00	Finance	Low	☑	20
M004	Move stock to GR to meet delivery schedule	MM00	Materials Management	Low	☑	78
F011	Alter activity type used for cost allocation purposes	FI00	Finance	Low	☑	12
M001	Increase production to reduce cost variances	MM00	Materials Management	Low	☑	104

5A-3	Click on the 'Rule Count' link for each Access Risk to view the actual rule definitions. In this case, clicking on '3' for Access Risk 'F009' shows the details of the 3 rules that make up that Risk.	 

Rule Library Risk Management Report - Mozilla Firefox

https://tabit.mit.edu:44365/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Access Risks with Risk Level Low

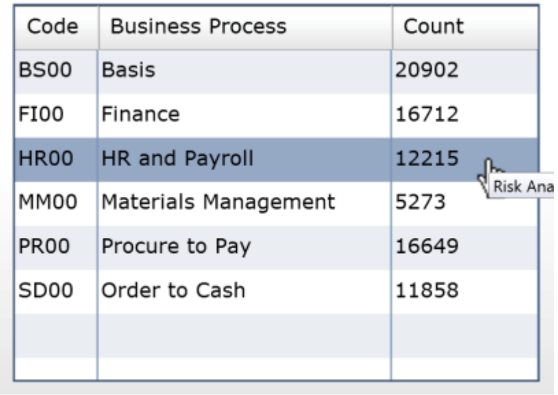
View: [Standard View] Display As: Table

Access Risk ID	Description	Business Process	Business Process Description	Risk Level	Active	Rule Count
F009	Allocate costs to unauthorized cost centers	FI00	Finance	Low	☑	3
M003	Inc production to reduce cost var due to productivity loss	MM00	Materials Management	Low	☑	[illegible]
M002	Production Order Processing & Confirmation	MM00	Materials Management	Low	☑	56
F010	Settle expenses from an unauthorized order	FI00	Finance	Low	☑	20
M004	Move stock to GR to meet delivery schedule	MM00	Materials Management	Low	☑	78
F011	Alter activity type used for cost allocation purposes	FI00	Finance	Low	☑	12
M001	Increase production to reduce cost variances	MM00	Materials Management	Low	☑	104

Rule Details

View: [Standard View]
Display As: Table

Access Risk ID	Rule ID	Function ID	Target Connector	Action	Active
F009	0001	CC01	SAP_NHR_LG	FCOEX	☑
F009	0001	CC04	SAP_NHR_LG	KSV5	☑
F009	0002	CC01	SAP_NHR_LG	KSV1	☑
F009	0002	CC04	SAP_NHR_LG	KSV5	☑
F009	0003	CC01	SAP_NHR_LG	KSV2	☑
F009	0003	CC04	SAP_NHR_LG	KSV5	☑

5B-1	Analyze Access Rules by Business Process. Scroll over the different line items of the Business Process Table to see information about rules for Risks mapped to each Business Process. Click on the ‘HR and Payroll’ Risk row of the Table for more information about rules for HR/Payroll Risks.	

Code	Business Process	Count
BS00	Basis	20902
FI00	Finance	16712
HR00	HR and Payroll	12215
MM00	Materials Management	5273
PR00	Procure to Pay	16649
SD00	Order to Cash	11858

5B-2

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

Access Risk: The 4-digit ID representing each Finance-Risk (as defined in the standard rule set) for which violations exist

Description: Business description of the Access Risk

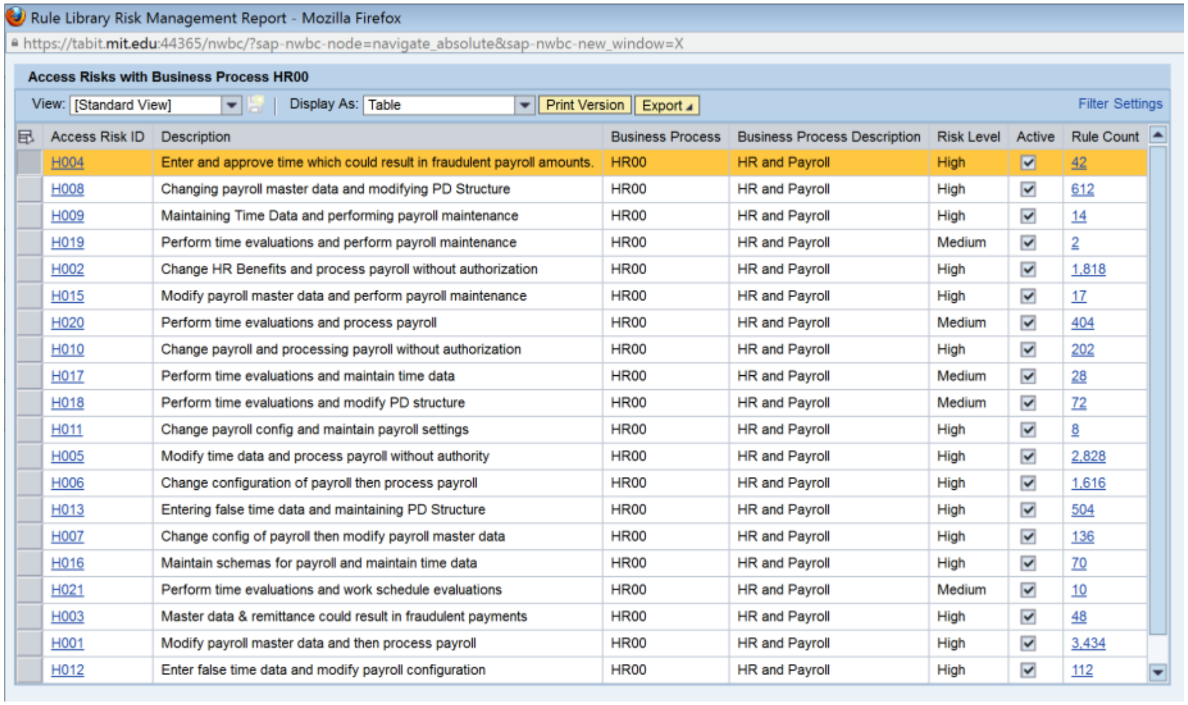
Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set

Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set

Risk Level: The risk level defined for each Access Risk in the standard rule set

Active: Whether the rule is active

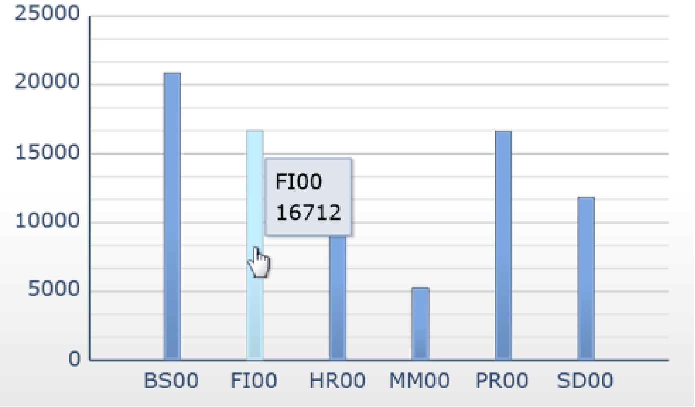
Rule Count: The number of rules for each Access Risk that exist

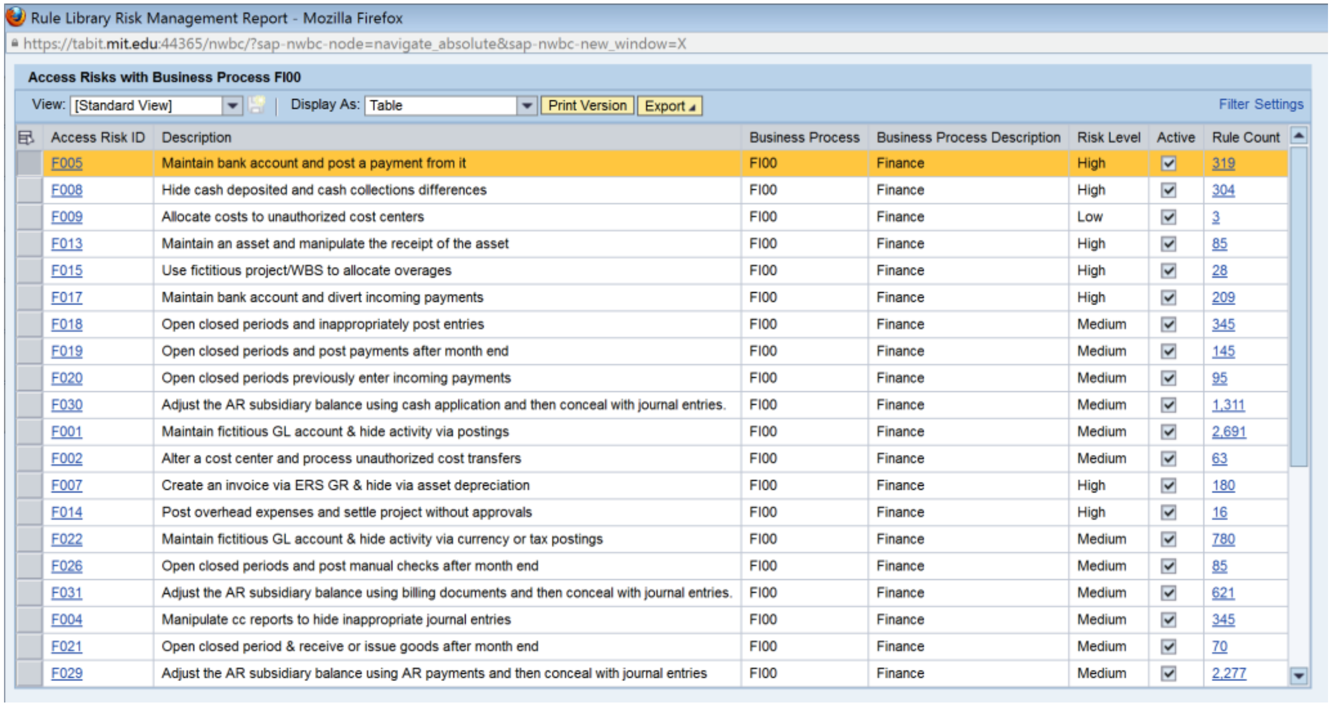

Rule Library Risk Management Report - Mozilla Firefox
https://tabit.mit.edu:44365/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Print Version
Export
Filter Settings

Access Risks with Business Process HR00

View: [Standard View]   Display As: Table

Access Risk ID	Description	Business Process	Business Process Description	Risk Level	Active	Rule Count
H004	Enter and approve time which could result in fraudulent payroll amounts.	HR00	HR and Payroll	High	☑	42
H008	Changing payroll master data and modifying PD Structure	HR00	HR and Payroll	High	☑	612
H009	Maintaining Time Data and performing payroll maintenance	HR00	HR and Payroll	High	☑	14
H019	Perform time evaluations and perform payroll maintenance	HR00	HR and Payroll	Medium	☑	2
H002	Change HR Benefits and process payroll without authorization	HR00	HR and Payroll	High	☑	1,818
H015	Modify payroll master data and perform payroll maintenance	HR00	HR and Payroll	High	☑	17
H020	Perform time evaluations and process payroll	HR00	HR and Payroll	Medium	☑	404
H010	Change payroll and processing payroll without authorization	HR00	HR and Payroll	High	☑	202
H017	Perform time evaluations and maintain time data	HR00	HR and Payroll	Medium	☑	28
H018	Perform time evaluations and modify PD structure	HR00	HR and Payroll	Medium	☑	72
H011	Change payroll config and maintain payroll settings	HR00	HR and Payroll	High	☑	8
H005	Modify time data and process payroll without authority	HR00	HR and Payroll	High	☑	2,828
H006	Change configuration of payroll then process payroll	HR00	HR and Payroll	High	☑	1,616
H013	Entering false time data and maintaining PD Structure	HR00	HR and Payroll	High	☑	504
H007	Change config of payroll then modify payroll master data	HR00	HR and Payroll	High	☑	136
H016	Maintain schemas for payroll and maintain time data	HR00	HR and Payroll	High	☑	70
H021	Perform time evaluations and work schedule evaluations	HR00	HR and Payroll	Medium	☑	10
H003	Master data & remittance could result in fraudulent payments	HR00	HR and Payroll	High	☑	48
H001	Modify payroll master data and then process payroll	HR00	HR and Payroll	High	☑	3,434
H012	Enter false time data and modify payroll configuration	HR00	HR and Payroll	High	☑	112

5C-1	Analyze report data by Business Process. Scroll over the different bars of the Business Process Bar Graph to see information about Rules for Risks tied to each Business Process. Click on the 'FI00' Risk bar of the Graph for more information about Rules related to Finance Risks.	

5C-2	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. Access Risk: The 4-digit ID representing each Finance-Risk (as defined in the standard rule set) for which violations exist Description: Business description of the Access Risk Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set Risk Level: The risk level defined for each Access Risk in the standard rule set Active: Whether the rule is active Rule Count: The number of rules for each Access Risk that exist	

Rule Library Risk Management Report - Mozilla Firefox

https://tabit.mit.edu:44365/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Access Risks with Business Process FI00

View: [Standard View] Display As: Table Print Version Export

Filter Settings

Access Risk ID	Description	Business Process	Business Process Description	Risk Level	Active	Rule Count
F005	Maintain bank account and post a payment from it	FI00	Finance	High	☑	319
F008	Hide cash deposited and cash collections differences	FI00	Finance	High	☑	304
F009	Allocate costs to unauthorized cost centers	FI00	Finance	Low	☑	3
F013	Maintain an asset and manipulate the receipt of the asset	FI00	Finance	High	☑	85
F015	Use fictitious project/WBS to allocate overages	FI00	Finance	High	☑	28
F017	Maintain bank account and divert incoming payments	FI00	Finance	High	☑	209
F018	Open closed periods and inappropriately post entries	FI00	Finance	Medium	☑	345
F019	Open closed periods and post payments after month end	FI00	Finance	Medium	☑	145
F020	Open closed periods previously enter incoming payments	FI00	Finance	Medium	☑	95
F030	Adjust the AR subsidiary balance using cash application and then conceal with journal entries.	FI00	Finance	Medium	☑	1,311
F001	Maintain fictitious GL account & hide activity via postings	FI00	Finance	Medium	☑	2,691
F002	Alter a cost center and process unauthorized cost transfers	FI00	Finance	Medium	☑	63
F007	Create an invoice via ERS GR & hide via asset depreciation	FI00	Finance	High	☑	180
F014	Post overhead expenses and settle project without approvals	FI00	Finance	High	☑	16
F022	Maintain fictitious GL account & hide activity via currency or tax postings	FI00	Finance	Medium	☑	780
F026	Open closed periods and post manual checks after month end	FI00	Finance	Medium	☑	85
F031	Adjust the AR subsidiary balance using billing documents and then conceal with journal entries.	FI00	Finance	Medium	☑	621
F004	Manipulate cc reports to hide inappropriate journal entries	FI00	Finance	Medium	☑	345
F021	Open closed period & receive or issue goods after month end	FI00	Finance	Medium	☑	70
F029	Adjust the AR subsidiary balance using AR payments and then conceal with journal entries	FI00	Finance	Medium	☑	2,277

Job Aid 05 SUIM Roles by Role Name

USE

This report can be used to understand the mapping between single and composite roles. The report displays which single roles are assigned to a composite role.

INFORMATION

Report shows:

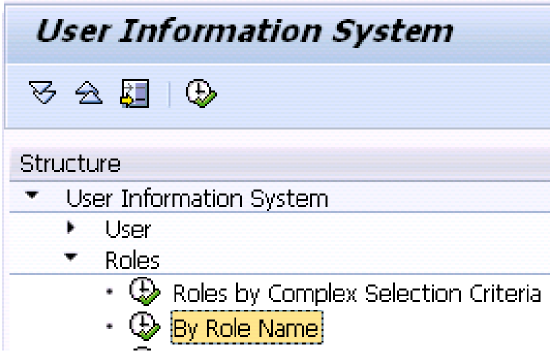
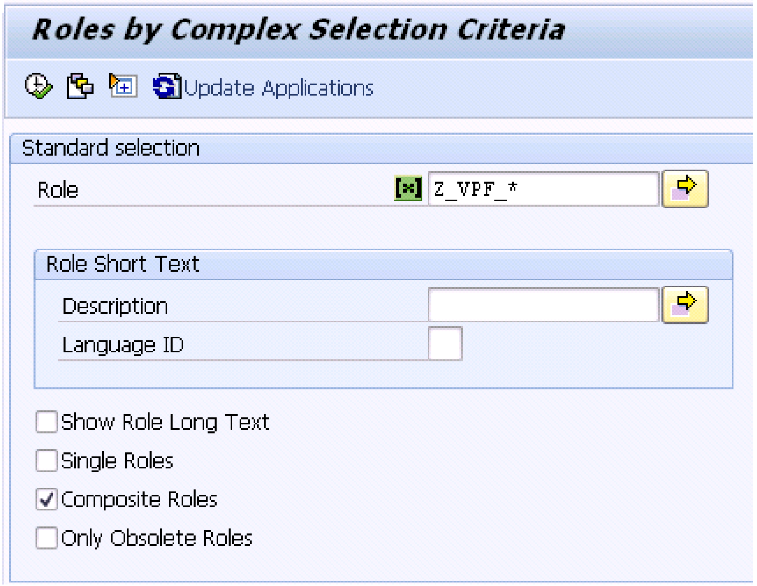
- List of transaction codes included in the roles
- Other composite roles which have a selected single role
- Users assigned to the roles

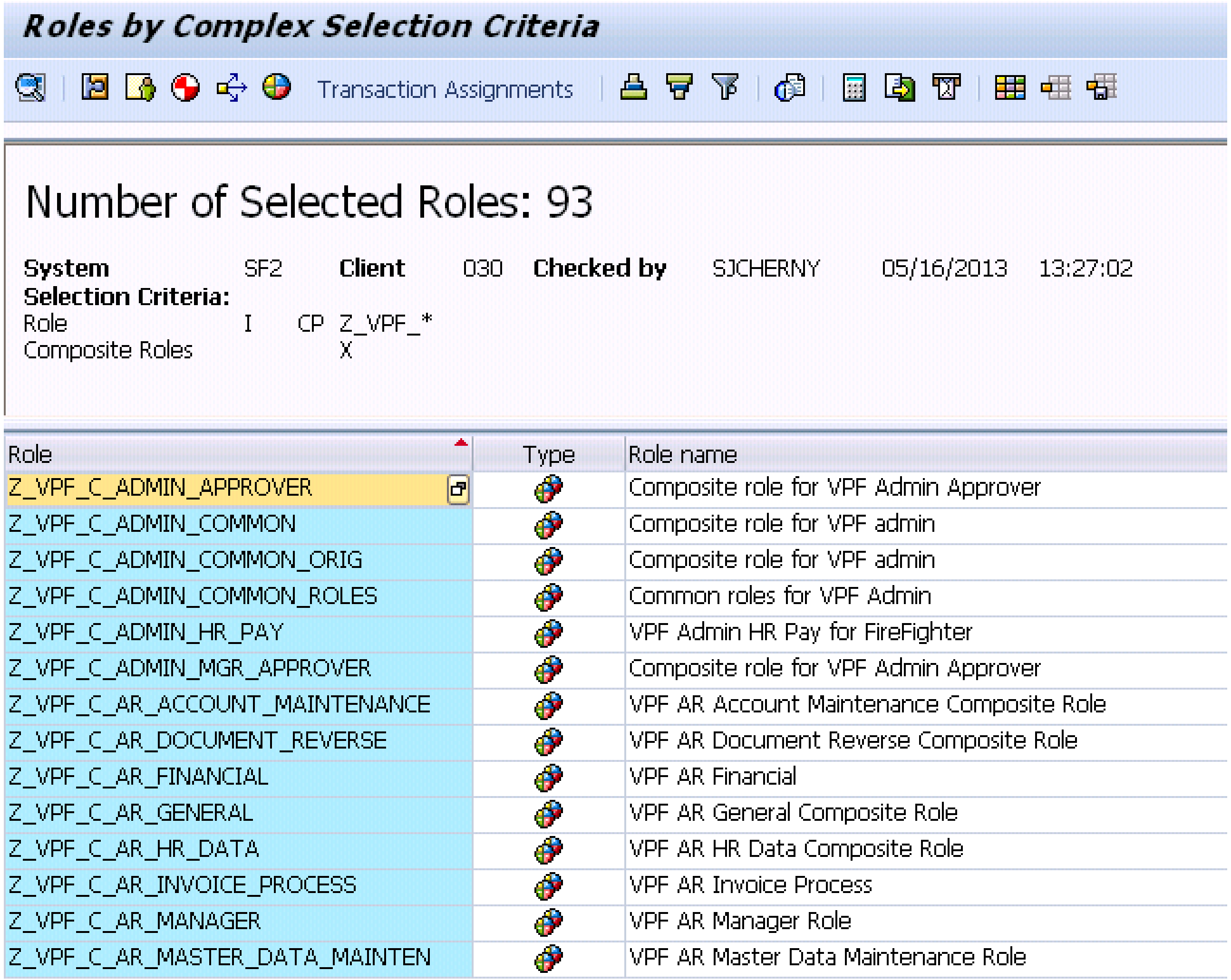
RELATED PROCESSES

- Process 1: New or Amended Roles

SPECIFIC SCENARIOS

- N/A

Step	Description	Screenshot
1	In SAP R/3 EEC– use transaction code SUIM. Then click on the ‘Roles’ node and double click on the option for “By Role Name” Or use Transaction Code • S_BCE_68001418	 **User Information System** Structure User Information System User Roles • Roles by Complex Selection Criteria • By Role Name
2	Select the Composite Role or Roles to be analyzed – e.g. Z_VPF* Also, check the “Composite Roles” selection only, so that single roles are not listed at this point.	 **Roles by Complex Selection Criteria** Update Applications Standard selection Role: Z_VPF_* Role Short Text Description: Language ID: ☐ Show Role Long Text ☐ Single Roles ☑ Composite Roles ☐ Only Obsolete Roles

3	The report will show a list of Composite Roles matching the selection criteria. It shows : • Role id • Role name From this report, you can drill down to get the following information : • Administrative Details • Transaction Assignments • Contained Single roles • Users Assigned the composite role	

Roles by Complex Selection Criteria

Number of Selected Roles: 93

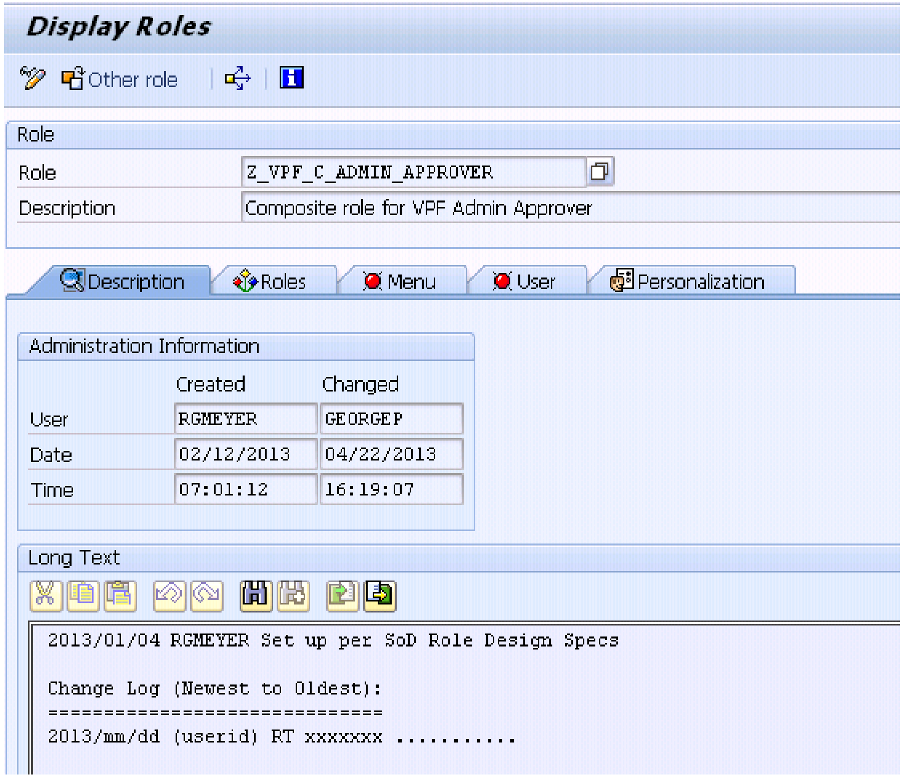
System SF2 **Client** 030 **Checked by** SJCHERNY 05/16/2013 13:27:02

Selection Criteria:

Role I CP Z_VPF_*

Composite Roles X

Role	Type	Role name
Z_VPF_C_ADMIN_APPROVER	●	Composite role for VPF Admin Approver
Z_VPF_C_ADMIN_COMMON	●	Composite role for VPF admin
Z_VPF_C_ADMIN_COMMON_ORIG	●	Composite role for VPF admin
Z_VPF_C_ADMIN_COMMON_ROLES	●	Common roles for VPF Admin
Z_VPF_C_ADMIN_HR_PAY	●	VPF Admin HR Pay for FireFighter
Z_VPF_C_ADMIN_MGR_APPROVER	●	Composite role for VPF Admin Approver
Z_VPF_C_AR_ACCOUNT_MAINTENANCE	●	VPF AR Account Maintenance Composite Role
Z_VPF_C_AR_DOCUMENT_REVERSE	●	VPF AR Document Reverse Composite Role
Z_VPF_C_AR_FINANCIAL	●	VPF AR Financial
Z_VPF_C_AR_GENERAL	●	VPF AR General Composite Role
Z_VPF_C_AR_HR_DATA	●	VPF AR HR Data Composite Role
Z_VPF_C_AR_INVOICE_PROCESS	●	VPF AR Invoice Process
Z_VPF_C_AR_MANAGER	●	VPF AR Manager Role
Z_VPF_C_AR_MASTER_DATA_MAINTEN	●	VPF AR Master Data Maintenance Role

3a	ADMINISTRATIVE DETAILS Double click on a Composite role or Click on a Composite Role to highlight it, then : Menu : GoTo → Display details or Icon To exit back to the list, click on Back (F3). Click on Roles tab to see a list of roles – but this the long way – see 3.c instead.	

Role

Role	Z_VPF_C_ADMIN_APPROVER
Description	Composite role for VPF Admin Approver

Administration Information

	Created	Changed
User	RGMEYER	GEORGEP
Date	02/12/2013	04/22/2013
Time	07:01:12	16:19:07

```
2013/01/04 RGMEYER Set up per SoD Role Design Specs

Change Log (Newest to Oldest):
==============================
2013/mm/dd (userid) RT xxxxxxx ..........
```

3b

TRANSACTIONS

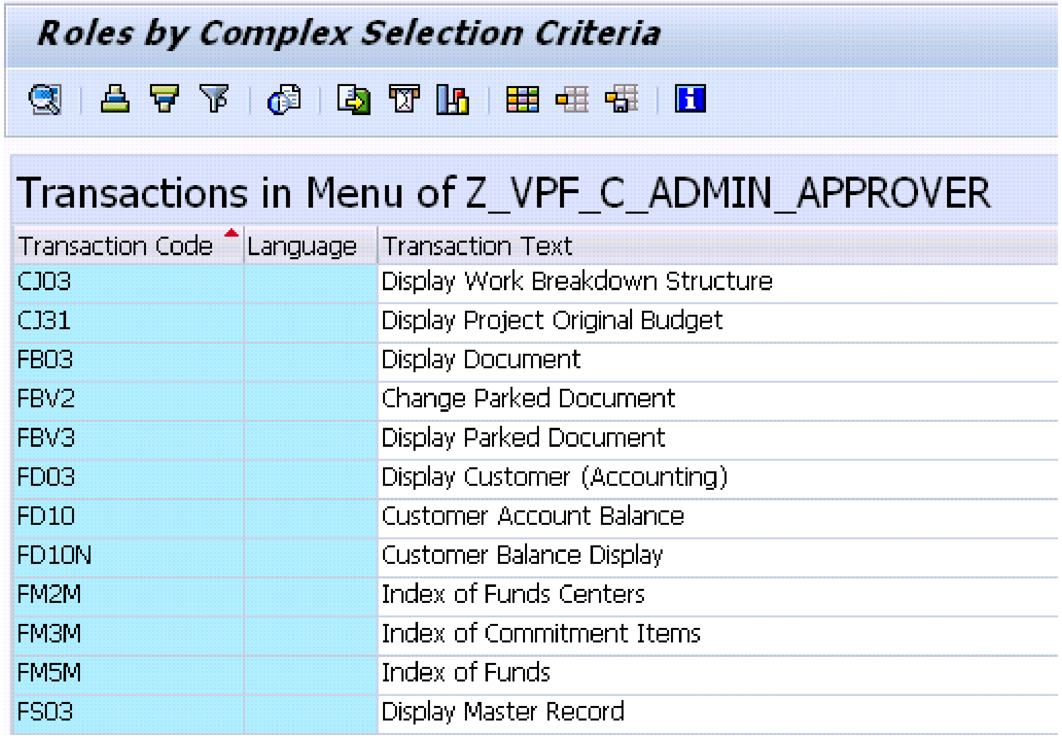
For the Transaction List , click on a Composite Role to highlight it, then :

Menu : Role → Transaction Assignments
or Icon
Transaction Assignments

There is no more drill down from here.

To exit the list, click on

Back (F3).



Roles by Complex Selection Criteria

Transactions in Menu of Z_VPF_C_ADMIN_APPROVER

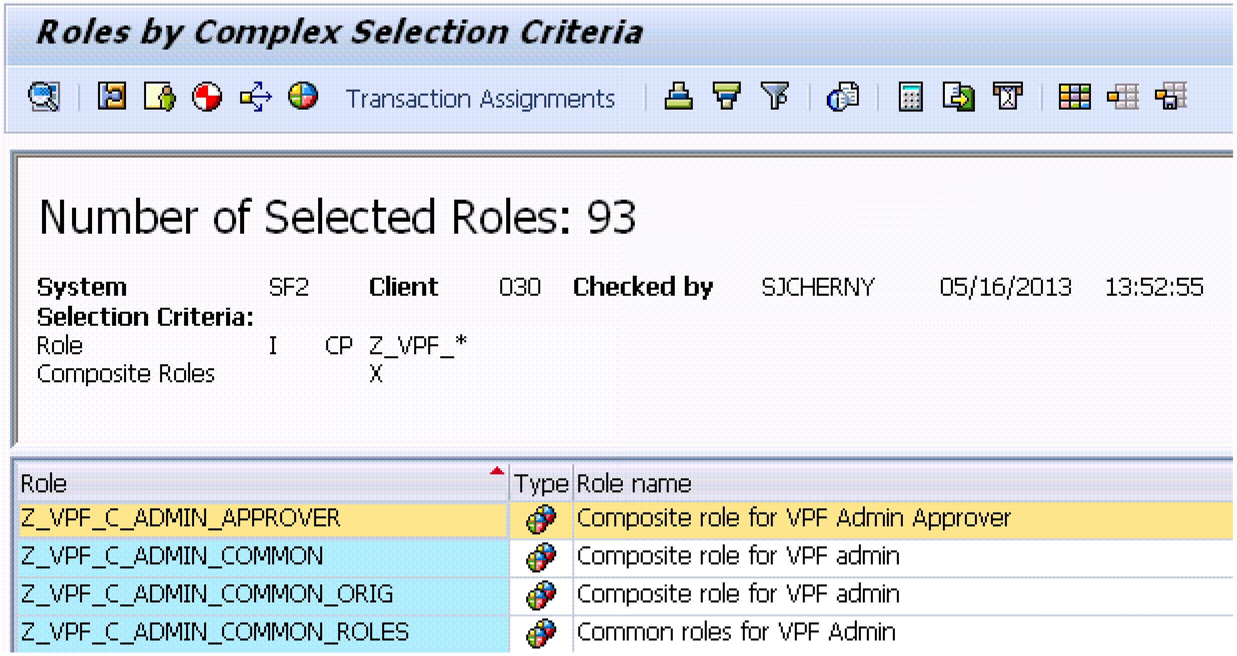
Transaction Code	Language	Transaction Text
CJ03		Display Work Breakdown Structure
CJ31		Display Project Original Budget
FB03		Display Document
FBV2		Change Parked Document
FBV3		Display Parked Document
FD03		Display Customer (Accounting)
FD10		Customer Account Balance
FD10N		Customer Balance Display
FM2M		Index of Funds Centers
FM3M		Index of Commitment Items
FM5M		Index of Funds
FS03		Display Master Record

<table>
<tr>
<td>3c</td>
<td>ROLES CONTAINED

For the quick Role List , click on a Composite Role to highlight it, then :

Menu : Role → Contained Single Roles
or
Click on Icon

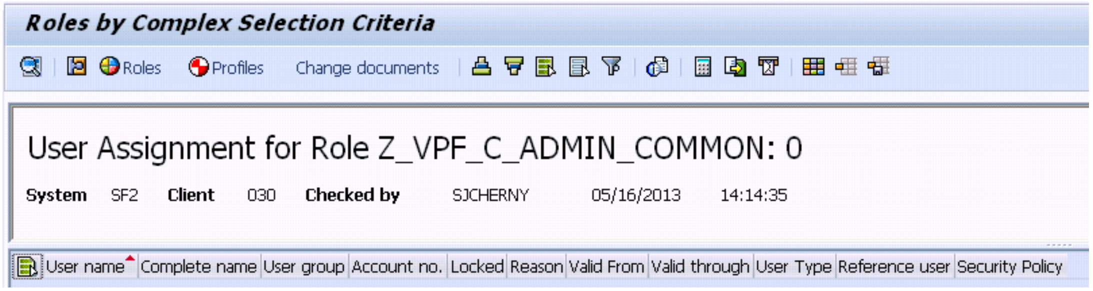
To drilldown further on the single role – see Step 4 for details.

To exit the list, click on
Back (F3).</td>
<td>
Roles by Complex Selection Criteria
Transaction Assignments

Number of Selected Roles: 93

<table>
<tr><td>System</td><td>SF2</td><td>Client</td><td>030</td><td>Checked by</td><td>SJCHERNY</td><td>05/16/2013</td><td>13:52:55</td></tr>
<tr><td>Selection Criteria:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Role</td><td>I</td><td>CP Z_VPF_*</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Composite Roles</td><td></td><td>X</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

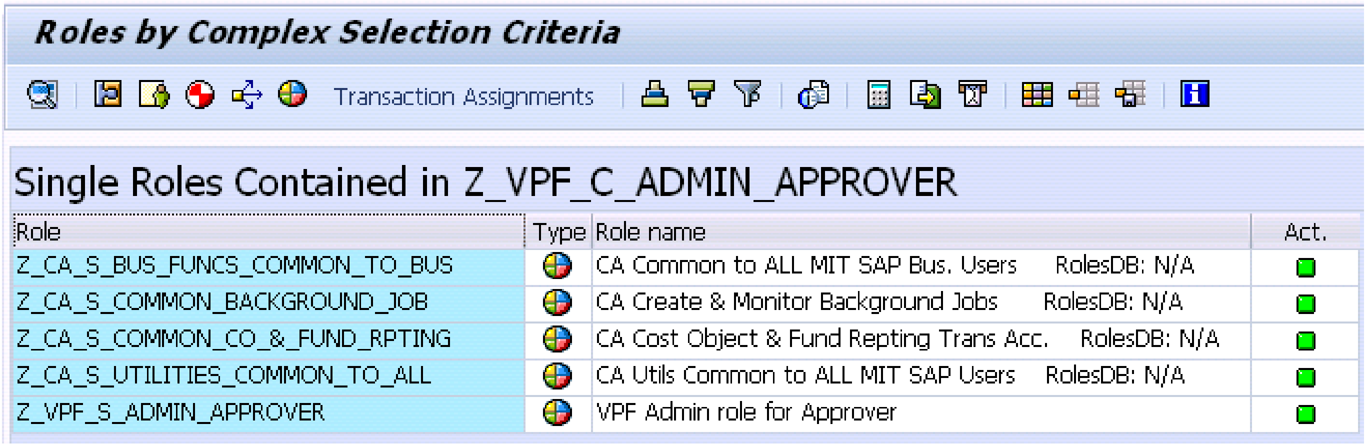
<table>
<tr><th>Role</th><th>Type</th><th>Role name</th></tr>
<tr><td>Z_VPF_C_ADMIN_APPROVER</td><td></td><td>Composite role for VPF Admin Approver</td></tr>
<tr><td>Z_VPF_C_ADMIN_COMMON</td><td></td><td>Composite role for VPF admin</td></tr>
<tr><td>Z_VPF_C_ADMIN_COMMON_ORIG</td><td></td><td>Composite role for VPF admin</td></tr>
<tr><td>Z_VPF_C_ADMIN_COMMON_ROLES</td><td></td><td>Common roles for VPF Admin</td></tr>
</table>
</td>
</tr>
<tr>
<td>3d</td>
<td>USERS ASSIGNED

Menu : Role → User Assignment
or
Click on Icon</td>
<td>
Roles by Complex Selection Criteria
Roles Profiles Change documents

User Assignment for Role Z_VPF_C_ADMIN_COMMON: 0

<table>
<tr><td>System</td><td>SF2</td><td>Client</td><td>030</td><td>Checked by</td><td>SJCHERNY</td><td>05/16/2013</td><td>14:14:35</td></tr>
</table>

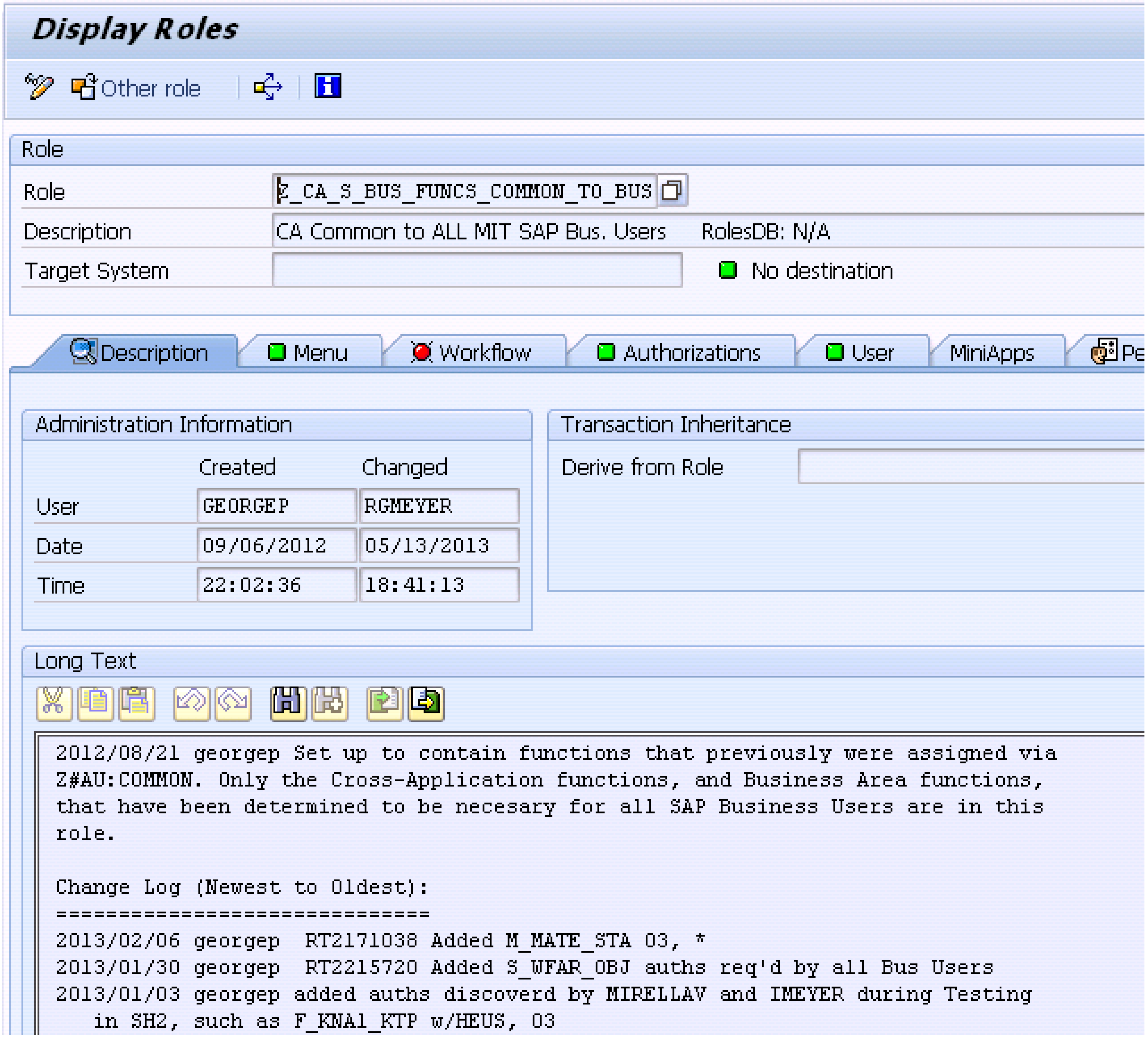
<table>
<tr><th>User name</th><th>Complete name</th><th>User group</th><th>Account no.</th><th>Locked</th><th>Reason</th><th>Valid From</th><th>Valid through</th><th>User Type</th><th>Reference user</th><th>Security Policy</th></tr>
</table>
</td>
</tr>
</table>

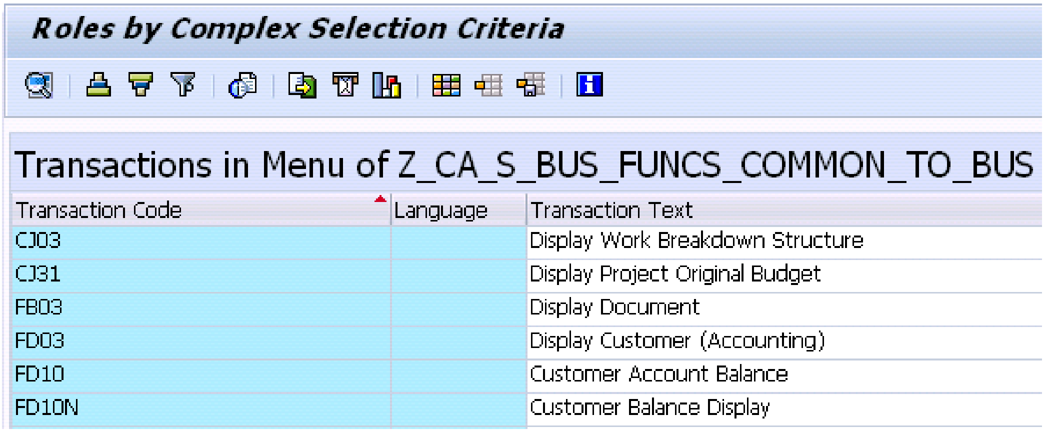
4	From the list of Single Roles you can click on a role to highlight it and use the icons or menu to : a. Display (Administrative) Details b. See transactions for the single role. c. Find which other Composite Roles include this single role	

Roles by Complex Selection Criteria

Single Roles Contained in Z_VPF_C_ADMIN_APPROVER

Role	Type	Role name	Act.
Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	●	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	🟩
Z_CA_S_COMMON_BACKGROUND_JOB	●	CA Create & Monitor Background Jobs RolesDB: N/A	🟩
Z_CA_S_COMMON_CO_&_FUND_RPTING	●	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	🟩
Z_CA_S_UTILITIES_COMMON_TO_ALL	●	CA Utils Common to ALL MIT SAP Users RolesDB: N/A	🟩
Z_VPF_S_ADMIN_APPROVER	●	VPF Admin role for Approver	🟩

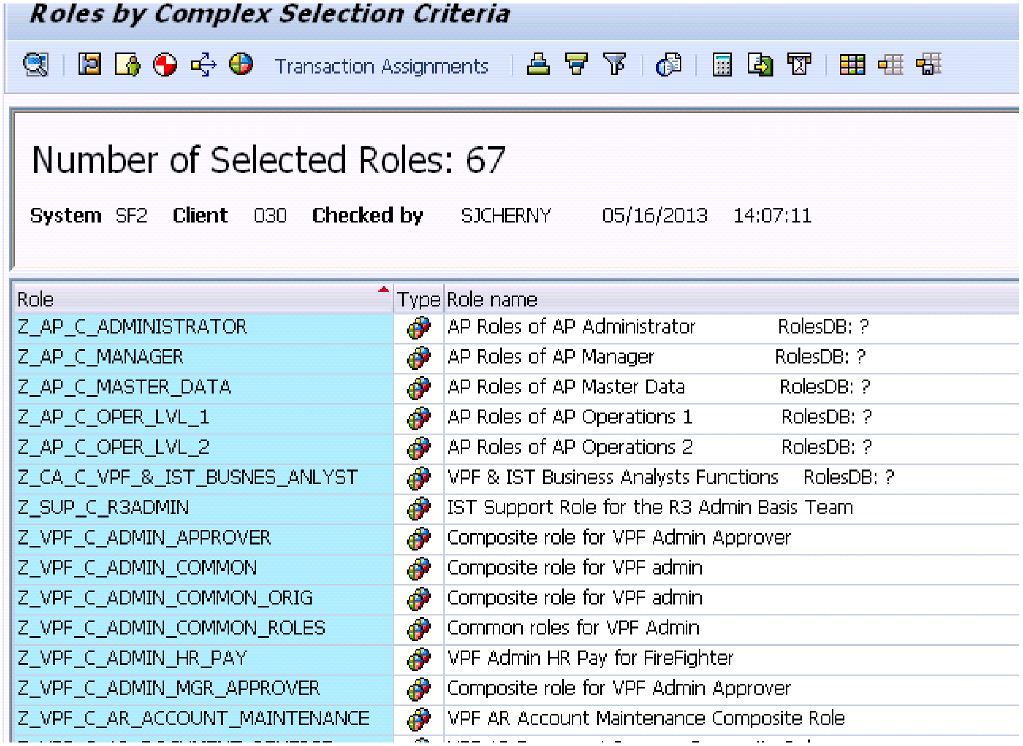
4a	DATE LAST CHANGED Click on a role to highlight it then Click on Icon or use Menu : GoTo → Display (Administrative) Details Or double click on the role. To exit, click on Back (F3).	 **Display Roles** Role Role: Z_CA_S_BUS_FUNCS_COMMON_TO_BUS Description: CA Common to ALL MIT SAP Bus. Users RolesDB: N/A Target System: 🟩 No destination Description 🟩 Menu 🔴 Workflow 🟩 Authorizations 🟩 User MiniApps Pe Administration Information Created / Changed User: GEORGEP / RGMEYER Date: 09/06/2012 / 05/13/2013 Time: 22:02:36 / 18:41:13 Transaction Inheritance Derive from Role: Long Text 2012/08/21 georgep Set up to contain functions that previously were assigned via Z#AU:COMMON. Only the Cross-Application functions, and Business Area functions, that have been determined to be necesary for all SAP Business Users are in this role. Change Log (Newest to Oldest): ============================== 2013/02/06 georgep RT2171038 Added M_MATE_STA 03, * 2013/01/30 georgep RT2215720 Added S_WFAR_OBJ auths req'd by all Bus Users 2013/01/03 georgep added auths discovered by MIRELLAV and IMEYER during Testing in SH2, such as F_KNA1_KTP w/HEUS, 03

4b	TRANSACTION ASSIGNMENT Click on a role to highlight it then Click on Icon Transaction Assignments or use Menu : Role → Transaction Assignments To exit, click on Back (F3).	

Roles by Complex Selection Criteria

Transactions in Menu of Z_CA_S_BUS_FUNCS_COMMON_TO_BUS

Transaction Code	Language	Transaction Text
CJ03		Display Work Breakdown Structure
CJ31		Display Project Original Budget
FB03		Display Document
FD03		Display Customer (Accounting)
FD10		Customer Account Balance
FD10N		Customer Balance Display

4c	WHERE USED IN COMP ROLES Click on a role to highlight it then Click on Icon To exit, click on Back (F3).	

Roles by Complex Selection Criteria

Number of Selected Roles: 67

System SF2 Client 030 Checked by SJCHERNY 05/16/2013 14:07:11

Role	Type	Role name
Z_AP_C_ADMINISTRATOR		AP Roles of AP Administrator RolesDB: ?
Z_AP_C_MANAGER		AP Roles of AP Manager RolesDB: ?
Z_AP_C_MASTER_DATA		AP Roles of AP Master Data RolesDB: ?
Z_AP_C_OPER_LVL_1		AP Roles of AP Operations 1 RolesDB: ?
Z_AP_C_OPER_LVL_2		AP Roles of AP Operations 2 RolesDB: ?
Z_CA_C_VPF_&_IST_BUSNES_ANLYST		VPF & IST Business Analysts Functions RolesDB: ?
Z_SUP_C_R3ADMIN		IST Support Role for the R3 Admin Basis Team
Z_VPF_C_ADMIN_APPROVER		Composite role for VPF Admin Approver
Z_VPF_C_ADMIN_COMMON		Composite role for VPF admin
Z_VPF_C_ADMIN_COMMON_ORIG		Composite role for VPF admin
Z_VPF_C_ADMIN_COMMON_ROLES		Common roles for VPF Admin
Z_VPF_C_ADMIN_HR_PAY		VPF Admin HR Pay for FireFighter
Z_VPF_C_ADMIN_MGR_APPROVER		Composite role for VPF Admin Approver
Z_VPF_C_AR_ACCOUNT_MAINTENANCE		VPF AR Account Maintenance Composite Role

Job Aid 06 User to Role Relationship

USE

This report can be used to determine all users assigned to a role.

INFORMATION

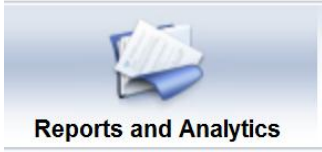
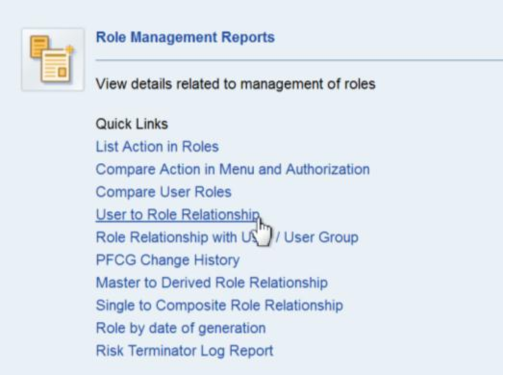
List of all users with access to a particular role or set of roles.

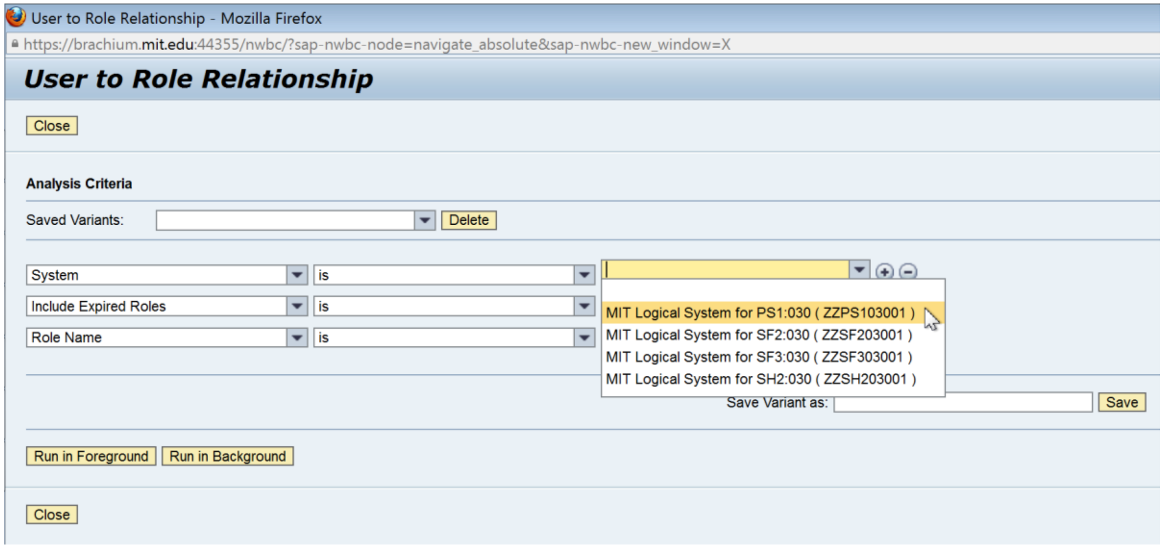
RELATED PROCESSES

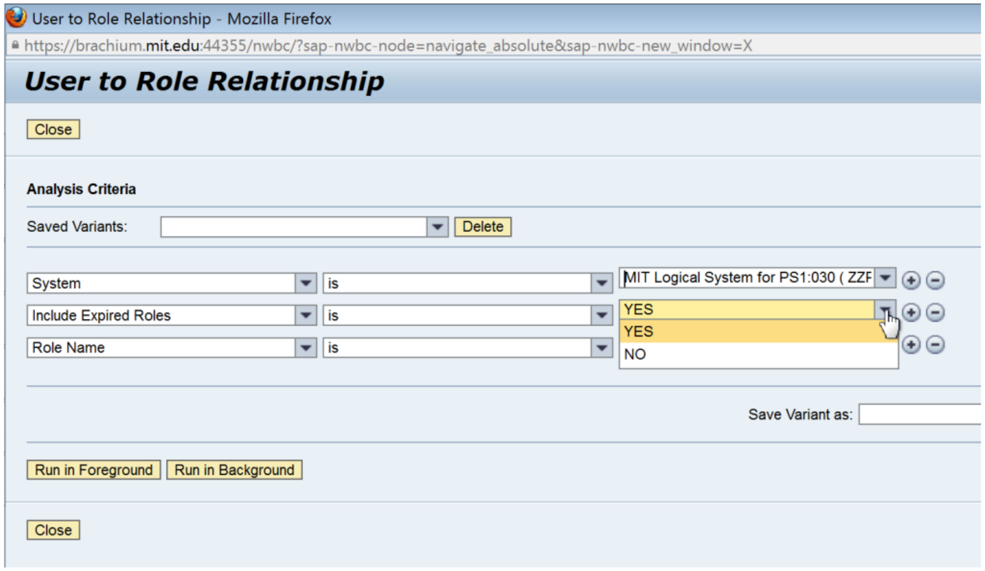
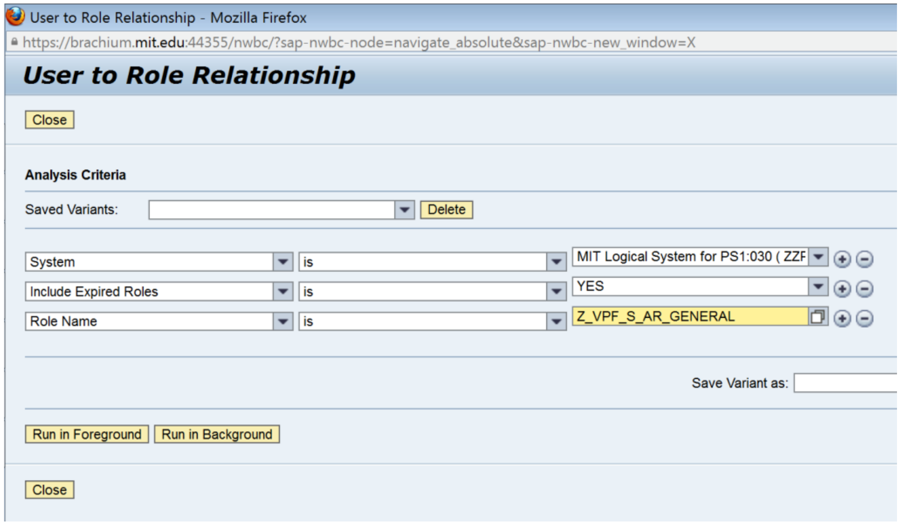
- Process 1: New or Amended Roles

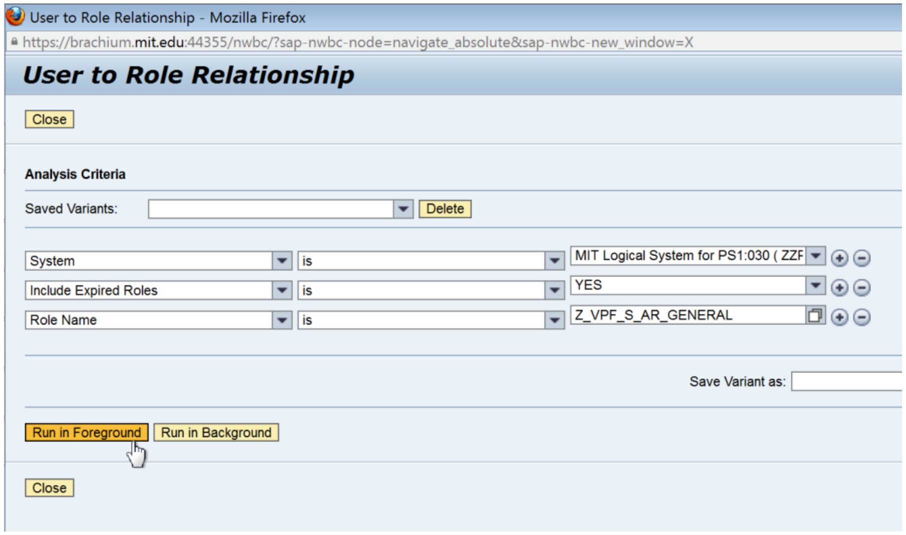
SPECIFIC SCENARIOS

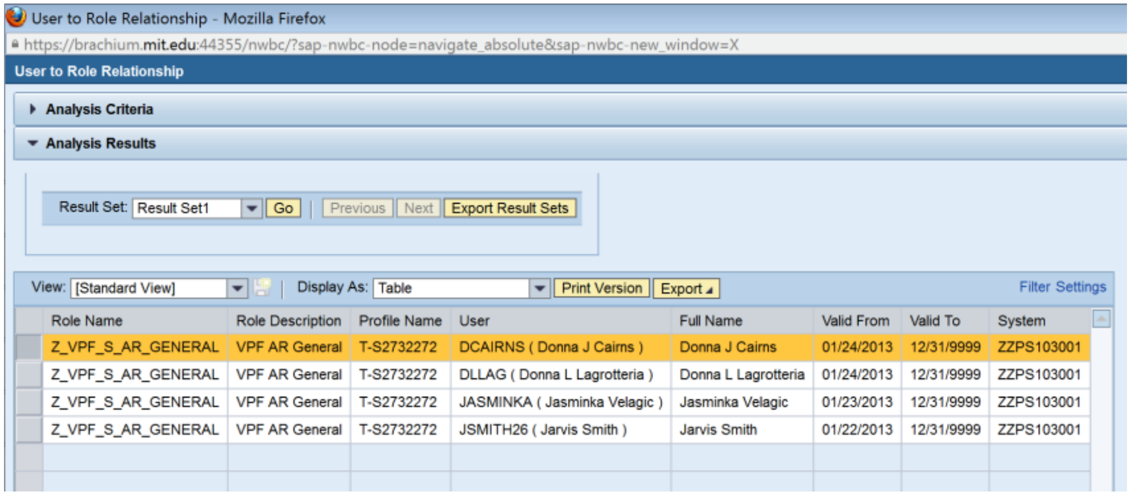
- Step 5A: Analyze for a single role.
- Step 5B: Analyze for multiple roles by specific role names.
- Step 5C: Analyze for multiple roles by using a wild card (*) in the role name.

Step	Description	Screenshot
1	Navigate to the ‘Reports and Analytics’ tab.	
2	Click on the ‘User to Role Relationship’ report located in the ‘Role Management Reports’ section.	 Role Management Reports View details related to management of roles Quick Links List Action in Roles Compare Action in Menu and Authorization Compare User Roles User to Role Relationship Role Relationship with User / User Group PFCG Change History Master to Derived Role Relationship Single to Composite Role Relationship Role by date of generation Risk Terminator Log Report

3	Select the system for which information is required. In this case, the selection is PS1.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **User to Role Relationship** Close **Analysis Criteria** Saved Variants: Delete System is Include Expired Roles is Role Name is MIT Logical System for PS1:030 (ZZPS103001) MIT Logical System for SF2:030 (ZZSF203001) MIT Logical System for SF3:030 (ZZSF303001) MIT Logical System for SH2:030 (ZZSH203001) Save Variant as: Save Run in Foreground Run in Background Close

4	Select whether to include information on role assignments which have expired for users (i.e. that have assignment end-dates prior to the current date). In this case, the selection is 'Yes'.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X User to Role Relationship Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Include Expired Roles is YES Role Name is Save Variant as: Close Delete YES YES NO Run in Foreground Run in Background Close
5A-1	Analyze for a single role. Add the role name. In this case, 'Z_VPF_S_AR_GENERAL' was typed in. The search option can also be used to search for a role. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X User to Role Relationship Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Include Expired Roles is YES Role Name is Z_VPF_S_AR_GENERAL Save Variant as: Close Delete Run in Foreground Run in Background Close

5A-2	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X User to Role Relationship Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Include Expired Roles is YES Role Name is Z_VPF_S_AR_GENERAL Save Variant as: Run in Foreground Run in Background Close

5A-3	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. Role Name: SAP role name Role Description: Business name for SAP role Profile Name: Name of SAP profile associated with SAP role (technical information) User: User ID of the user with access to the role Full Name: User name of user with access to role Valid From: Date on which assignment of the role to the user begins Valid To: Date on which assignment of the role to the user ends System: The system in which the role is assigned to the user	

User to Role Relationship - Mozilla Firefox

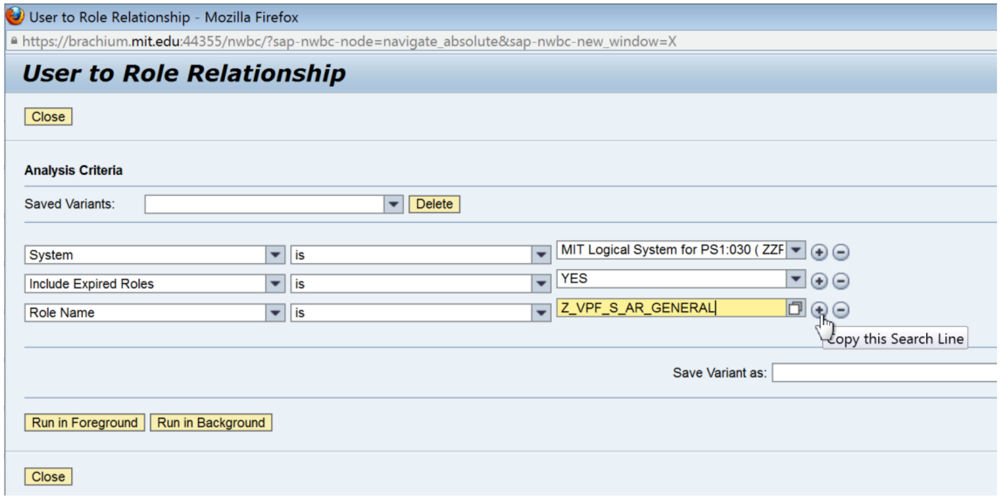
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

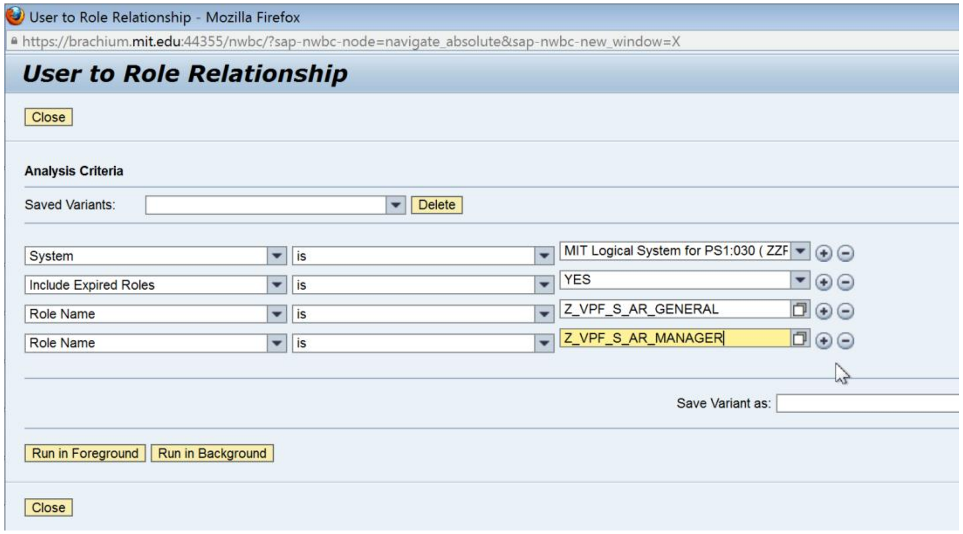
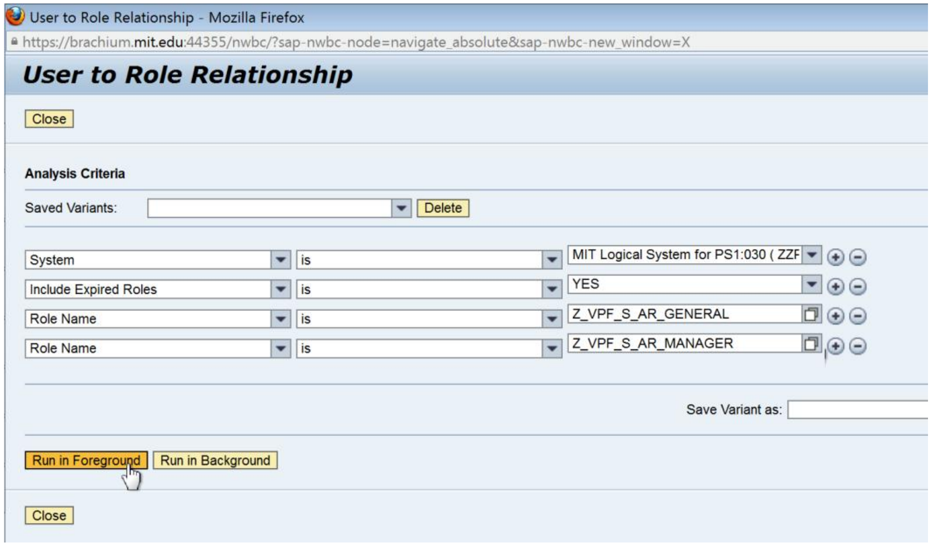
User to Role Relationship

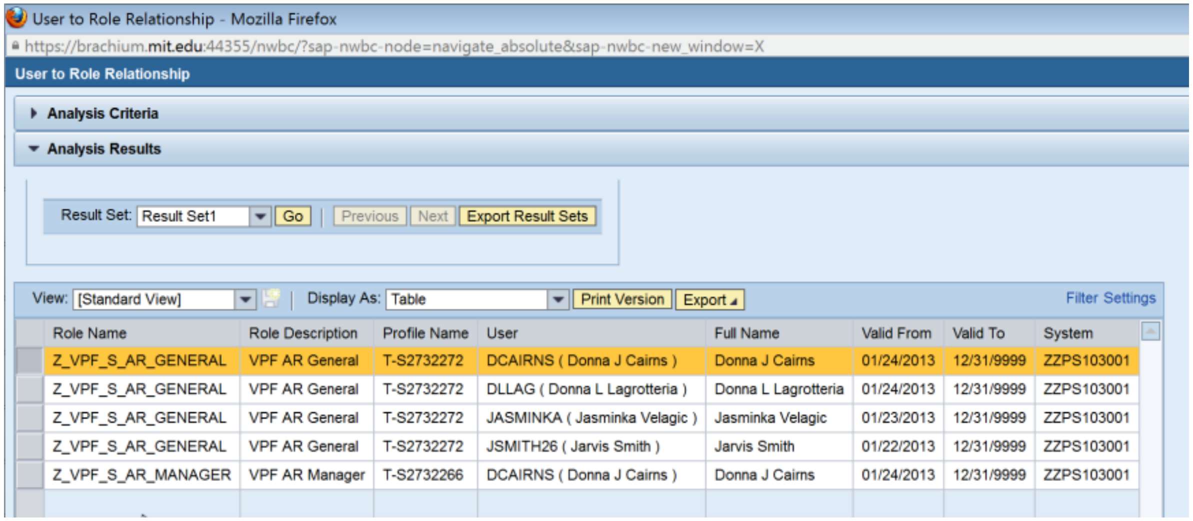
Result Set: Result Set1

View: [Standard View]   Display As: Table

Role Name	Role Description	Profile Name	User	Full Name	Valid From	Valid To	System
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001

5B-1	Analyze for multiple roles by specific role names. To do this, we can add the first role name. In this case, ‘Z_VPF_S_AR_GENERAL’ was typed in. The search option can also be used to search for a role. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. Next, add an additional Search Line. See the ‘Add or Remove Search Lines to a Report’ reference document (R2) for further information.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X User to Role Relationship Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Include Expired Roles is YES Role Name is Z_VPF_S_AR_GENERAL Save Variant as: Close Delete Copy this Search Line Run in Foreground Run in Background Close

5B-2	Add the additional role name. In this case, 'Z_VPF_S_AR_MANAGER' was typed in. The search option can also be used to search for a role.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **User to Role Relationship** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Include Expired Roles is YES Role Name is Z_VPF_S_AR_GENERAL Role Name is Z_VPF_S_AR_MANAGER Save Variant as: Run in Foreground Run in Background Close
5B-3	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **User to Role Relationship** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Include Expired Roles is YES Role Name is Z_VPF_S_AR_GENERAL Role Name is Z_VPF_S_AR_MANAGER Save Variant as: Run in Foreground Run in Background Close

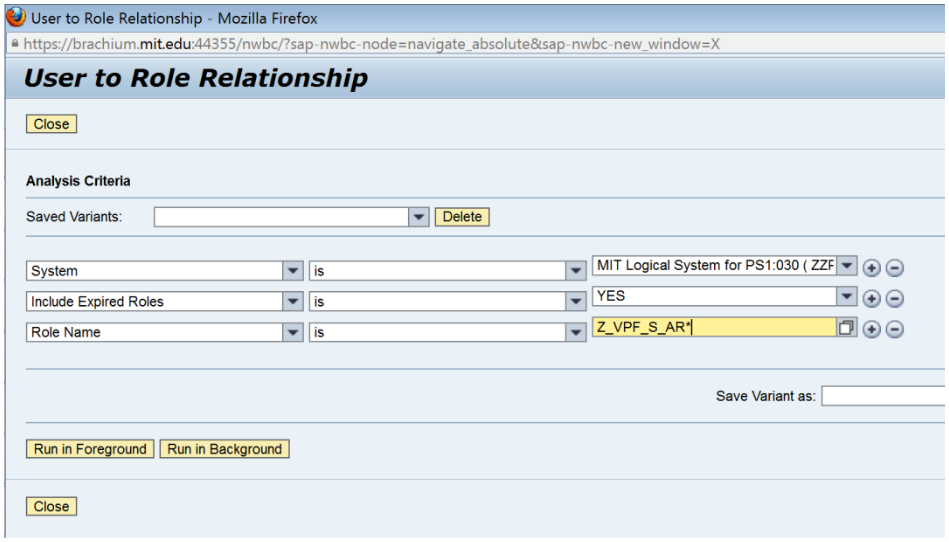
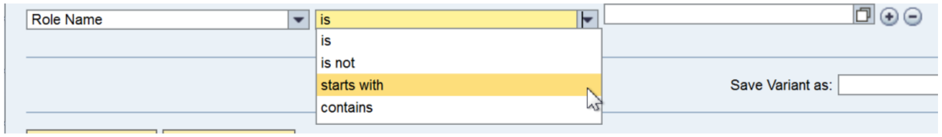
5B-4	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. Role Name: SAP role name Role Description: Business name for SAP role Profile Name: Name of SAP profile associated with SAP role (technical information) User: User ID of the user with access to the role Full Name: User name of user with access to role Valid From: Date on which assignment of the role to the user begins Valid To: Date on which assignment of the role to the user ends System: The system in which the role is assigned to the user	

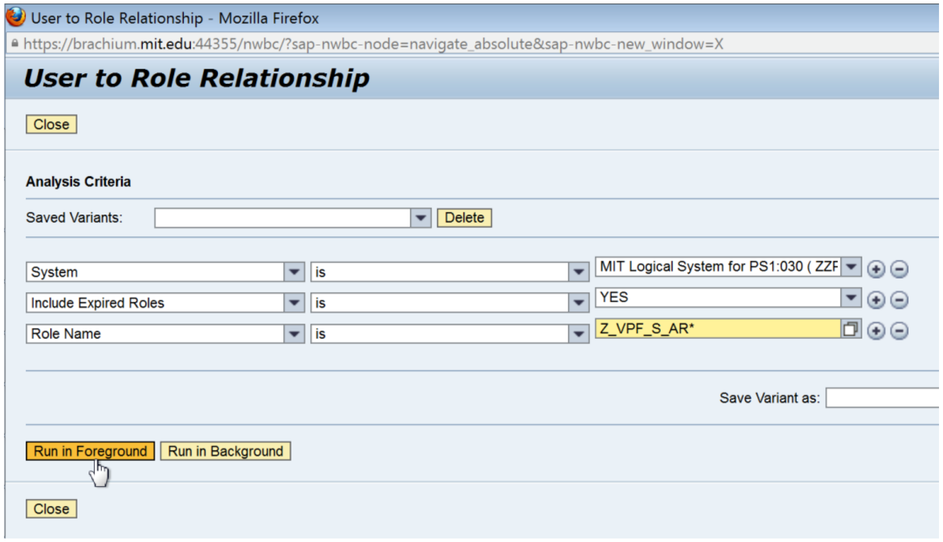
User to Role Relationship - Mozilla Firefox

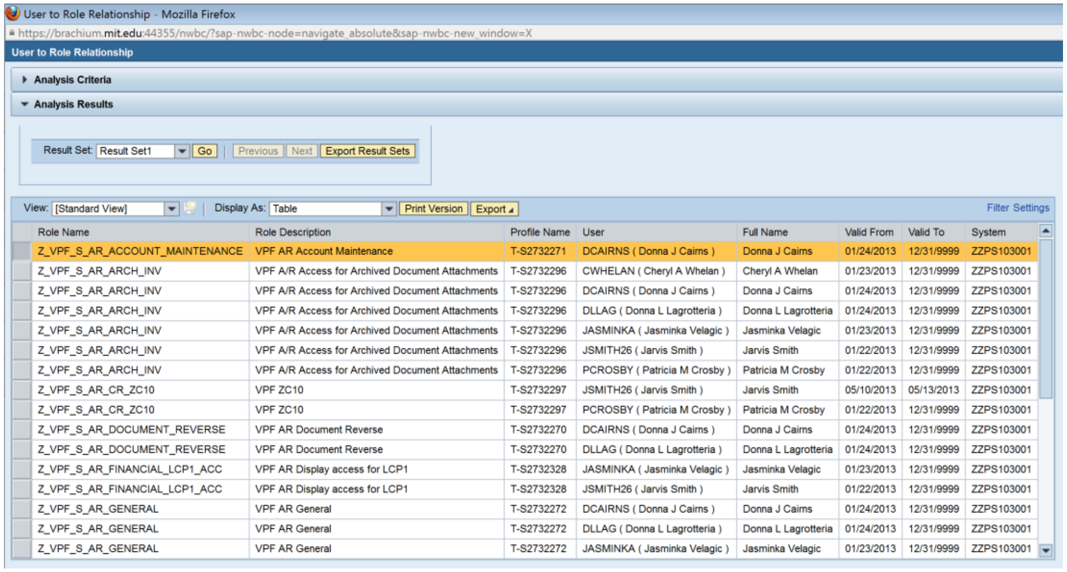
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

User to Role Relationship

Role Name	Role Description	Profile Name	User	Full Name	Valid From	Valid To	System
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_MANAGER	VPF AR Manager	T-S2732266	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001

5C-1	Analyze for multiple roles by using a wild card (*) in the role name. In this case, 'Z_VPF_S_AR*' is the selection. Alternatively, the operand for the 'Role Name' search criteron can be changed from 'is' to 'starts with'/'contains' and 'Z_VPF_S_AR' can be used as the selection.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X User to Role Relationship Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Include Expired Roles is YES Role Name is Z_VPF_S_AR* Save Variant as: Run in Foreground Run in Background Close  Role Name is is is not starts with contains Save Variant as:

5C-2	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 User to Role Relationship - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X User to Role Relationship Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Include Expired Roles is YES Role Name is Z_VPF_S_AR* Save Variant as: Close Delete Run in Foreground Run in Background Close

5C-3	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. Role Name: SAP role name Role Description: Business name for SAP role Profile Name: Name of SAP profile associated with SAP role (technical information) User: User ID of the user with access to the role Full Name: User name of user with access to role Valid From: Date on which assignment of the role to the user begins Valid To: Date on which assignment of the role to the user ends System: The system in which the role is assigned to the user	

User to Role Relationship - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

User to Role Relationship

Analysis Criteria

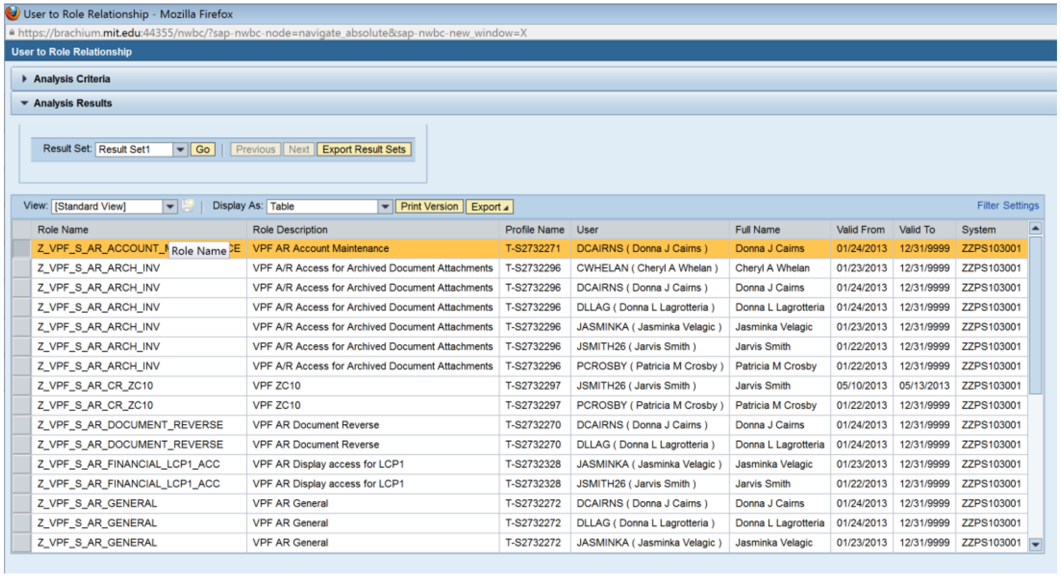
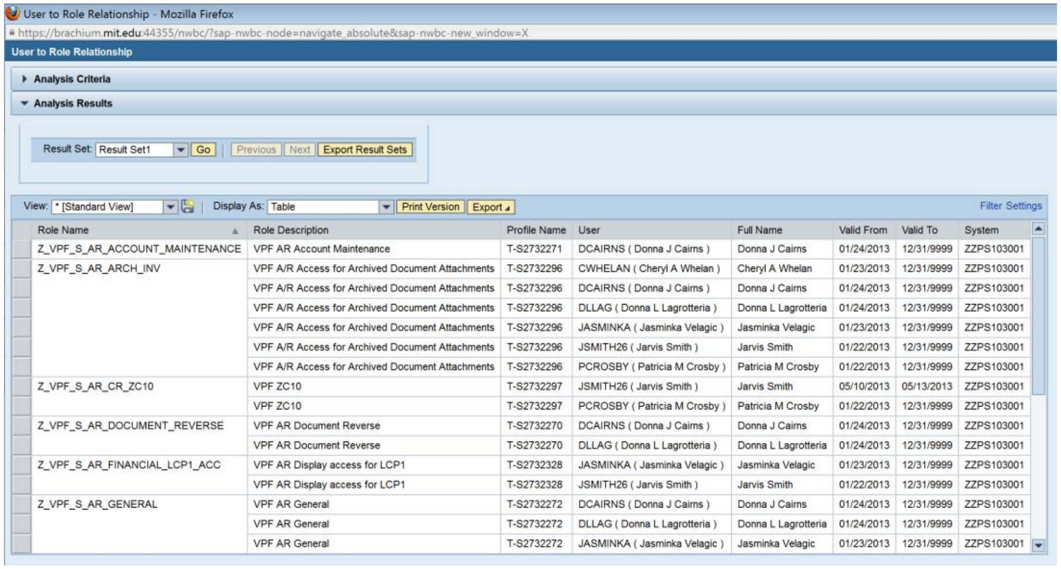
Analysis Results

Result Set: Result Set1

View: [Standard View]

Display As: Table

Role Name	Role Description	Profile Name	User	Full Name	Valid From	Valid To	System
Z_VPF_S_AR_ACCOUNT_MAINTENANCE	VPF AR Account Maintenance	T-S2732271	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	CWHELAN (Cheryl A Whelan)	Cheryl A Whelan	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	PCROSBY (Patricia M Crosby)	Patricia M Crosby	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_CR_ZC10	VPF ZC10	T-S2732297	JSMITH26 (Jarvis Smith)	Jarvis Smith	05/10/2013	05/13/2013	ZZPS103001
Z_VPF_S_AR_CR_ZC10	VPF ZC10	T-S2732297	PCROSBY (Patricia M Crosby)	Patricia M Crosby	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	T-S2732328	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	T-S2732328	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001

5C-4	Sorting on role by clicking on the 'Role Name' column header will show the users grouped by role.	 

User to Role Relationship - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

User to Role Relationship

Analysis Criteria

Analysis Results

Result Set: Result Set1 | Go | Previous | Next | Export Result Sets

View: [Standard View] | Display As: Table | Print Version | Export | Filter Settings

Role Name	Role Description	Profile Name	User	Full Name	Valid From	Valid To	System
Z_VPF_S_AR_ACCOUNT_M Role Name CE	VPF AR Account Maintenance	T-S2732271	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	CWHELAN (Cheryl A Whelan)	Cheryl A Whelan	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	PCROSBY (Patricia M Crosby)	Patricia M Crosby	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_CR_ZC10	VPF ZC10	T-S2732297	JSMITH26 (Jarvis Smith)	Jarvis Smith	05/10/2013	05/13/2013	ZZPS103001
Z_VPF_S_AR_CR_ZC10	VPF ZC10	T-S2732297	PCROSBY (Patricia M Crosby)	Patricia M Crosby	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	T-S2732328	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	T-S2732328	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001

User to Role Relationship - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

User to Role Relationship

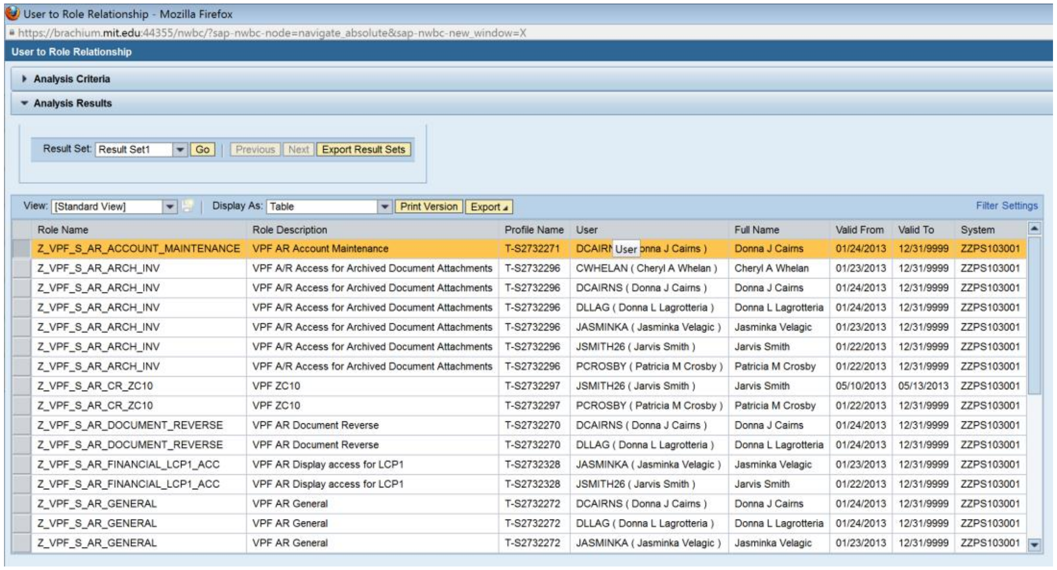
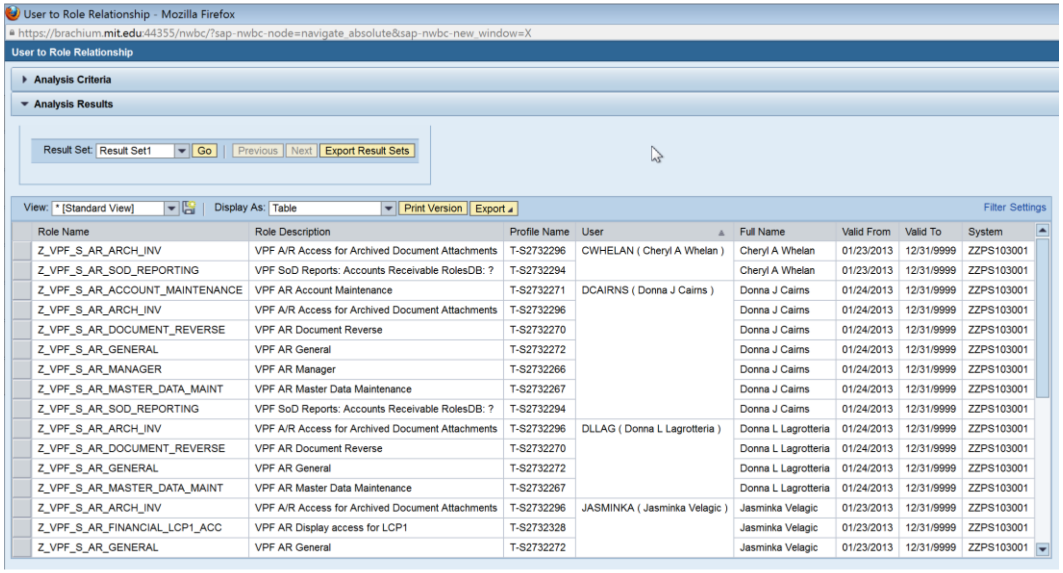
Analysis Criteria

Analysis Results

Result Set: Result Set1 | Go | Previous | Next | Export Result Sets

View: * [Standard View] | Display As: Table | Print Version | Export | Filter Settings

Role Name ▲	Role Description	Profile Name	User	Full Name	Valid From	Valid To	System
Z_VPF_S_AR_ACCOUNT_MAINTENANCE	VPF AR Account Maintenance	T-S2732271	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	CWHELAN (Cheryl A Whelan)	Cheryl A Whelan	01/23/2013	12/31/9999	ZZPS103001
	VPF A/R Access for Archived Document Attachments	T-S2732296	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
	VPF A/R Access for Archived Document Attachments	T-S2732296	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
	VPF A/R Access for Archived Document Attachments	T-S2732296	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
	VPF A/R Access for Archived Document Attachments	T-S2732296	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
	VPF A/R Access for Archived Document Attachments	T-S2732296	PCROSBY (Patricia M Crosby)	Patricia M Crosby	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_CR_ZC10	VPF ZC10	T-S2732297	JSMITH26 (Jarvis Smith)	Jarvis Smith	05/10/2013	05/13/2013	ZZPS103001
	VPF ZC10	T-S2732297	PCROSBY (Patricia M Crosby)	Patricia M Crosby	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
	VPF AR Document Reverse	T-S2732270	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	T-S2732328	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
	VPF AR Display access for LCP1	T-S2732328	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
	VPF AR General	T-S2732272	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
	VPF AR General	T-S2732272	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001

5C-5	Sorting on user by clicking on the 'User' column header will show the roles grouped by user.	 

User to Role Relationship - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

User to Role Relationship

Analysis Criteria

Analysis Results

Result Set: Result Set1 | Go | Previous | Next | Export Result Sets

View: [Standard View] | Display As: Table | Print Version | Export | Filter Settings

Role Name	Role Description	Profile Name	User	Full Name	Valid From	Valid To	System
Z_VPF_S_AR_ACCOUNT_MAINTENANCE	VPF AR Account Maintenance	T-S2732271	DCAIRN User onna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	CWHELAN (Cheryl A Whelan)	Cheryl A Whelan	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	PCROSBY (Patricia M Crosby)	Patricia M Crosby	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_CR_ZC10	VPF ZC10	T-S2732297	JSMITH26 (Jarvis Smith)	Jarvis Smith	05/10/2013	05/13/2013	ZZPS103001
Z_VPF_S_AR_CR_ZC10	VPF ZC10	T-S2732297	PCROSBY (Patricia M Crosby)	Patricia M Crosby	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	T-S2732328	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	T-S2732328	JSMITH26 (Jarvis Smith)	Jarvis Smith	01/22/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001

User to Role Relationship - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

User to Role Relationship

Analysis Criteria

Analysis Results

Result Set: Result Set1 | Go | Previous | Next | Export Result Sets

View: * [Standard View] | Display As: Table | Print Version | Export | Filter Settings

Role Name	Role Description	Profile Name	User ▲	Full Name	Valid From	Valid To	System
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	CWHELAN (Cheryl A Whelan)	Cheryl A Whelan	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_SOD_REPORTING	VPF SoD Reports: Accounts Receivable RolesDB: ?	T-S2732294		Cheryl A Whelan	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ACCOUNT_MAINTENANCE	VPF AR Account Maintenance	T-S2732271	DCAIRNS (Donna J Cairns)	Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296		Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270		Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272		Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_MANAGER	VPF AR Manager	T-S2732266		Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_MASTER_DATA_MAINT	VPF AR Master Data Maintenance	T-S2732267		Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_SOD_REPORTING	VPF SoD Reports: Accounts Receivable RolesDB: ?	T-S2732294		Donna J Cairns	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	DLLAG (Donna L Lagrotteria)	Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	T-S2732270		Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272		Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_MASTER_DATA_MAINT	VPF AR Master Data Maintenance	T-S2732267		Donna L Lagrotteria	01/24/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	T-S2732296	JASMINKA (Jasminka Velagic)	Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	T-S2732328		Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001
Z_VPF_S_AR_GENERAL	VPF AR General	T-S2732272		Jasminka Velagic	01/23/2013	12/31/9999	ZZPS103001

Job Aid 07 Role Relationship with User - User Group

USE

This report can be used to determine what roles are assigned to a user.

INFORMATION

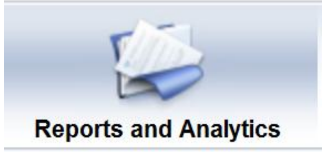
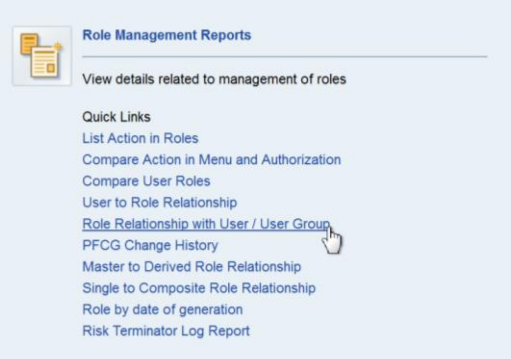
List of all roles assigned to a user or users in a user group.

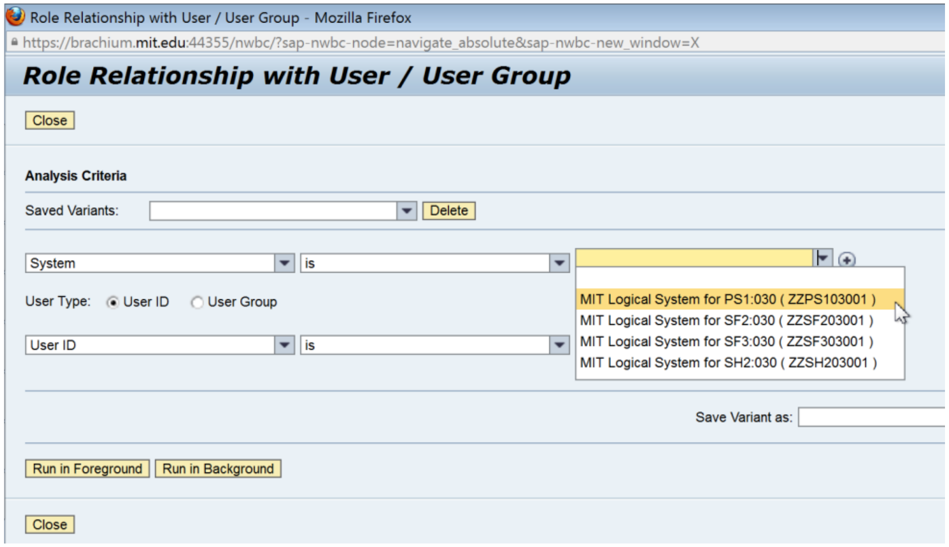
RELATED PROCESSES

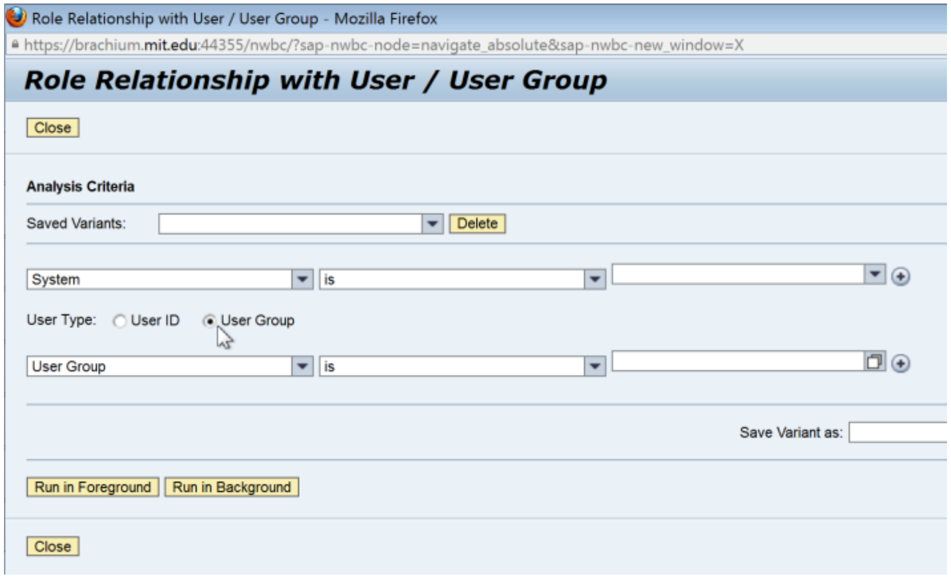
- Process 1: New or Amended Roles

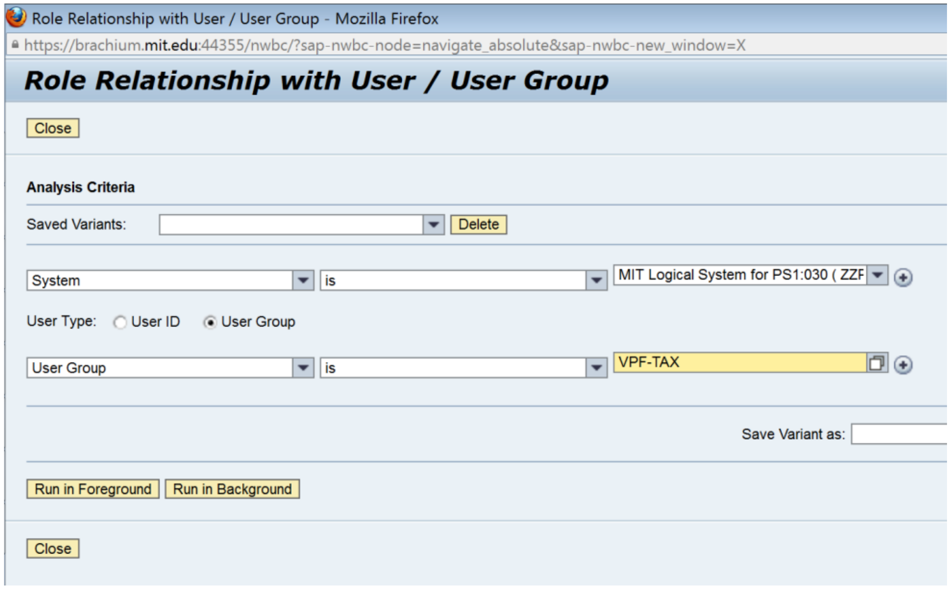
SPECIFIC SCENARIOS

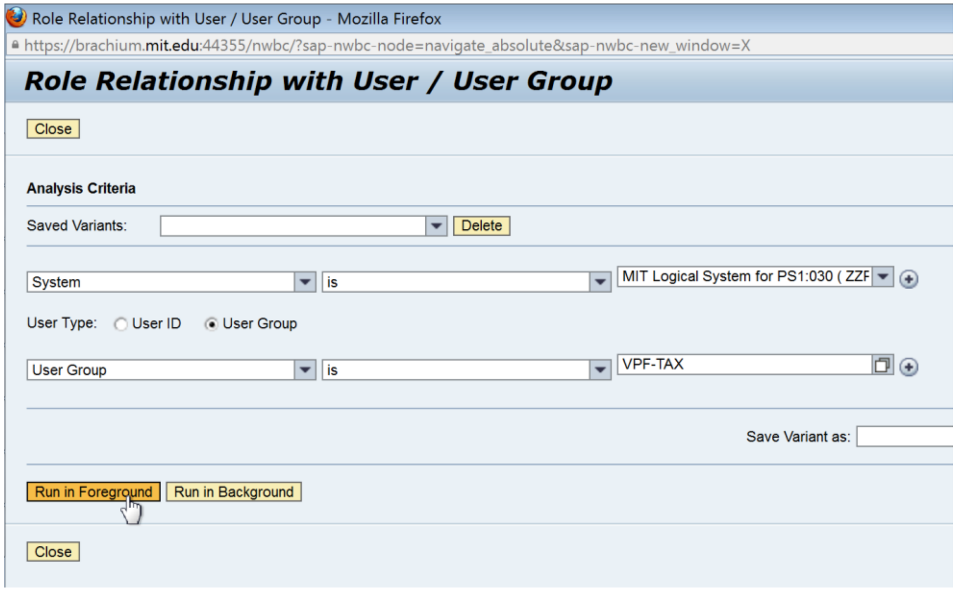
- Step 4A: Analyze for a single user group.
- Step 4B: Analyze by for a single user by user ID.
- Step 4C: Analyze by for multiple users by user ID.

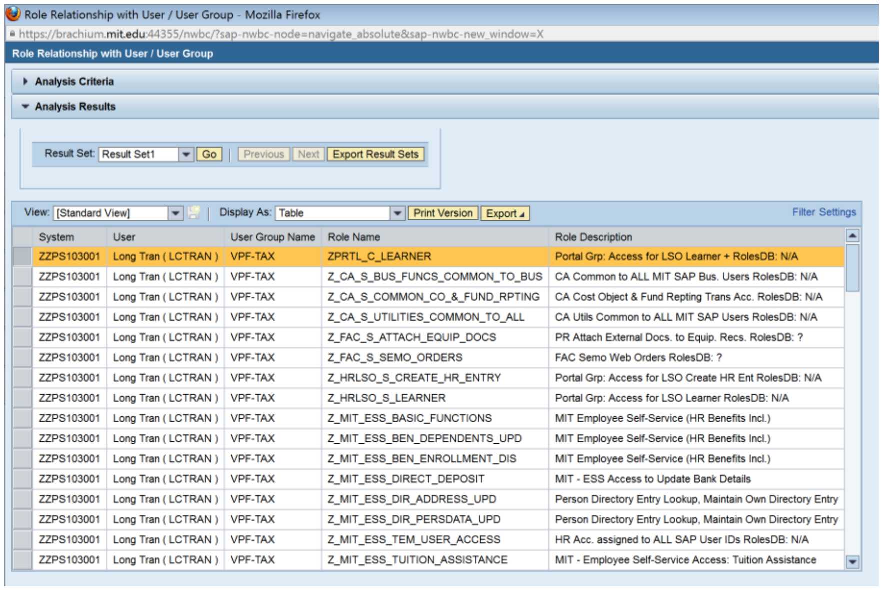
Step	Description	Screenshot
1	Navigate to the 'Reports and Analytics' tab.	
2	Click on the 'Role Relationship with User / User Group' report located in the 'Role Management Reports' section.	 Role Management Reports View details related to management of roles Quick Links List Action in Roles Compare Action in Menu and Authorization Compare User Roles User to Role Relationship Role Relationship with User / User Group PFCG Change History Master to Derived Role Relationship Single to Composite Role Relationship Role by date of generation Risk Terminator Log Report

3	Select the system for which information is required. In this case, the selection is PS1.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Role Relationship with User / User Group** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZPS103001) MIT Logical System for SF2:030 (ZZSF203001) MIT Logical System for SF3:030 (ZZSF303001) MIT Logical System for SH2:030 (ZZSH203001) User Type: ● User ID ○ User Group User ID is Save Variant as: Run in Foreground Run in Background Close

4A-1	Analyze for a single user group. Click on the dial button next to 'User Group'. NOTE: The report can also be executed for multiple user groups by following steps similar to those outlined for multiple user IDs in steps 4C.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Role Relationship with User / User Group Close Analysis Criteria Saved Variants: Delete System is User Type: ○ User ID ● User Group User Group is Save Variant as: Run in Foreground Run in Background Close

4A-2	Add the user group name. In this case, 'VPF-TAX', the user group containing all users in VPF who are part of the Tax area, was typed in. The search option can also be used to search for user groups. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Role Relationship with User / User Group** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF User Type: ○ User ID ● User Group User Group is VPF-TAX Save Variant as: Run in Foreground Run in Background Close

4A-3	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Role Relationship with User / User Group Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF User Type: ○ User ID ● User Group User Group is VPF-TAX Save Variant as: Run in Foreground Run in Background Close

4A-4	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. System: The system in which the role is assigned to the user User: User ID of the user with access to the role User Group Name: User group code Role Name: SAP role name Role Description: Business name for SAP role	

Role Relationship with User / User Group - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

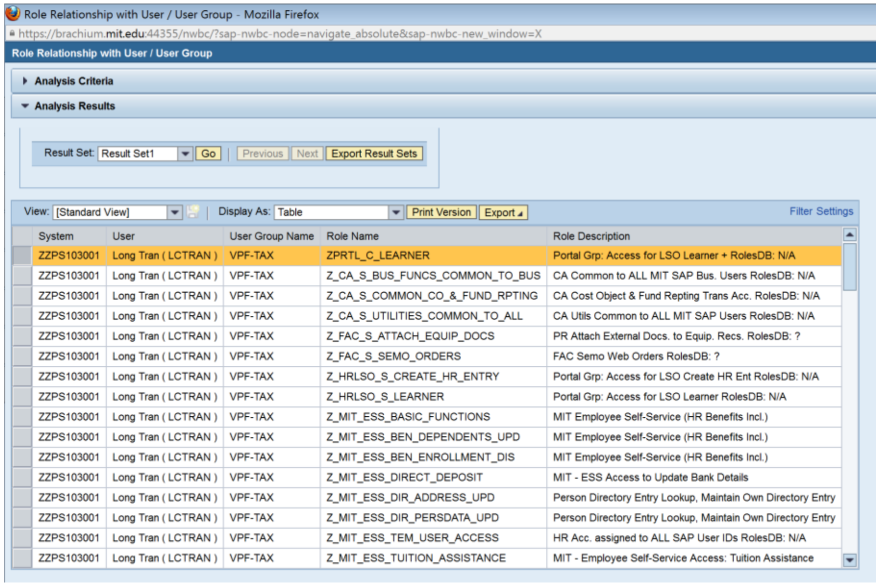
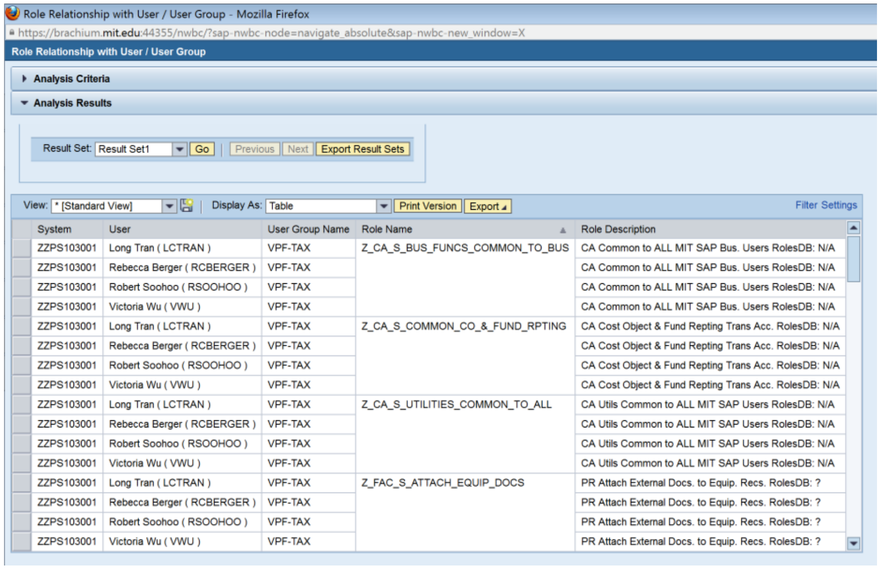
Role Relationship with User / User Group

Result Set: Result Set1

View: [Standard View]

Display As: Table

System	User	User Group Name	Role Name	Role Description
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	ZPRTL_C_LEARNER	Portal Grp: Access for LSO Learner + RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_FAC_S_ATTACH_EQUIP_DOCS	PR Attach External Docs. to Equip. Recs. RolesDB: ?
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_FAC_S_SEMO_ORDERS	FAC Semo Web Orders RolesDB: ?
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_HRLSO_S_CREATE_HR_ENTRY	Portal Grp: Access for LSO Create HR Ent RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_HRLSO_S_LEARNER	Portal Grp: Access for LSO Learner RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_BASIC_FUNCTIONS	MIT Employee Self-Service (HR Benefits Incl.)
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_BEN_DEPENDENTS_UPD	MIT Employee Self-Service (HR Benefits Incl.)
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_BEN_ENROLLMENT_DIS	MIT Employee Self-Service (HR Benefits Incl.)
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_DIRECT_DEPOSIT	MIT - ESS Access to Update Bank Details
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_DIR_ADDRESS_UPD	Person Directory Entry Lookup, Maintain Own Directory Entry
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_DIR_PERSDATA_UPD	Person Directory Entry Lookup, Maintain Own Directory Entry
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_TEM_USER_ACCESS	HR Acc. assigned to ALL SAP User IDs RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_TUITION_ASSISTANCE	MIT - Employee Self-Service Access: Tuition Assistance

4A-5	Sorting on role by clicking on the ‘Role Name’ column header will show the users grouped by role.	 

Role Relationship with User / User Group - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Role Relationship with User / User Group

Result Set: Result Set1

View: [Standard View]

Display As: Table

System	User	User Group Name	Role Name	Role Description
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	ZPRTL_C_LEARNER	Portal Grp: Access for LSO Learner + RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_FAC_S_ATTACH_EQUIP_DOCS	PR Attach External Docs. to Equip. Recs. RolesDB: ?
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_FAC_S_SEMO_ORDERS	FAC Semo Web Orders RolesDB: ?
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_HRLSO_S_CREATE_HR_ENTRY	Portal Grp: Access for LSO Create HR Ent RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_HRLSO_S_LEARNER	Portal Grp: Access for LSO Learner RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_BASIC_FUNCTIONS	MIT Employee Self-Service (HR Benefits Incl.)
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_BEN_DEPENDENTS_UPD	MIT Employee Self-Service (HR Benefits Incl.)
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_BEN_ENROLLMENT_DIS	MIT Employee Self-Service (HR Benefits Incl.)
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_DIRECT_DEPOSIT	MIT - ESS Access to Update Bank Details
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_DIR_ADDRESS_UPD	Person Directory Entry Lookup, Maintain Own Directory Entry
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_DIR_PERSDATA_UPD	Person Directory Entry Lookup, Maintain Own Directory Entry
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_TEM_USER_ACCESS	HR Acc. assigned to ALL SAP User IDs RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_MIT_ESS_TUITION_ASSISTANCE	MIT - Employee Self-Service Access: Tuition Assistance

Role Relationship with User / User Group - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

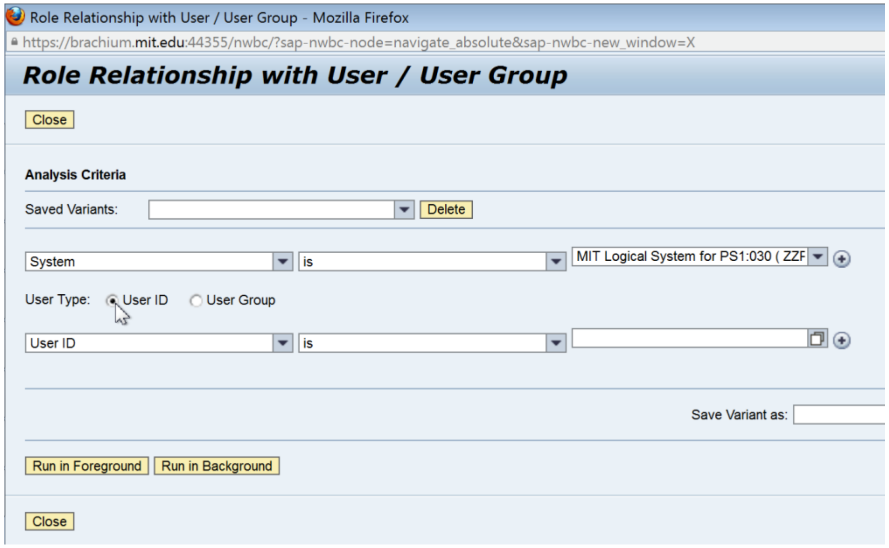
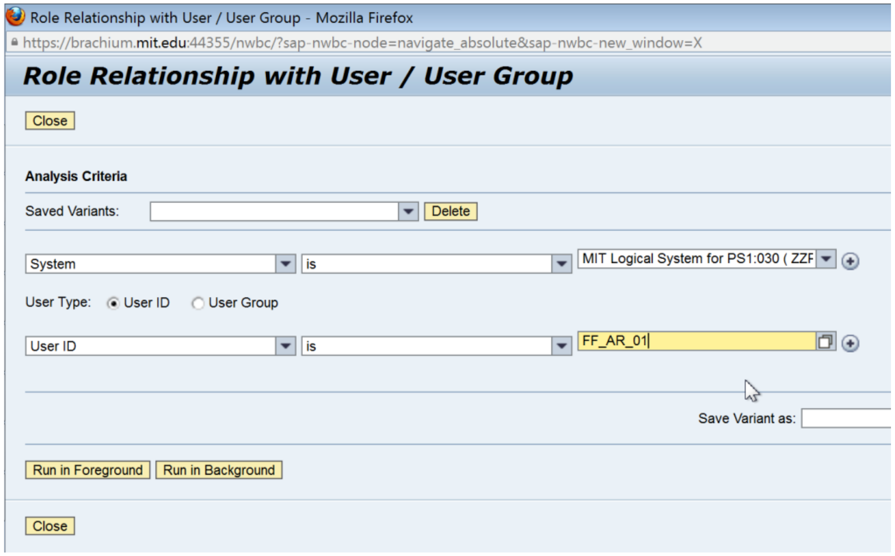
Role Relationship with User / User Group

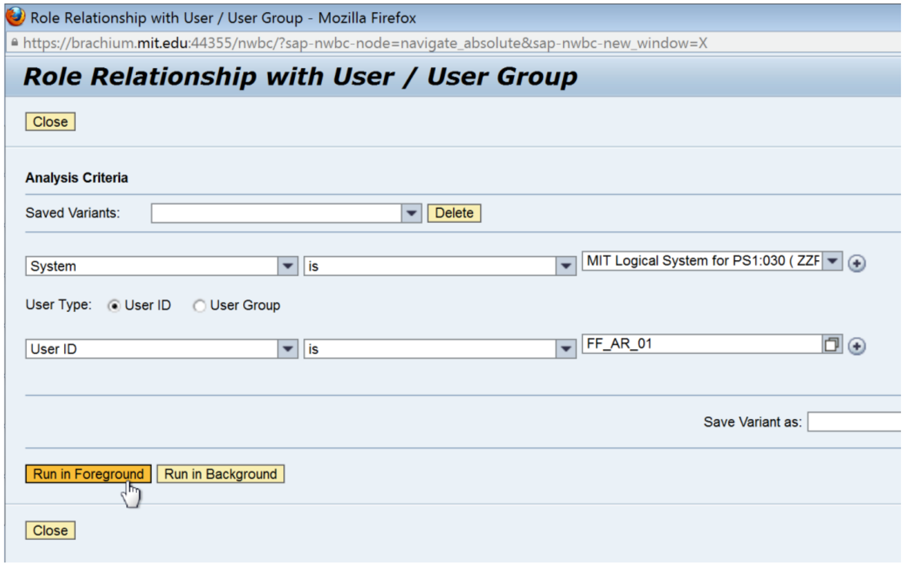
Result Set: Result Set1

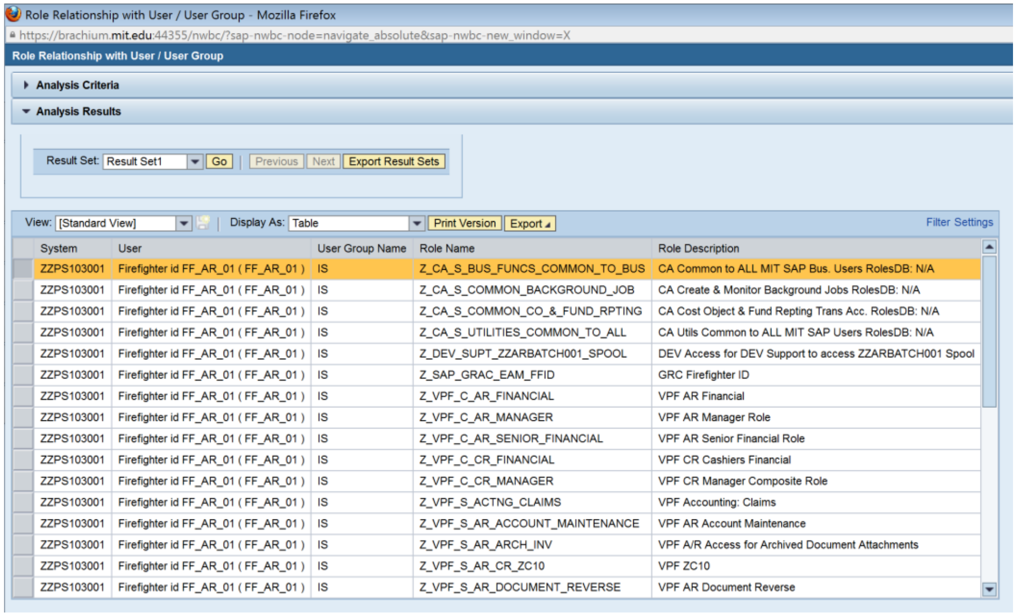
View: * [Standard View]

Display As: Table

System	User	User Group Name	Role Name ▲	Role Description
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Rebecca Berger (RCBERGER)	VPF-TAX		CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Robert Soohoo (RSOOHOO)	VPF-TAX		CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Victoria Wu (VWU)	VPF-TAX		CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Rebecca Berger (RCBERGER)	VPF-TAX		CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Robert Soohoo (RSOOHOO)	VPF-TAX		CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Victoria Wu (VWU)	VPF-TAX		CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Rebecca Berger (RCBERGER)	VPF-TAX		CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Robert Soohoo (RSOOHOO)	VPF-TAX		CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Victoria Wu (VWU)	VPF-TAX		CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Long Tran (LCTRAN)	VPF-TAX	Z_FAC_S_ATTACH_EQUIP_DOCS	PR Attach External Docs. to Equip. Recs. RolesDB: ?
ZZPS103001	Rebecca Berger (RCBERGER)	VPF-TAX		PR Attach External Docs. to Equip. Recs. RolesDB: ?
ZZPS103001	Robert Soohoo (RSOOHOO)	VPF-TAX		PR Attach External Docs. to Equip. Recs. RolesDB: ?
ZZPS103001	Victoria Wu (VWU)	VPF-TAX		PR Attach External Docs. to Equip. Recs. RolesDB: ?

4B-1	Analyze by for a single user by user ID. Click on the dial button next to 'User ID'.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Role Relationship with User / User Group** Close **Analysis Criteria** Saved Variants: Delete System — is — MIT Logical System for PS1:030 (ZZF User Type: ● User ID ○ User Group User ID — is — Save Variant as: Run in Foreground Run in Background Close
4B-2	Add the user ID. In this case, 'FF_AR_01', an AR Cashiers FireFighter ID, was typed in. The search option can also be used to search for an ID. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Role Relationship with User / User Group** Close **Analysis Criteria** Saved Variants: Delete System — is — MIT Logical System for PS1:030 (ZZF User Type: ● User ID ○ User Group User ID — is — FF_AR_01 Save Variant as: Run in Foreground Run in Background Close

4B-3	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Role Relationship with User / User Group Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF User Type: ● User ID ○ User Group User ID is FF_AR_01 Save Variant as: Run in Foreground Run in Background Close

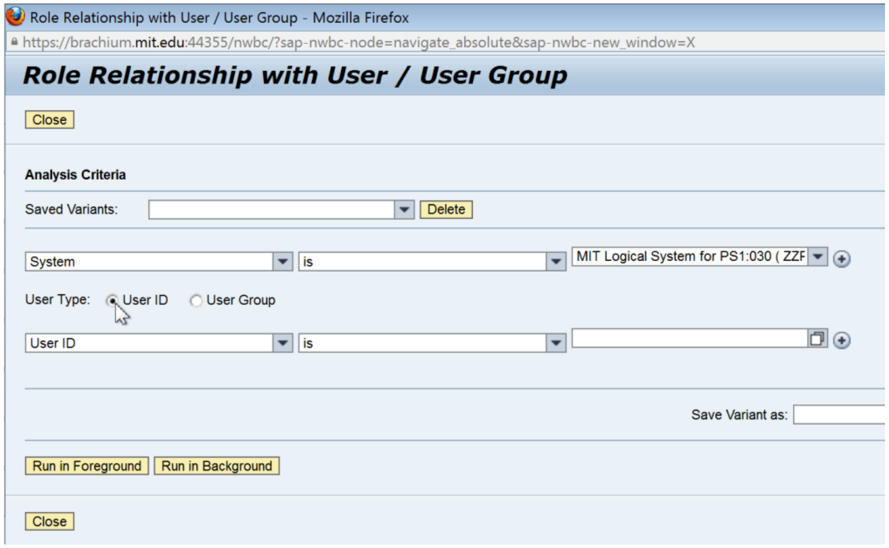
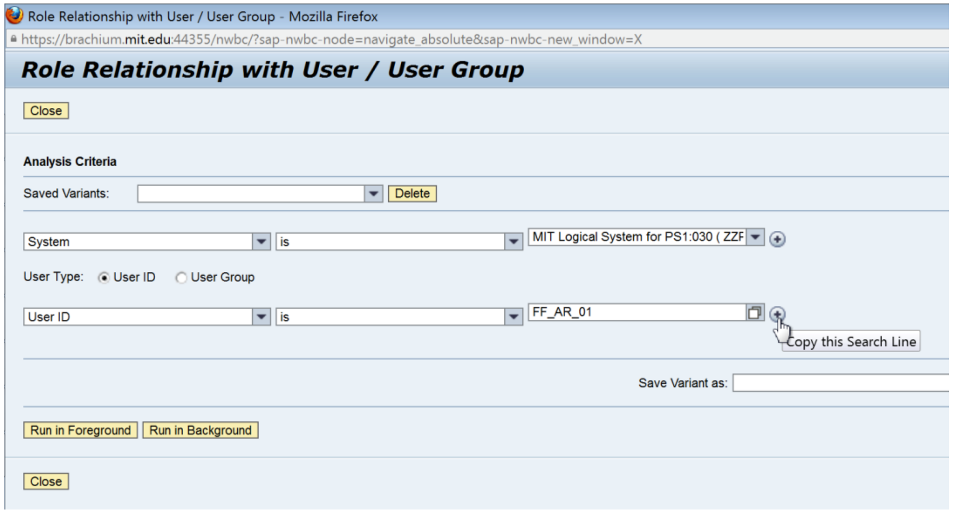
4B-4	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. System: The system in which the role is assigned to the user User: User ID of the user with access to the role User Group Name: User group code (not relevant for this scenario) Role Name: SAP role name Role Description: Business name for SAP role	

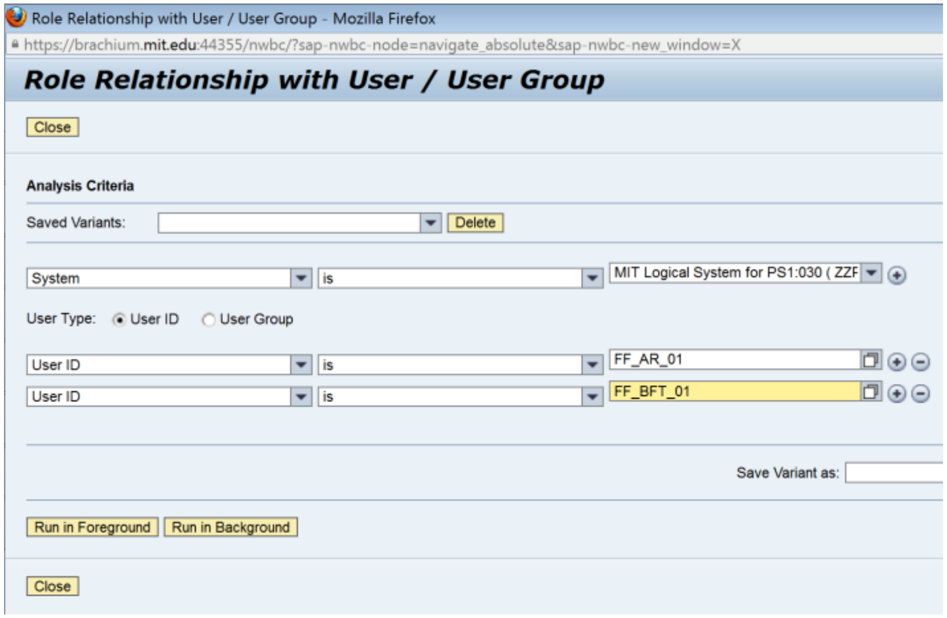
Role Relationship with User / User Group - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Role Relationship with User / User Group

System	User	User Group Name	Role Name	Role Description
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_COMMON_BACKGROUND_JOB	CA Create & Monitor Background Jobs RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_DEV_SUPT_ZZARBATCH001_SPOOL	DEV Access for DEV Support to access ZZARBATCH001 Spool
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_SAP_GRAC_EAM_FFID	GRC Firefighter ID
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_FINANCIAL	VPF AR Financial
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_MANAGER	VPF AR Manager Role
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_SENIOR_FINANCIAL	VPF AR Senior Financial Role
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_CR_FINANCIAL	VPF CR Cashiers Financial
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_CR_MANAGER	VPF CR Manager Composite Role
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_ACTNG_CLAIMS	VPF Accounting: Claims
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_AR_ACCOUNT_MAINTENANCE	VPF AR Account Maintenance
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_AR_CR_ZC10	VPF ZC10
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse

4C-1	Analyze by for multiple users by user ID. Click on the dial button next to 'User ID'.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Role Relationship with User / User Group Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User Type: ● User ID ○ User Group User ID is Save Variant as:
4C-2	Click on the '+' at the end of the 'User ID' row to add an additional user ID search criterion row for each ID. In this case, one additional row is added; thus, we can analyze for a total of two user IDs.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Role Relationship with User / User Group Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User Type: ● User ID ○ User Group User ID is FF_AR_01 Copy this Search Line Save Variant as:

4C-3	Add the user IDs. In this case, 'FF_AR_01' and 'FF_BFT_01', two FireFighter IDs, were typed in. The search option can also be used to search for IDs. Please refer to the 'Search for Input Values' reference document (R3) for further information.	

Role Relationship with User / User Group - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Role Relationship with User / User Group

Close

Analysis Criteria

Saved Variants: Delete

System | is | MIT Logical System for PS1:030 (ZZF

User Type: ● User ID ○ User Group

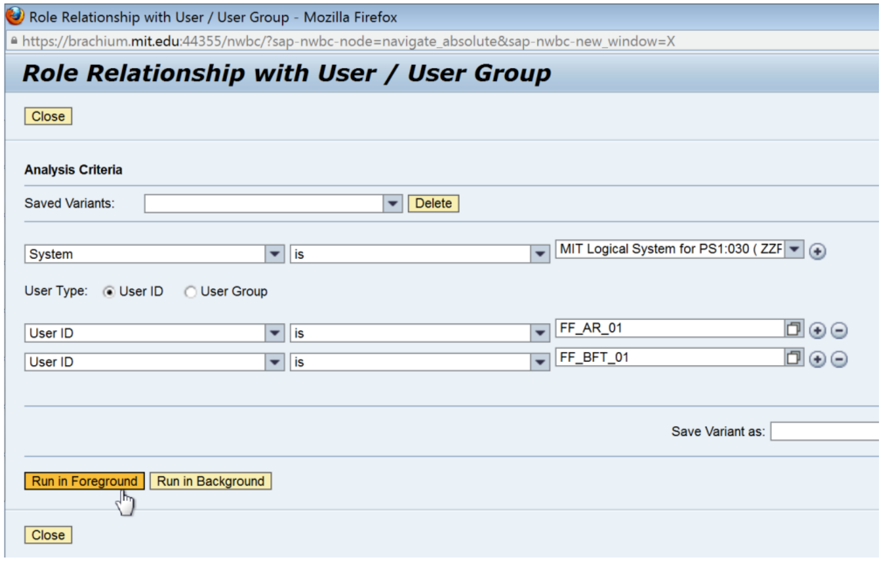
User ID | is | FF_AR_01

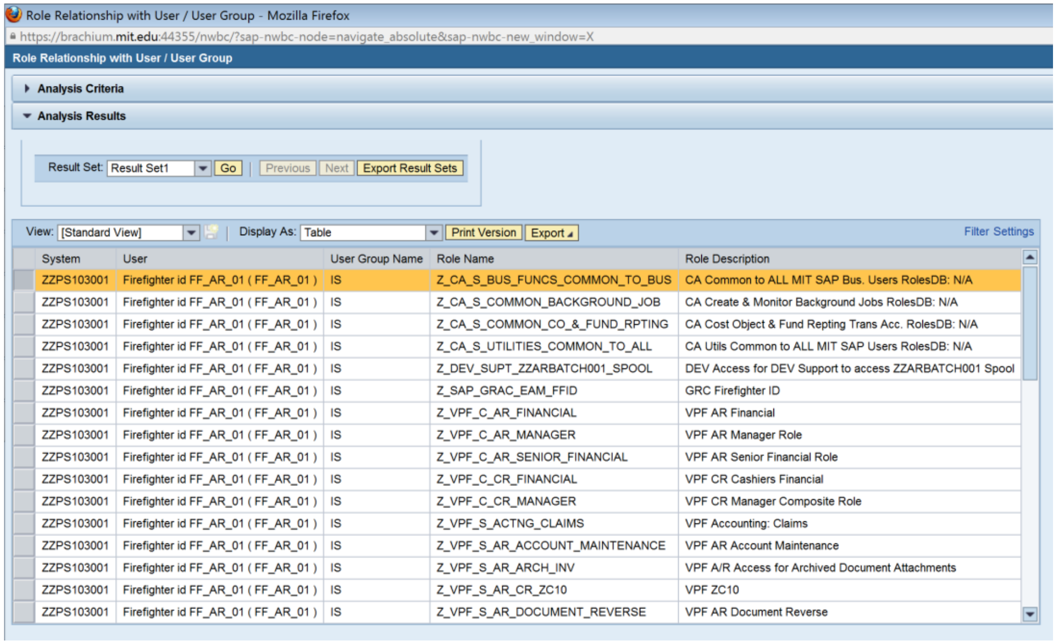
User ID | is | FF_BFT_01

Save Variant as:

Run in Foreground Run in Background

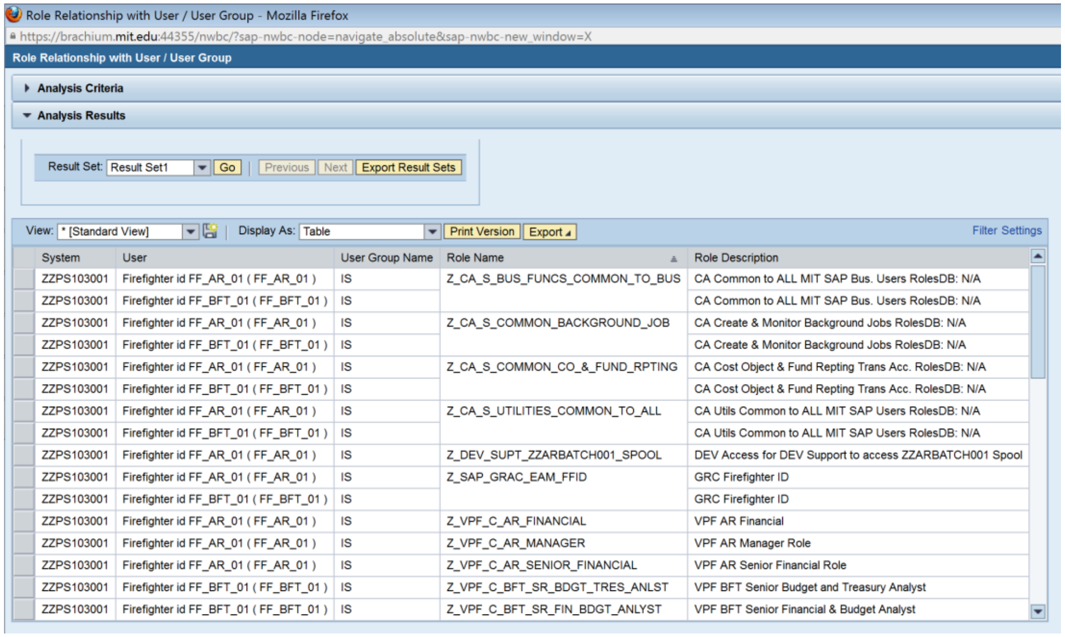
Close

4C-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Role Relationship with User / User Group - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Role Relationship with User / User Group Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User Type: ● User ID ○ User Group User ID is FF_AR_01 User ID is FF_BFT_01 Save Variant as: Close Delete Run in Foreground Run in Background Close

4C-5	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. System: The system in which the role is assigned to the user User: User ID of the user with access to the role User Group Name: User group code (not relevant for this scenario) Role Name: SAP role name Role Description: Business name for SAP role	

Role Relationship with User / User Group - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Role Relationship with User / User Group
Analysis Criteria
Analysis Results
Result Set: Result Set1
Go
Previous
Next
Export Result Sets
View: [Standard View]
Display As: Table
Print Version
Export
Filter Settings

System	User	User Group Name	Role Name	Role Description
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_COMMON_BACKGROUND_JOB	CA Create & Monitor Background Jobs RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_DEV_SUPT_ZZARBATCH001_SPOOL	DEV Access for DEV Support to access ZZARBATCH001 Spool
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_SAP_GRAC_EAM_FFID	GRC Firefighter ID
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_FINANCIAL	VPF AR Financial
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_MANAGER	VPF AR Manager Role
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_SENIOR_FINANCIAL	VPF AR Senior Financial Role
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_CR_FINANCIAL	VPF CR Cashiers Financial
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_CR_MANAGER	VPF CR Manager Composite Role
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_ACTNG_CLAIMS	VPF Accounting: Claims
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_AR_ACCOUNT_MAINTENANCE	VPF AR Account Maintenance
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_AR_CR_ZC10	VPF ZC10
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse

4C-6	Sorting on role by clicking on the 'Role Name' column header will show the users grouped by role.	

Role Relationship with User / User Group - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Role Relationship with User / User Group
Analysis Criteria
Analysis Results
Result Set: Result Set1
Go
Previous
Next
Export Result Sets
View: * [Standard View]
Display As: Table
Print Version
Export
Filter Settings

System	User	User Group Name	Role Name	Role Description
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Firefighter id FF_BFT_01 (FF_BFT_01)	IS		CA Common to ALL MIT SAP Bus. Users RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_COMMON_BACKGROUND_JOB	CA Create & Monitor Background Jobs RolesDB: N/A
ZZPS103001	Firefighter id FF_BFT_01 (FF_BFT_01)	IS		CA Create & Monitor Background Jobs RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Firefighter id FF_BFT_01 (FF_BFT_01)	IS		CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Firefighter id FF_BFT_01 (FF_BFT_01)	IS		CA Utils Common to ALL MIT SAP Users RolesDB: N/A
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_DEV_SUPT_ZZARBATCH001_SPOOL	DEV Access for DEV Support to access ZZARBATCH001 Spool
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_SAP_GRAC_EAM_FFID	GRC Firefighter ID
ZZPS103001	Firefighter id FF_BFT_01 (FF_BFT_01)	IS		GRC Firefighter ID
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_FINANCIAL	VPF AR Financial
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_MANAGER	VPF AR Manager Role
ZZPS103001	Firefighter id FF_AR_01 (FF_AR_01)	IS	Z_VPF_C_AR_SENIOR_FINANCIAL	VPF AR Senior Financial Role
ZZPS103001	Firefighter id FF_BFT_01 (FF_BFT_01)	IS	Z_VPF_C_BFT_SR_BDGT_TRES_ANLST	VPF BFT Senior Budget and Treasury Analyst
ZZPS103001	Firefighter id FF_BFT_01 (FF_BFT_01)	IS	Z_VPF_C_BFT_SR_FIN_BDGT_ANLYST	VPF BFT Senior Financial & Budget Analyst

Job Aid 08 SUIM Users by User ID

USE

This report can be used to display which roles users have and compare their access by sorting by role.

INFORMATION

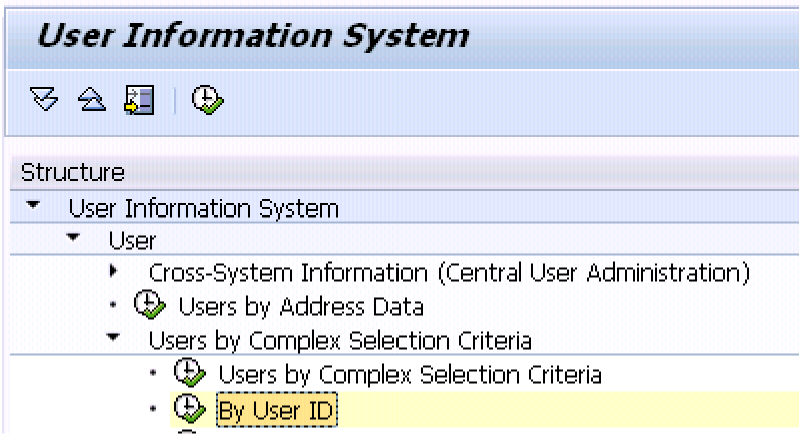
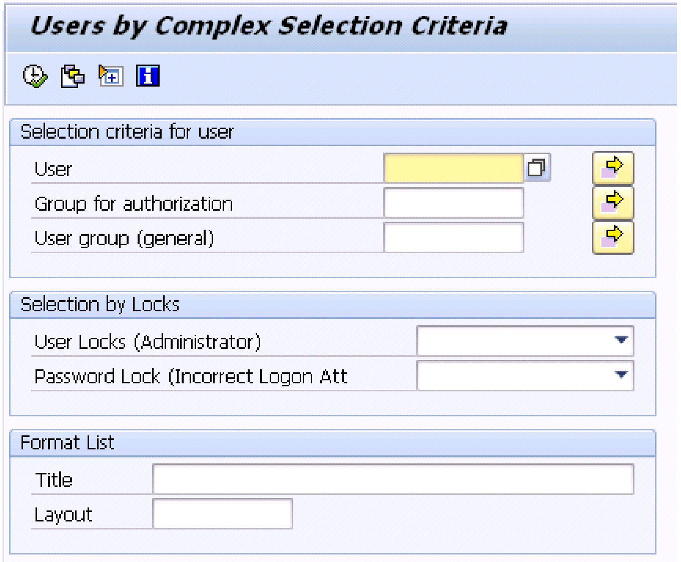
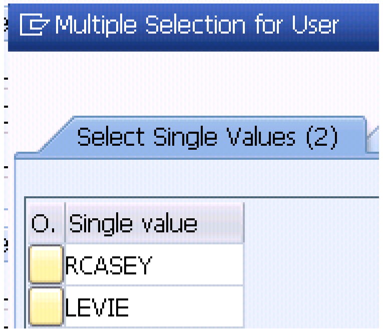
Roles and profiles assigned to users.

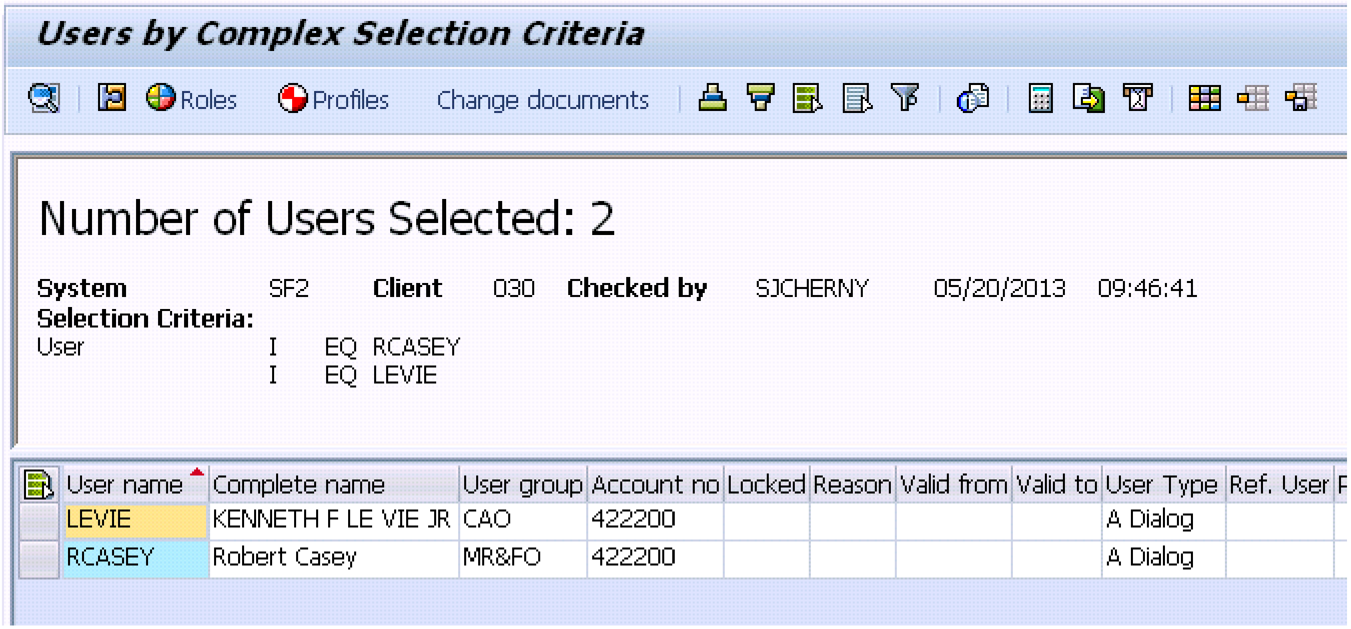
RELATED PROCESSES

- Process 1: New or Amended Roles

SPECIFIC SCENARIOS

- N/A

Step	Description	Screenshot
1	In SAP R/3 EEC– use transaction code SUIM. Then click on the “User” node and then “Users by Complex Selection Criteria” – then finally double click on the option for “ByUserId” Or use Transaction Code • S_BCE_68001394	 User Information System Structure ▾ User Information System ▾ User ▸ Cross-System Information (Central User Administration) • Users by Address Data ▾ Users by Complex Selection Criteria • Users by Complex Selection Criteria • By User ID
2	Select the Users to be analyzed Use the “Multiple Selection” button ➪ to specify the users, then ✓ to save and exit the multiple selection screen.	 Users by Complex Selection Criteria Selection criteria for user User Group for authorization User group (general) Selection by Locks User Locks (Administrator) Password Lock (Incorrect Logon Att Format List Title Layout  Multiple Selection for User Select Single Values (2) O. Single value RCASEY LEVIE

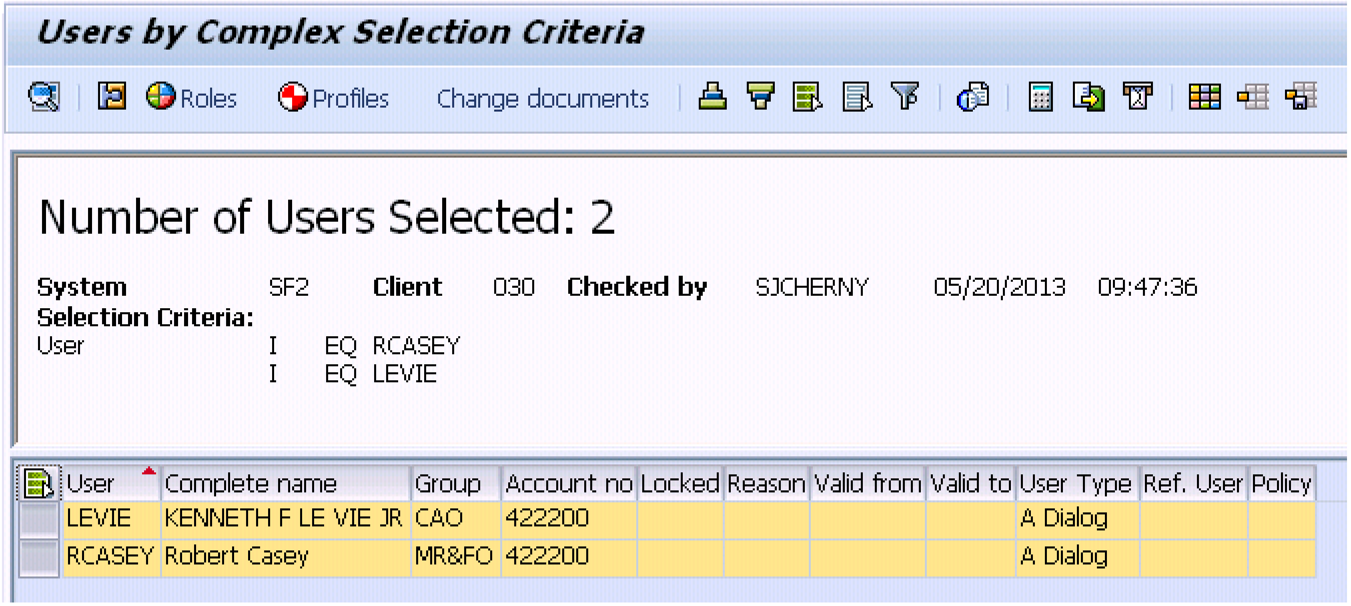
3	The report will show a list of Users matching the selection criteria. It shows : • User Id and name • User Group From this report, you can drill down to get the role assignments.	

Users by Complex Selection Criteria

Number of Users Selected: 2

System SF2 **Client** 030 **Checked by** SJCHERNY 05/20/2013 09:46:41
Selection Criteria:
User I EQ RCASEY
I EQ LEVIE

User name	Complete name	User group	Account no	Locked	Reason	Valid from	Valid to	User Type	Ref. User	F
LEVIE	KENNETH F LE VIE JR	CAO	422200					A Dialog		
RCASEY	Robert Casey	MR&FO	422200					A Dialog		

4a	Click on ▦ to select both (all) users	

Users by Complex Selection Criteria

Roles Profiles Change documents

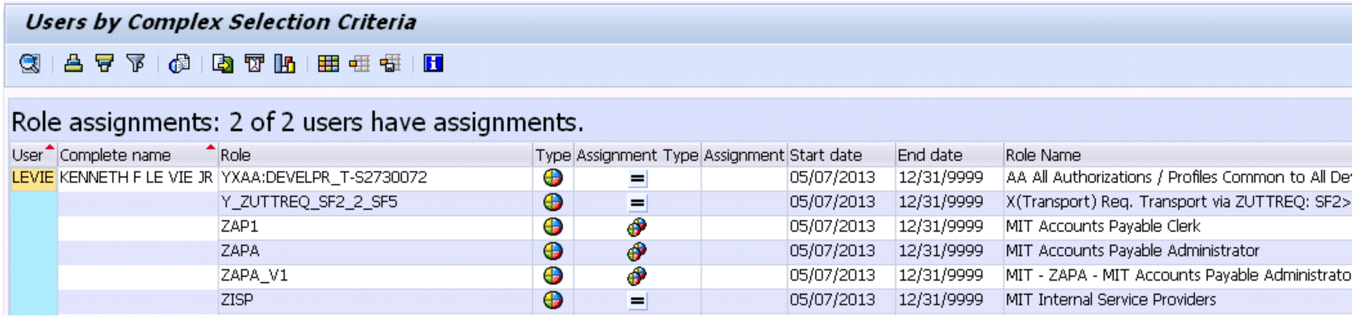
Number of Users Selected: 2

System	SF2	Client	030	Checked by	SJCHERNY	05/20/2013	09:47:36

Selection Criteria:

User	I	EQ	RCASEY
	I	EQ	LEVIE

User	Complete name	Group	Account no	Locked	Reason	Valid from	Valid to	User Type	Ref. User	Policy
LEVIE	KENNETH F LE VIE JR	CAO	422200					A Dialog		
RCASEY	Robert Casey	MR&FO	422200					A Dialog		

4b	Click on Roles to list all the roles for the selected users	

Users by Complex Selection Criteria

Role assignments: 2 of 2 users have assignments.

User	Complete name	Role	Type	Assignment Type	Assignment	Start date	End date	Role Name
LEVIE	KENNETH F LE VIE JR	YXAA:DEVELPR_T-S2730072	●	=		05/07/2013	12/31/9999	AA All Authorizations / Profiles Common to All De
		Y_ZUTTREQ_SF2_2_SF5	●	=		05/07/2013	12/31/9999	X(Transport) Req. Transport via ZUTTREQ: SF2>
		ZAP1	●	●		05/07/2013	12/31/9999	MIT Accounts Payable Clerk
		ZAPA	●	●		05/07/2013	12/31/9999	MIT Accounts Payable Administrator
		ZAPA_V1	●	●		05/07/2013	12/31/9999	MIT - ZAPA - MIT Accounts Payable Administrato
		ZISP	●	=		05/07/2013	12/31/9999	MIT Internal Service Providers

4c

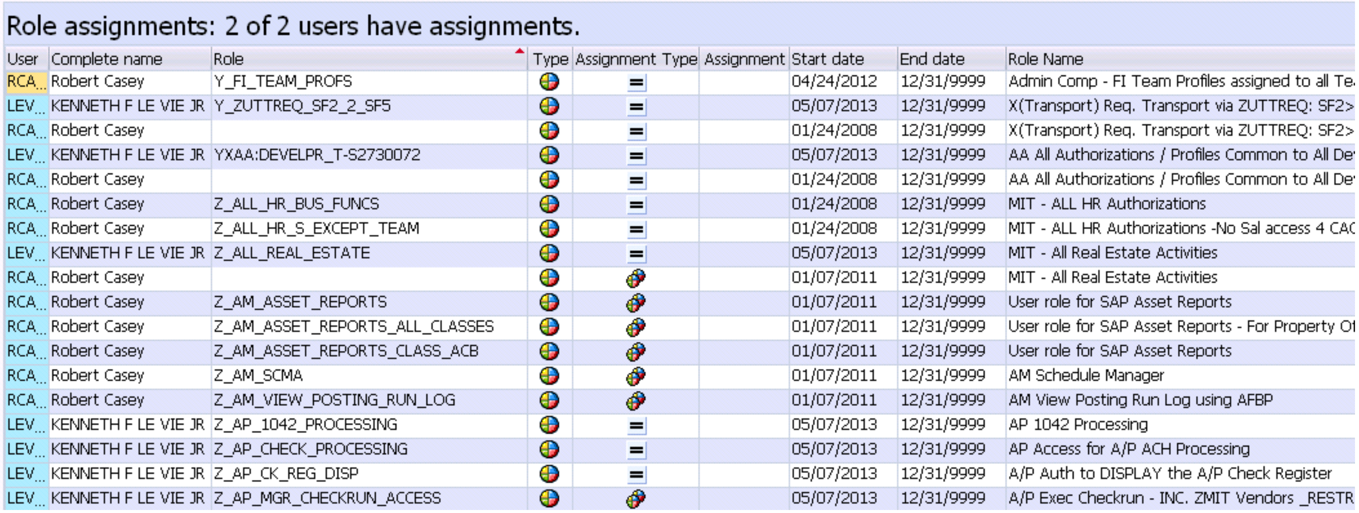
Click on the Role Column header and then click on the ▲ Sort (Ascending) icon .

This gives a list of Users per role showing :

- User Id and name
- Role Id and name
- Type of role
  - ❖ Composite
  - ⊕ Single
- Start & end date

Analysis : either one or both the users have a role.

There is no more detailed drilldown from this report.



Role assignments: 2 of 2 users have assignments.

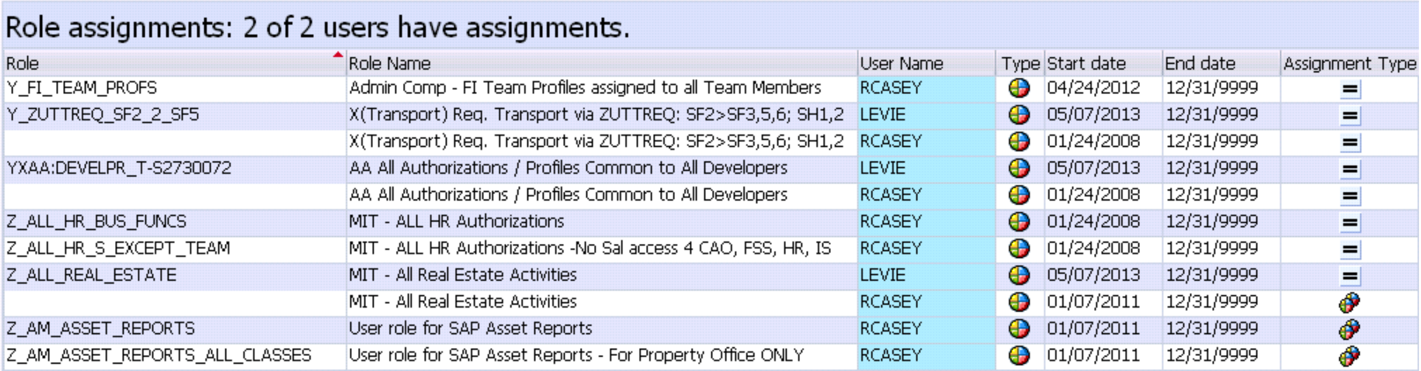
User	Complete name	Role	Type	Assignment Type	Assignment	Start date	End date	Role Name
RCA...	Robert Casey	Y_FI_TEAM_PROFS	⊕	=		04/24/2012	12/31/9999	Admin Comp - FI Team Profiles assigned to all Te
LEV...	KENNETH F LE VIE JR	Y_ZUTTREQ_SF2_2_SF5	⊕	=		05/07/2013	12/31/9999	X(Transport) Req. Transport via ZUTTREQ: SF2>
RCA...	Robert Casey		⊕	=		01/24/2008	12/31/9999	X(Transport) Req. Transport via ZUTTREQ: SF2>
LEV...	KENNETH F LE VIE JR	YXAA:DEVELPR_T-S2730072	⊕	=		05/07/2013	12/31/9999	AA All Authorizations / Profiles Common to All De
RCA...	Robert Casey		⊕	=		01/24/2008	12/31/9999	AA All Authorizations / Profiles Common to All De
RCA...	Robert Casey	Z_ALL_HR_BUS_FUNCS	⊕	=		01/24/2008	12/31/9999	MIT - ALL HR Authorizations
RCA...	Robert Casey	Z_ALL_HR_S_EXCEPT_TEAM	⊕	=		01/24/2008	12/31/9999	MIT - ALL HR Authorizations -No Sal access 4 CAC
LEV...	KENNETH F LE VIE JR	Z_ALL_REAL_ESTATE	⊕	=		05/07/2013	12/31/9999	MIT - All Real Estate Activities
RCA...	Robert Casey		⊕	❖		01/07/2011	12/31/9999	MIT - All Real Estate Activities
RCA...	Robert Casey	Z_AM_ASSET_REPORTS	⊕	❖		01/07/2011	12/31/9999	User role for SAP Asset Reports
RCA...	Robert Casey	Z_AM_ASSET_REPORTS_ALL_CLASSES	⊕	❖		01/07/2011	12/31/9999	User role for SAP Asset Reports - For Property Of
RCA...	Robert Casey	Z_AM_ASSET_REPORTS_CLASS_ACB	⊕	❖		01/07/2011	12/31/9999	User role for SAP Asset Reports
RCA...	Robert Casey	Z_AM_SCMA	⊕	❖		01/07/2011	12/31/9999	AM Schedule Manager
RCA...	Robert Casey	Z_AM_VIEW_POSTING_RUN_LOG	⊕	❖		01/07/2011	12/31/9999	AM View Posting Run Log using AFBP
LEV...	KENNETH F LE VIE JR	Z_AP_1042_PROCESSING	⊕	=		05/07/2013	12/31/9999	AP 1042 Processing
LEV...	KENNETH F LE VIE JR	Z_AP_CHECK_PROCESSING	⊕	=		05/07/2013	12/31/9999	AP Access for A/P ACH Processing
LEV...	KENNETH F LE VIE JR	Z_AP_CK_REG_DISP	⊕	=		05/07/2013	12/31/9999	A/P Auth to DISPLAY the A/P Check Register
LEV...	KENNETH F LE VIE JR	Z_AP_MGR_CHECKRUN_ACCESS	⊕	❖		05/07/2013	12/31/9999	A/P Exec Checkrun - INC. ZMIT Vendors _RESTR

4d

If this report is to be used frequently, change and save display layout.

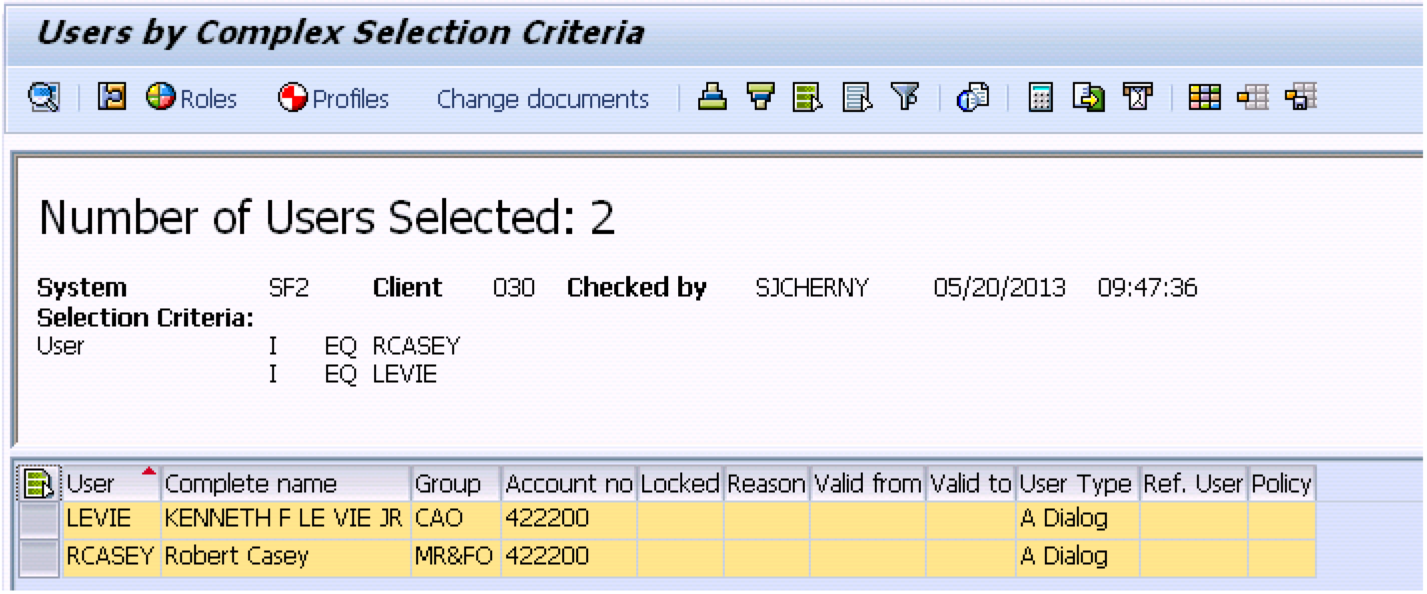
Use the standard layout management icons : ▦ ▦ ▦

Example layout – sorted on Role then User



Role assignments: 2 of 2 users have assignments.

Role	Role Name	User Name	Type	Start date	End date	Assignment Type
Y_FI_TEAM_PROFS	Admin Comp - FI Team Profiles assigned to all Team Members	RCASEY	⊕	04/24/2012	12/31/9999	=
Y_ZUTTREQ_SF2_2_SF5	X(Transport) Req. Transport via ZUTTREQ: SF2>SF3,5,6; SH1,2	LEVIE	⊕	05/07/2013	12/31/9999	=
	X(Transport) Req. Transport via ZUTTREQ: SF2>SF3,5,6; SH1,2	RCASEY	⊕	01/24/2008	12/31/9999	=
YXAA:DEVELPR_T-S2730072	AA All Authorizations / Profiles Common to All Developers	LEVIE	⊕	05/07/2013	12/31/9999	=
	AA All Authorizations / Profiles Common to All Developers	RCASEY	⊕	01/24/2008	12/31/9999	=
Z_ALL_HR_BUS_FUNCS	MIT - ALL HR Authorizations	RCASEY	⊕	01/24/2008	12/31/9999	=
Z_ALL_HR_S_EXCEPT_TEAM	MIT - ALL HR Authorizations -No Sal access 4 CAO, FSS, HR, IS	RCASEY	⊕	01/24/2008	12/31/9999	=
Z_ALL_REAL_ESTATE	MIT - All Real Estate Activities	LEVIE	⊕	05/07/2013	12/31/9999	=
	MIT - All Real Estate Activities	RCASEY	⊕	01/07/2011	12/31/9999	❖
Z_AM_ASSET_REPORTS	User role for SAP Asset Reports	RCASEY	⊕	01/07/2011	12/31/9999	❖
Z_AM_ASSET_REPORTS_ALL_CLASSES	User role for SAP Asset Reports - For Property Office ONLY	RCASEY	⊕	01/07/2011	12/31/9999	❖

5a	Back to the User list – an alternative display for a single user shows all profiles (not just those from roles) Click on to select both (all) users Then click on Profiles to list the profiles	

Users by Complex Selection Criteria

Number of Users Selected: 2

System SF2 **Client** 030 **Checked by** SJCHERNY 05/20/2013 09:47:36
Selection Criteria:
User I EQ RCASEY
I EQ LEVIE

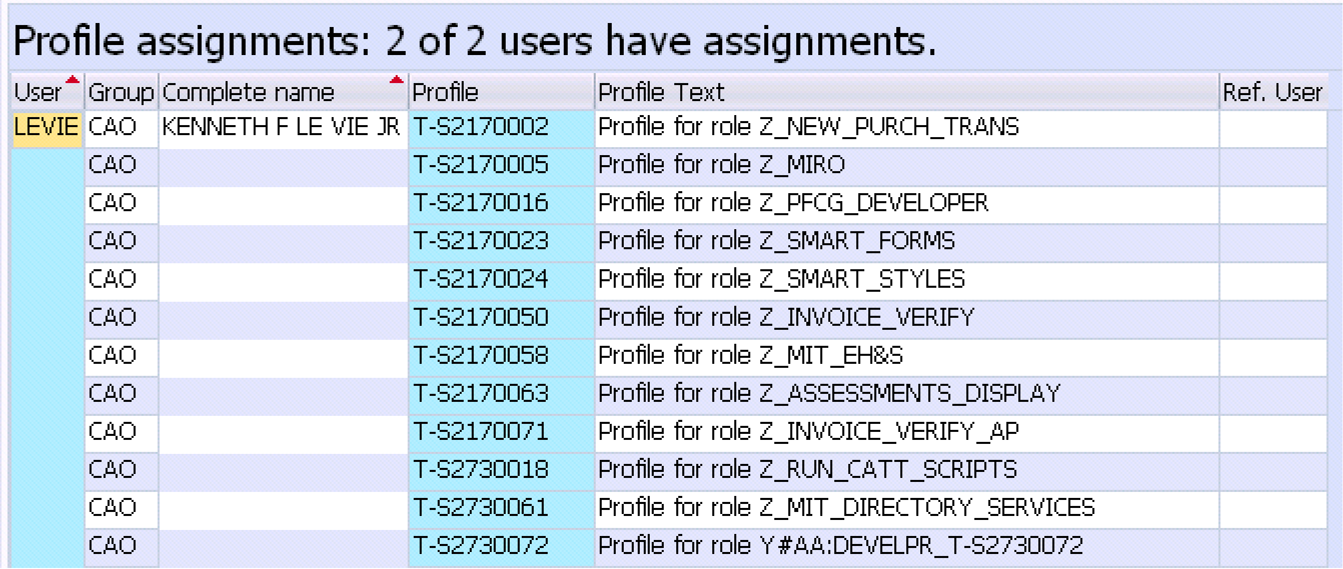
User	Complete name	Group	Account no	Locked	Reason	Valid from	Valid to	User Type	Ref. User	Policy
LEVIE	KENNETH F LE VIE JR	CAO	422200					A Dialog		
RCASEY	Robert Casey	MR&FO	422200					A Dialog		

5b

Report shows :

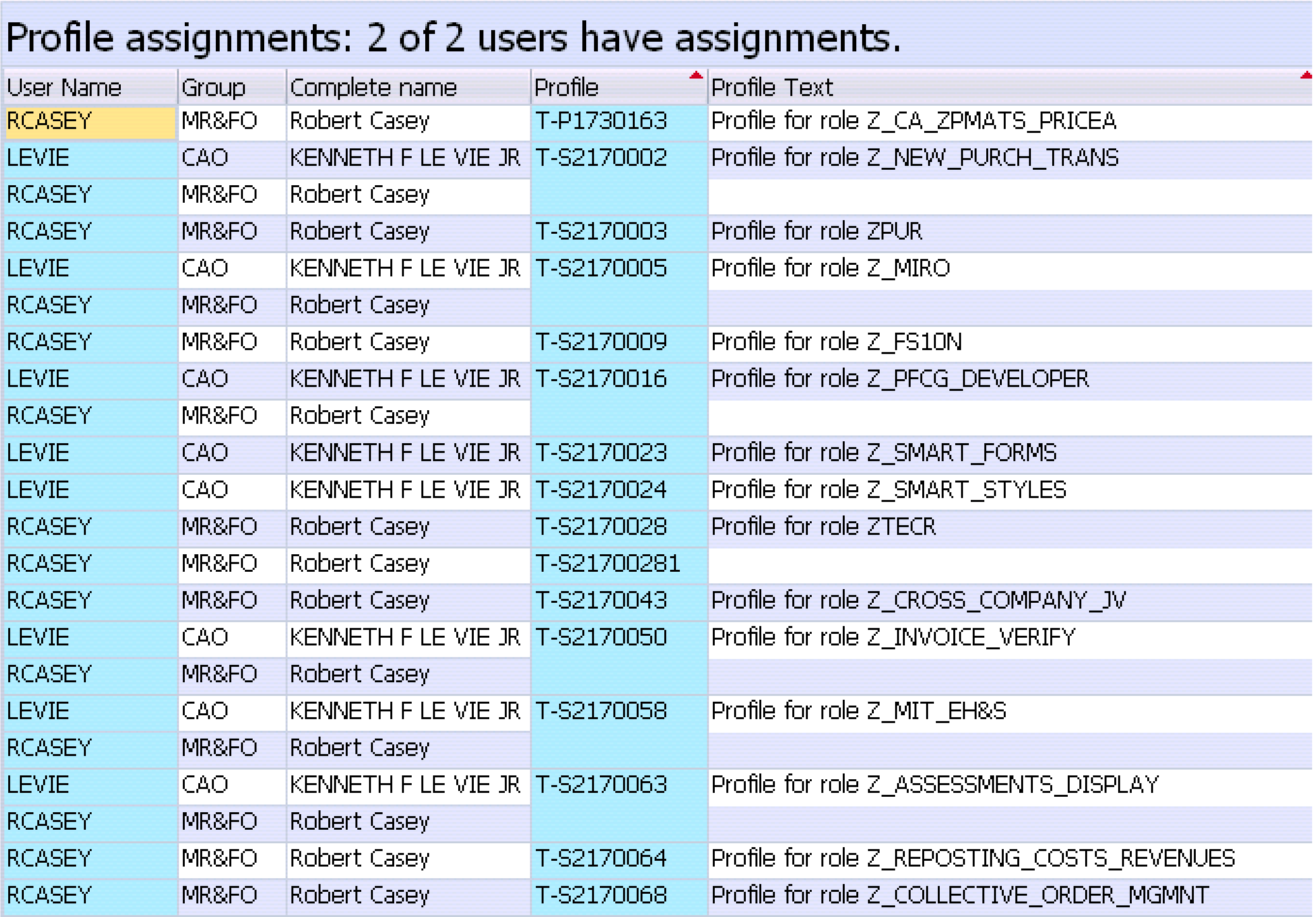
- User Id
- User Group
- Profile Id
- Profile text (may include Role Id if generated from a role)

Note :
The profiles starting with “Z” are mostly related to manual profiles (MIT Custom RolesDB assignment)
The profiles starting with “T-S” are from the SAP Profile Generator (based on SAP Security Roles – one profile per role).



Profile assignments: 2 of 2 users have assignments.

User	Group	Complete name	Profile	Profile Text	Ref. User
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170002	Profile for role Z_NEW_PURCH_TRANS	
	CAO		T-S2170005	Profile for role Z_MIRO	
	CAO		T-S2170016	Profile for role Z_PFCG_DEVELOPER	
	CAO		T-S2170023	Profile for role Z_SMART_FORMS	
	CAO		T-S2170024	Profile for role Z_SMART_STYLES	
	CAO		T-S2170050	Profile for role Z_INVOICE_VERIFY	
	CAO		T-S2170058	Profile for role Z_MIT_EH&S	
	CAO		T-S2170063	Profile for role Z_ASSESSMENTS_DISPLAY	
	CAO		T-S2170071	Profile for role Z_INVOICE_VERIFY_AP	
	CAO		T-S2730018	Profile for role Z_RUN_CATT_SCRIPTS	
	CAO		T-S2730061	Profile for role Z_MIT_DIRECTORY_SERVICES	
	CAO		T-S2730072	Profile for role Y#AA:DEVELPR_T-S2730072	

5c	Sort by Profile / User columns to get a different view. Only one or both the users have the profiles.	

Profile assignments: 2 of 2 users have assignments.

User Name	Group	Complete name	Profile	Profile Text
RCASEY	MR&FO	Robert Casey	T-P1730163	Profile for role Z_CA_ZPMATS_PRICEA
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170002	Profile for role Z_NEW_PURCH_TRANS
RCASEY	MR&FO	Robert Casey		
RCASEY	MR&FO	Robert Casey	T-S2170003	Profile for role ZPUR
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170005	Profile for role Z_MIRO
RCASEY	MR&FO	Robert Casey		
RCASEY	MR&FO	Robert Casey	T-S2170009	Profile for role Z_FS10N
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170016	Profile for role Z_PFCG_DEVELOPER
RCASEY	MR&FO	Robert Casey		
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170023	Profile for role Z_SMART_FORMS
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170024	Profile for role Z_SMART_STYLES
RCASEY	MR&FO	Robert Casey	T-S2170028	Profile for role ZTECR
RCASEY	MR&FO	Robert Casey	T-S21700281	
RCASEY	MR&FO	Robert Casey	T-S2170043	Profile for role Z_CROSS_COMPANY_JV
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170050	Profile for role Z_INVOICE_VERIFY
RCASEY	MR&FO	Robert Casey		
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170058	Profile for role Z_MIT_EH&S
RCASEY	MR&FO	Robert Casey		
LEVIE	CAO	KENNETH F LE VIE JR	T-S2170063	Profile for role Z_ASSESSMENTS_DISPLAY
RCASEY	MR&FO	Robert Casey		
RCASEY	MR&FO	Robert Casey	T-S2170064	Profile for role Z_REPOSTING_COSTS_REVENUES
RCASEY	MR&FO	Robert Casey	T-S2170068	Profile for role Z_COLLECTIVE_ORDER_MGMNT

Job Aid 09 Count Authorizations for Users

USE

This report can be used to view the roles and profiles assigned to a user.

INFORMATION

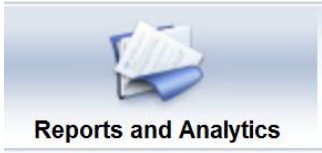
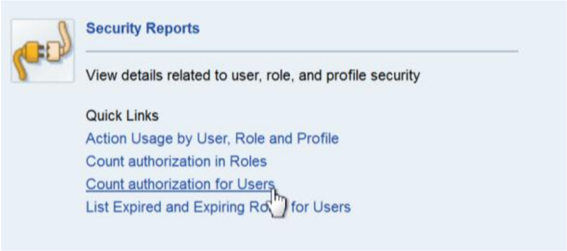
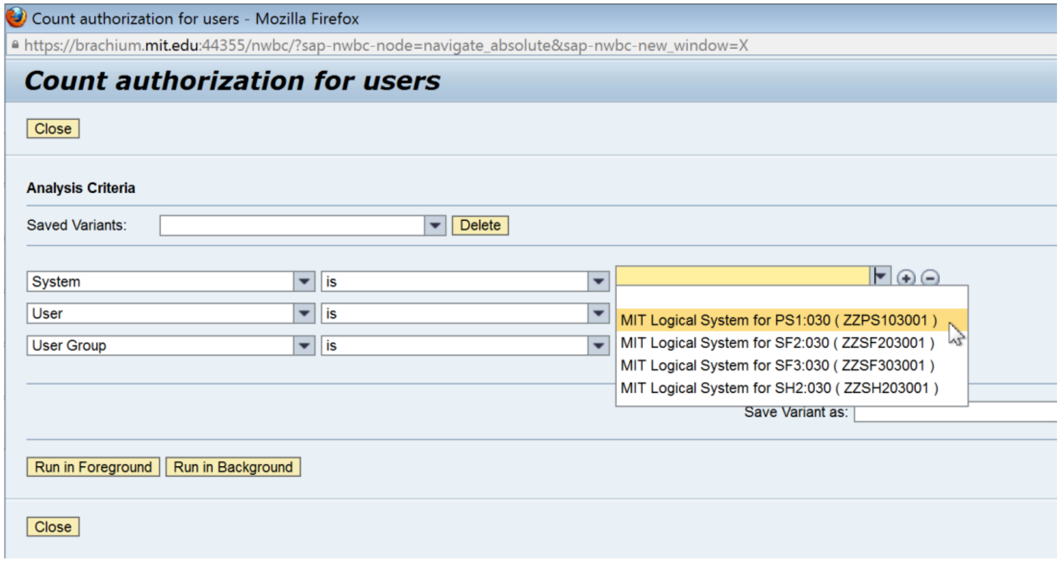
Roles and profiles assigned to a user/users (composite roles are not included; however, single roles assigned via composite roles are) along with the number of authorizations in each.

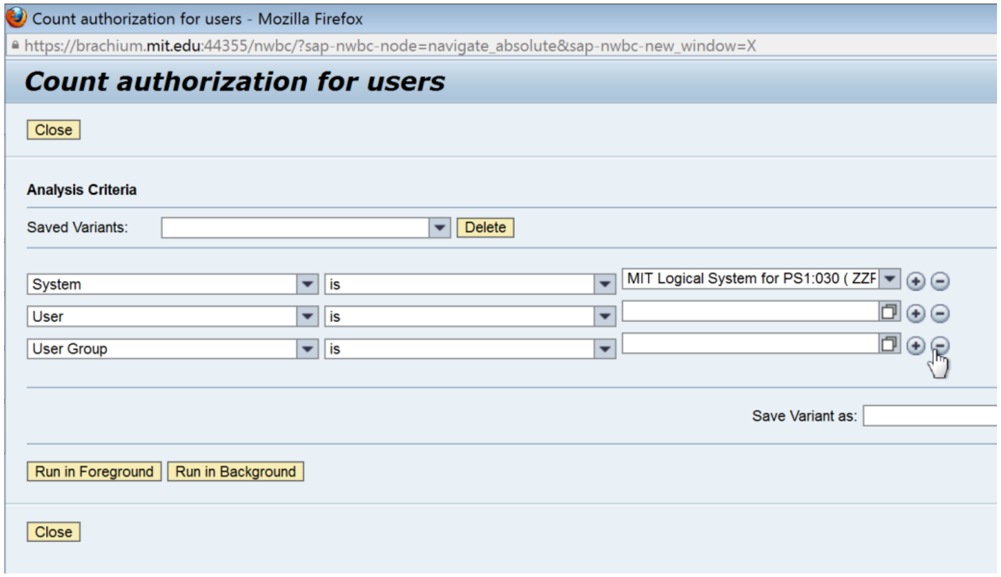
RELATED PROCESSES

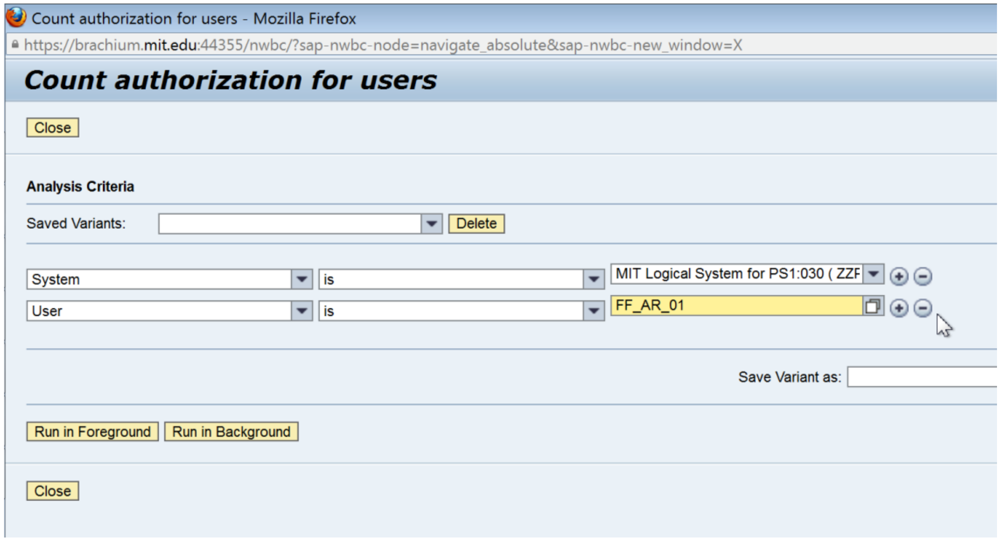
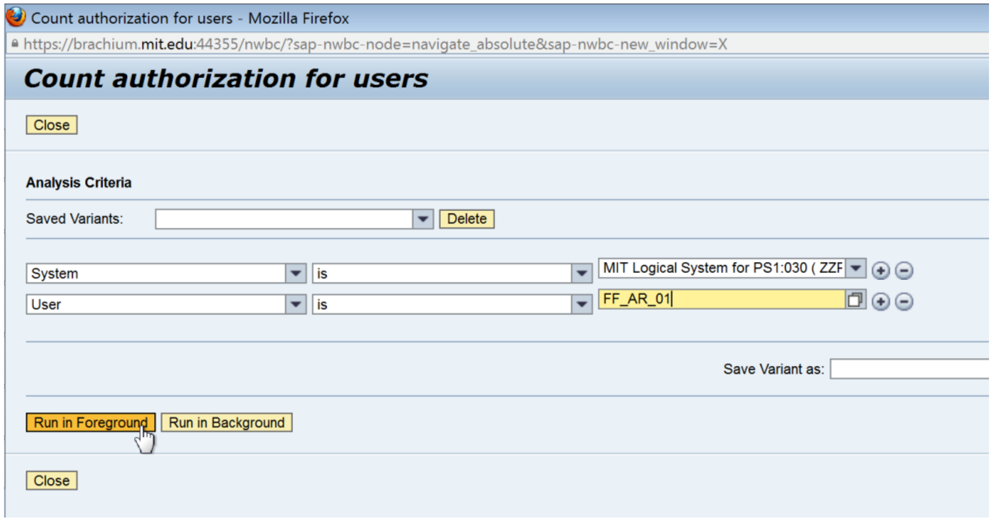
- Process 1: New or Amended Roles

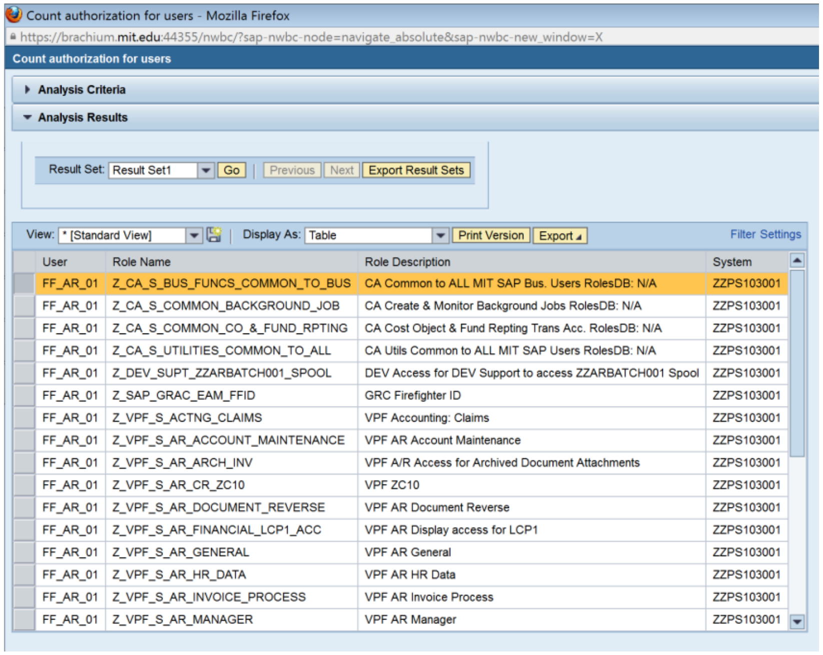
SPECIFIC SCENARIOS

- Step 4A: Analyze for a single user.
- Step 4B: Analyze for a multiple users by user ID.
- Step 4C: Analyze for a multiple users by user group.

Step	Description	Screenshot
1	Navigate to the 'Reports and Analytics' tab.	 Reports and Analytics
2	Click on the 'Count authorization for Users' report located in the 'Security Reports' section.	 Security Reports View details related to user, role, and profile security Quick Links Action Usage by User, Role and Profile Count authorization in Roles Count authorization for Users List Expired and Expiring Roles for Users
3	Select the system for which information is required. In this case, the selection is PS1.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Count authorization for users Close Analysis Criteria Saved Variants: Delete System is User is User Group is MIT Logical System for PS1:030 (ZZPS103001) MIT Logical System for SF2:030 (ZZSF203001) MIT Logical System for SF3:030 (ZZSF303001) MIT Logical System for SH2:030 (ZZSH203001) Save Variant as: Run in Foreground Run in Background Close

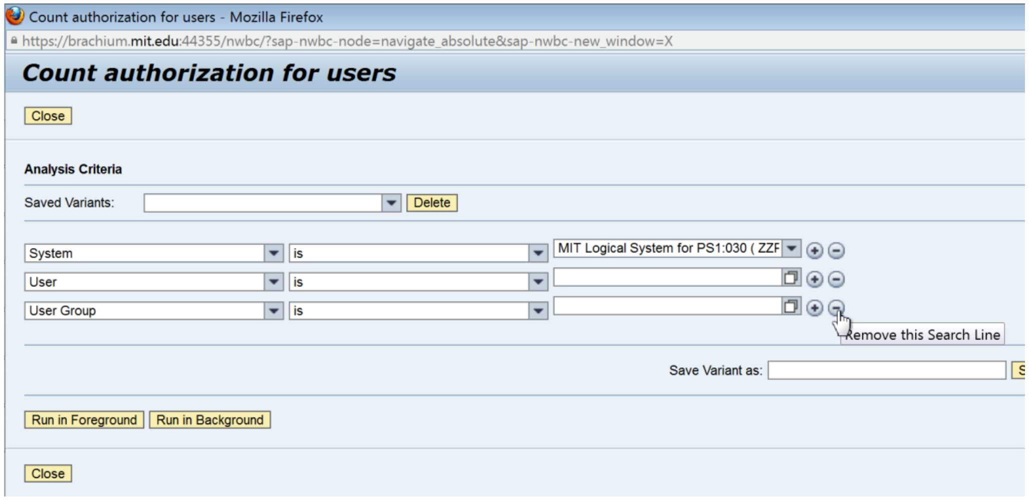
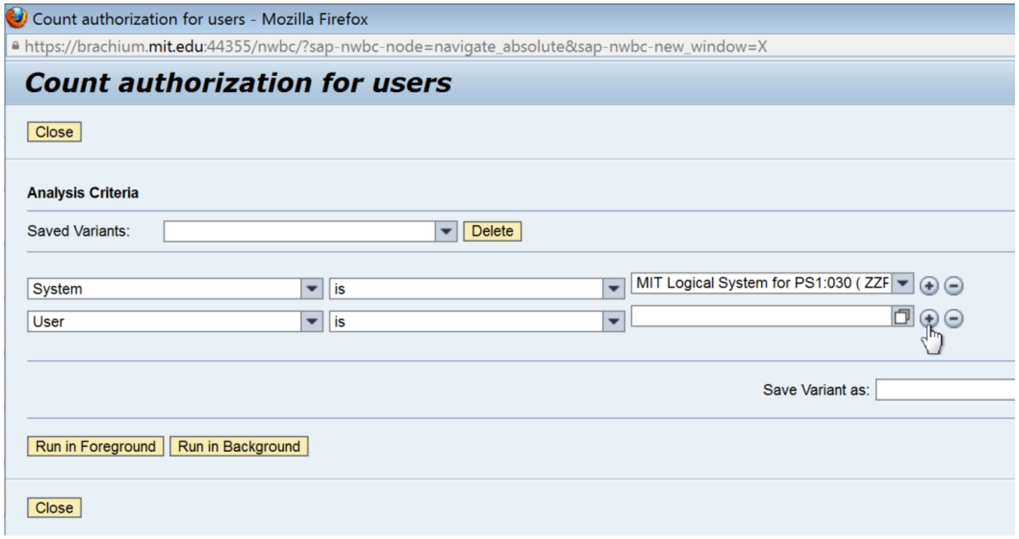
4A-1	Analyze for a single user. Click on the '-' at the end of the 'User Group' row to delete the user group search criterion.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Count authorization for users** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF User is User Group is Save Variant as: Run in Foreground Run in Background Close

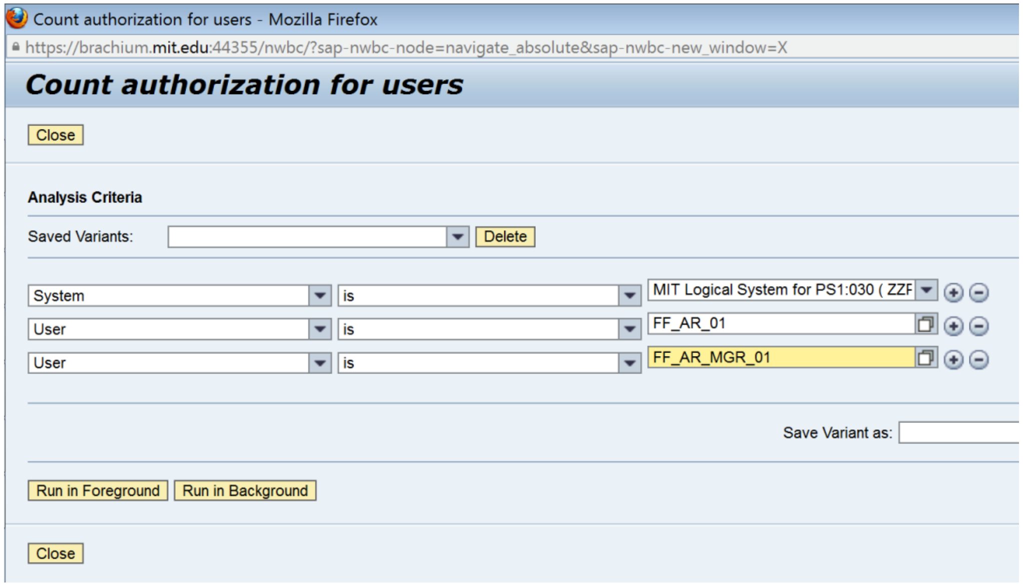
4A-2	Add the user ID. In this case, ‘FF_AR_01’, an AR Cashiers FireFighter ID, was typed in. The search option can also be used to search for an ID. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Count authorization for users Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User is FF_AR_01 Save Variant as: Close Delete Run in Foreground Run in Background Close
4A-3	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Count authorization for users Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User is FF_AR_01 Save Variant as: Close Delete Run in Foreground Run in Background Close

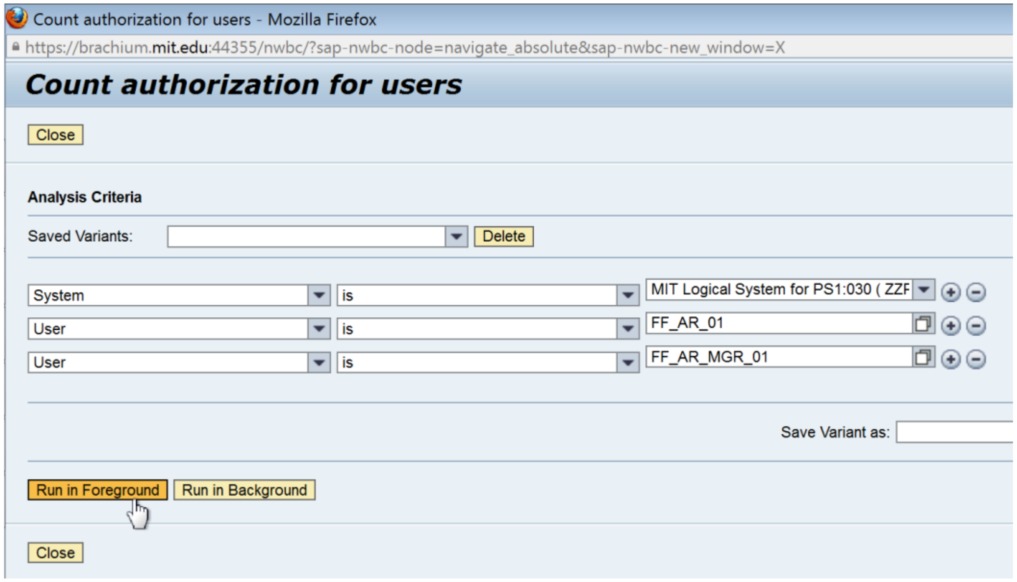
4A-4	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. User: User ID of the user with access to the role Role Name: SAP role name Role Description: Business name for SAP role System: The system in which the role is assigned to the user	

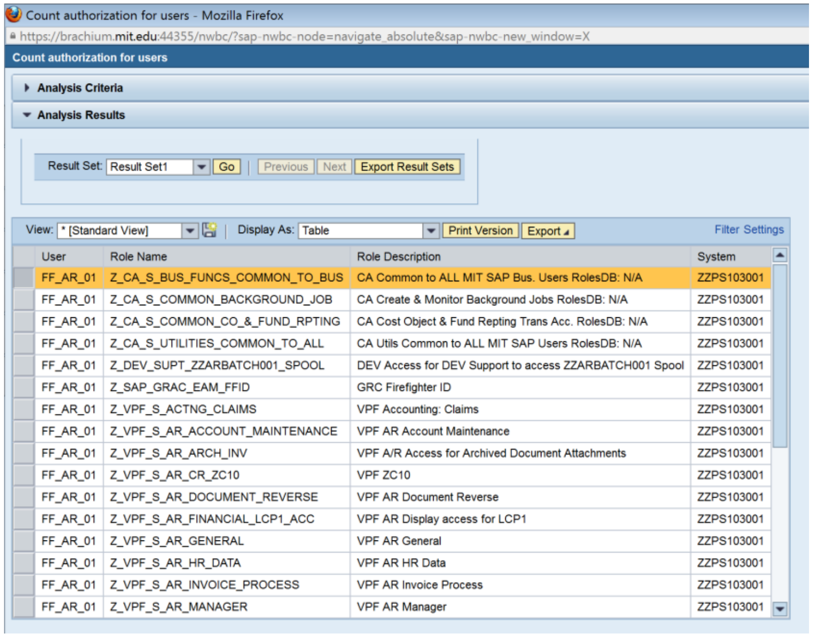
Count authorization for users - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Count authorization for users
Analysis Criteria
Analysis Results
Result Set: Result Set1
Go
Previous
Next
Export Result Sets
View: * [Standard View]
Display As: Table
Print Version
Export
Filter Settings

User	Role Name	Role Description	System
FF_AR_01	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	ZZPS103001
FF_AR_01	Z_CA_S_COMMON_BACKGROUND_JOB	CA Create & Monitor Background Jobs RolesDB: N/A	ZZPS103001
FF_AR_01	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	ZZPS103001
FF_AR_01	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A	ZZPS103001
FF_AR_01	Z_DEV_SUPT_ZZARBATCH001_SPOOL	DEV Access for DEV Support to access ZZARBATCH001 Spool	ZZPS103001
FF_AR_01	Z_SAP_GRAC_EAM_FFID	GRC Firefighter ID	ZZPS103001
FF_AR_01	Z_VPF_S_ACTNG_CLAIMS	VPF Accounting: Claims	ZZPS103001
FF_AR_01	Z_VPF_S_AR_ACCOUNT_MAINTENANCE	VPF AR Account Maintenance	ZZPS103001
FF_AR_01	Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	ZZPS103001
FF_AR_01	Z_VPF_S_AR_CR_ZC10	VPF ZC10	ZZPS103001
FF_AR_01	Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	ZZPS103001
FF_AR_01	Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	ZZPS103001
FF_AR_01	Z_VPF_S_AR_GENERAL	VPF AR General	ZZPS103001
FF_AR_01	Z_VPF_S_AR_HR_DATA	VPF AR HR Data	ZZPS103001
FF_AR_01	Z_VPF_S_AR_INVOICE_PROCESS	VPF AR Invoice Process	ZZPS103001
FF_AR_01	Z_VPF_S_AR_MANAGER	VPF AR Manager	ZZPS103001

4B-1	Analyze for a multiple users by user ID. Click on the '-' at the end of the 'User Group' row to delete the user group search criterion.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Count authorization for users Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User is User Group is Save Variant as: Close Delete Remove this Search Line S Run in Foreground Run in Background Close
4B-2	Click on the '+' at the end of the 'User' row to add an additional user ID search criterion row for each ID. In this case, one additional row is added; thus, we can analyze for a total of two user IDs.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Count authorization for users Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User is Save Variant as: Close Delete Run in Foreground Run in Background Close

4B-3	Add the user IDs. In this case, ‘FF_AR_01’ and ‘FF_AR_MGR_01’, two AR Cashiers FireFighter IDs, were typed in. The search option can also be used to search for IDs. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Count authorization for users** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF User is FF_AR_01 User is FF_AR_MGR_01 Save Variant as: Run in Foreground Run in Background Close

4B-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Count authorization for users** Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User is FF_AR_01 User is FF_AR_MGR_01 Save Variant as: Close Delete Run in Foreground Run in Background Close

4B-5	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. User: User ID of the user with access to the role Role Name: SAP role name Role Description: Business name for SAP role System: The system in which the role is assigned to the user	

Count authorization for users - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Count authorization for users

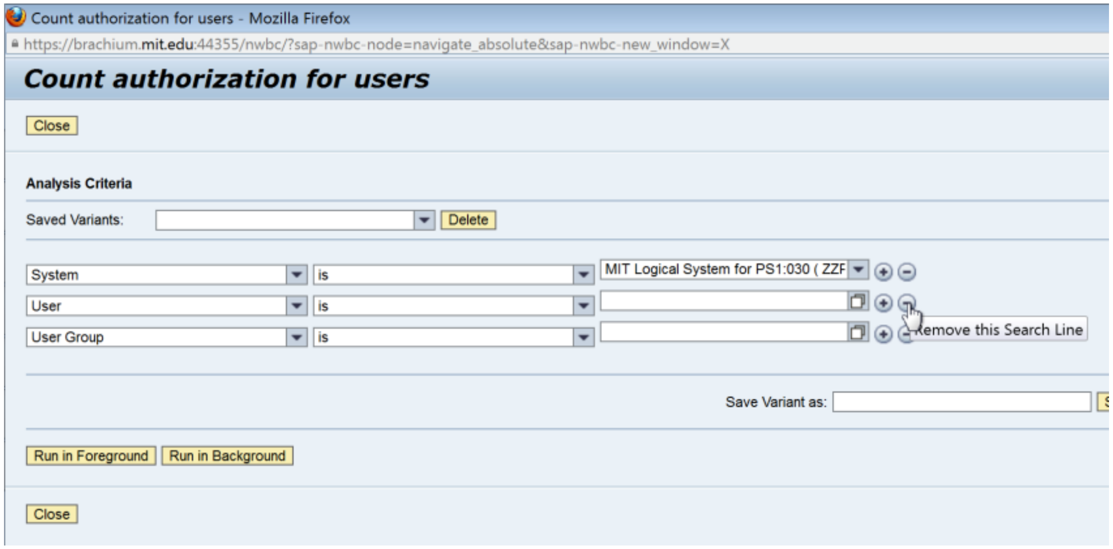
Analysis Criteria

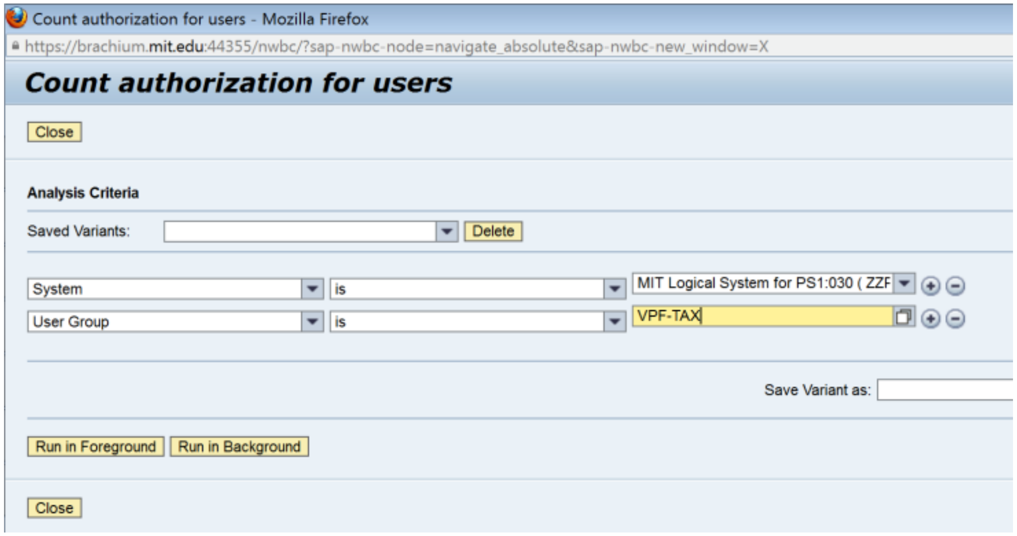
Analysis Results

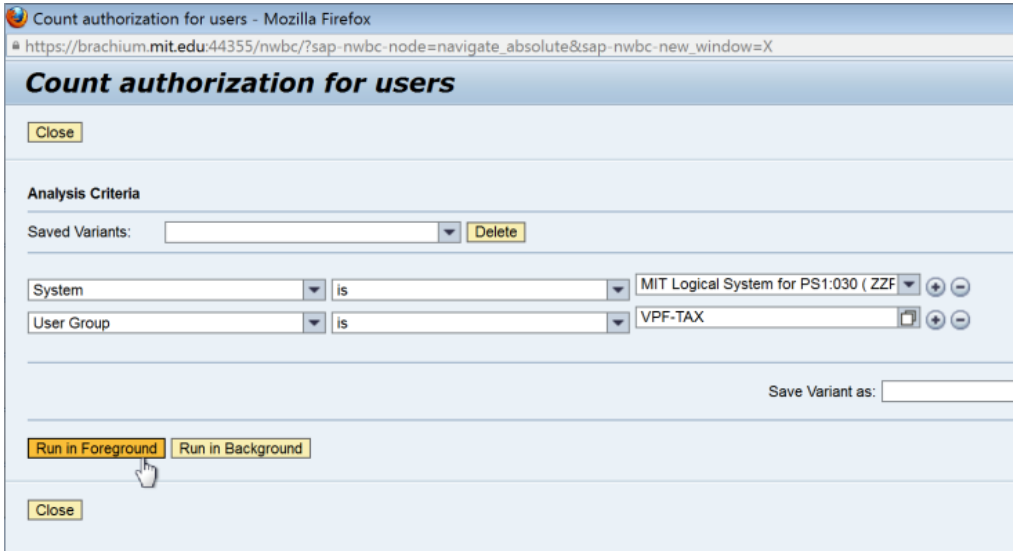
Result Set: Result Set1

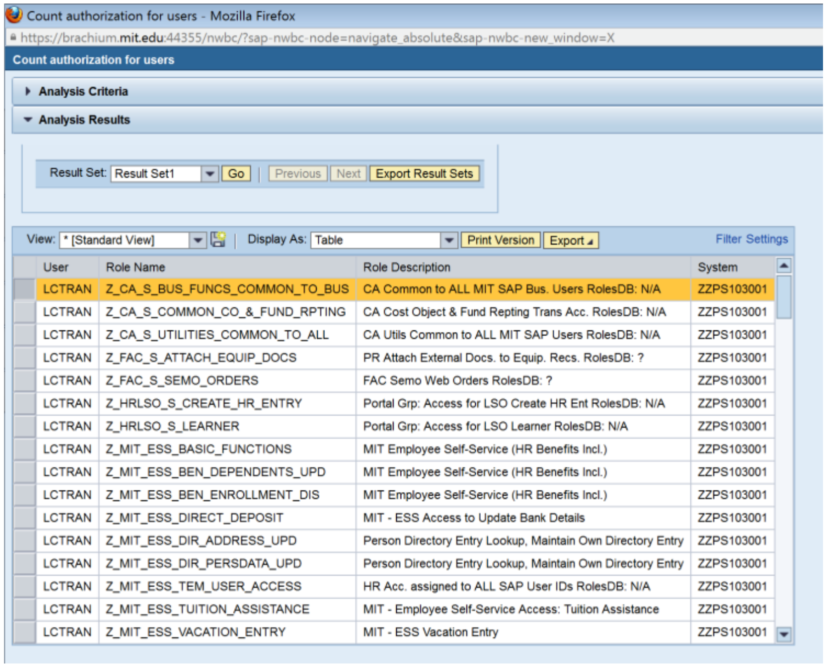
View: * [Standard View]   Display As: Table

User	Role Name	Role Description	System
FF_AR_01	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	ZZPS103001
FF_AR_01	Z_CA_S_COMMON_BACKGROUND_JOB	CA Create & Monitor Background Jobs RolesDB: N/A	ZZPS103001
FF_AR_01	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	ZZPS103001
FF_AR_01	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A	ZZPS103001
FF_AR_01	Z_DEV_SUPT_ZZARBATCH001_SPOOL	DEV Access for DEV Support to access ZZARBATCH001 Spool	ZZPS103001
FF_AR_01	Z_SAP_GRAC_EAM_FFID	GRC Firefighter ID	ZZPS103001
FF_AR_01	Z_VPF_S_ACTNG_CLAIMS	VPF Accounting: Claims	ZZPS103001
FF_AR_01	Z_VPF_S_AR_ACCOUNT_MAINTENANCE	VPF AR Account Maintenance	ZZPS103001
FF_AR_01	Z_VPF_S_AR_ARCH_INV	VPF A/R Access for Archived Document Attachments	ZZPS103001
FF_AR_01	Z_VPF_S_AR_CR_ZC10	VPF ZC10	ZZPS103001
FF_AR_01	Z_VPF_S_AR_DOCUMENT_REVERSE	VPF AR Document Reverse	ZZPS103001
FF_AR_01	Z_VPF_S_AR_FINANCIAL_LCP1_ACC	VPF AR Display access for LCP1	ZZPS103001
FF_AR_01	Z_VPF_S_AR_GENERAL	VPF AR General	ZZPS103001
FF_AR_01	Z_VPF_S_AR_HR_DATA	VPF AR HR Data	ZZPS103001
FF_AR_01	Z_VPF_S_AR_INVOICE_PROCESS	VPF AR Invoice Process	ZZPS103001
FF_AR_01	Z_VPF_S_AR_MANAGER	VPF AR Manager	ZZPS103001

4C-1	Analyze for a multiple users by user group. Click on the '-' at the end of the 'User' row to delete the user ID search criterion.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Count authorization for users Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF User is User Group is Remove this Search Line Save Variant as: Run in Foreground Run in Background Close

4C-2	Add the user group. In this case, 'VPF-TAX', the user group containing all user in VPF who are part of the Tax area, was typed in. The search option can also be used to search for user groups. Please refer to the 'Search for Input Values' reference document (R3) for further information. NOTE: The report can also be executed for multiple user groups by following steps similar to those outlined for multiple user IDs in steps 4B.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Count authorization for users Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF User Group is VPF-TAX Save Variant as: Close Delete Run in Foreground Run in Background Close

4C-3	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Count authorization for users - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Count authorization for users Saved Variants: System is MIT Logical System for PS1:030 (ZZF User Group is VPF-TAX Save Variant as: Close Analysis Criteria Delete Run in Foreground Run in Background Close

4C-4	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. User: User ID of the user with access to the role Role Name: SAP role name Role Description: Business name for SAP role System: The system in which the role is assigned to the user	

Count authorization for users - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Count authorization for users

Analysis Criteria

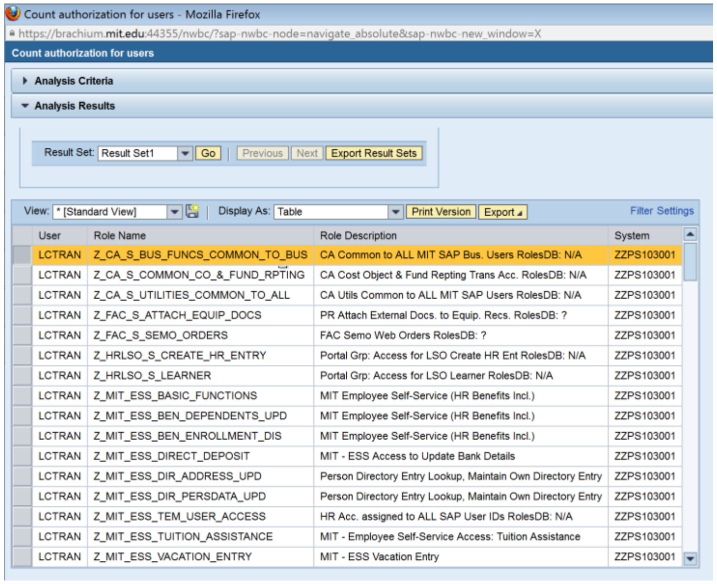
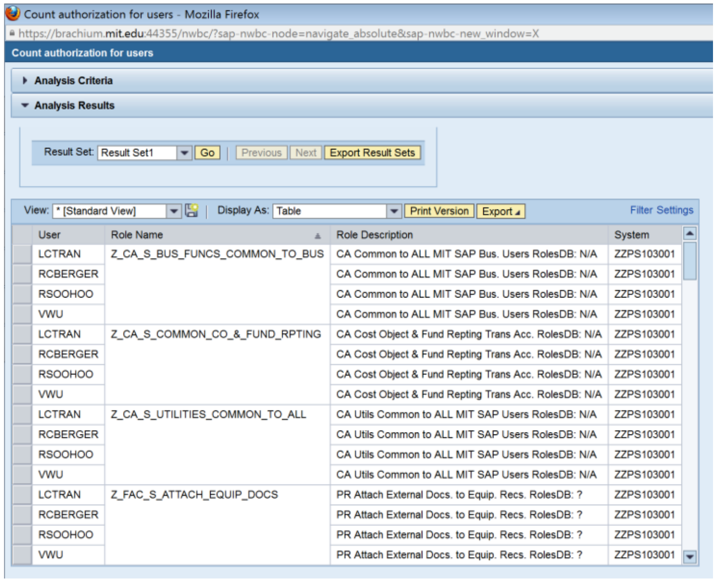
Analysis Results

Result Set: Result Set1

View: * [Standard View]

Display As: Table

User	Role Name	Role Description	System
LCTRAN	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	ZZPS103001
LCTRAN	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	ZZPS103001
LCTRAN	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A	ZZPS103001
LCTRAN	Z_FAC_S_ATTACH_EQUIP_DOCS	PR Attach External Docs. to Equip. Recs. RolesDB: ?	ZZPS103001
LCTRAN	Z_FAC_S_SEMO_ORDERS	FAC Semo Web Orders RolesDB: ?	ZZPS103001
LCTRAN	Z_HRLSO_S_CREATE_HR_ENTRY	Portal Grp: Access for LSO Create HR Ent RolesDB: N/A	ZZPS103001
LCTRAN	Z_HRLSO_S_LEARNER	Portal Grp: Access for LSO Learner RolesDB: N/A	ZZPS103001
LCTRAN	Z_MIT_ESS_BASIC_FUNCTIONS	MIT Employee Self-Service (HR Benefits Incl.)	ZZPS103001
LCTRAN	Z_MIT_ESS_BEN_DEPENDENTS_UPD	MIT Employee Self-Service (HR Benefits Incl.)	ZZPS103001
LCTRAN	Z_MIT_ESS_BEN_ENROLLMENT_DIS	MIT Employee Self-Service (HR Benefits Incl.)	ZZPS103001
LCTRAN	Z_MIT_ESS_DIRECT_DEPOSIT	MIT - ESS Access to Update Bank Details	ZZPS103001
LCTRAN	Z_MIT_ESS_DIR_ADDRESS_UPD	Person Directory Entry Lookup, Maintain Own Directory Entry	ZZPS103001
LCTRAN	Z_MIT_ESS_DIR_PERSDATA_UPD	Person Directory Entry Lookup, Maintain Own Directory Entry	ZZPS103001
LCTRAN	Z_MIT_ESS_TEM_USER_ACCESS	HR Acc. assigned to ALL SAP User IDs RolesDB: N/A	ZZPS103001
LCTRAN	Z_MIT_ESS_TUITION_ASSISTANCE	MIT - Employee Self-Service Access: Tuition Assistance	ZZPS103001
LCTRAN	Z_MIT_ESS_VACATION_ENTRY	MIT - ESS Vacation Entry	ZZPS103001

4C-5	Sorting on role by clicking on the ‘Role Name’ column header will show the users grouped by role.	 

Count authorization for users - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Count authorization for users

Analysis Criteria

Analysis Results

Result Set: Result Set1 Go | Previous Next Export Result Sets

View: * [Standard View] | Display As: Table | Print Version | Export | Filter Settings

User	Role Name	Role Description	System
LCTRAN	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	ZZPS103001
LCTRAN	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	ZZPS103001
LCTRAN	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A	ZZPS103001
LCTRAN	Z_FAC_S_ATTACH_EQUIP_DOCS	PR Attach External Docs. to Equip. Recs. RolesDB: ?	ZZPS103001
LCTRAN	Z_FAC_S_SEMO_ORDERS	FAC Semo Web Orders RolesDB: ?	ZZPS103001
LCTRAN	Z_HRLSO_S_CREATE_HR_ENTRY	Portal Grp: Access for LSO Create HR Ent RolesDB: N/A	ZZPS103001
LCTRAN	Z_HRLSO_S_LEARNER	Portal Grp: Access for LSO Learner RolesDB: N/A	ZZPS103001
LCTRAN	Z_MIT_ESS_BASIC_FUNCTIONS	MIT Employee Self-Service (HR Benefits Incl.)	ZZPS103001
LCTRAN	Z_MIT_ESS_BEN_DEPENDENTS_UPD	MIT Employee Self-Service (HR Benefits Incl.)	ZZPS103001
LCTRAN	Z_MIT_ESS_BEN_ENROLLMENT_DIS	MIT Employee Self-Service (HR Benefits Incl.)	ZZPS103001
LCTRAN	Z_MIT_ESS_DIRECT_DEPOSIT	MIT - ESS Access to Update Bank Details	ZZPS103001
LCTRAN	Z_MIT_ESS_DIR_ADDRESS_UPD	Person Directory Entry Lookup, Maintain Own Directory Entry	ZZPS103001
LCTRAN	Z_MIT_ESS_DIR_PERSDATA_UPD	Person Directory Entry Lookup, Maintain Own Directory Entry	ZZPS103001
LCTRAN	Z_MIT_ESS_TEM_USER_ACCESS	HR Acc. assigned to ALL SAP User IDs RolesDB: N/A	ZZPS103001
LCTRAN	Z_MIT_ESS_TUITION_ASSISTANCE	MIT - Employee Self-Service Access: Tuition Assistance	ZZPS103001
LCTRAN	Z_MIT_ESS_VACATION_ENTRY	MIT - ESS Vacation Entry	ZZPS103001

Count authorization for users - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Count authorization for users

Analysis Criteria

Analysis Results

Result Set: Result Set1 Go | Previous Next Export Result Sets

View: * [Standard View] | Display As: Table | Print Version | Export | Filter Settings

User	Role Name ▲	Role Description	System
LCTRAN	Z_CA_S_BUS_FUNCS_COMMON_TO_BUS	CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	ZZPS103001
RCBERGER		CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	ZZPS103001
RSOOHOO		CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	ZZPS103001
VWU		CA Common to ALL MIT SAP Bus. Users RolesDB: N/A	ZZPS103001
LCTRAN	Z_CA_S_COMMON_CO_&_FUND_RPTING	CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	ZZPS103001
RCBERGER		CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	ZZPS103001
RSOOHOO		CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	ZZPS103001
VWU		CA Cost Object & Fund Repting Trans Acc. RolesDB: N/A	ZZPS103001
LCTRAN	Z_CA_S_UTILITIES_COMMON_TO_ALL	CA Utils Common to ALL MIT SAP Users RolesDB: N/A	ZZPS103001
RCBERGER		CA Utils Common to ALL MIT SAP Users RolesDB: N/A	ZZPS103001
RSOOHOO		CA Utils Common to ALL MIT SAP Users RolesDB: N/A	ZZPS103001
VWU		CA Utils Common to ALL MIT SAP Users RolesDB: N/A	ZZPS103001
LCTRAN	Z_FAC_S_ATTACH_EQUIP_DOCS	PR Attach External Docs. to Equip. Recs. RolesDB: ?	ZZPS103001
RCBERGER		PR Attach External Docs. to Equip. Recs. RolesDB: ?	ZZPS103001
RSOOHOO		PR Attach External Docs. to Equip. Recs. RolesDB: ?	ZZPS103001
VWU		PR Attach External Docs. to Equip. Recs. RolesDB: ?	ZZPS103001

Job Aid 10 Action Usage by User Role and Profile

USE

This report can be used to determine transaction usage by a user.

INFORMATION

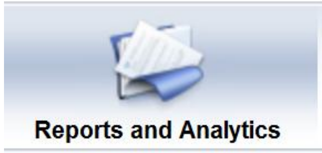
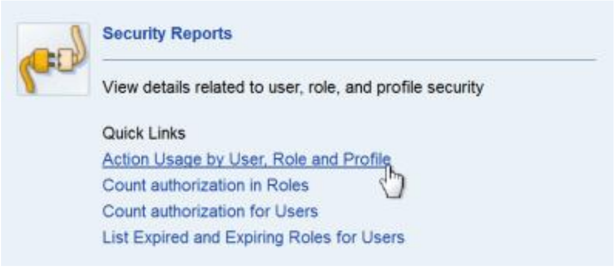
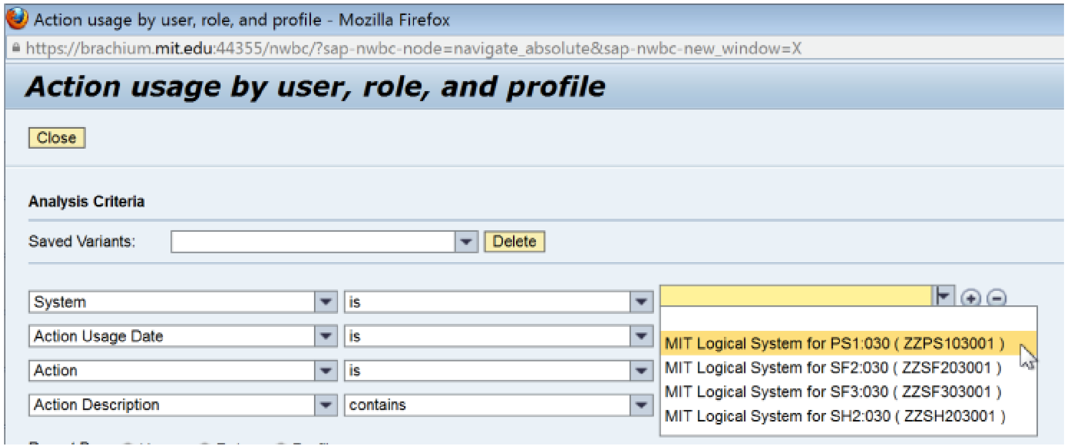
Count and last execution of transaction usage by a user or set of users during a period or on a particular date.

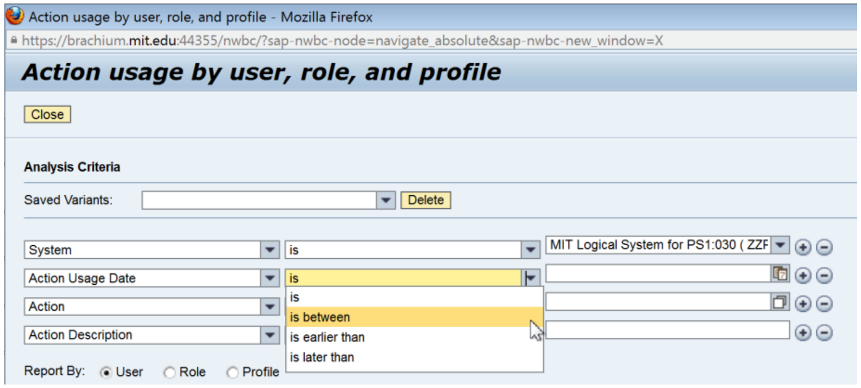
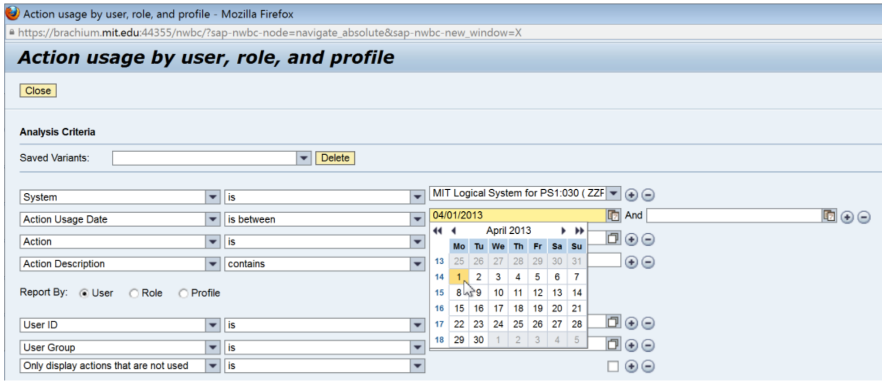
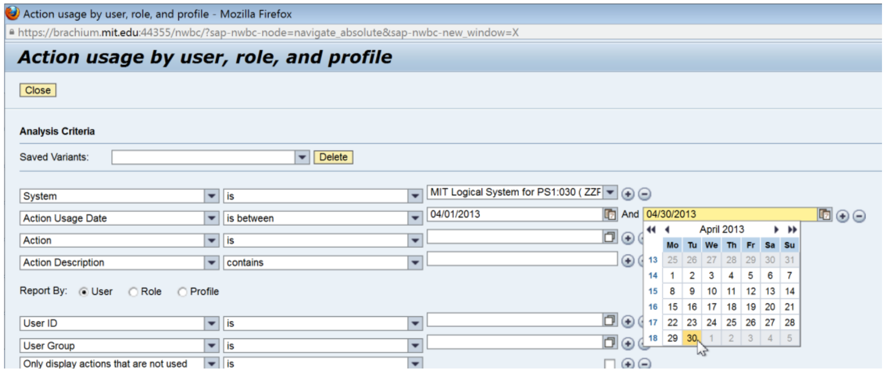
RELATED PROCESSES

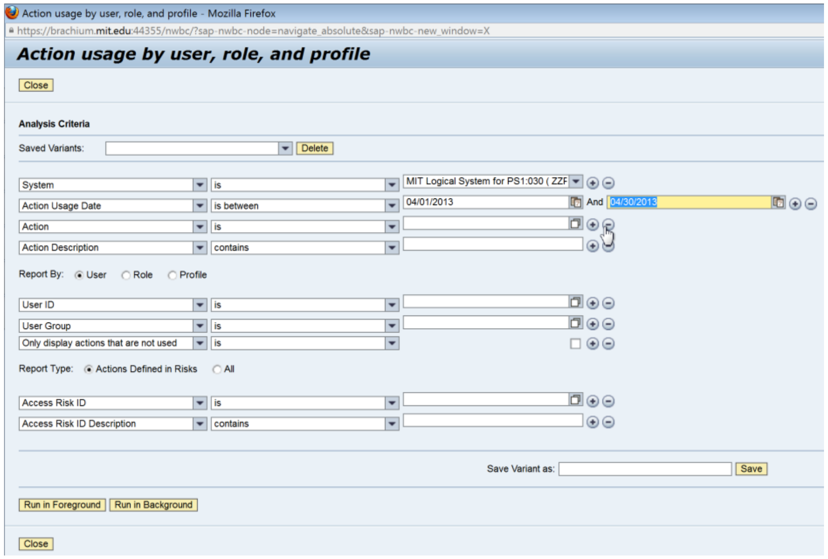
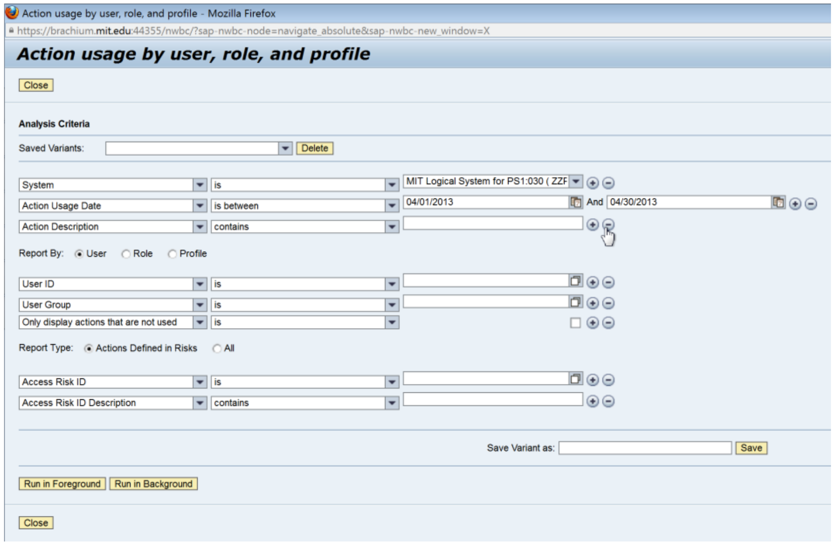
- Process 1: New or Amended Roles

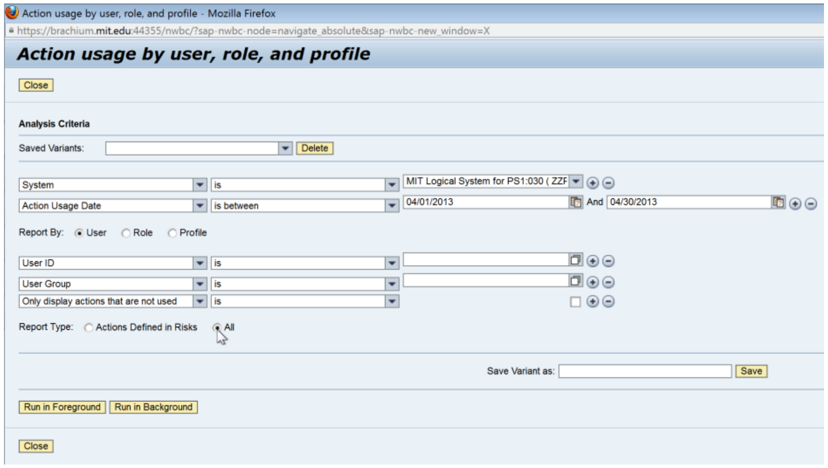
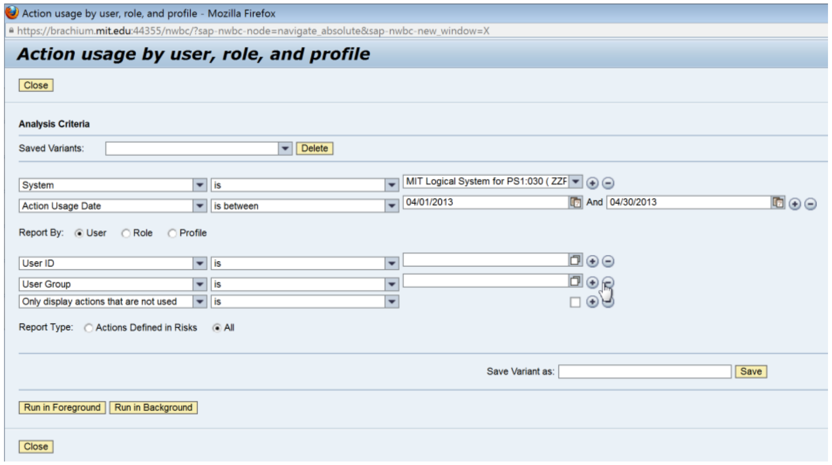
SPECIFIC SCENARIOS

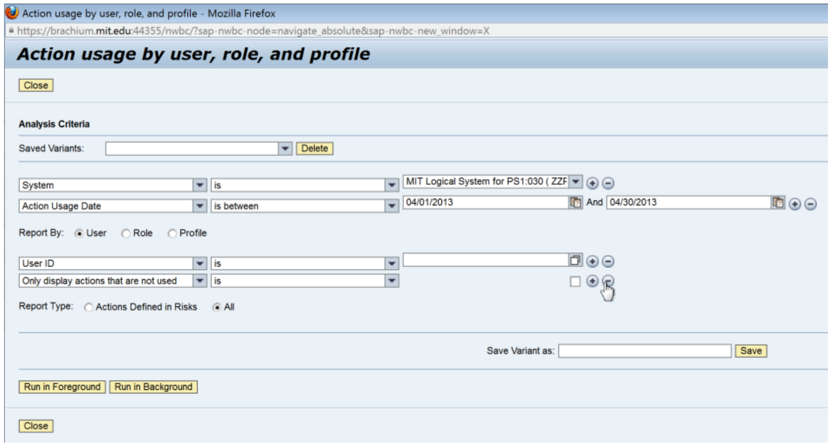
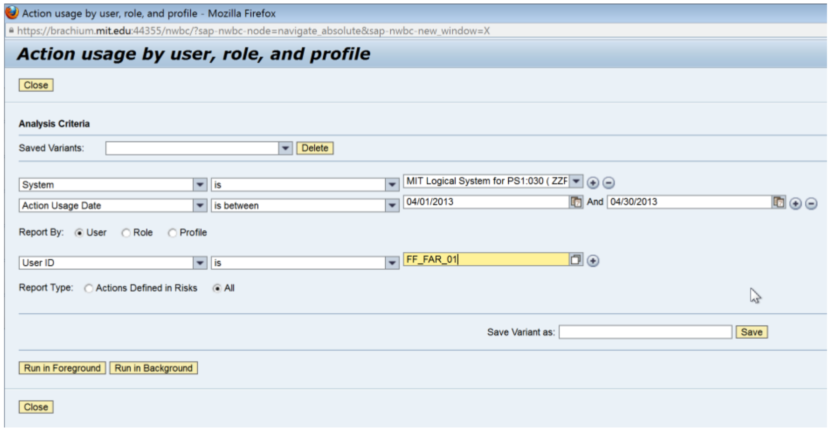
- Step 8A: Analyze by for a single user by user ID.
- Step 8B: Analyze by for multiple users by user ID.
- Step 8C: Analyze by for a single user group.
- Step 8D: Analyze by for a single role.
- Step 8E: Analyze by for a single profile.

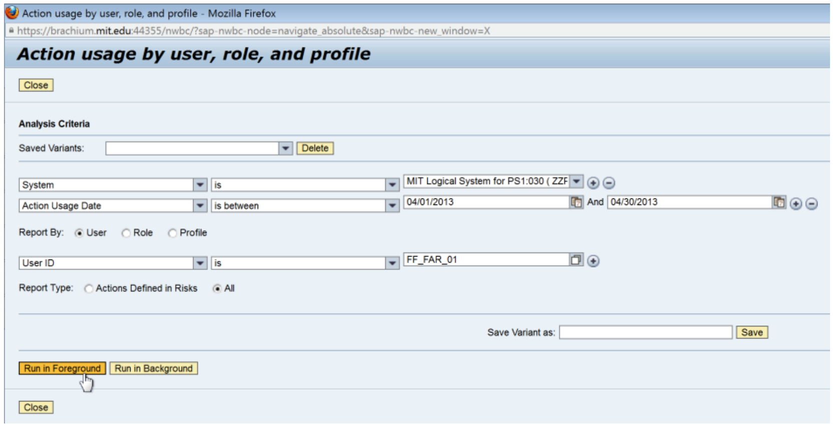
Step	Description	Screenshot
1	Navigate to the 'Reports and Analytics' tab.	 Reports and Analytics
2	Click on the 'Action Usage by User, Role and Profile' report located in the 'Security Reports' section.	 Security Reports View details related to user, role, and profile security Quick Links Action Usage by User, Role and Profile Count authorization in Roles Count authorization for Users List Expired and Expiring Roles for Users
3	Select the system for which information is required. In this case, the selection is PS1.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System is Action Usage Date is Action is Action Description contains MIT Logical System for PS1:030 (ZZPS103001) MIT Logical System for SF2:030 (ZZSF203001) MIT Logical System for SF3:030 (ZZSF303001) MIT Logical System for SH2:030 (ZZSH203001)

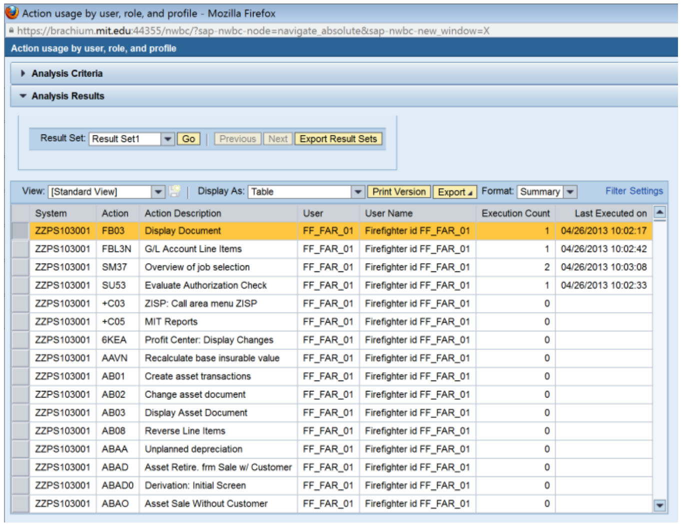
4	Select the period for which the report will be executed. The operand for the 'Action Usage Date' search criteron can be changed from 'is' to 'is between', 'is earlier than', and 'is later than'. Most often, analysis will be needed for a period of time; therefore, the 'is between' perand is recommended. Click on the calendar icons to select a period. In this case, a period is defined of 04/01/2013 to 04/30/2013.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System: is: MIT Logical System for PS1:030 (ZZF Action Usage Date: is is is between is earlier than is later than Action Action Description Report By: ● User ○ Role ○ Profile  Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System: is: MIT Logical System for PS1:030 (ZZF Action Usage Date: is between: 04/01/2013 And Action: is Action Description: contains Report By: ● User ○ Role ○ Profile User ID: is User Group: is Only display actions that are not used: is April 2013 Mo Tu We Th Fr Sa Su 13 25 26 27 28 29 30 31 14 1 2 3 4 5 6 7 15 8 9 10 11 12 13 14 16 15 16 17 18 19 20 21 17 22 23 24 25 26 27 28 18 29 30 1 2 3 4 5  Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System: is: MIT Logical System for PS1:030 (ZZF Action Usage Date: is between: 04/01/2013 And 04/30/2013 Action: is Action Description: contains Report By: ● User ○ Role ○ Profile User ID: is User Group: is Only display actions that are not used: is April 2013 Mo Tu We Th Fr Sa Su 13 25 26 27 28 29 30 31 14 1 2 3 4 5 6 7 15 8 9 10 11 12 13 14 16 15 16 17 18 19 20 21 17 22 23 24 25 26 27 28 18 29 30 1 2 3 4 5

5	Click on the '-' at the end of the 'Action' row to remove the Action search criterion row; this criterion can be used for scenarios where analysis is required for a particular transaction only.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Analysis Criteria Saved Variants: System · is · MIT Logical System for PS1:030 (ZZF Action Usage Date · is between · 04/01/2013 And 04/30/2013 Action · is Action Description · contains Report By: ● User ○ Role ○ Profile User ID · is User Group · is Only display actions that are not used · is · □ Report Type: ● Actions Defined in Risks ○ All Access Risk ID · is Access Risk ID Description · contains Save Variant as: Close Delete Save Run in Foreground Run in Background Close
6	Click on the '-' at the end of the 'Action Description' row to remove the Action Description search criterion row.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Analysis Criteria Saved Variants: System · is · MIT Logical System for PS1:030 (ZZF Action Usage Date · is between · 04/01/2013 And 04/30/2013 Action Description · contains Report By: ● User ○ Role ○ Profile User ID · is User Group · is Only display actions that are not used · is · □ Report Type: ● Actions Defined in Risks ○ All Access Risk ID · is Access Risk ID Description · contains Save Variant as: Close Delete Save Run in Foreground Run in Background Close

7	In the ‘Report Type’ section, click on the dial button next to ‘All’; if necessary, this criterion can be used to limit report information to only transactions that are defined in risks within the GLOBAL rule set.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is User Group is Only display actions that are not used is □ Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground Run in Background Close
8A-1	Analyze by for a single user by user ID. In the ‘Report By’ section, click on the dial button next to ‘User’. Click on the ‘-‘ at the end of the ‘User Group’ row to remove the user group search criterion row.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is User Group is Only display actions that are not used is □ Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground Run in Background Close

8A-2	Click on the '-' at the end of the 'Only display actions that are not used' row to remove the option; if necessary, this criterion can be used to limit report information to only transactions that have not been executed (i.e. have 0 execution counts).	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is Only display actions that are not used is □ Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground Run in Background Close
8A-3	Add the user ID. In this case, 'FF_AR_01', an AR Cashiers FireFighter ID, was typed in. The search option can also be used to search for an ID. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is FF_FAR_01 Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground Run in Background Close

8A-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is FF_FAR_01 Report Type: ○ Actions Defined in Risks ● All Save Variant as: Close Delete Save Run in Foreground Run in Background Close

8A-5	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. System: The system in which the role is assigned to the user Action: SAP transaction Action Description: SAP transaction name User: User ID User Name: User name associated with user ID Execution Count: Number of times transaction was executed for a specified time period Last Executed On: Date of last execution of transaction	

Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

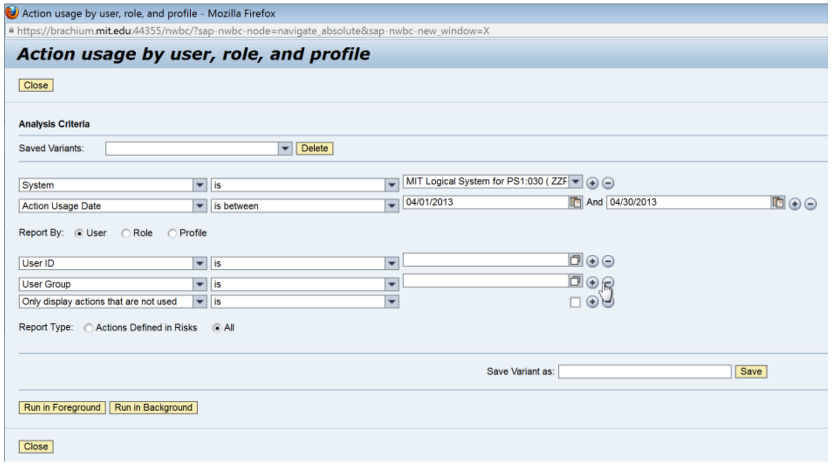
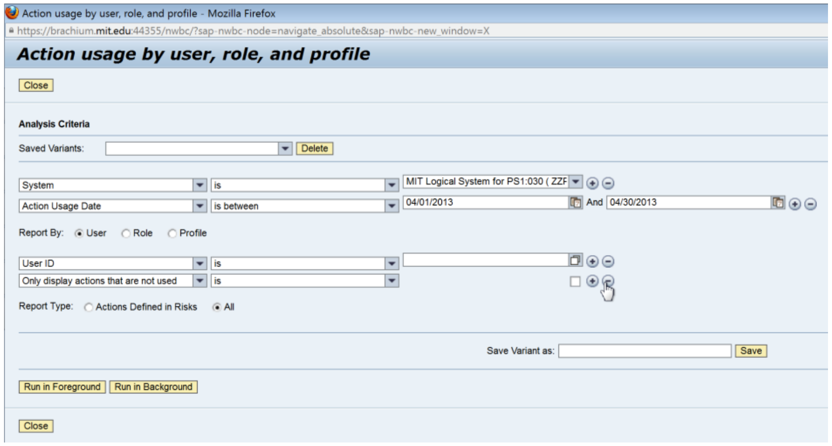
Analysis Criteria

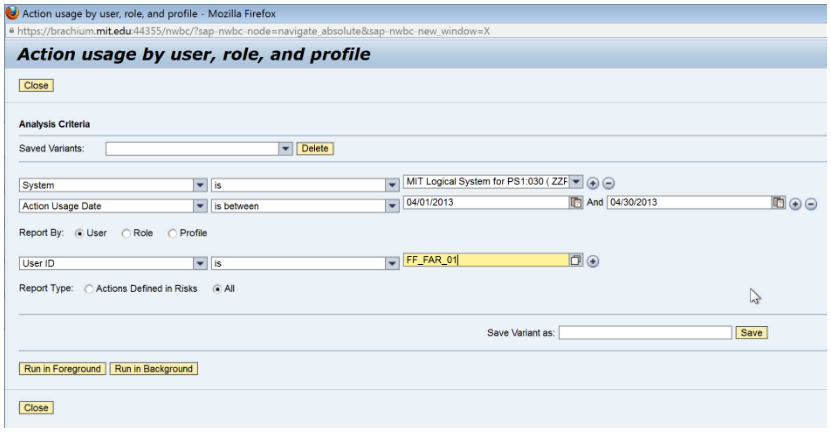
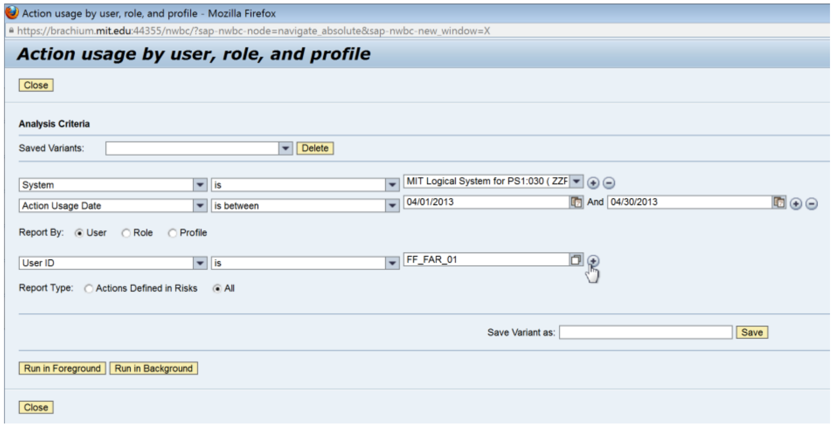
Analysis Results

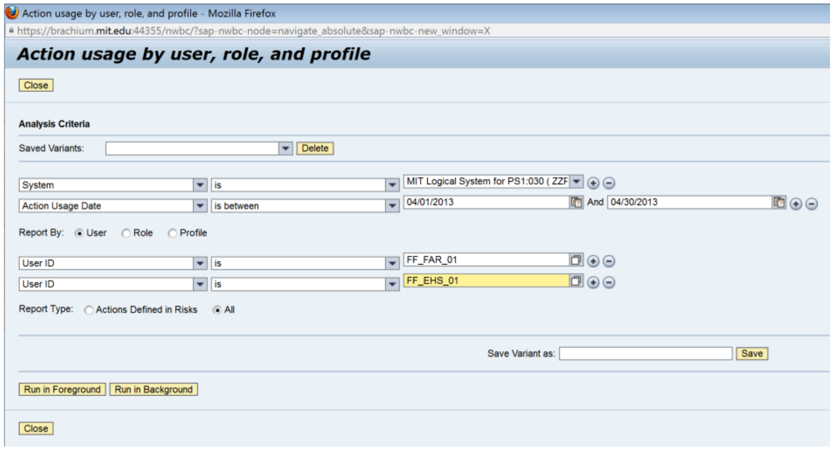
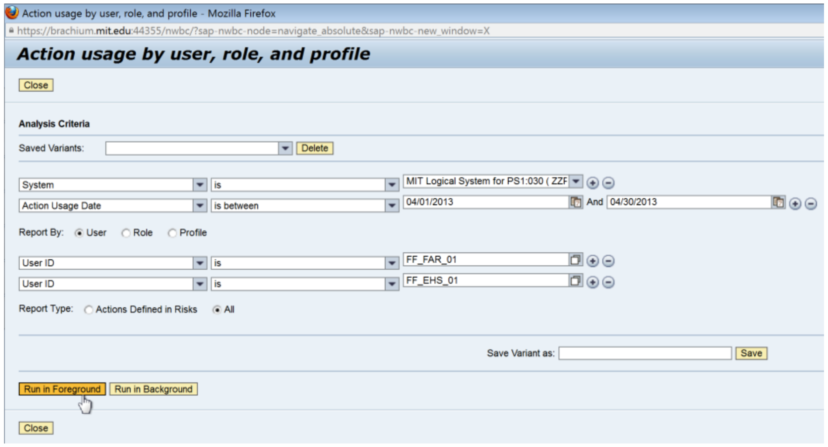
Result Set: Result Set1

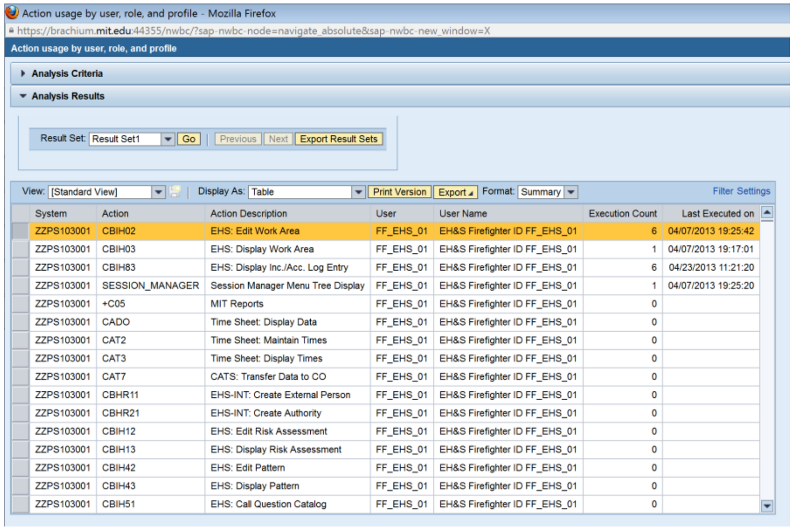
View: [Standard View] Display As: Table Format: Summary

System	Action	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	FB03	Display Document	FF_FAR_01	Firefighter id FF_FAR_01	1	04/26/2013 10:02:17
ZZPS103001	FBL3N	G/L Account Line Items	FF_FAR_01	Firefighter id FF_FAR_01	1	04/26/2013 10:02:42
ZZPS103001	SM37	Overview of job selection	FF_FAR_01	Firefighter id FF_FAR_01	2	04/26/2013 10:03:08
ZZPS103001	SU53	Evaluate Authorization Check	FF_FAR_01	Firefighter id FF_FAR_01	1	04/26/2013 10:02:33
ZZPS103001	+C03	ZISP: Call area menu ZISP	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	+C05	MIT Reports	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	6KEA	Profit Center: Display Changes	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AAVN	Recalculate base insurable value	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AB01	Create asset transactions	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AB02	Change asset document	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AB03	Display Asset Document	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AB08	Reverse Line Items	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAA	Unplanned depreciation	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAD	Asset Retire. frm Sale w/ Customer	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAD0	Derivation: Initial Screen	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAO	Asset Sale Without Customer	FF_FAR_01	Firefighter id FF_FAR_01	0	

8B-1	Analyze by for multiple users by user ID. In the ‘Report By’ section, click on the dial button next to ‘User’. Click on the ‘-‘ at the end of the ‘User Group’ row to remove the user group search criterion row.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is User Group is Only display actions that are not used is □ Report Type: ○ Actions Defined in Risks ● All Save Variant as: Close Delete Save Run in Foreground Run in Background Close
8B-2	Click on the ‘-‘ at the end of the ‘Only display actions that are not used’ row to remove the option; if necessary, this criterion can be used to limit report information to only transactions that have not been executed (i.e. have 0 execution counts).	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is Only display actions that are not used is □ Report Type: ○ Actions Defined in Risks ● All Save Variant as: Close Delete Save Run in Foreground Run in Background Close

8B-3	Add the user ID. In this case, 'FF_AR_01', an AR Cashiers FireFighter ID, was typed in. The search option can also be used to search for an ID. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is FF_FAR_01 Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground Run in Background Close
8B-4	Click on the '+' at the end of the 'User ID' row to add an additional user ID search criterion row for each ID. In this case, one additional row is added; thus, we can analyze for a total of two user IDs.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Close **Analysis Criteria** Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is FF_FAR_01 Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground Run in Background Close

8B-5	Add the second user ID. In this case, 'FF_EHS_01', an EHS FireFighter ID, was typed in. The search option can also be used to search for an ID. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is FF_FAR_01 User ID is FF_EHS_01 Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground Run in Background Close
8B-6	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID is FF_FAR_01 User ID is FF_EHS_01 Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground Run in Background Close

8B-7	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. System: The system in which the role is assigned to the user Action: SAP transaction Action Description: SAP transaction name User: User ID User Name: User name associated with user ID Execution Count: Number of times transaction was executed for a specified time period Last Executed On: Date of last execution of transaction	

Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

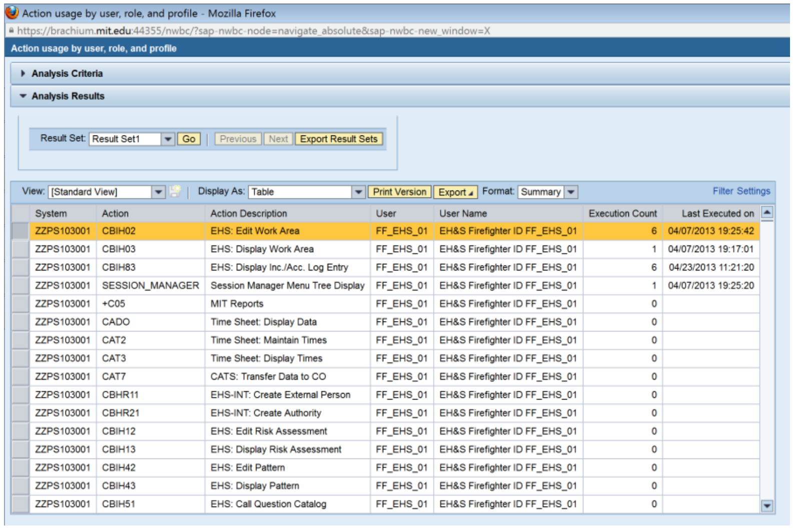
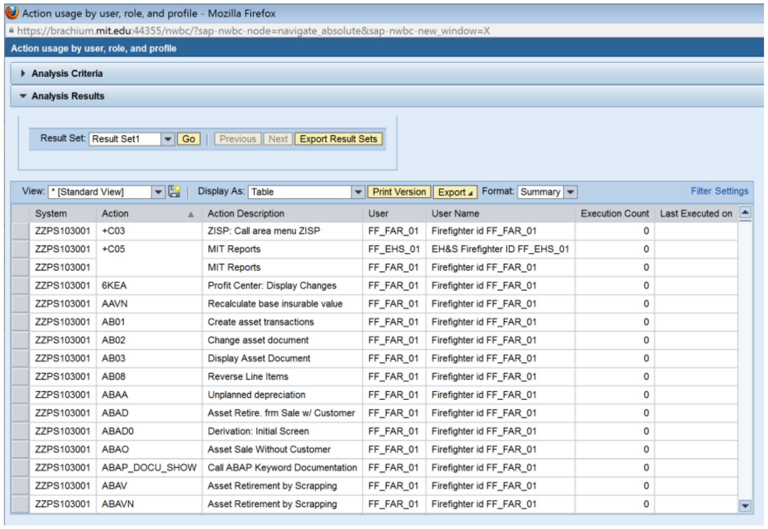
Result Set: Result Set1

View: [Standard View]

Display As: Table

Format: Summary

System	Action	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	CBIH02	EHS: Edit Work Area	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	6	04/07/2013 19:25:42
ZZPS103001	CBIH03	EHS: Display Work Area	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	1	04/07/2013 19:17:01
ZZPS103001	CBIH83	EHS: Display Inc./Acc. Log Entry	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	6	04/23/2013 11:21:20
ZZPS103001	SESSION_MANAGER	Session Manager Menu Tree Display	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	1	04/07/2013 19:25:20
ZZPS103001	+C05	MIT Reports	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CADO	Time Sheet: Display Data	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT2	Time Sheet: Maintain Times	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT3	Time Sheet: Display Times	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT7	CATS: Transfer Data to CO	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBHR11	EHS-INT: Create External Person	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBHR21	EHS-INT: Create Authority	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH12	EHS: Edit Risk Assessment	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH13	EHS: Display Risk Assessment	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH42	EHS: Edit Pattern	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH43	EHS: Display Pattern	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH51	EHS: Call Question Catalog	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	

8B-8	Sorting on transaction by clicking on the ‘Action’ column header will show the users grouped by transaction.	 

Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

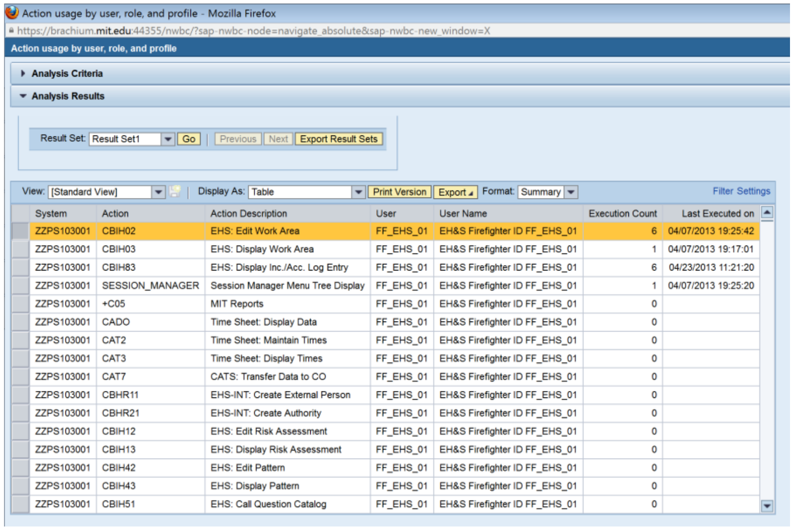
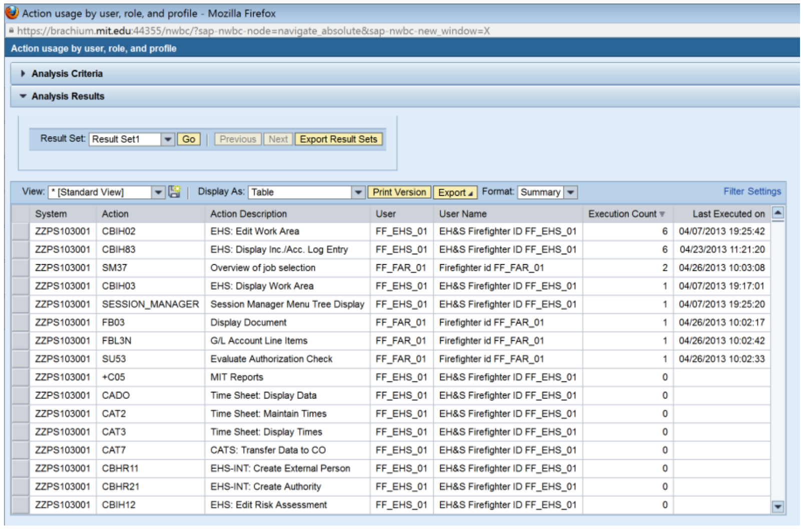
System	Action	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	CBIH02	EHS: Edit Work Area	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	6	04/07/2013 19:25:42
ZZPS103001	CBIH03	EHS: Display Work Area	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	1	04/07/2013 19:17:01
ZZPS103001	CBIH83	EHS: Display Inc./Acc. Log Entry	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	6	04/23/2013 11:21:20
ZZPS103001	SESSION_MANAGER	Session Manager Menu Tree Display	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	1	04/07/2013 19:25:20
ZZPS103001	+C05	MIT Reports	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CADO	Time Sheet: Display Data	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT2	Time Sheet: Maintain Times	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT3	Time Sheet: Display Times	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT7	CATS: Transfer Data to CO	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBHR11	EHS-INT: Create External Person	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBHR21	EHS-INT: Create Authority	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH12	EHS: Edit Risk Assessment	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH13	EHS: Display Risk Assessment	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH42	EHS: Edit Pattern	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH43	EHS: Display Pattern	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH51	EHS: Call Question Catalog	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	

Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

System	Action	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	+C03	ZISP: Call area menu ZISP	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	+C05	MIT Reports	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001		MIT Reports	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	6KEA	Profit Center: Display Changes	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AAVN	Recalculate base insurable value	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AB01	Create asset transactions	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AB02	Change asset document	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AB03	Display Asset Document	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	AB08	Reverse Line Items	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAA	Unplanned depreciation	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAD	Asset Retire. frm Sale w/ Customer	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAD0	Derivation: Initial Screen	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAO	Asset Sale Without Customer	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAP_DOCU_SHOW	Call ABAP Keyword Documentation	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAV	Asset Retirement by Scrapping	FF_FAR_01	Firefighter id FF_FAR_01	0	
ZZPS103001	ABAVN	Asset Retirement by Scrapping	FF_FAR_01	Firefighter id FF_FAR_01	0	

8B-9	Sorting on execution count by clicking on the 'Execution Count' column header twice will show the transactions sorted from highest execution count to lowest.	 

Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

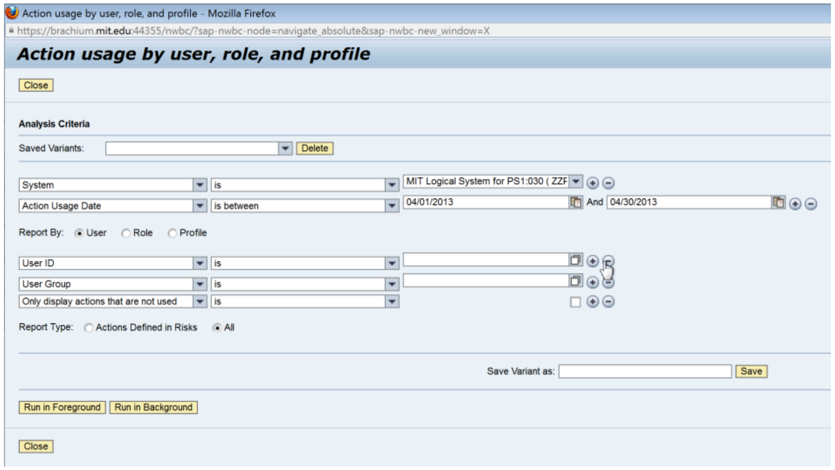
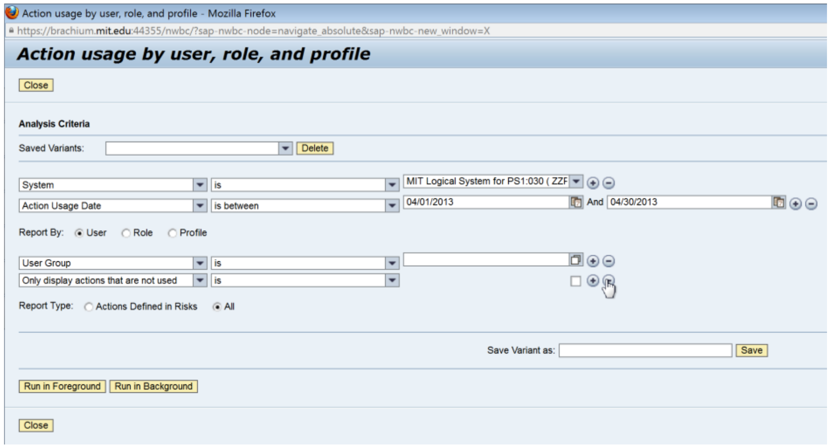
System	Action	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	CBIH02	EHS: Edit Work Area	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	6	04/07/2013 19:25:42
ZZPS103001	CBIH03	EHS: Display Work Area	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	1	04/07/2013 19:17:01
ZZPS103001	CBIH83	EHS: Display Inc./Acc. Log Entry	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	6	04/23/2013 11:21:20
ZZPS103001	SESSION_MANAGER	Session Manager Menu Tree Display	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	1	04/07/2013 19:25:20
ZZPS103001	+C05	MIT Reports	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CADO	Time Sheet: Display Data	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT2	Time Sheet: Maintain Times	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT3	Time Sheet: Display Times	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT7	CATS: Transfer Data to CO	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBHR11	EHS-INT: Create External Person	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBHR21	EHS-INT: Create Authority	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH12	EHS: Edit Risk Assessment	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH13	EHS: Display Risk Assessment	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH42	EHS: Edit Pattern	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH43	EHS: Display Pattern	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH51	EHS: Call Question Catalog	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	

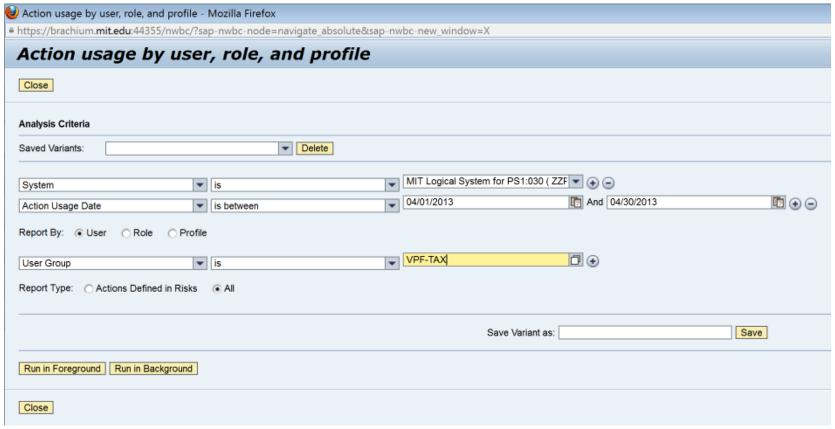
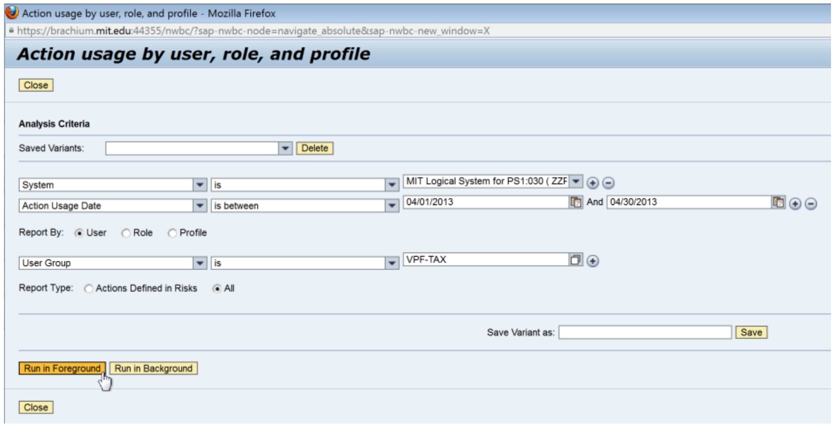
Action usage by user, role, and profile - Mozilla Firefox

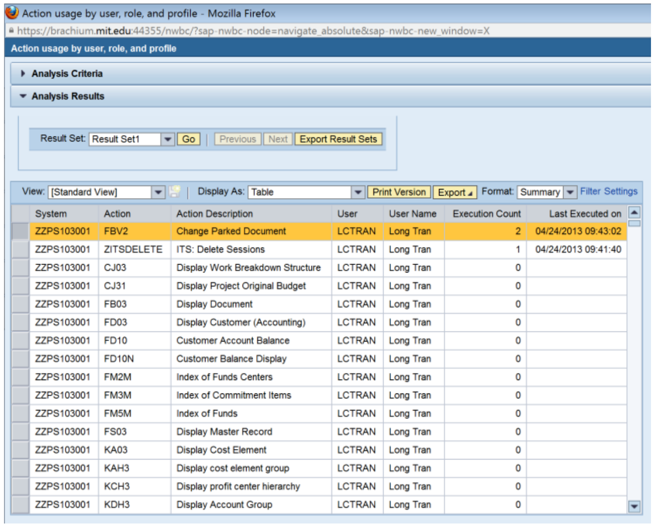
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

System	Action	Action Description	User	User Name	Execution Count ▾	Last Executed on
ZZPS103001	CBIH02	EHS: Edit Work Area	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	6	04/07/2013 19:25:42
ZZPS103001	CBIH83	EHS: Display Inc./Acc. Log Entry	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	6	04/23/2013 11:21:20
ZZPS103001	SM37	Overview of job selection	FF_FAR_01	Firefighter id FF_FAR_01	2	04/26/2013 10:03:08
ZZPS103001	CBIH03	EHS: Display Work Area	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	1	04/07/2013 19:17:01
ZZPS103001	SESSION_MANAGER	Session Manager Menu Tree Display	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	1	04/07/2013 19:25:20
ZZPS103001	FB03	Display Document	FF_FAR_01	Firefighter id FF_FAR_01	1	04/26/2013 10:02:17
ZZPS103001	FBL3N	G/L Account Line Items	FF_FAR_01	Firefighter id FF_FAR_01	1	04/26/2013 10:02:42
ZZPS103001	SU53	Evaluate Authorization Check	FF_FAR_01	Firefighter id FF_FAR_01	1	04/26/2013 10:02:33
ZZPS103001	+C05	MIT Reports	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CADO	Time Sheet: Display Data	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT2	Time Sheet: Maintain Times	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT3	Time Sheet: Display Times	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CAT7	CATS: Transfer Data to CO	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBHR11	EHS-INT: Create External Person	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBHR21	EHS-INT: Create Authority	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	
ZZPS103001	CBIH12	EHS: Edit Risk Assessment	FF_EHS_01	EH&S Firefighter ID FF_EHS_01	0	

8C-1	Analyze by for a single user group. In the 'Report By' section, click on the dial button next to 'User'. Click on the '-' at the end of the 'User ID' row to remove the user ID search criterion row. NOTE: The report can also be executed for multiple user groups by following steps similar to those outlined for multiple user IDs in steps 8B.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Close Analysis Criteria Saved Variants: Delete System · is · MIT Logical System for PS1:030 (ZZF Action Usage Date · is between · 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User ID · is User Group · is Only display actions that are not used · is · □ Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground · Run in Background Close
8C-2	Click on the '-' at the end of the 'Only display actions that are not used' row to remove the option; if necessary, this criterion can be used to limit report information to only transactions that have not been executed (i.e. have 0 execution counts).	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Close Analysis Criteria Saved Variants: Delete System · is · MIT Logical System for PS1:030 (ZZF Action Usage Date · is between · 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User Group · is Only display actions that are not used · is · □ Report Type: ○ Actions Defined in Risks ● All Save Variant as: Save Run in Foreground · Run in Background Close

8C-3	Add the user group name. In this case, 'VPF-TAX', the user group containing all user in VPF who are part of the Tax area, was typed in. The search option can also be used to search for user groups. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User Group is VPF-TAX Report Type: ○ Actions Defined in Risks ● All Save Variant as:
8C-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ● User ○ Role ○ Profile User Group is VPF-TAX Report Type: ○ Actions Defined in Risks ● All Save Variant as:

8C-5	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. System: The system in which the role is assigned to the user Action: SAP transaction Action Description: SAP transaction name User: User ID User Name: User name associated with user ID Execution Count: Number of times transaction was executed for a specified time period Last Executed On: Date of last execution of transaction	

Action usage by user, role, and profile - Mozilla Firefox

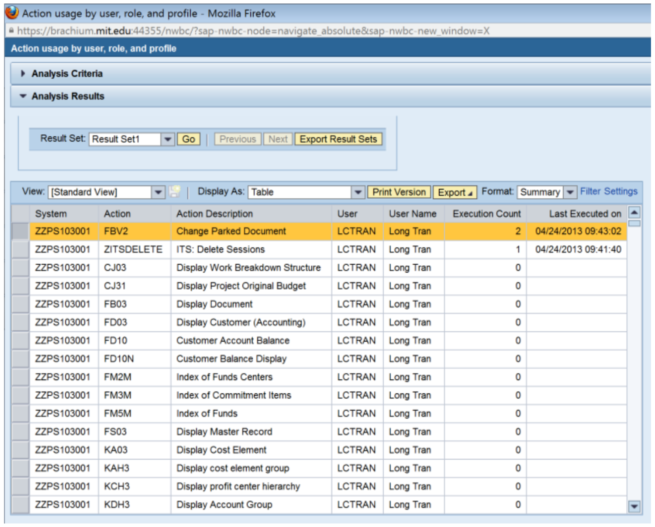
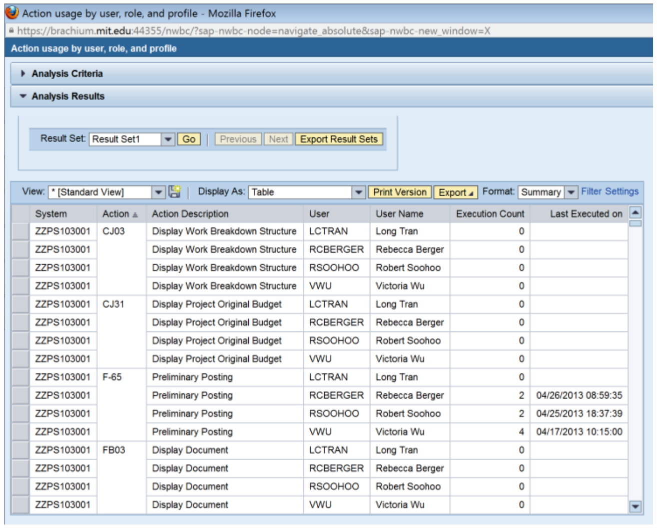
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

Result Set: Result Set1

View: [Standard View]   Display As: Table   Format: Summary

System	Action	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	FBV2	Change Parked Document	LCTRAN	Long Tran	2	04/24/2013 09:43:02
ZZPS103001	ZITSDELETE	ITS: Delete Sessions	LCTRAN	Long Tran	1	04/24/2013 09:41:40
ZZPS103001	CJ03	Display Work Breakdown Structure	LCTRAN	Long Tran	0	
ZZPS103001	CJ31	Display Project Original Budget	LCTRAN	Long Tran	0	
ZZPS103001	FB03	Display Document	LCTRAN	Long Tran	0	
ZZPS103001	FD03	Display Customer (Accounting)	LCTRAN	Long Tran	0	
ZZPS103001	FD10	Customer Account Balance	LCTRAN	Long Tran	0	
ZZPS103001	FD10N	Customer Balance Display	LCTRAN	Long Tran	0	
ZZPS103001	FM2M	Index of Funds Centers	LCTRAN	Long Tran	0	
ZZPS103001	FM3M	Index of Commitment Items	LCTRAN	Long Tran	0	
ZZPS103001	FM5M	Index of Funds	LCTRAN	Long Tran	0	
ZZPS103001	FS03	Display Master Record	LCTRAN	Long Tran	0	
ZZPS103001	KA03	Display Cost Element	LCTRAN	Long Tran	0	
ZZPS103001	KAH3	Display cost element group	LCTRAN	Long Tran	0	
ZZPS103001	KCH3	Display profit center hierarchy	LCTRAN	Long Tran	0	
ZZPS103001	KDH3	Display Account Group	LCTRAN	Long Tran	0	

8C-6	Sorting on transaction by clicking on the 'Action' column header will show the users grouped by transaction.	 

Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

Result Set: Result Set1

View: [Standard View]   Display As: Table

Format: Summary

System	Action	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	FBV2	Change Parked Document	LCTRAN	Long Tran	2	04/24/2013 09:43:02
ZZPS103001	ZITSDELETE	ITS: Delete Sessions	LCTRAN	Long Tran	1	04/24/2013 09:41:40
ZZPS103001	CJ03	Display Work Breakdown Structure	LCTRAN	Long Tran	0	
ZZPS103001	CJ31	Display Project Original Budget	LCTRAN	Long Tran	0	
ZZPS103001	FB03	Display Document	LCTRAN	Long Tran	0	
ZZPS103001	FD03	Display Customer (Accounting)	LCTRAN	Long Tran	0	
ZZPS103001	FD10	Customer Account Balance	LCTRAN	Long Tran	0	
ZZPS103001	FD10N	Customer Balance Display	LCTRAN	Long Tran	0	
ZZPS103001	FM2M	Index of Funds Centers	LCTRAN	Long Tran	0	
ZZPS103001	FM3M	Index of Commitment Items	LCTRAN	Long Tran	0	
ZZPS103001	FM5M	Index of Funds	LCTRAN	Long Tran	0	
ZZPS103001	FS03	Display Master Record	LCTRAN	Long Tran	0	
ZZPS103001	KA03	Display Cost Element	LCTRAN	Long Tran	0	
ZZPS103001	KAH3	Display cost element group	LCTRAN	Long Tran	0	
ZZPS103001	KCH3	Display profit center hierarchy	LCTRAN	Long Tran	0	
ZZPS103001	KDH3	Display Account Group	LCTRAN	Long Tran	0	

Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

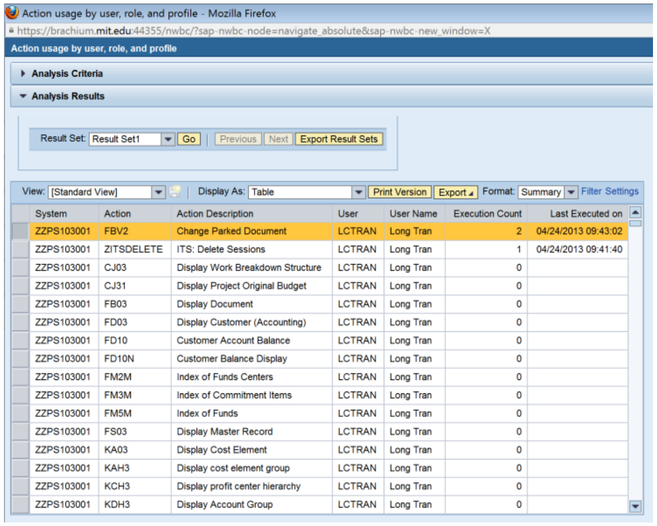
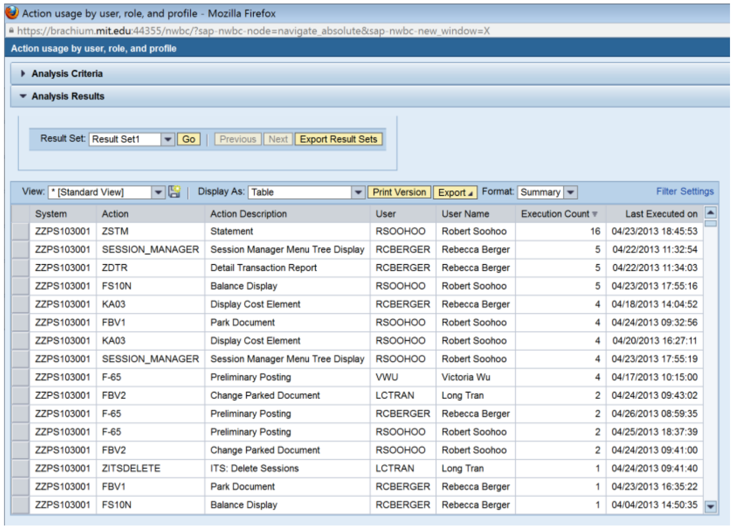
Action usage by user, role, and profile

Result Set: Result Set1

View: * [Standard View]   Display As: Table

Format: Summary

System	Action ▲	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	CJ03	Display Work Breakdown Structure	LCTRAN	Long Tran	0	
ZZPS103001		Display Work Breakdown Structure	RCBERGER	Rebecca Berger	0	
ZZPS103001		Display Work Breakdown Structure	RSOOHOO	Robert Soohoo	0	
ZZPS103001		Display Work Breakdown Structure	VWU	Victoria Wu	0	
ZZPS103001	CJ31	Display Project Original Budget	LCTRAN	Long Tran	0	
ZZPS103001		Display Project Original Budget	RCBERGER	Rebecca Berger	0	
ZZPS103001		Display Project Original Budget	RSOOHOO	Robert Soohoo	0	
ZZPS103001		Display Project Original Budget	VWU	Victoria Wu	0	
ZZPS103001	F-65	Preliminary Posting	LCTRAN	Long Tran	0	
ZZPS103001		Preliminary Posting	RCBERGER	Rebecca Berger	2	04/26/2013 08:59:35
ZZPS103001		Preliminary Posting	RSOOHOO	Robert Soohoo	2	04/25/2013 18:37:39
ZZPS103001		Preliminary Posting	VWU	Victoria Wu	4	04/17/2013 10:15:00
ZZPS103001	FB03	Display Document	LCTRAN	Long Tran	0	
ZZPS103001		Display Document	RCBERGER	Rebecca Berger	0	
ZZPS103001		Display Document	RSOOHOO	Robert Soohoo	0	
ZZPS103001		Display Document	VWU	Victoria Wu	0	

8C-7	Sorting on execution count by clicking on the 'Execution Count' column header twice will show the transactions sorted from highest execution count to lowest.	 

Action usage by user, role, and profile - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Action usage by user, role, and profile
Analysis Criteria
Analysis Results
Go
Previous
Next
Export Result Sets
Print Version
Export
Filter Settings

Result Set: Result Set1

View: [Standard View]   Display As: Table   Format: Summary

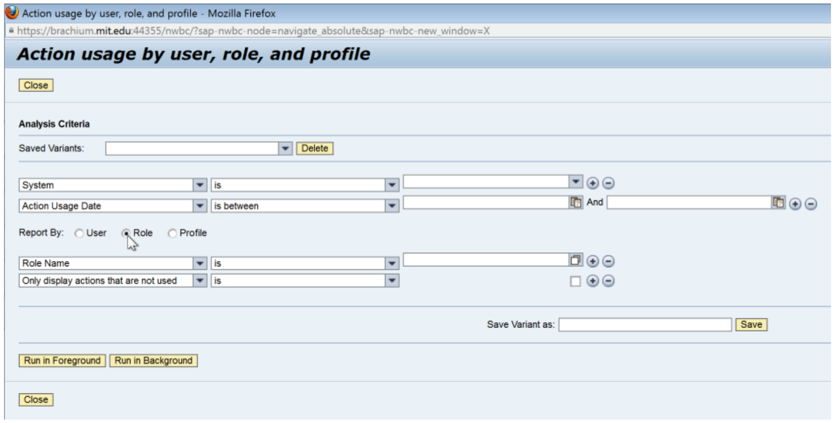
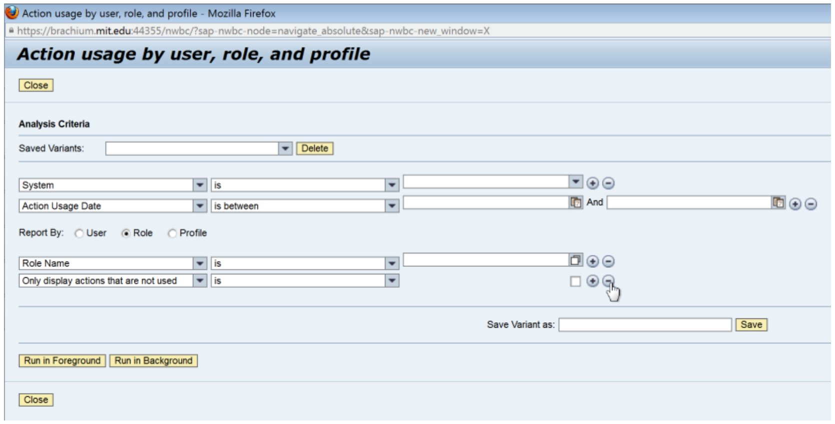
System	Action	Action Description	User	User Name	Execution Count	Last Executed on
ZZPS103001	FBV2	Change Parked Document	LCTRAN	Long Tran	2	04/24/2013 09:43:02
ZZPS103001	ZITSDELETE	ITS: Delete Sessions	LCTRAN	Long Tran	1	04/24/2013 09:41:40
ZZPS103001	CJ03	Display Work Breakdown Structure	LCTRAN	Long Tran	0	
ZZPS103001	CJ31	Display Project Original Budget	LCTRAN	Long Tran	0	
ZZPS103001	FB03	Display Document	LCTRAN	Long Tran	0	
ZZPS103001	FD03	Display Customer (Accounting)	LCTRAN	Long Tran	0	
ZZPS103001	FD10	Customer Account Balance	LCTRAN	Long Tran	0	
ZZPS103001	FD10N	Customer Balance Display	LCTRAN	Long Tran	0	
ZZPS103001	FM2M	Index of Funds Centers	LCTRAN	Long Tran	0	
ZZPS103001	FM3M	Index of Commitment Items	LCTRAN	Long Tran	0	
ZZPS103001	FM5M	Index of Funds	LCTRAN	Long Tran	0	
ZZPS103001	FS03	Display Master Record	LCTRAN	Long Tran	0	
ZZPS103001	KA03	Display Cost Element	LCTRAN	Long Tran	0	
ZZPS103001	KAH3	Display cost element group	LCTRAN	Long Tran	0	
ZZPS103001	KCH3	Display profit center hierarchy	LCTRAN	Long Tran	0	
ZZPS103001	KDH3	Display Account Group	LCTRAN	Long Tran	0	

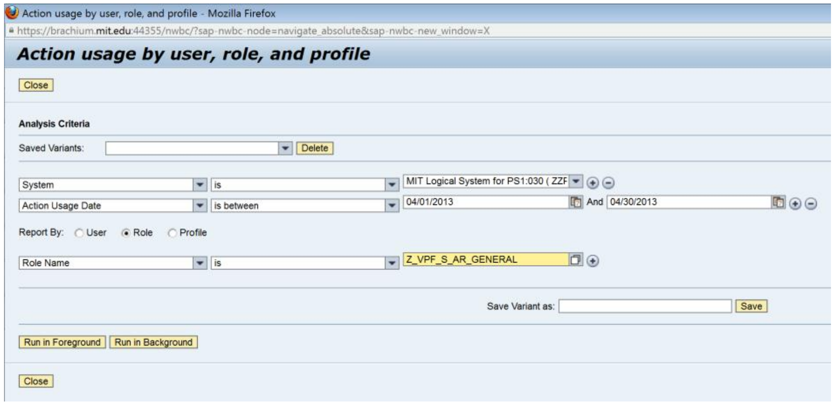
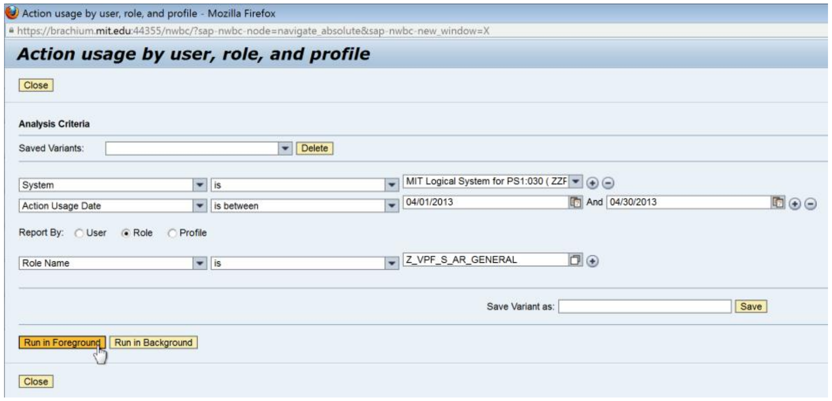
Action usage by user, role, and profile - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Action usage by user, role, and profile
Analysis Criteria
Analysis Results
Go
Previous
Next
Export Result Sets
Print Version
Export
Filter Settings

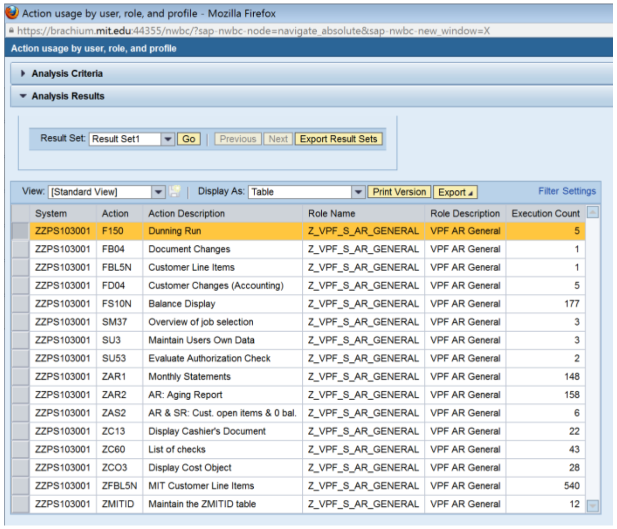
Result Set: Result Set1

View: * [Standard View]   Display As: Table   Format: Summary

System	Action	Action Description	User	User Name	Execution Count ▾	Last Executed on
ZZPS103001	ZSTM	Statement	RSOOHOO	Robert Soohoo	16	04/23/2013 18:45:53
ZZPS103001	SESSION_MANAGER	Session Manager Menu Tree Display	RCBERGER	Rebecca Berger	5	04/22/2013 11:32:54
ZZPS103001	ZDTR	Detail Transaction Report	RCBERGER	Rebecca Berger	5	04/22/2013 11:34:03
ZZPS103001	FS10N	Balance Display	RSOOHOO	Robert Soohoo	5	04/23/2013 17:55:16
ZZPS103001	KA03	Display Cost Element	RCBERGER	Rebecca Berger	4	04/18/2013 14:04:52
ZZPS103001	FBV1	Park Document	RSOOHOO	Robert Soohoo	4	04/24/2013 09:32:56
ZZPS103001	KA03	Display Cost Element	RSOOHOO	Robert Soohoo	4	04/20/2013 16:27:11
ZZPS103001	SESSION_MANAGER	Session Manager Menu Tree Display	RSOOHOO	Robert Soohoo	4	04/23/2013 17:55:19
ZZPS103001	F-65	Preliminary Posting	VWU	Victoria Wu	4	04/17/2013 10:15:00
ZZPS103001	FBV2	Change Parked Document	LCTRAN	Long Tran	2	04/24/2013 09:43:02
ZZPS103001	F-65	Preliminary Posting	RCBERGER	Rebecca Berger	2	04/26/2013 08:59:35
ZZPS103001	F-65	Preliminary Posting	RSOOHOO	Robert Soohoo	2	04/25/2013 18:37:39
ZZPS103001	FBV2	Change Parked Document	RSOOHOO	Robert Soohoo	2	04/24/2013 09:41:00
ZZPS103001	ZITSDELETE	ITS: Delete Sessions	LCTRAN	Long Tran	1	04/24/2013 09:41:40
ZZPS103001	FBV1	Park Document	RCBERGER	Rebecca Berger	1	04/23/2013 16:35:22
ZZPS103001	FS10N	Balance Display	RCBERGER	Rebecca Berger	1	04/04/2013 14:50:35

8D-1	Analyze by for a single role. In the ‘Report By’ section, click on the dial button next to ‘Role’. NOTE: The report can also be executed for multiple roles by following steps similar to those outlined for multiple user IDs in steps 8B.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System · is Action Usage Date · is between · And Report By: ○ User ● Role ○ Profile Role Name · is Only display actions that are not used · is · □ Save Variant as: Save Run in Foreground · Run in Background Close
8D-2	Click on the ‘-‘ at the end of the ‘Only display actions that are not used’ row to remove the option; if necessary, this criterion can be used to limit report information to only transactions that have not been executed (i.e. have 0 execution counts).	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System · is Action Usage Date · is between · And Report By: ○ User ● Role ○ Profile Role Name · is Only display actions that are not used · is · □ Save Variant as: Save Run in Foreground · Run in Background Close

8D-3	Add the role name. In this case, ‘Z_VPF_S_AR_GENERAL’ was typed in. The search option can also be used to search for a role. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ○ User ● Role ○ Profile Role Name is Z_VPF_S_AR_GENERAL Save Variant as:
8D-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Action usage by user, role, and profile** Analysis Criteria Saved Variants: System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ○ User ● Role ○ Profile Role Name is Z_VPF_S_AR_GENERAL Save Variant as:

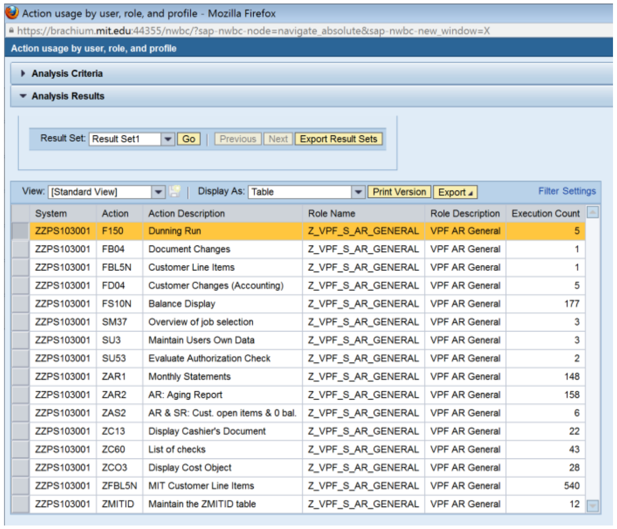
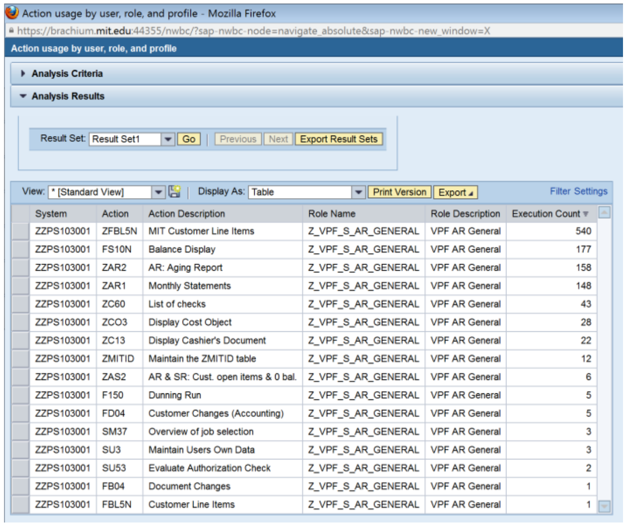
8D-5	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. System: The system in which the role is assigned to the user Action: SAP transaction Action Description: SAP transaction name Role Name: SAP role name Role Description: Business name for SAP role Execution Count: Number of times transaction was executed for a specified time period	

Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

System	Action	Action Description	Role Name	Role Description	Execution Count
ZZPS103001	F150	Dunning Run	Z_VPF_S_AR_GENERAL	VPF AR General	5
ZZPS103001	FB04	Document Changes	Z_VPF_S_AR_GENERAL	VPF AR General	1
ZZPS103001	FBL5N	Customer Line Items	Z_VPF_S_AR_GENERAL	VPF AR General	1
ZZPS103001	FD04	Customer Changes (Accounting)	Z_VPF_S_AR_GENERAL	VPF AR General	5
ZZPS103001	FS10N	Balance Display	Z_VPF_S_AR_GENERAL	VPF AR General	177
ZZPS103001	SM37	Overview of job selection	Z_VPF_S_AR_GENERAL	VPF AR General	3
ZZPS103001	SU3	Maintain Users Own Data	Z_VPF_S_AR_GENERAL	VPF AR General	3
ZZPS103001	SU53	Evaluate Authorization Check	Z_VPF_S_AR_GENERAL	VPF AR General	2
ZZPS103001	ZAR1	Monthly Statements	Z_VPF_S_AR_GENERAL	VPF AR General	148
ZZPS103001	ZAR2	AR: Aging Report	Z_VPF_S_AR_GENERAL	VPF AR General	158
ZZPS103001	ZAS2	AR & SR: Cust. open items & 0 bal.	Z_VPF_S_AR_GENERAL	VPF AR General	6
ZZPS103001	ZC13	Display Cashier's Document	Z_VPF_S_AR_GENERAL	VPF AR General	22
ZZPS103001	ZC60	List of checks	Z_VPF_S_AR_GENERAL	VPF AR General	43
ZZPS103001	ZCO3	Display Cost Object	Z_VPF_S_AR_GENERAL	VPF AR General	28
ZZPS103001	ZFBL5N	MIT Customer Line Items	Z_VPF_S_AR_GENERAL	VPF AR General	540
ZZPS103001	ZMITID	Maintain the ZMITID table	Z_VPF_S_AR_GENERAL	VPF AR General	12

8D-6	Sorting on execution count by clicking on the 'Execution Count' column header twice will show the transactions sorted from highest execution count to lowest.	 

Action usage by user, role, and profile - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Action usage by user, role, and profile

▸ Analysis Criteria
▾ Analysis Results

Result Set: Result Set1

Go | Previous | Next | Export Result Sets

View: [Standard View] | Display As: Table

Print Version | Export | Filter Settings

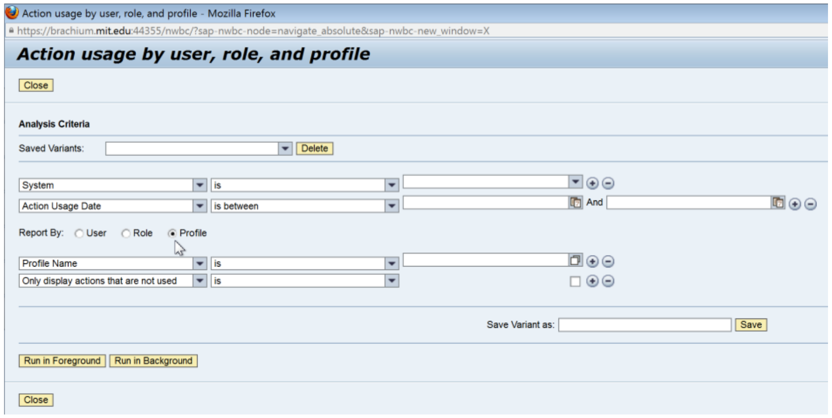
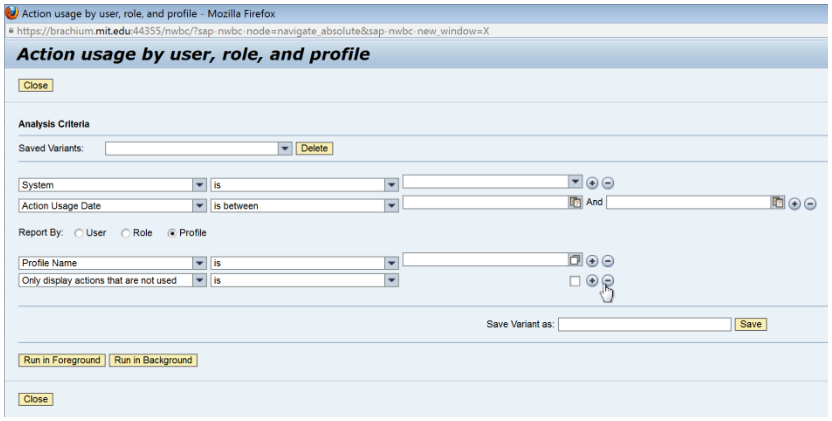
System	Action	Action Description	Role Name	Role Description	Execution Count
ZZPS103001	F150	Dunning Run	Z_VPF_S_AR_GENERAL	VPF AR General	5
ZZPS103001	FB04	Document Changes	Z_VPF_S_AR_GENERAL	VPF AR General	1
ZZPS103001	FBL5N	Customer Line Items	Z_VPF_S_AR_GENERAL	VPF AR General	1
ZZPS103001	FD04	Customer Changes (Accounting)	Z_VPF_S_AR_GENERAL	VPF AR General	5
ZZPS103001	FS10N	Balance Display	Z_VPF_S_AR_GENERAL	VPF AR General	177
ZZPS103001	SM37	Overview of job selection	Z_VPF_S_AR_GENERAL	VPF AR General	3
ZZPS103001	SU3	Maintain Users Own Data	Z_VPF_S_AR_GENERAL	VPF AR General	3
ZZPS103001	SU53	Evaluate Authorization Check	Z_VPF_S_AR_GENERAL	VPF AR General	2
ZZPS103001	ZAR1	Monthly Statements	Z_VPF_S_AR_GENERAL	VPF AR General	148
ZZPS103001	ZAR2	AR: Aging Report	Z_VPF_S_AR_GENERAL	VPF AR General	158
ZZPS103001	ZAS2	AR & SR: Cust. open items & 0 bal.	Z_VPF_S_AR_GENERAL	VPF AR General	6
ZZPS103001	ZC13	Display Cashier's Document	Z_VPF_S_AR_GENERAL	VPF AR General	22
ZZPS103001	ZC60	List of checks	Z_VPF_S_AR_GENERAL	VPF AR General	43
ZZPS103001	ZCO3	Display Cost Object	Z_VPF_S_AR_GENERAL	VPF AR General	28
ZZPS103001	ZFBL5N	MIT Customer Line Items	Z_VPF_S_AR_GENERAL	VPF AR General	540
ZZPS103001	ZMITID	Maintain the ZMITID table	Z_VPF_S_AR_GENERAL	VPF AR General	12

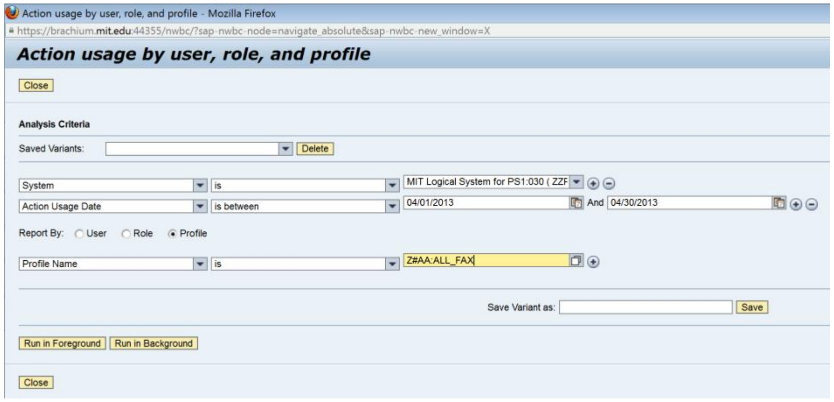
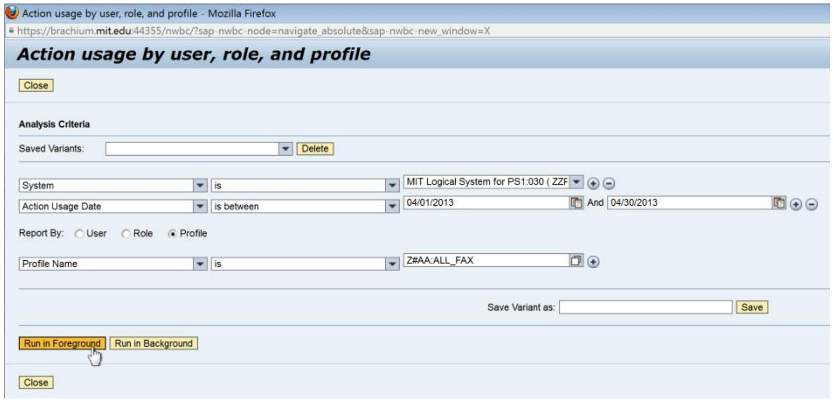
Action usage by user, role, and profile - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Action usage by user, role, and profile

Result Set: Result Set1

View: * [Standard View] | Display As: Table

System	Action	Action Description	Role Name	Role Description	Execution Count ▾
ZZPS103001	ZFBL5N	MIT Customer Line Items	Z_VPF_S_AR_GENERAL	VPF AR General	540
ZZPS103001	FS10N	Balance Display	Z_VPF_S_AR_GENERAL	VPF AR General	177
ZZPS103001	ZAR2	AR: Aging Report	Z_VPF_S_AR_GENERAL	VPF AR General	158
ZZPS103001	ZAR1	Monthly Statements	Z_VPF_S_AR_GENERAL	VPF AR General	148
ZZPS103001	ZC60	List of checks	Z_VPF_S_AR_GENERAL	VPF AR General	43
ZZPS103001	ZCO3	Display Cost Object	Z_VPF_S_AR_GENERAL	VPF AR General	28
ZZPS103001	ZC13	Display Cashier's Document	Z_VPF_S_AR_GENERAL	VPF AR General	22
ZZPS103001	ZMITID	Maintain the ZMITID table	Z_VPF_S_AR_GENERAL	VPF AR General	12
ZZPS103001	ZAS2	AR & SR: Cust. open items & 0 bal.	Z_VPF_S_AR_GENERAL	VPF AR General	6
ZZPS103001	F150	Dunning Run	Z_VPF_S_AR_GENERAL	VPF AR General	5
ZZPS103001	FD04	Customer Changes (Accounting)	Z_VPF_S_AR_GENERAL	VPF AR General	5
ZZPS103001	SM37	Overview of job selection	Z_VPF_S_AR_GENERAL	VPF AR General	3
ZZPS103001	SU3	Maintain Users Own Data	Z_VPF_S_AR_GENERAL	VPF AR General	3
ZZPS103001	SU53	Evaluate Authorization Check	Z_VPF_S_AR_GENERAL	VPF AR General	2
ZZPS103001	FB04	Document Changes	Z_VPF_S_AR_GENERAL	VPF AR General	1
ZZPS103001	FBL5N	Customer Line Items	Z_VPF_S_AR_GENERAL	VPF AR General	1

8E-1	Analyze by for a single profile. In the 'Report By' section, click on the dial button next to 'Role'. NOTE: The report can also be executed for multiple profiles by following steps similar to those outlined for multiple user IDs in steps 8B.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Analysis Criteria Saved Variants: System | is Action Usage Date | is between | And Report By: ○ User ○ Role ● Profile Profile Name | is Only display actions that are not used | is | □ Save Variant as: Close Delete Save Run in Foreground Run in Background Close
8E-2	Click on the '-' at the end of the 'Only display actions that are not used' row to remove the option; if necessary, this criterion can be used to limit report information to only transactions that have not been executed (i.e. have 0 execution counts).	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Analysis Criteria Saved Variants: System | is Action Usage Date | is between | And Report By: ○ User ○ Role ● Profile Profile Name | is Only display actions that are not used | is | □ Save Variant as: Close Delete Save Run in Foreground Run in Background Close

8E-3	Add the profile name. In this case, 'Z#AA:ALL_FAX' was typed in. The search option can also be used to search for a role. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ○ User ○ Role ● Profile Profile Name is Z#AA:ALL_FAX Save Variant as: Save Run in Foreground Run in Background Close
8E-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Action usage by user, role, and profile - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Action usage by user, role, and profile Close Analysis Criteria Saved Variants: Delete System is MIT Logical System for PS1:030 (ZZF Action Usage Date is between 04/01/2013 And 04/30/2013 Report By: ○ User ○ Role ● Profile Profile Name is Z#AA:ALL_FAX Save Variant as: Save Run in Foreground Run in Background Close

<table>
<tr>
<td>8E-5</td>
<td>
Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

System: The system in which the role is assigned to the user

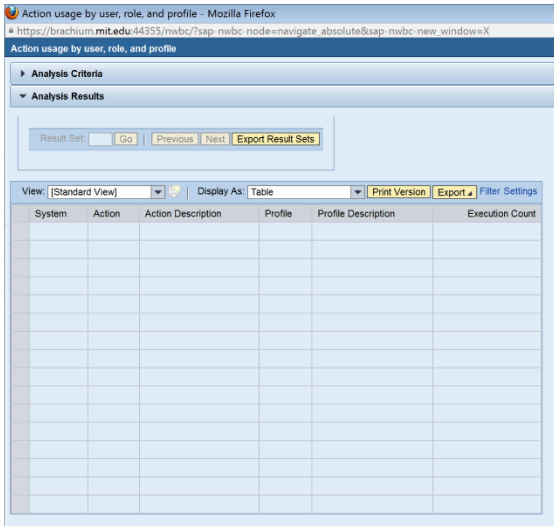
Action: SAP transaction

Action Description: SAP transaction name

Profile: SAP profile name

Profile Description: Business name for SAP profile

Execution Count: Number of times transaction was executed for a specified time period

NOTE: This report is not as efficient for profiles and may need to be executed as a background job for any profile analysis.
</td>
<td>


Action usage by user, role, and profile - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Action usage by user, role, and profile

</td>
</tr>
</table>

Job Aid 11 Mitigation Control Report

USE

This report can be used to find information on the mitigating controls defined in GRC.

INFORMATION

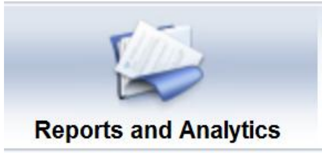
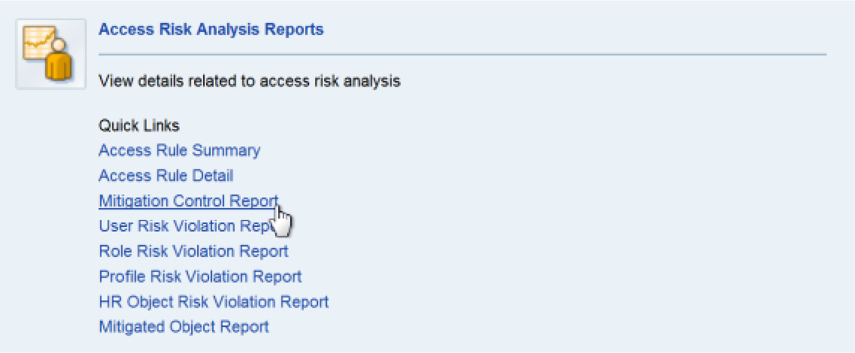
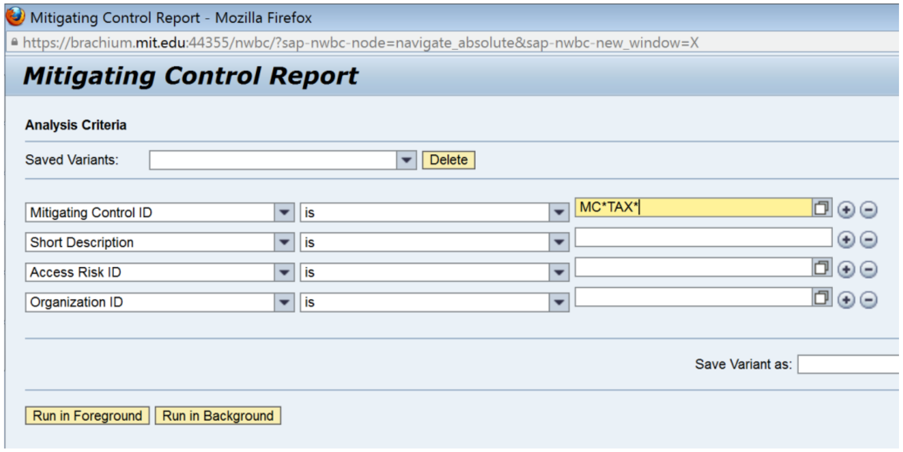
Approvers, monitors and risks mitigated by a mitigating control as defined in the system.

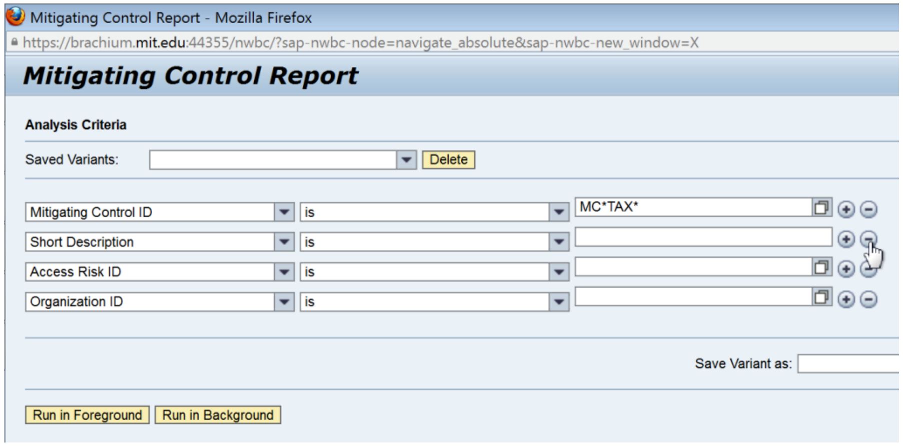
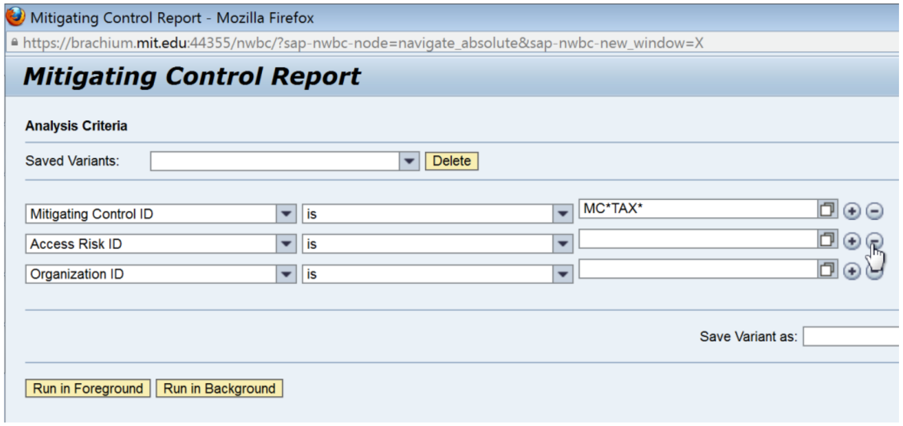
RELATED PROCESSES

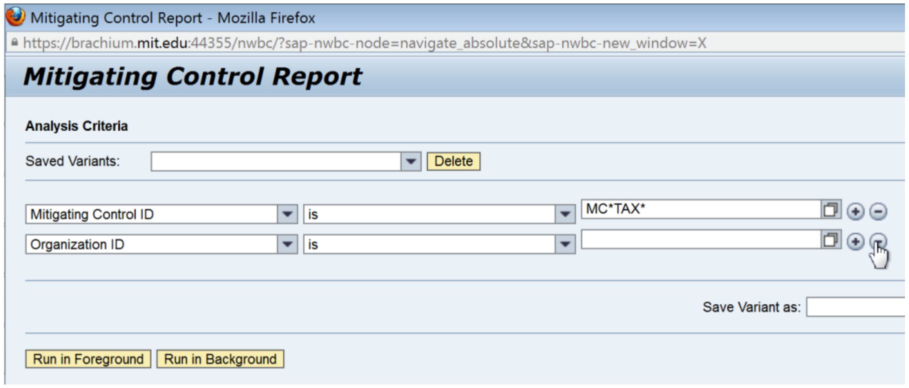
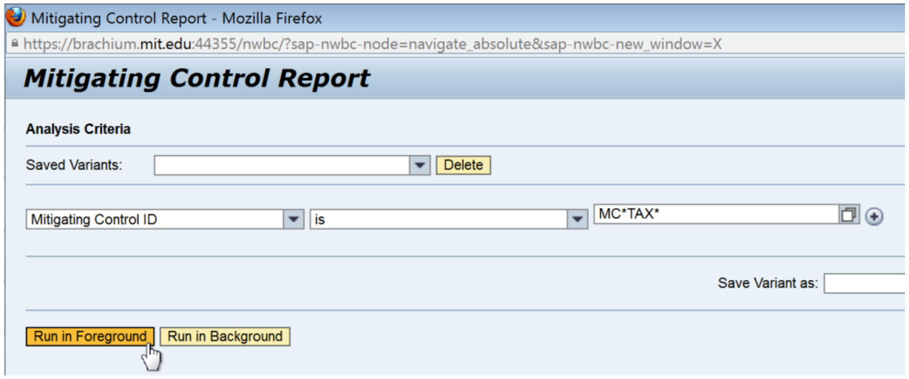
- Process 2: Mitigation Analysis

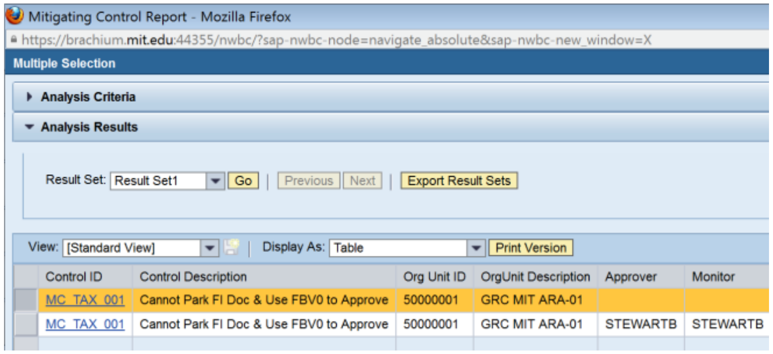
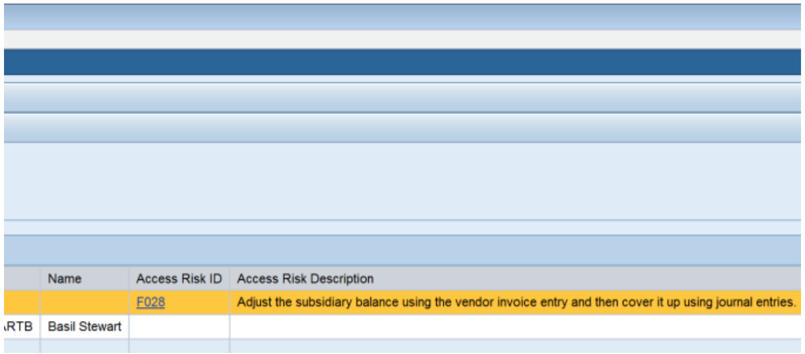
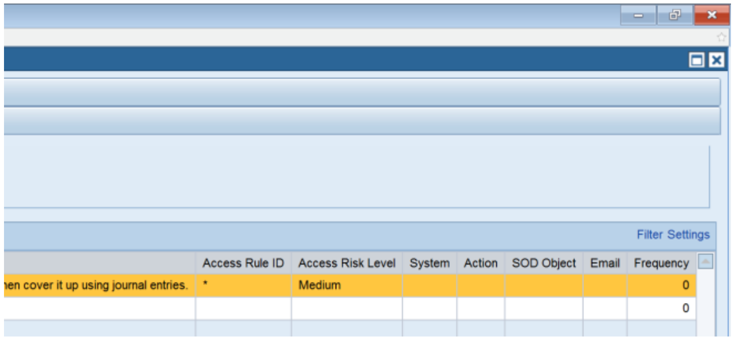
SPECIFIC SCENARIOS

- N/A

Step	Description	Screenshot
1	Navigate to the ‘Reports and Analytics’ tab.	 Reports and Analytics
2	Click on the ‘Mitigation Control Report’ report located in the ‘Access Risk Analysis Reports’ section.	 **Access Risk Analysis Reports** View details related to access risk analysis Quick Links Access Rule Summary Access Rule Detail Mitigation Control Report User Risk Violation Rep Role Risk Violation Report Profile Risk Violation Report HR Object Risk Violation Report Mitigated Object Report
3	Add the Mitigating Control ID. In this case, ‘MC*TAX*’was typed in to include all Mitigating Controls for the VPF-TAX area. The search option can also be used to search for a specific ID. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Mitigating Control Report - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X ***Mitigating Control Report*** **Analysis Criteria** Saved Variants: [Delete] Mitigating Control ID · is · MC*TAX* Short Description · is · Access Risk ID · is · Organization ID · is · Save Variant as: [Run in Foreground] [Run in Background]

4	Click on the '-' at the end of the 'Short Description' row to remove the row for that search criterion; this criterion can be used with wild cards (*) for scenarios where information is only required for Mitigating Controls relating to some specific criteria noted in the short description.	 Mitigating Control Report - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Mitigating Control Report Analysis Criteria Saved Variants: Delete Mitigating Control ID is MC*TAX* Short Description is Access Risk ID is Organization ID is Save Variant as: Run in Foreground Run in Background
5	Click on the '-' at the end of the 'Access Risk ID' row to remove the row for the Access Risk search criterion; this criterion can be used for scenarios where information is only required for Mitigating Controls relating to specific Access Risks.	 Mitigating Control Report - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Mitigating Control Report Analysis Criteria Saved Variants: Delete Mitigating Control ID is MC*TAX* Access Risk ID is Organization ID is Save Variant as: Run in Foreground Run in Background

6	Click on the '-' at the end of the 'Organization ID' row to remove the row for the Organization search criterion; this criterion can be used for scenarios where information is only required for Mitigating Controls mapped to a certain Organization in the Organizational Structure defined in GRC. At this initial phase, this criterion will likely not be of use to MIT.	 Mitigating Control Report - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Mitigating Control Report Analysis Criteria Saved Variants: Delete Mitigating Control ID is MC*TAX* Organization ID is Save Variant as: Run in Foreground Run in Background
7	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Mitigating Control Report - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Mitigating Control Report Analysis Criteria Saved Variants: Delete Mitigating Control ID is MC*TAX* Save Variant as: Run in Foreground Run in Background

8	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. Control ID: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk Control Description: Business description of the Mitigating Control Org Unit ID: Numerical code of Org Unit defined in GRC OrgUnit Description: Business name of Org Unit Approver: The user ID of the Approver responsible for the Mitigating Control Monitor: The user ID of the Monitor responsible for the Mitigating Control Name: Name tied to the user ID of the Monitor Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist Access Risk Description: Business description of the Access Risk System: The system in which the role is assigned to the user Access Risk Level: The risk level defined for each Access Risk in the standard rule set	  

Mitigating Control Report - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Multiple Selection

Analysis Criteria

Analysis Results

Result Set: Result Set1 | Go | Previous | Next | Export Result Sets

View: [Standard View] | Display As: Table | Print Version

Control ID	Control Description	Org Unit ID	OrgUnit Description	Approver	Monitor
MC_TAX_001	Cannot Park FI Doc & Use FBV0 to Approve	50000001	GRC MIT ARA-01		
MC_TAX_001	Cannot Park FI Doc & Use FBV0 to Approve	50000001	GRC MIT ARA-01	STEWARTB	STEWARTB

	Name	Access Risk ID	Access Risk Description
		F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.
RTB	Basil Stewart		

Filter Settings

	Access Rule ID	Access Risk Level	System	Action	SOD Object	Email	Frequency
en cover it up using journal entries.	*	Medium					0
							0

Job Aid 12 User Level

USE

This report can be used analyze for risk violations at the user level. The report can also be used to find the mitigating controls assigned to users, as well as any invalid mitigating control assignments.

INFORMATION

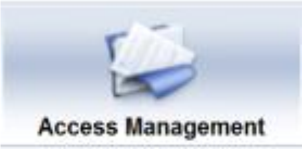
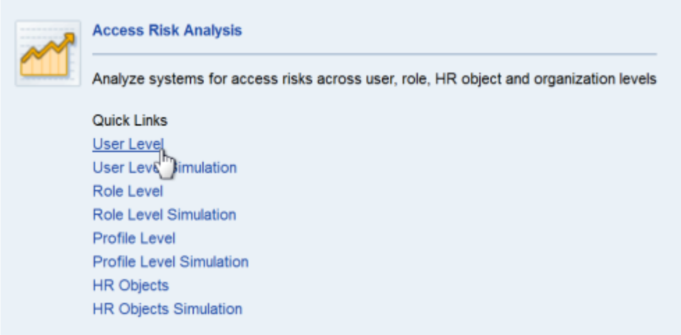
SODs, critical actions or permissions and critical roles or profiles.

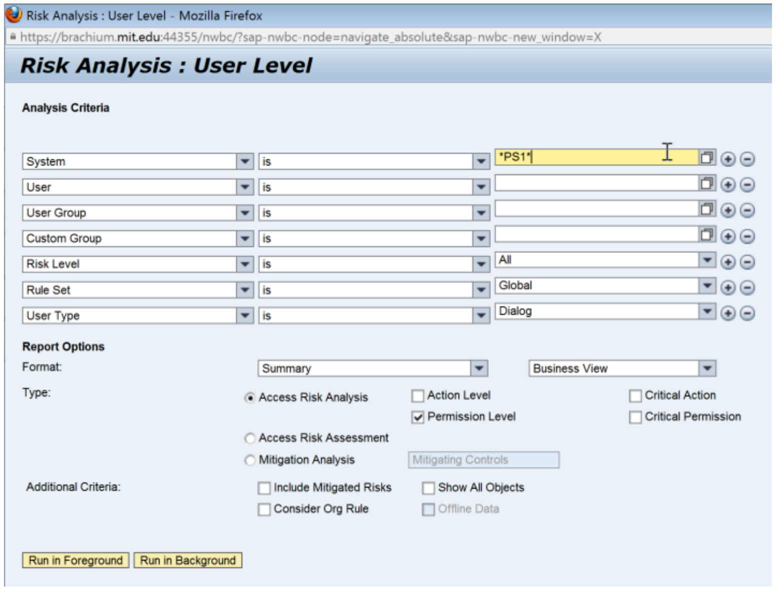
RELATED PROCESSES

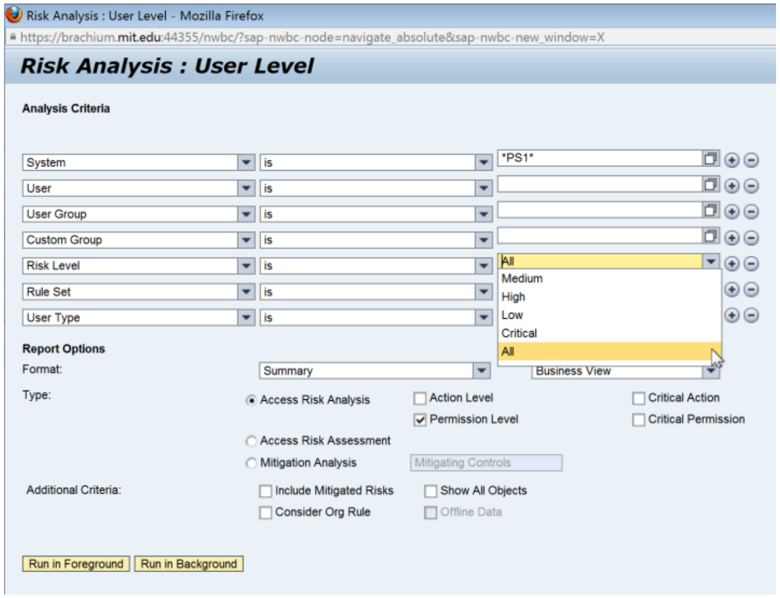
- Process 1: New or Amended Roles
- Process 2: Mitigation Analysis

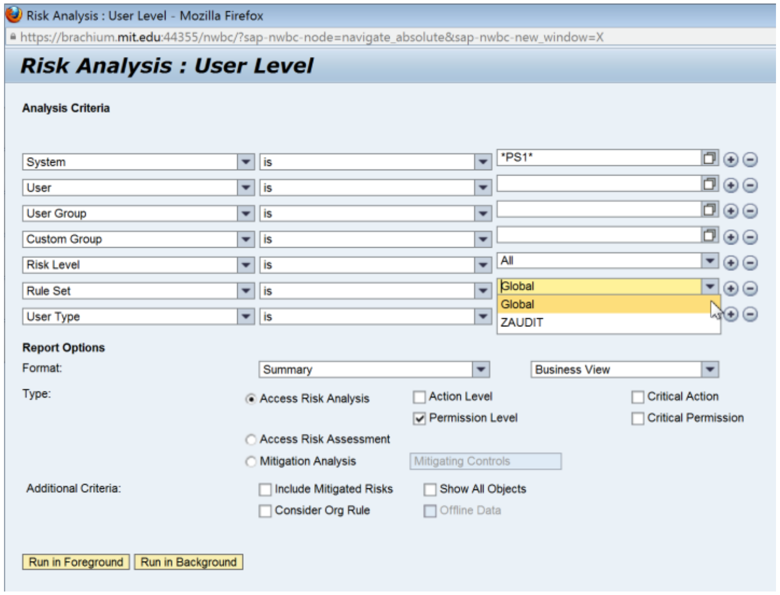
SPECIFIC SCENARIOS

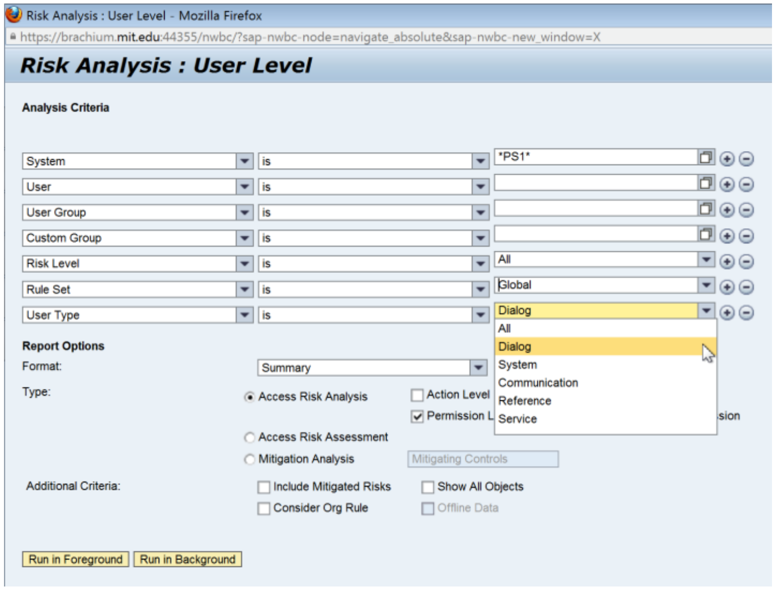
- Step 10A: Analyze for SODs based on User ID.
- Step 10B: Analyze for SODs based on User Group.
- Step 10C: Analyze for SODs based on Custom Group.
- Step 10D: Carry out an Access Risk Assessment by User ID.
- Step 10E: Carry out an analysis of Mitigating Controls by User ID.

Step	Description	Screenshot
1	Navigate to the 'Access Management' tab.	
2	Click on the 'User Level' report located in the 'Access Risk Analysis' section.	Access Risk Analysis Analyze systems for access risks across user, role, HR object and organization levels Quick Links User Level User Level Simulation Role Level Role Level Simulation Profile Level Profile Level Simulation HR Objects HR Objects Simulation

3	In the 'Analysis Criteria' section, select the System for which information is required. Since the desired selection is PS1 (Production), '*PS1*' was typed in as the system. The search option can also be used to search for the correct system. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** Analysis Criteria System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

4	In the 'Analysis Criteria' section, select the 'Risk Level' drop down and select the risk level for which information is required. In this case, 'All' was selected so that the report evaluates for all risk levels.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is User Type is Report Options Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Medium High Low Critical All Run in Foreground Run in Background

5	In the ‘Analysis Criteria’ section, select the ‘Rule Set’ drop down and select the Rule Set against which the report should be executed. In this case, ‘Global’, the MIT Rule Set, was selected. Unless advised otherwise, the selection should always be ‘Global’ for this report.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global Global ZAUDIT User Type is Report Options Format: Summary Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

6	In the 'Analysis Criteria' section, select the User Type' drop down and select the type of users for which information is required. In this case, 'Dialog' was selected so that the report only evaluates for dialog users.	

Risk Analysis : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Risk Analysis : User Level

Analysis Criteria

System	is	*PS1*
User	is	
User Group	is	
Custom Group	is	
Risk Level	is	All
Rule Set	is	Global
User Type	is	Dialog

Report Options

Format: Summary

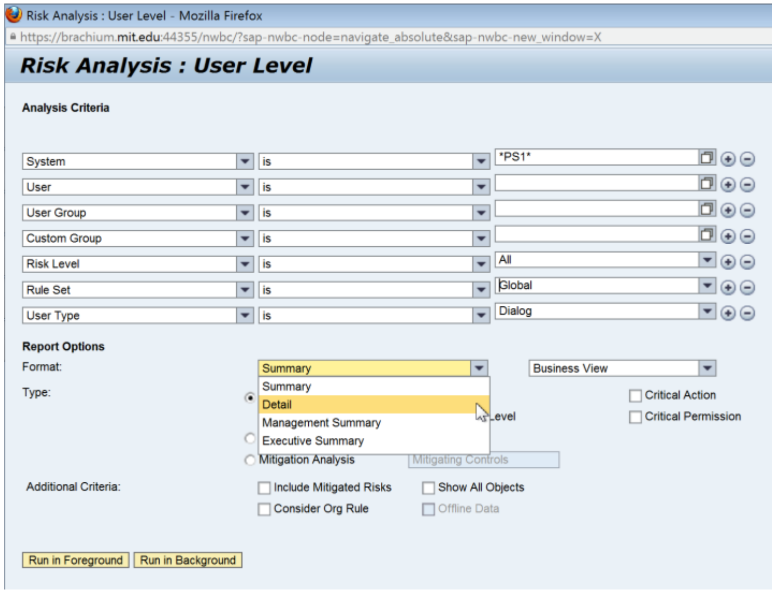
Type: ● Access Risk Analysis ☐ Action Level ☑ Permission L...sion

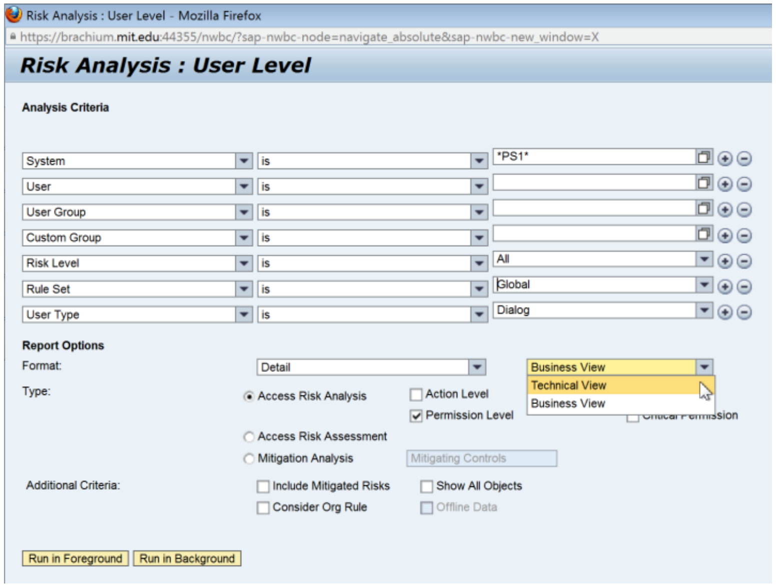
○ Access Risk Assessment

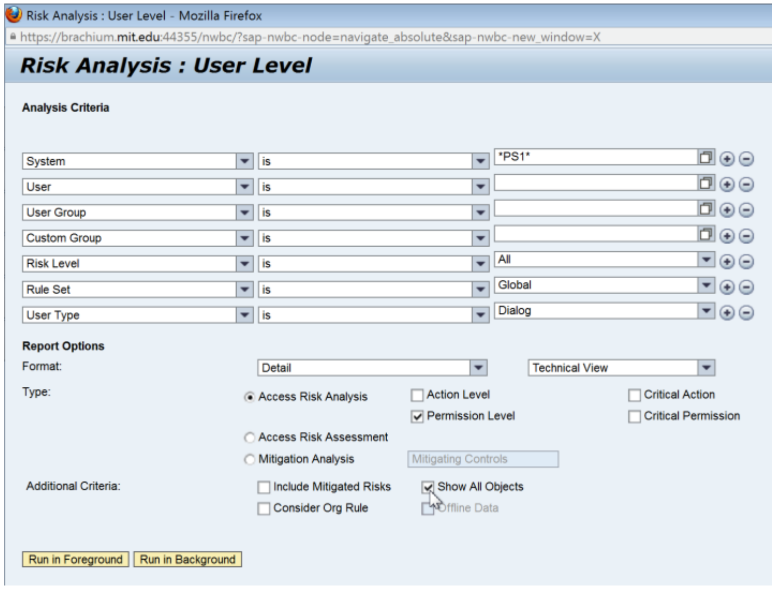
○ Mitigation Analysis   Mitigating Controls

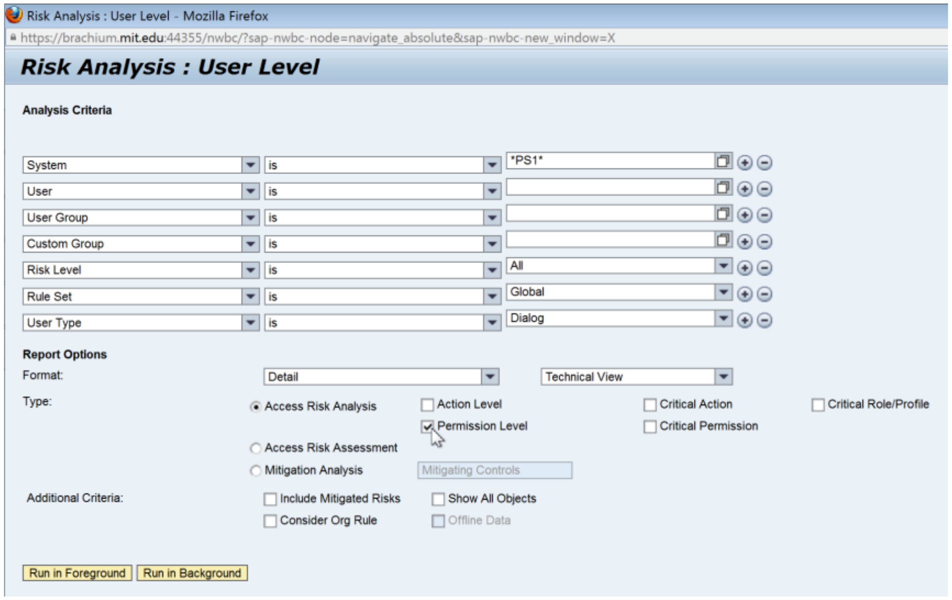
Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects

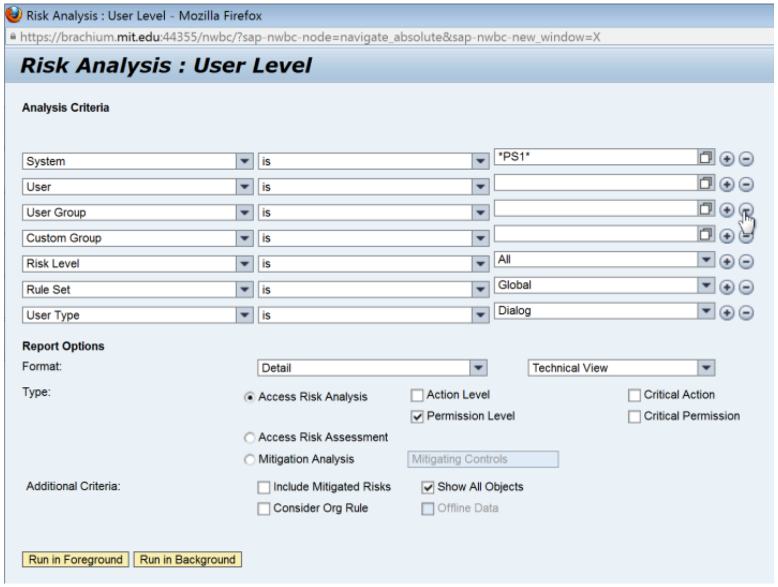
☐ Consider Org Rule ☐ Offline Data

7	In the 'Report Options' section, select the first drop down for 'Format' and select the level of detail at which information is required. In this case, 'Detail' was selected so that the report will show information about why Risks exists.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Summary Business View Type: ● Summary / Detail / Management Summary / Executive Summary Level ○ ○ Mitigation Analysis Mitigating Controls □ Critical Action □ Critical Permission Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule □ Offline Data

8	In the ‘Report Options’ section, select the second drop down for ‘Format’ and select the type of information that is required. In this case, ‘Technical View’ was selected so that the report will show technical information about why Risks exists.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Business View Technical View Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

9	In the 'Report Options' section, check 'Show All Objects' under 'Additional Criteria'. This will ensure that Users with no violations are explicitly listed as such (i.e. 'No Violations' will be listed as a line item for such users' IDs).	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data

10A-1	Analyze for SODs based on user ID. In the 'Report Options' section, select the first dial button for 'Access Risk Analysis'. Next, select the type of analysis that is required. The options available are: Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level) Permission Level: SODs at the authorization level Critical Action: Critical transactions that limited/no users should have Critical Permission: Critical authorizations that limited/no users should have Critical Role/Profile: Critical Roles/Profiles that limited/no users should have In this case, 'Permission Level' was selected so that the report will show SODs that exist at the Permission Level.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ☐ Critical Role/Profile ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

10A-2	In the 'Analysis Criteria' section, click on the '-' at the end of the 'User Group' row to remove the row for that search criterion; this criterion is not needed for this scenario.	

Risk Analysis : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Risk Analysis : User Level

Analysis Criteria

System	is	*PS1*
User	is	
User Group	is	
Custom Group	is	
Risk Level	is	All
Rule Set	is	Global
User Type	is	Dialog

Report Options

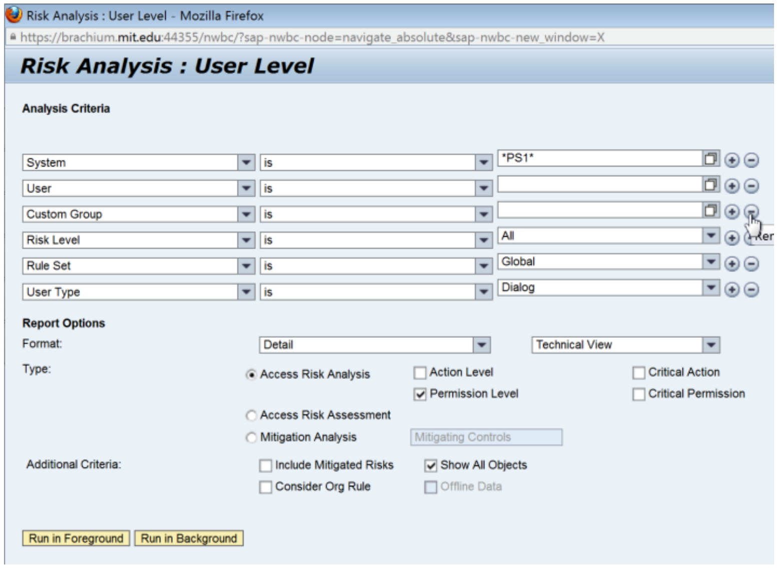
Format: Detail | Technical View

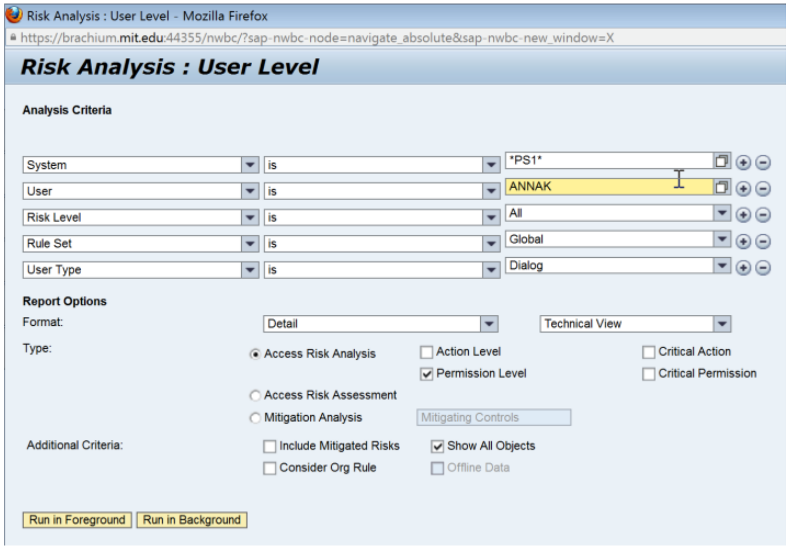
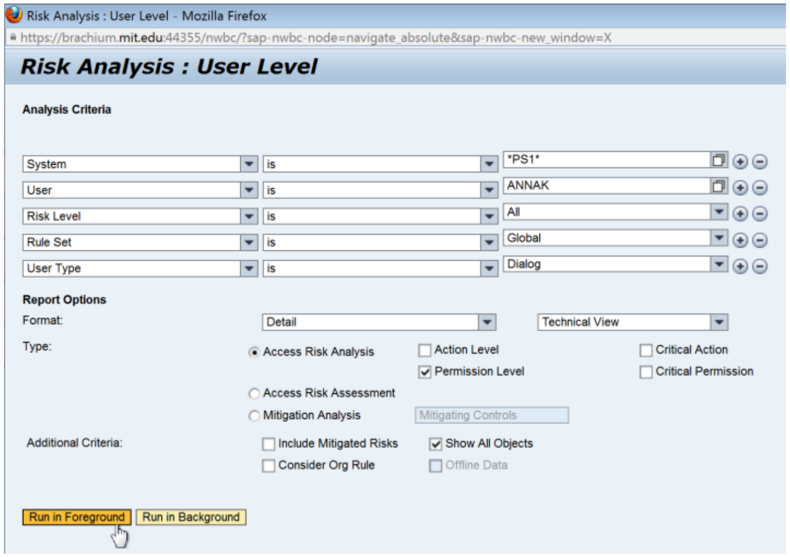
Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission

○ Access Risk Assessment

○ Mitigation Analysis | Mitigating Controls

Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data

10A-3	In the 'Analysis Criteria' section, click on the '-' at the end of the 'Custom Group' row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

10A-4	Add the user ID. In this case, ‘ANNAK’ was typed in. The search option can also be used to search for an ID. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background
10A-5	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

10A-6

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

User ID: User ID of the user with a Risk that has been mitigated

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Last Executed On: Date of last execution of transaction

Execution Count: Number of times transaction was executed for a specified time period

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

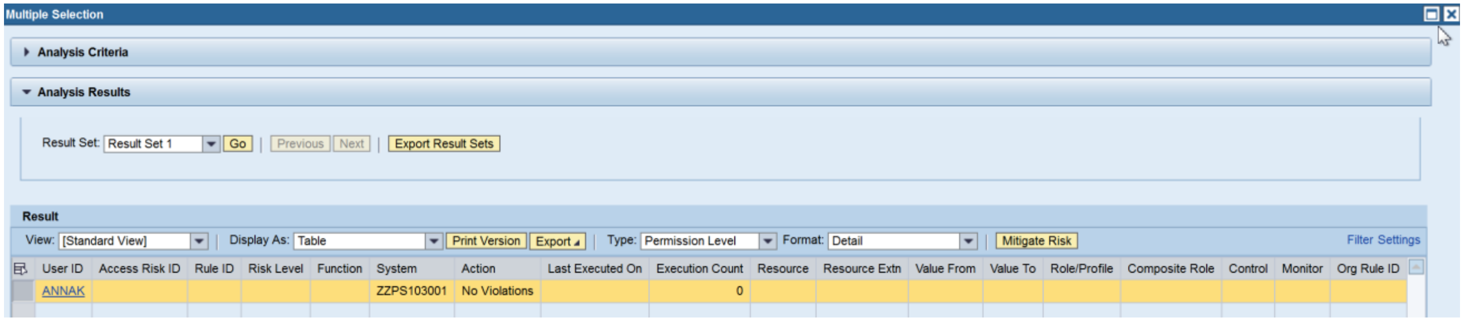
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control



Multiple Selection

Analysis Criteria

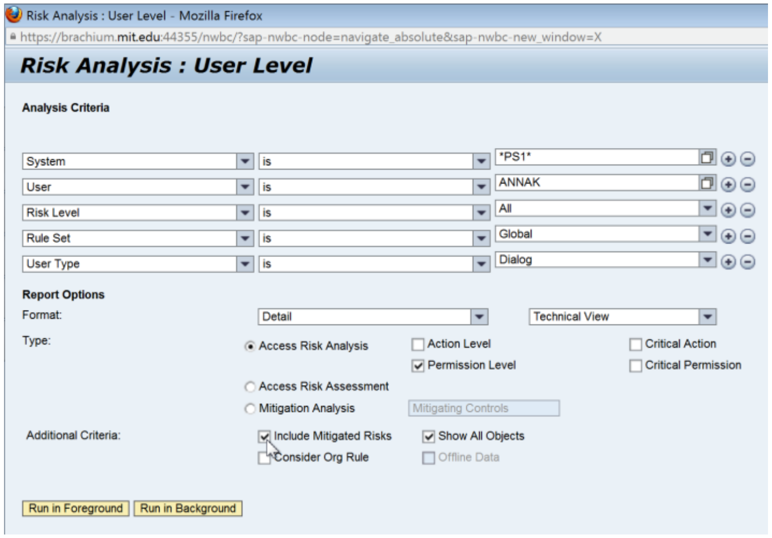
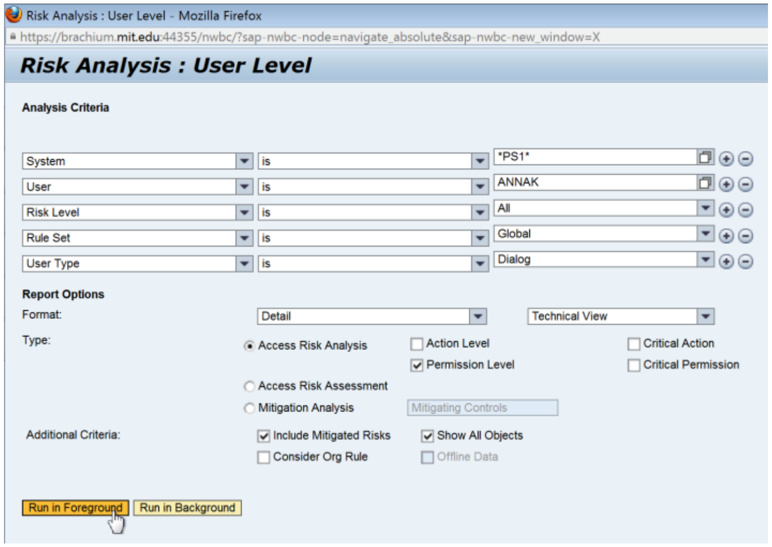
Analysis Results

Result Set: Result Set 1

Result

View: [Standard View] | Display As: Table | Type: Permission Level | Format: Detail

User ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
ANNAK					ZZPS103001	No Violations		0									

10A-7	In the ‘Report Options’ section, select the second drop down for ‘Format’ and select the type of information that is required. In this case, ‘Technical View’ was selected so that the report will show technical information about why Risks exists.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☑ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background
10A-8	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☑ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

10A-9

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

User ID: User ID of the user with a Risk that has been mitigated

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Last Executed On: Date of last execution of transaction

Execution Count: Number of times transaction was executed for a specified time period

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

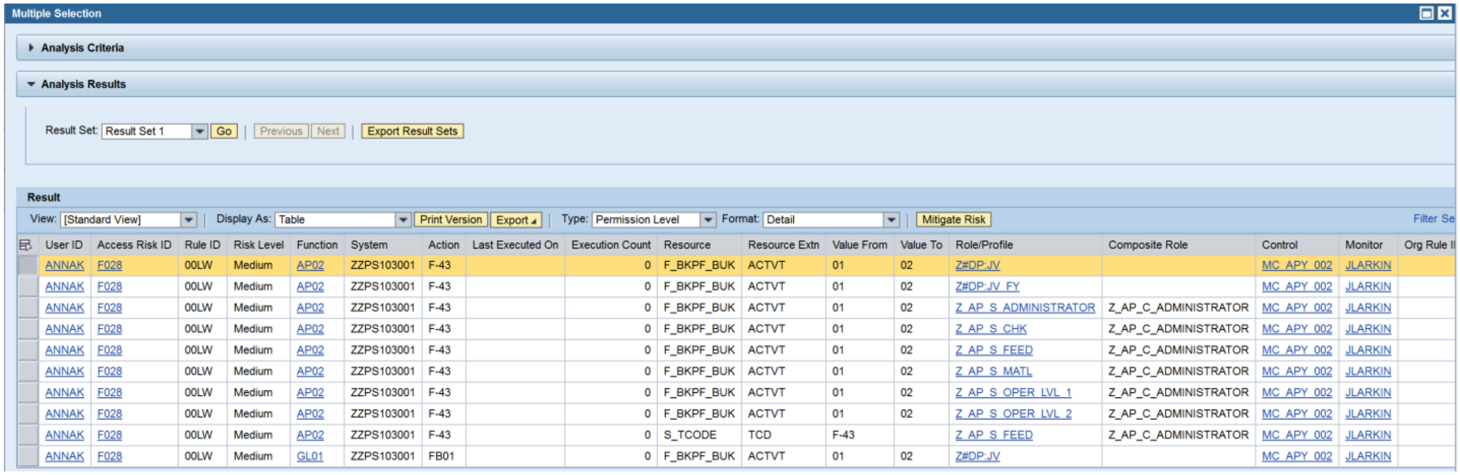
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control



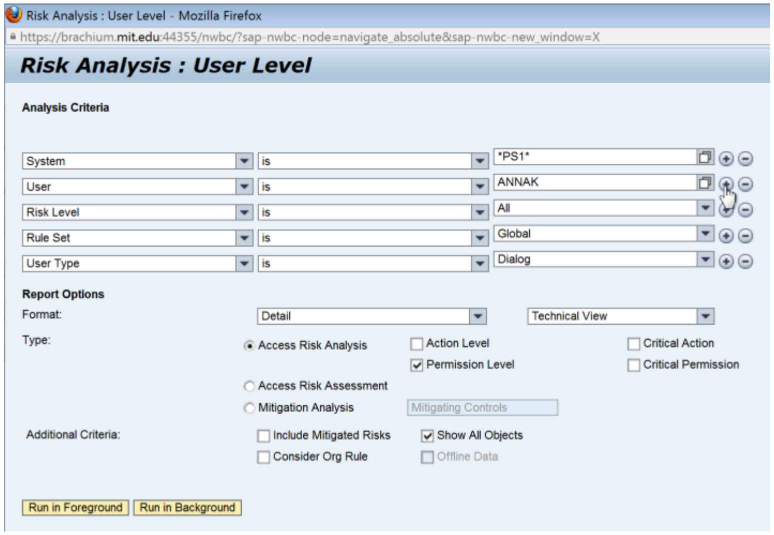
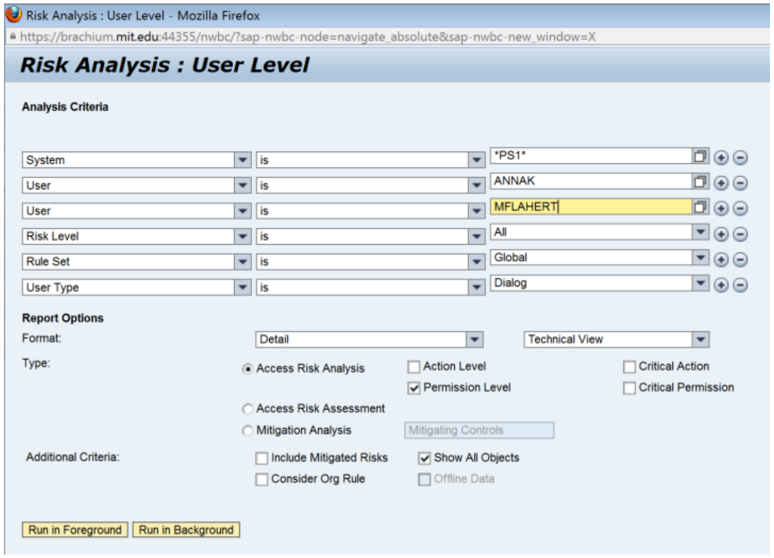
Multiple Selection

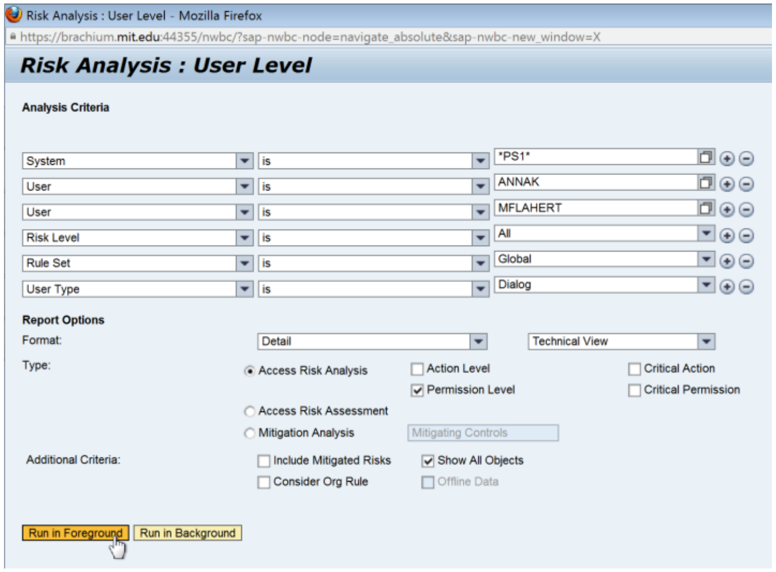
Result Set: Result Set 1

Result

View: [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Detail | Mitigate Risk | Filter Se

User ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule I
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV		MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV_FY		MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	F_BKPF_BUK	ACTVT	01	02	Z_AP_S_ADMINISTRATOR	Z_AP_C_ADMINISTRATOR	MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	F_BKPF_BUK	ACTVT	01	02	Z_AP_S_CHK	Z_AP_C_ADMINISTRATOR	MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	F_BKPF_BUK	ACTVT	01	02	Z_AP_S_FEED	Z_AP_C_ADMINISTRATOR	MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	F_BKPF_BUK	ACTVT	01	02	Z_AP_S_MATL	Z_AP_C_ADMINISTRATOR	MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	F_BKPF_BUK	ACTVT	01	02	Z_AP_S_OPER_LVL_1	Z_AP_C_ADMINISTRATOR	MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	F_BKPF_BUK	ACTVT	01	02	Z_AP_S_OPER_LVL_2	Z_AP_C_ADMINISTRATOR	MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	AP02	ZZPS103001	F-43		0	S_TCODE	TCD	F-43		Z_AP_S_FEED	Z_AP_C_ADMINISTRATOR	MC_APY_002	JLARKIN	
ANNAK	F028	00LW	Medium	GL01	ZZPS103001	FB01		0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV		MC_APY_002	JLARKIN	

10A-10	Click on the '+' at the end of the 'User' row to add an additional user ID search criterion row for each ID. In this case, one additional row is added; thus, we can analyze for a total of two user IDs.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background
10A-11	Add the additional user ID. In this case, 'ANNAK' was entered previously and 'MFLAHERT' was then typed in as an additional ID. The search option can also be used to search for IDs. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** Analysis Criteria System is *PS1* User is ANNAK User is MFLAHERT Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

10A-12	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is ANNAK User is MFLAHERT Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

10A-13

Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information.

User ID: User ID of the user with a Risk that has been mitigated

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Last Executed On: Date of last execution of transaction

Execution Count: Number of times transaction was executed for a specified time period

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

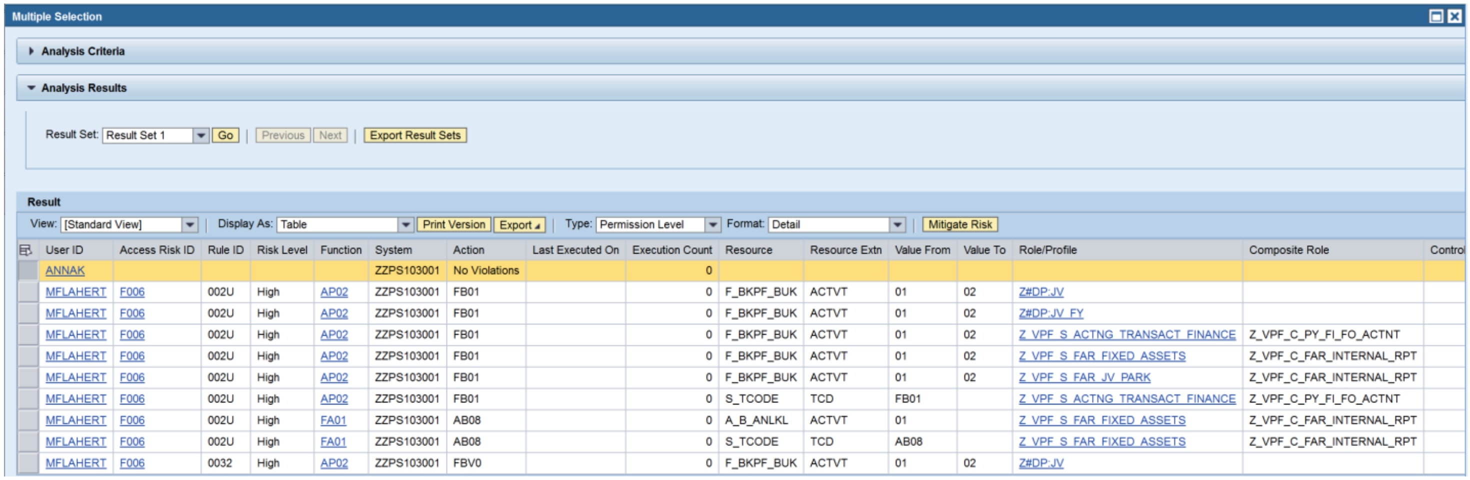
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control

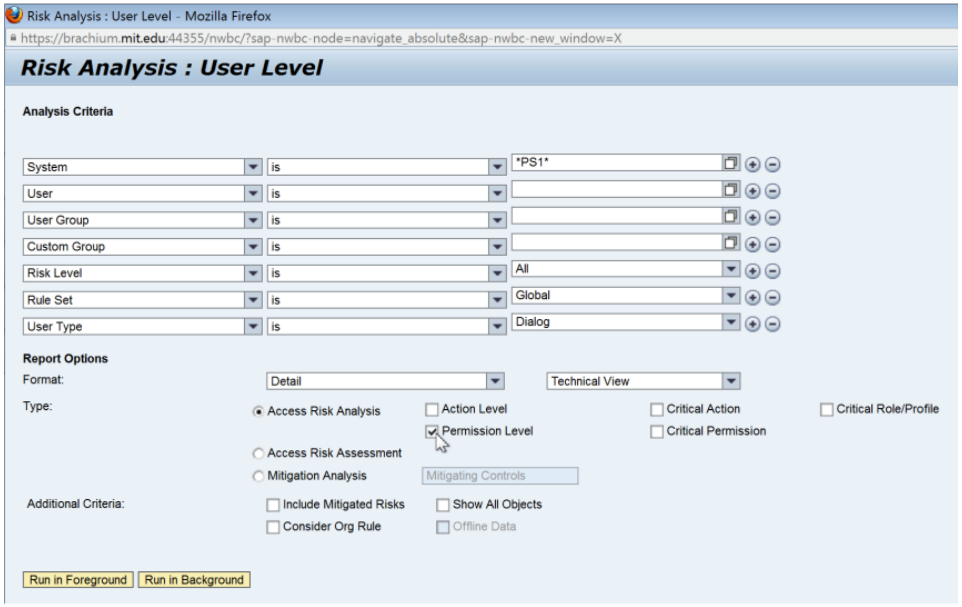


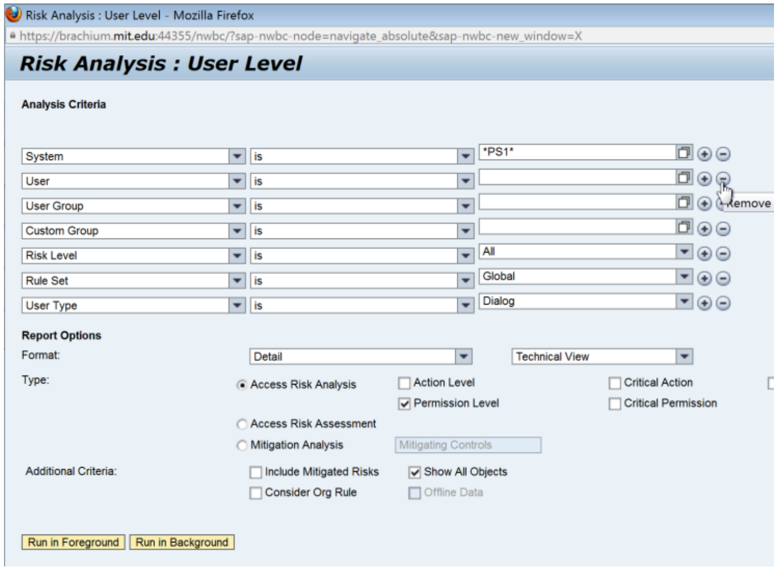
Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets

Result

View: [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Detail | Mitigate Risk

User ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control
ANNAK					ZZPS103001	No Violations		0							
MFLAHERT	F006	002U	High	AP02	ZZPS103001	FB01		0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV		
MFLAHERT	F006	002U	High	AP02	ZZPS103001	FB01		0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV_FY		
MFLAHERT	F006	002U	High	AP02	ZZPS103001	FB01		0	F_BKPF_BUK	ACTVT	01	02	Z_VPF_S_ACTNG_TRANSACT_FINANCE	Z_VPF_C_PY_FI_FO_ACTNT	
MFLAHERT	F006	002U	High	AP02	ZZPS103001	FB01		0	F_BKPF_BUK	ACTVT	01	02	Z_VPF_S_FAR_FIXED_ASSETS	Z_VPF_C_FAR_INTERNAL_RPT	
MFLAHERT	F006	002U	High	AP02	ZZPS103001	FB01		0	F_BKPF_BUK	ACTVT	01	02	Z_VPF_S_FAR_JV_PARK	Z_VPF_C_FAR_INTERNAL_RPT	
MFLAHERT	F006	002U	High	AP02	ZZPS103001	FB01		0	S_TCODE	TCD	FB01		Z_VPF_S_ACTNG_TRANSACT_FINANCE	Z_VPF_C_PY_FI_FO_ACTNT	
MFLAHERT	F006	002U	High	FA01	ZZPS103001	AB08		0	A_B_ANLKL	ACTVT	01		Z_VPF_S_FAR_FIXED_ASSETS	Z_VPF_C_FAR_INTERNAL_RPT	
MFLAHERT	F006	002U	High	FA01	ZZPS103001	AB08		0	S_TCODE	TCD	AB08		Z_VPF_S_FAR_FIXED_ASSETS	Z_VPF_C_FAR_INTERNAL_RPT	
MFLAHERT	F006	0032	High	AP02	ZZPS103001	FBV0		0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV		

10B-1	Analyze for SODs based on user group. In the ‘Report Options’ section, select the first dial button for ‘Access Risk Analysis’. Next, select the type of analysis that is required. The options available are: Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level) Permission Level: SODs at the authorization level Critical Action: Critical transactions that limited/no users should have Critical Permission: Critical authorizations that limited/no users should have Critical Role/Profile: Critical Roles/Profiles that limited/no users should have In this case, ‘Permission Level’ was selected so that the report will show SODs that exist at the Permission Level.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ☐ Critical Role/Profile ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Consider Org Rule ☐ Show All Objects ☐ Offline Data Run in Foreground Run in Background

10B-2	In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘User’ row to remove the row for that search criterion; this criterion is not needed for this scenario.	

Risk Analysis : User Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Risk Analysis : User Level

Analysis Criteria

System	is	*PS1*
User	is	
User Group	is	
Custom Group	is	
Risk Level	is	All
Rule Set	is	Global
User Type	is	Dialog

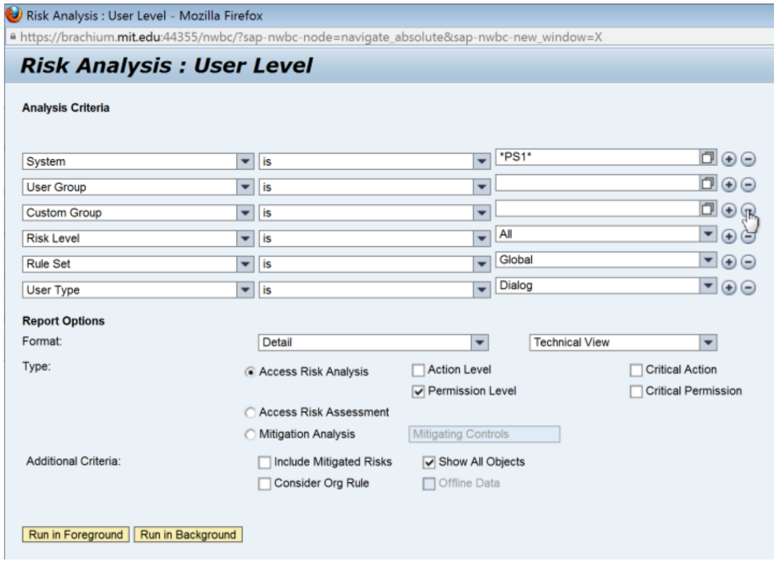
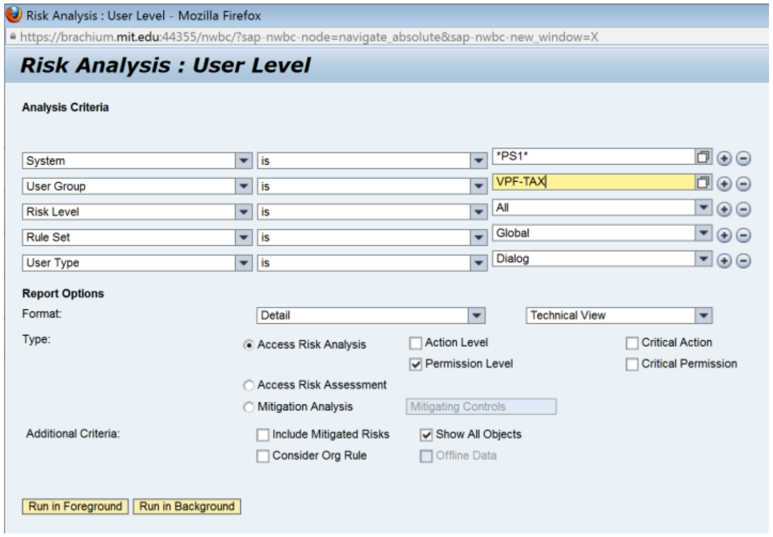
Remove

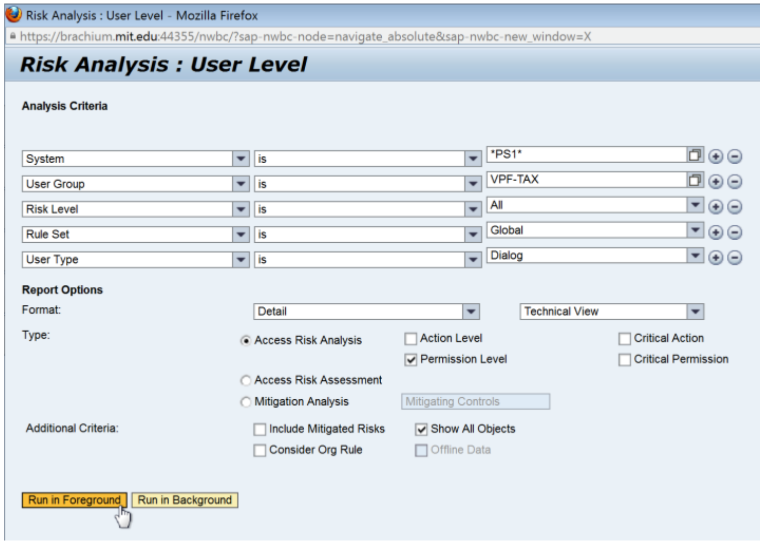
Report Options

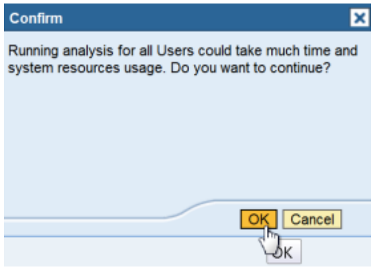
Format: Detail | Technical View

Type: ● Access Risk Analysis | □ Action Level | ☑ Permission Level | □ Critical Action | □ Critical Permission
○ Access Risk Assessment
○ Mitigation Analysis | Mitigating Controls

Additional Criteria: □ Include Mitigated Risks | ☑ Show All Objects | □ Consider Org Rule | □ Offline Data

10B-3	In the 'Analysis Criteria' section, click on the '-' at the end of the 'Custom Group' row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Consider Org Rule ☑ Show All Objects ☐ Offline Data Run in Foreground Run in Background
10B-4	Add the user group name. In this case, 'VPF-TAX', the user group containing all users in VPF who are part of the Tax area, was typed in. The search option can also be used to search for user groups. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User Group is VPF-TAX Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Consider Org Rule ☑ Show All Objects ☐ Offline Data Run in Foreground Run in Background

10B-5	Run the report in the foreground.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User Group is VPF-TAX Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data

10B-6	You may receive a message stating that running the report in the foreground “could take much time and system resources usage” and asking, “Do you want to continue?” If the report is expected to yield a large amount of data, click on ‘Cancel’ and execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information. Otherwise, click ‘OK’ to continue.	 Running analysis for all Users could take much time and system resources usage. Do you want to continue?

10B-7

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

User ID: User ID of the user with a Risk that has been mitigated

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Last Executed On: Date of last execution of transaction

Execution Count: Number of times transaction was executed for a specified time period

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

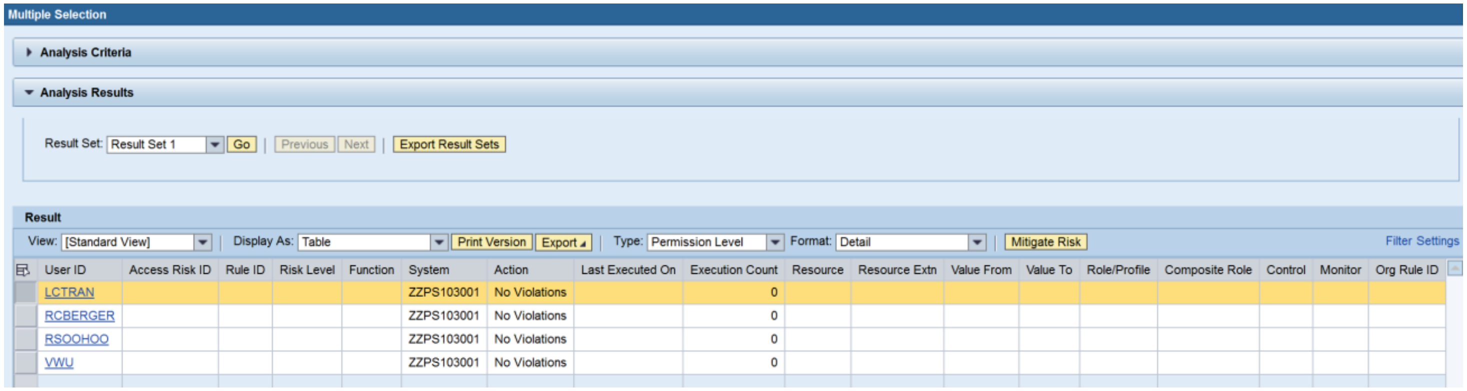
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

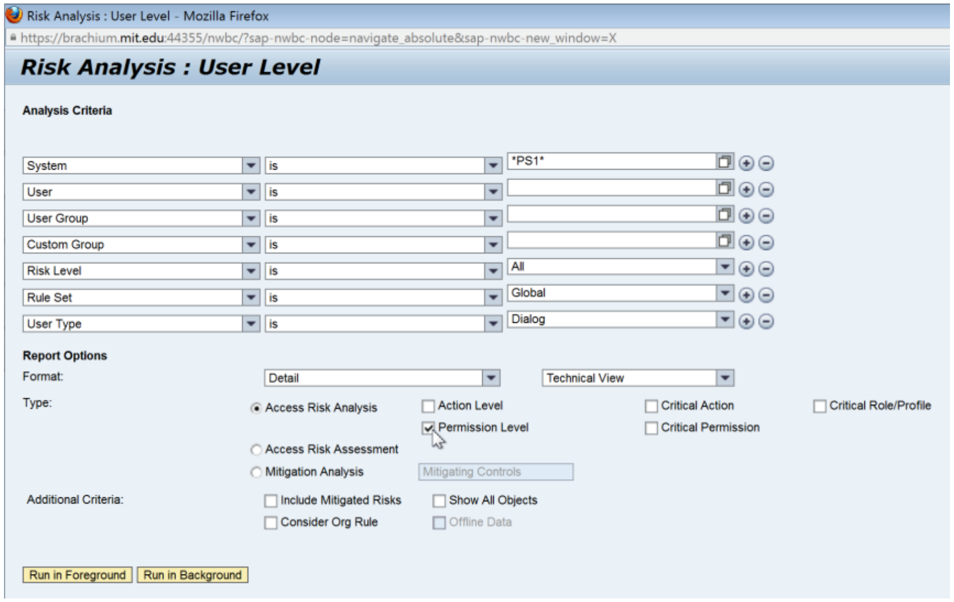
Monitor: The user ID of the Monitor responsible for the Mitigating Control

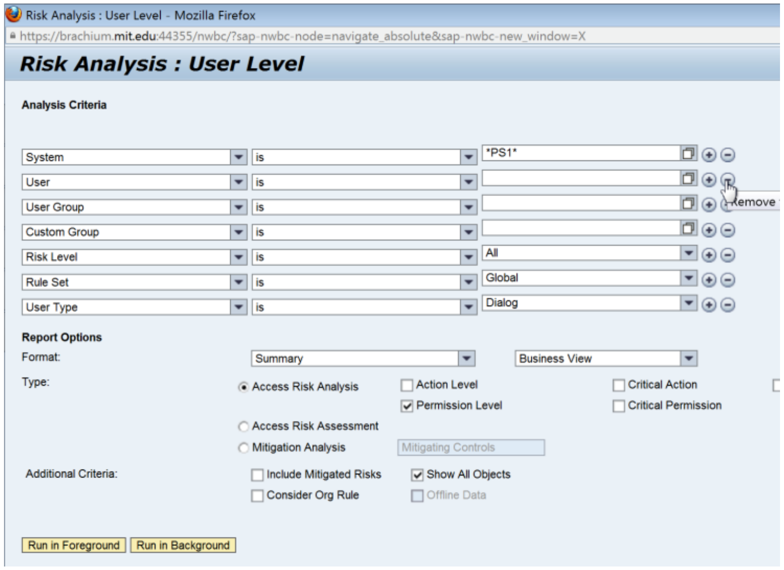


Result Set: Result Set 1

View: [Standard View] Display As: Table Type: Permission Level Format: Detail

User ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
LCTRAN					ZZPS103001	No Violations		0									
RCBERGER					ZZPS103001	No Violations		0									
RSOOHOO					ZZPS103001	No Violations		0									
VWU					ZZPS103001	No Violations		0									

10C-1	Analyze for SODs based on Custom Group. In the ‘Report Options’ section, select the first dial button for ‘Access Risk Analysis’. Next, select the type of analysis that is required. The options available are: Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level) Permission Level: SODs at the authorization level Critical Action: Critical transactions that limited/no users should have Critical Permission: Critical authorizations that limited/no users should have Critical Role/Profile: Critical Roles/Profiles that limited/no users should have In this case, ‘Permission Level’ was selected so that the report will show SODs that exist at the Permission Level.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ☐ Critical Role/Profile ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

10C-2	In the 'Analysis Criteria' section, click on the '-' at the end of the 'User' row to remove the row for that search criterion; this criterion is not needed for this scenario.	

Risk Analysis : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Risk Analysis : User Level

Analysis Criteria

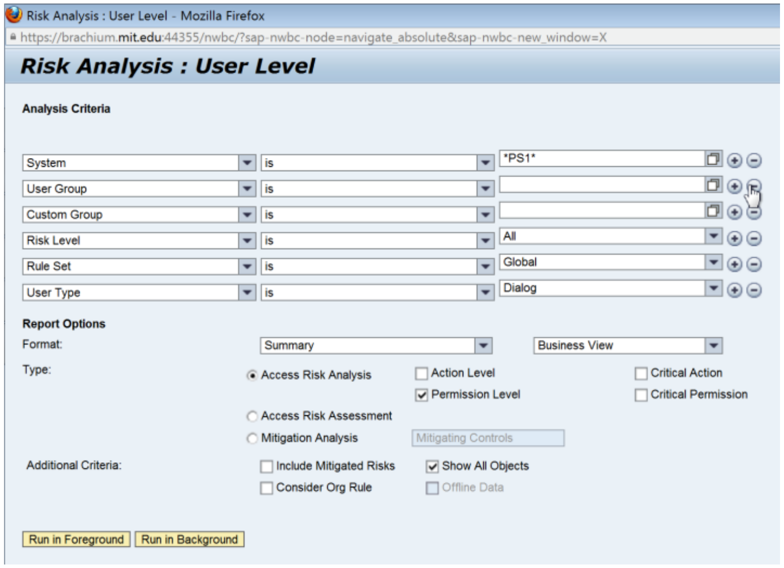
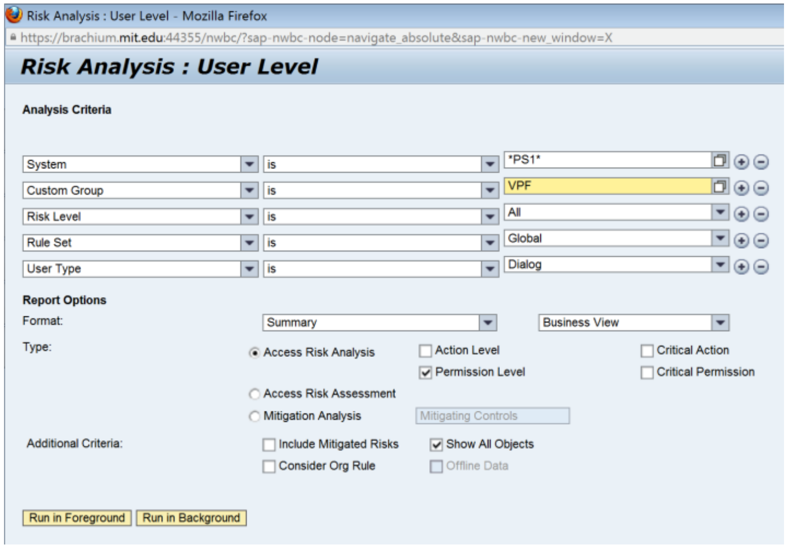
System	is	*PS1*
User	is	
User Group	is	
Custom Group	is	
Risk Level	is	All
Rule Set	is	Global
User Type	is	Dialog

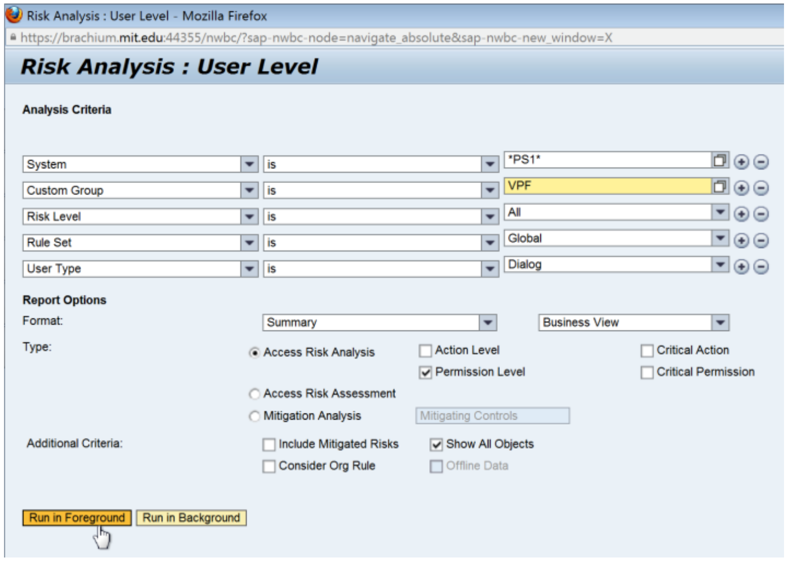
Report Options

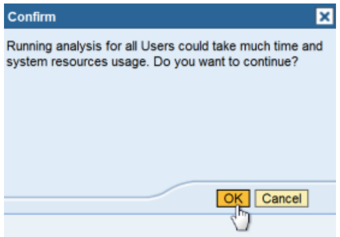
Format: Summary; Business View

Type: ● Access Risk Analysis; □ Action Level; ☑ Permission Level; □ Critical Action; □ Critical Permission; ○ Access Risk Assessment; ○ Mitigation Analysis; Mitigating Controls

Additional Criteria: □ Include Mitigated Risks; ☑ Show All Objects; □ Consider Org Rule; □ Offline Data

10C-3	In the 'Analysis Criteria' section, click on the '-' at the end of the 'User Group' row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background
10C-4	Add the custom group name. In this case, 'VPF', the custom group containing all users in VPF, was typed in. The search option can also be used to search for custom groups. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* Custom Group is VPF Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

10C-5	Run the report in the foreground.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* Custom Group is VPF Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Summary; Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis; Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground | Run in Background

10C-6	You may receive a message stating that running the report in the foreground "could take much time and system resources usage" and asking, "Do you want to continue?" If the report is expected to yield a large amount of data, click on 'Cancel' and execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information. Otherwise, click 'OK' to continue.	 Confirm Running analysis for all Users could take much time and system resources usage. Do you want to continue?

10C-7

Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information.

User ID: User ID of the user with a Risk that has been mitigated

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Last Executed On: Date of last execution of transaction

Execution Count: Number of times transaction was executed for a specified time period

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

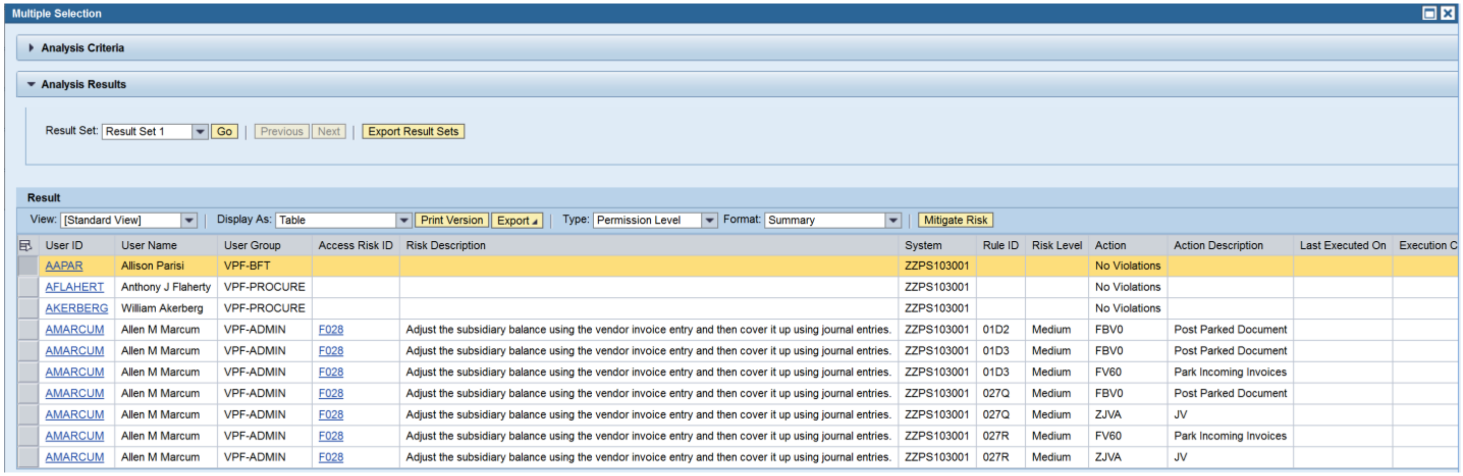
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

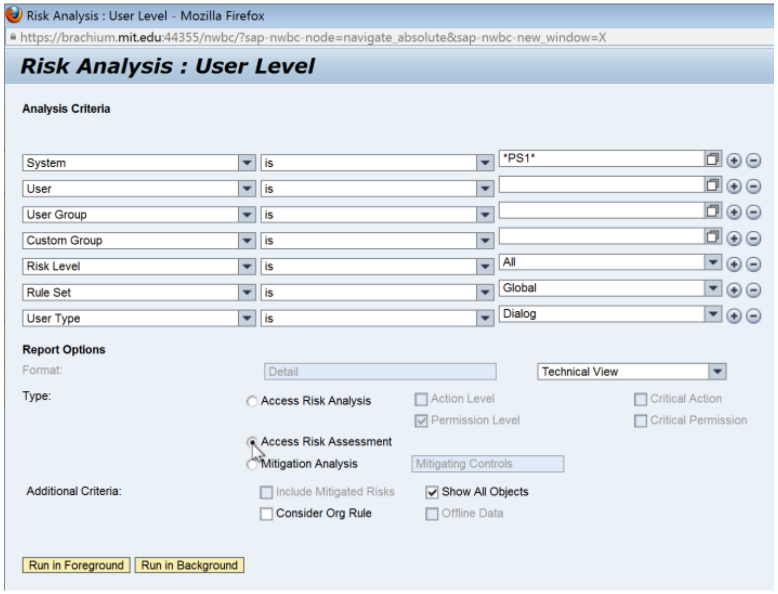
Monitor: The user ID of the Monitor responsible for the Mitigating Control

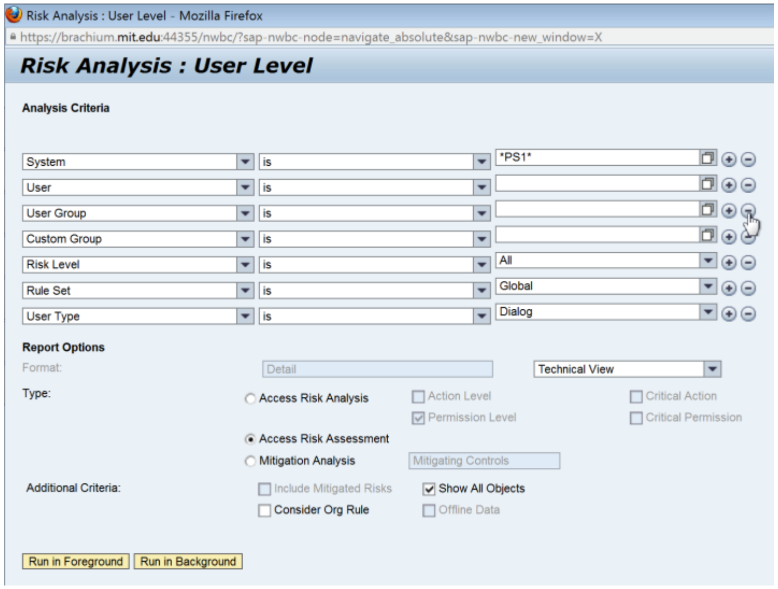


Result Set: Result Set 1

View: [Standard View] | Display As: Table | Type: Permission Level | Format: Summary

User ID	User Name	User Group	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action	Action Description	Last Executed On	Execution C
AAPAR	Allison Parisi	VPF-BFT			ZZPS103001			No Violations			
AFLAHERT	Anthony J Flaherty	VPF-PROCURE			ZZPS103001			No Violations			
AKERBERG	William Akerberg	VPF-PROCURE			ZZPS103001			No Violations			
AMARCUM	Allen M Marcum	VPF-ADMIN	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	01D2	Medium	FBV0	Post Parked Document		
AMARCUM	Allen M Marcum	VPF-ADMIN	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	01D3	Medium	FBV0	Post Parked Document		
AMARCUM	Allen M Marcum	VPF-ADMIN	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	01D3	Medium	FV60	Park Incoming Invoices		
AMARCUM	Allen M Marcum	VPF-ADMIN	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	027Q	Medium	FBV0	Post Parked Document		
AMARCUM	Allen M Marcum	VPF-ADMIN	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	027Q	Medium	ZJVA	JV		
AMARCUM	Allen M Marcum	VPF-ADMIN	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	027R	Medium	FV60	Park Incoming Invoices		
AMARCUM	Allen M Marcum	VPF-ADMIN	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	027R	Medium	ZJVA	JV		

10D-1	Carry out an Access Risk Assessment by user ID. In the 'Report Options' section, select the second dial button for 'Access Risk Assessment'.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ○ Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ● Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

10D-2	In the 'Analysis Criteria' section, click on the '-' at the end of the 'User Group' row to remove the row for that search criterion; this criterion is not needed for this scenario.	

Risk Analysis : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Risk Analysis : User Level

Analysis Criteria

System	is	*PS1*
User	is	
User Group	is	
Custom Group	is	
Risk Level	is	All
Rule Set	is	Global
User Type	is	Dialog

Report Options

Format: Detail | Technical View

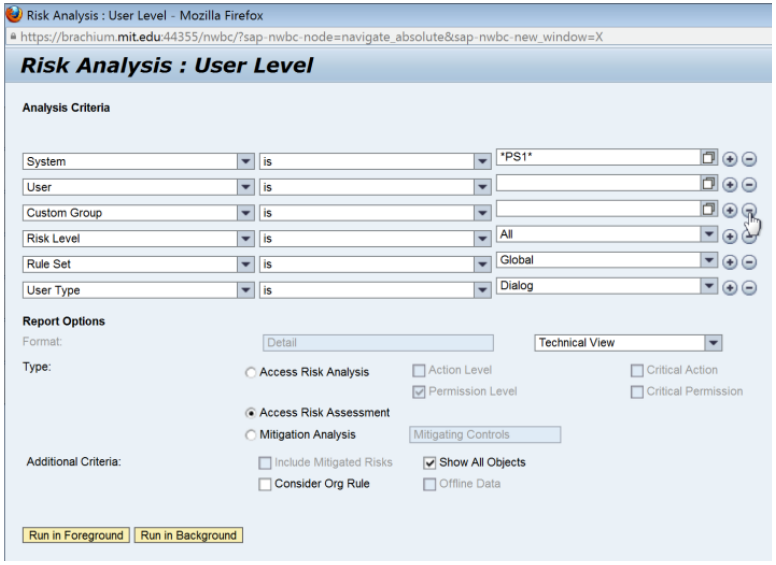
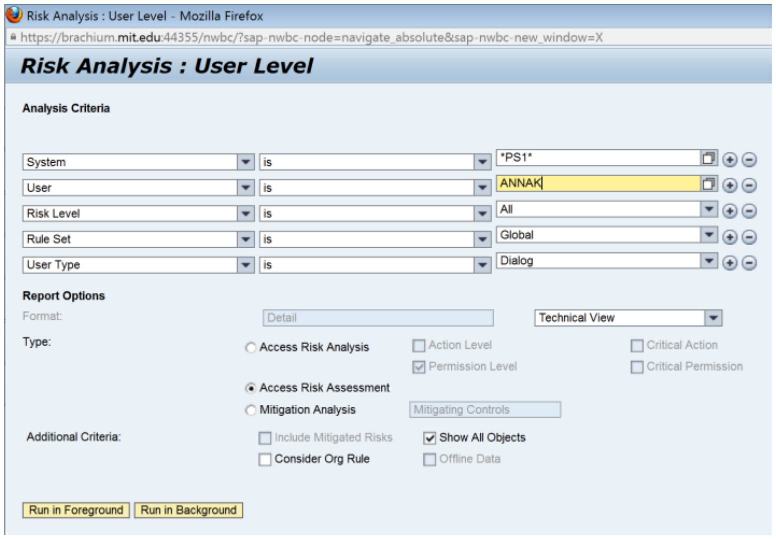
Type: ○ Access Risk Analysis ☐ Action Level ☐ Critical Action
☑ Permission Level ☐ Critical Permission

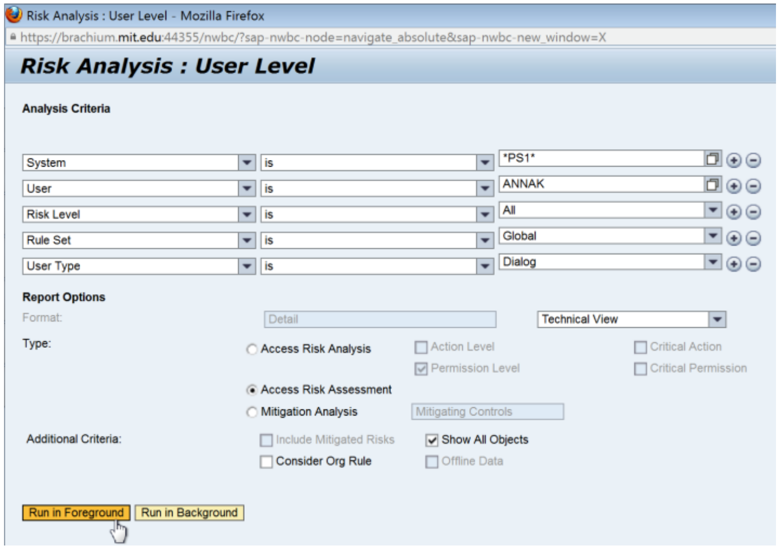
● Access Risk Assessment

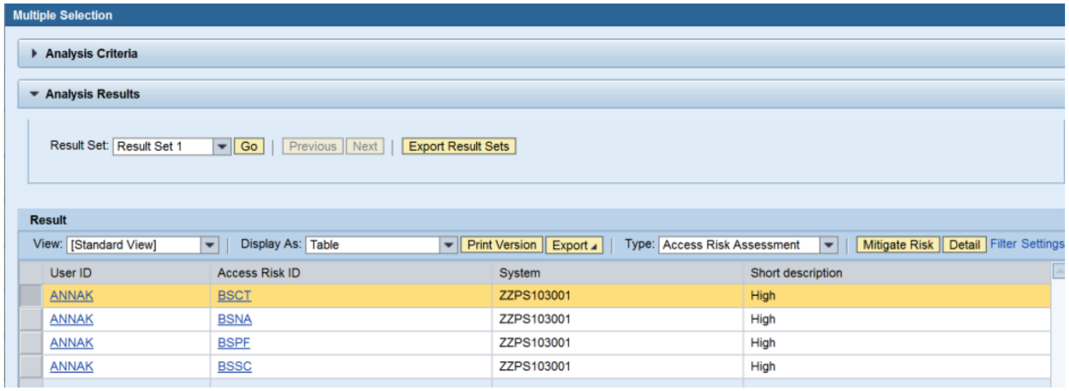
○ Mitigation Analysis | Mitigating Controls

Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects

☐ Consider Org Rule ☐ Offline Data

10D-3	In the 'Analysis Criteria' section, click on the '-' at the end of the 'Custom Group' row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ○ Access Risk Analysis □ Action Level □ Critical Action ☑ Permission Level □ Critical Permission ● Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background
10D-4	Add the user ID. In this case, 'ANNAK' was typed in. The search option can also be used to search for an ID. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ○ Access Risk Analysis □ Action Level □ Critical Action ☑ Permission Level □ Critical Permission ● Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

10D-5	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ○ Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ● Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data

10D-6	Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information. User ID: User ID of the user with a Risk that has been mitigated Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist System: The system in which the user has the risk Short Description: The risk level defined for each Access Risk in the standard rule set	

Multiple Selection

Analysis Criteria

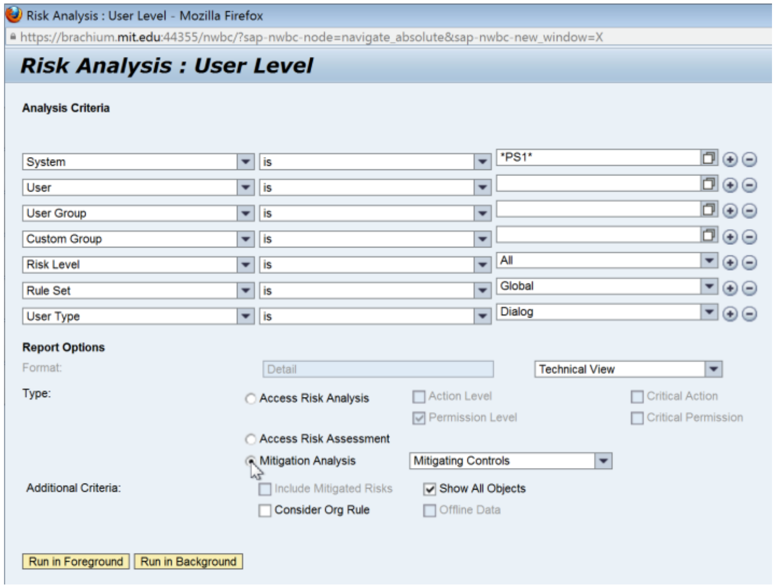
Analysis Results

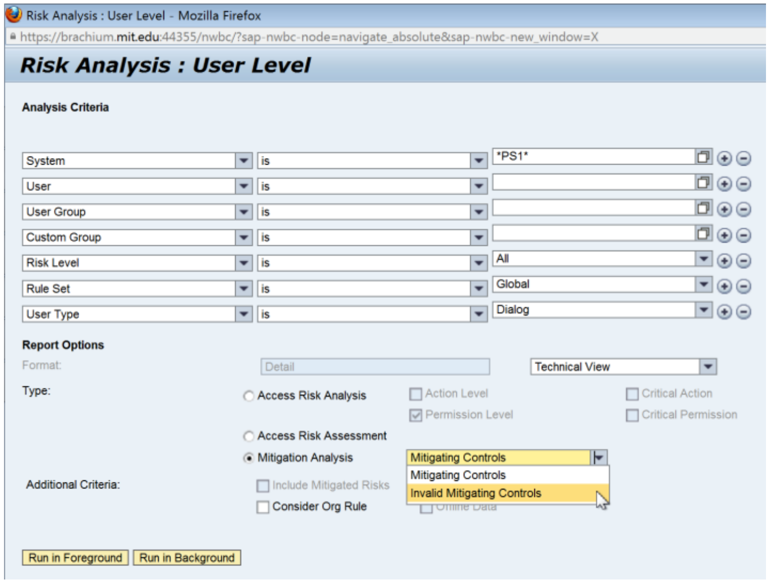
Result Set: Result Set 1

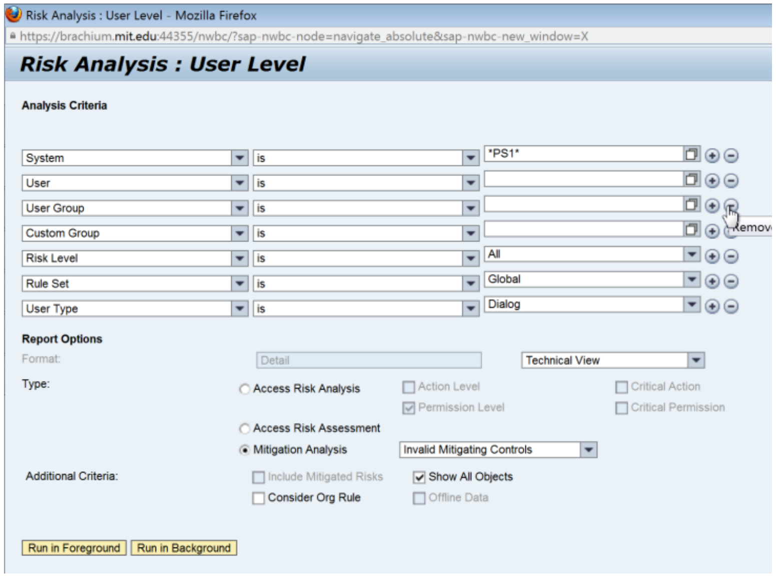
Result

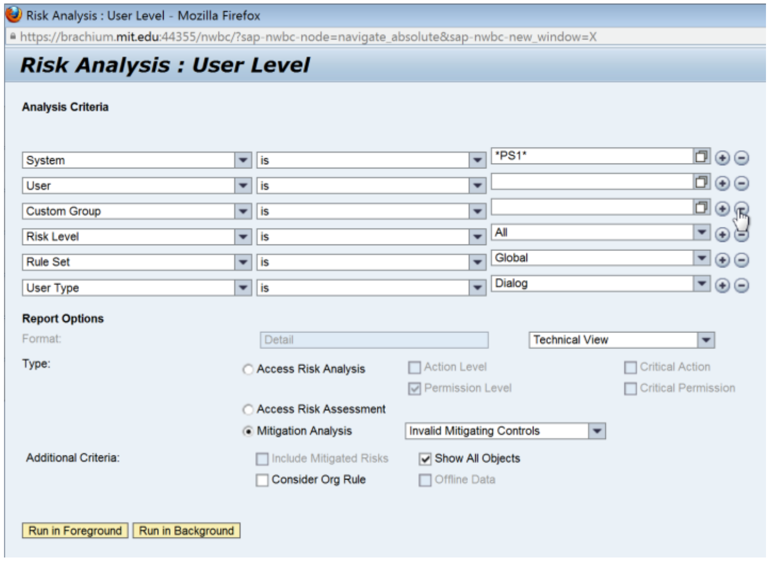
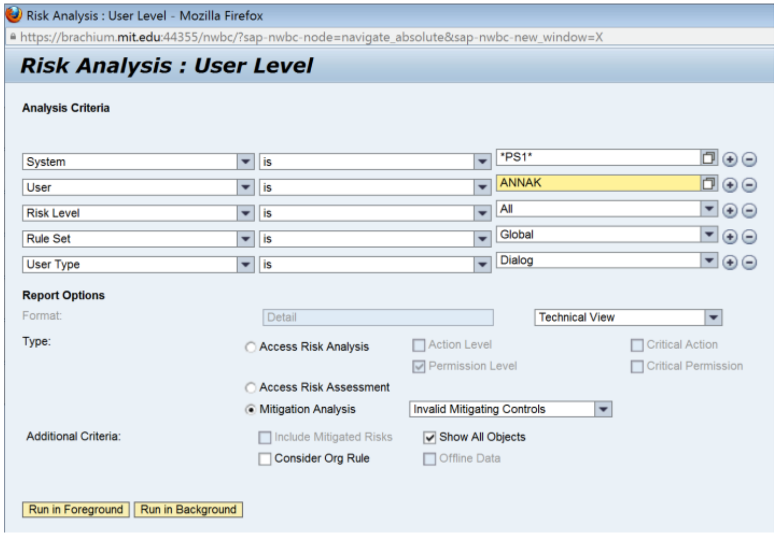
View: [Standard View]   Display As: Table   Type: Access Risk Assessment

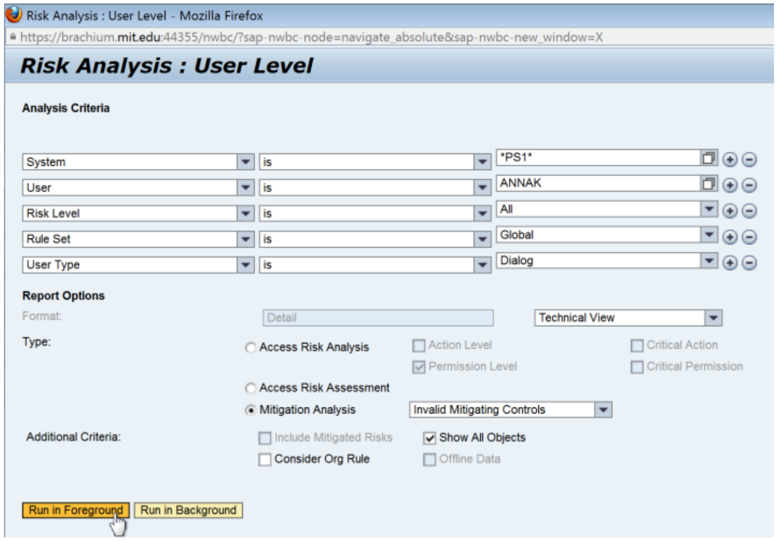
User ID	Access Risk ID	System	Short description
ANNAK	BSCT	ZZPS103001	High
ANNAK	BSNA	ZZPS103001	High
ANNAK	BSPF	ZZPS103001	High
ANNAK	BSSC	ZZPS103001	High

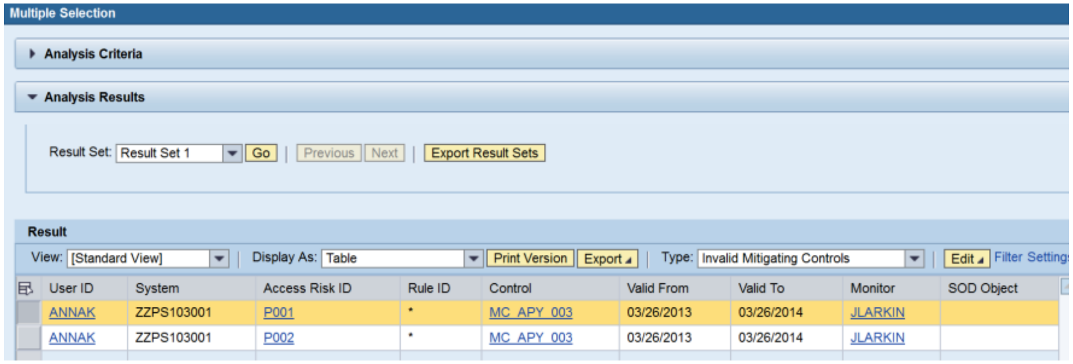
10E-1	Carry out an analysis of Mitigating Controls by user ID. In the 'Report Options' section, select the third dial button for 'Mitigation Analysis'.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ○ Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ○ Access Risk Assessment ● Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

10E-2	In the 'Report Options' section, select the drop down for 'Mitigation Analysis' and select the type of information that is required. The options available are: Mitigating Controls: Information on all Mitigating Controls assignments Invalid Mitigating Controls: Information on all invalid Mitigating Control assignments In this case, 'Invalid Mitigating Controls' was selected.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Detail Technical View Type: ○ Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ○ Access Risk Assessment ● Mitigation Analysis Mitigating Controls Mitigating Controls Invalid Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

10E-3	In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘User Group’ row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ○ Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ● Mitigation Analysis Invalid Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Consider Org Rule ☑ Show All Objects ☐ Offline Data

10E-4	In the 'Analysis Criteria' section, click on the '-' at the end of the 'Custom Group' row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ○ Access Risk Analysis □ Action Level □ Critical Action ☑ Permission Level □ Critical Permission ○ Access Risk Assessment ● Mitigation Analysis Invalid Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background
10E-5	Add the user ID. In this case, 'ANNAK' was typed in. The search option can also be used to search for an ID. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ○ Access Risk Analysis □ Action Level □ Critical Action ☑ Permission Level □ Critical Permission ○ Access Risk Assessment ● Mitigation Analysis Invalid Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

10E-6	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ○ Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ● Mitigation Analysis Invalid Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

10E-7	Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information. User ID: User ID of the user with a Risk that has been mitigated System: The system in which the user has the risk Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist Rule ID: The ID representing the particular rule that was triggered for that Risk Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk Valid From: Date on which assignment of the control to the user begins Valid To: Date on which assignment of the control to the user ends Monitor: The user ID of the Monitor responsible for the Mitigating Control	 Multiple Selection ▸ Analysis Criteria ▾ Analysis Results Result Set: Result Set 1 ▾ Go | Previous Next | Export Result Sets Result View: [Standard View] ▾ | Display As: Table ▾ Print Version Export ◢ | Type: Invalid Mitigating Controls ▾ | Edit ◢ Filter Setting

User ID	System	Access Risk ID	Rule ID	Control	Valid From	Valid To	Monitor	SOD Object
ANNAK	ZZPS103001	P001	*	MC_APY_003	03/26/2013	03/26/2014	JLARKIN	
ANNAK	ZZPS103001	P002	*	MC_APY_003	03/26/2013	03/26/2014	JLARKIN	

Job Aid 13 User Level Simulation

USE

This report can be used carry out simulations at the user level for the purpose of understanding whether the addition or removal of certain access either creates or eliminates SODs and other risks.

INFORMATION

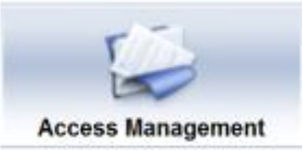
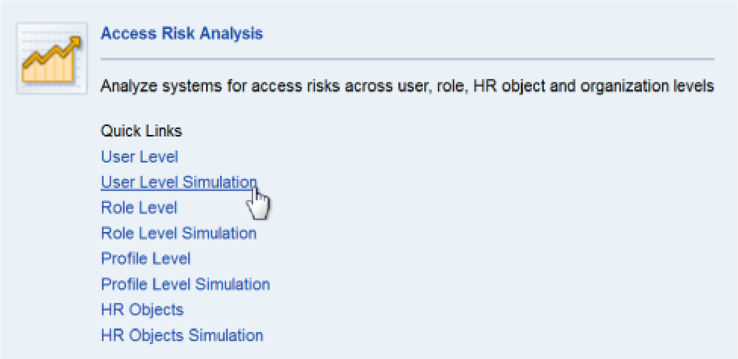
New risk violations that will result due to changes to user access.

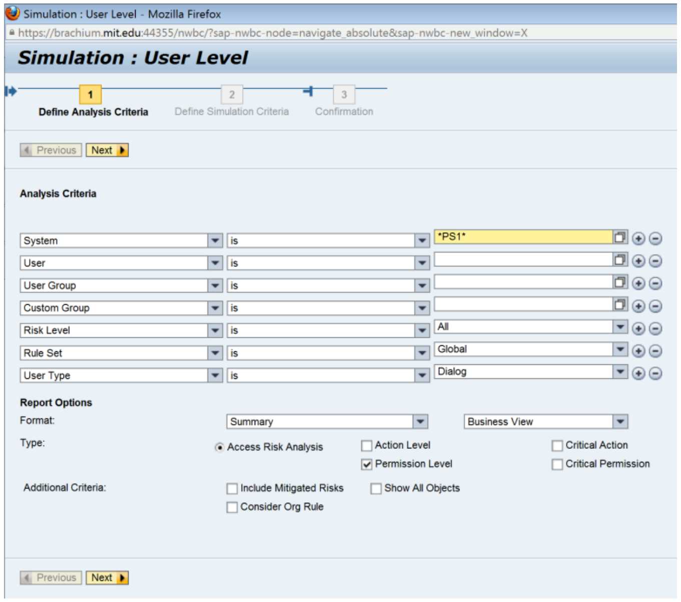
RELATED PROCESSES

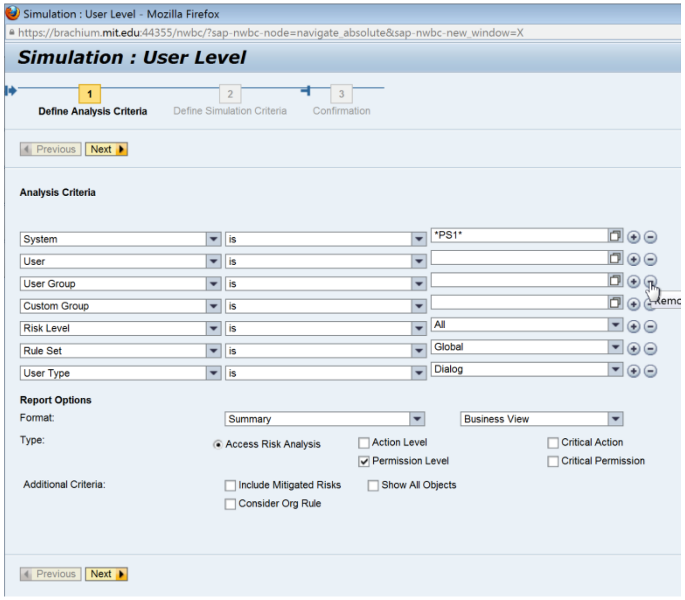
- Process 1: New or Amended Roles
- Process 2: Mitigation Analysis

SPECIFIC SCENARIOS

- Step 15A: Simulation by Action (transaction).
- Step 15B: Simulation by Role.
- Step 15C: Simulation by Profile.

Step	Description	Screenshot
1	Navigate to the 'Access Management' tab.	
2	Click on the 'User Level Simulation' report located in the 'Access Risk Analysis' section.	Access Risk Analysis Analyze systems for access risks across user, role, HR object and organization levels Quick Links User Level User Level Simulation Role Level Role Level Simulation Profile Level Profile Level Simulation HR Objects HR Objects Simulation

3	In the ‘Analysis Criteria’ section, select the System for which information is required. Since the desired selection is PS1 (Production), ‘*PS1*’ was typed in as the system. The search option can also be used to search for the correct system. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : User Level 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation Analysis Criteria System is *PS1* User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Summary; Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission Additional Criteria: □ Include Mitigated Risks □ Consider Org Rule □ Show All Objects

4	Run a simulation for a single User. In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘User Group’ row to remove the row for that search criterion; this criterion is not needed for this scenario.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

Analysis Criteria

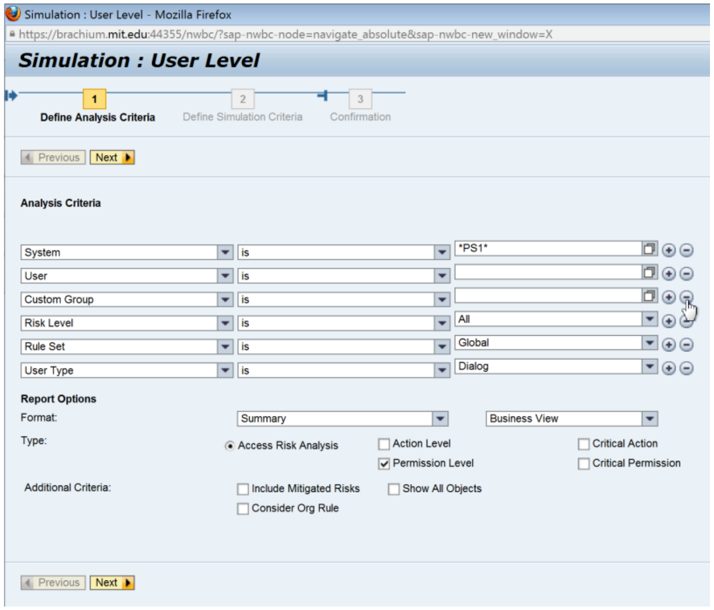
System	is	*PS1*
User	is	
User Group	is	
Custom Group	is	
Risk Level	is	All
Rule Set	is	Global
User Type	is	Dialog

Report Options

Format: Summary Business View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission

Additional Criteria: □ Include Mitigated Risks □ Consider Org Rule □ Show All Objects

5	In the 'Analysis Criteria' section, click on the '-' at the end of the 'Custom Group' row to remove the row for that search criterion; this criterion is not needed for this scenario.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

Analysis Criteria

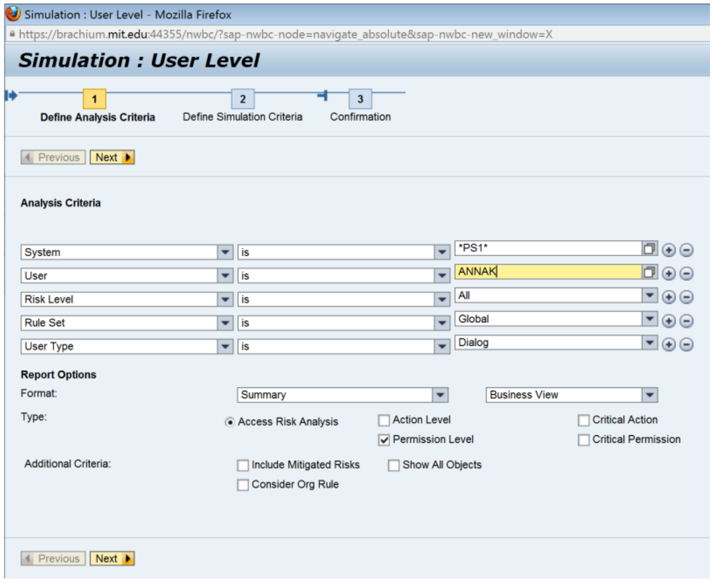
System	is	*PS1*
User	is	
Custom Group	is	
Risk Level	is	All
Rule Set	is	Global
User Type	is	Dialog

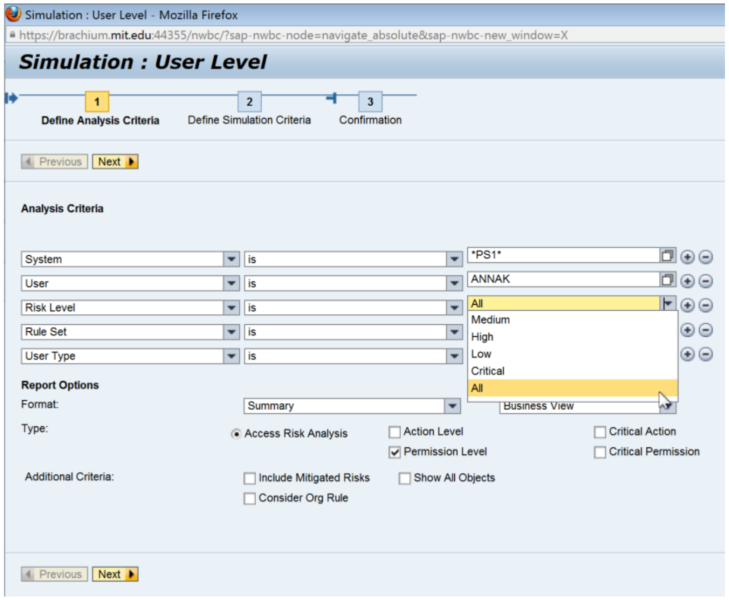
Report Options

Format: Summary Business View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission

Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule

6	Add the user ID. In this case, ‘ANNAK’ was typed in. The search option can also be used to search for an ID. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : User Level 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next Analysis Criteria System · is · *PS1* User · is · ANNAK Risk Level · is · All Rule Set · is · Global User Type · is · Dialog Report Options Format: Summary · Business View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission Additional Criteria: □ Include Mitigated Risks · □ Show All Objects · □ Consider Org Rule Previous · Next

7	In the 'Analysis Criteria' section, select the 'Risk Level' drop down and select the risk level for which information is required. In this case, 'All' was selected so that the report evaluates for all risk levels.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

Previous | Next

Analysis Criteria

System	is	*PS1*
User	is	ANNAK
Risk Level	is	All
Rule Set	is	
User Type	is	

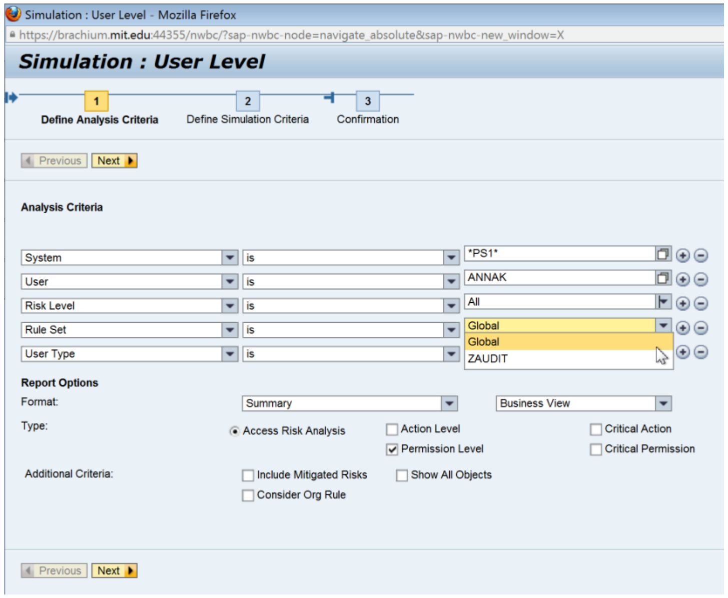
Report Options

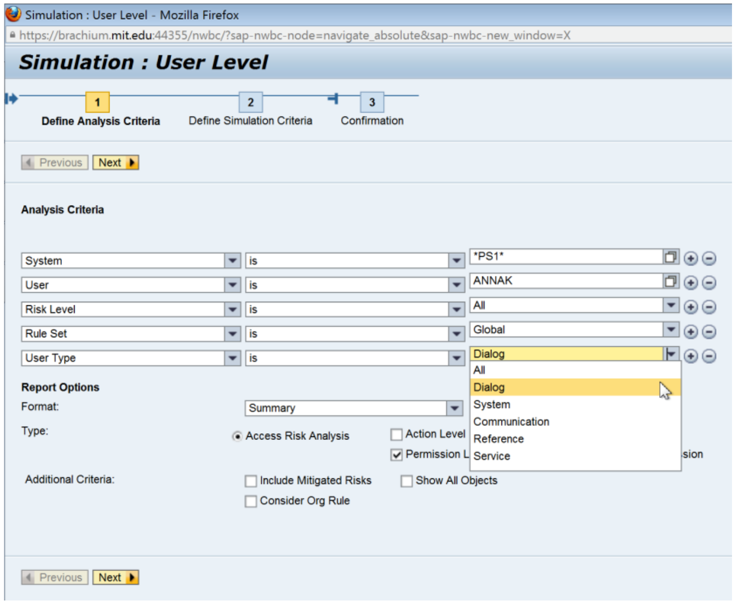
Format: Summary | Business View

Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission

Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule

Previous | Next

8	In the 'Analysis Criteria' section, select the 'Rule Set' drop down and select the Rule Set against which the report should be executed. In this case, 'Global', the MIT Rule Set, was selected. Unless advised otherwise, the selection should always be 'Global' for this report.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : User Level 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next Analysis Criteria System · is · *PS1* User · is · ANNAK Risk Level · is · All Rule Set · is · Global (Global, ZAUDIT) User Type · is Report Options Format: Summary · Business View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission Additional Criteria: □ Include Mitigated Risks · □ Show All Objects · □ Consider Org Rule Previous · Next

9	In the 'Analysis Criteria' section, select the User Type' drop down and select the type of users for which information is required. In this case, 'Dialog' was selected so that the report only evaluates for dialog users.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

1 Define Analysis Criteria | 2 Define Simulation Criteria | 3 Confirmation

Analysis Criteria

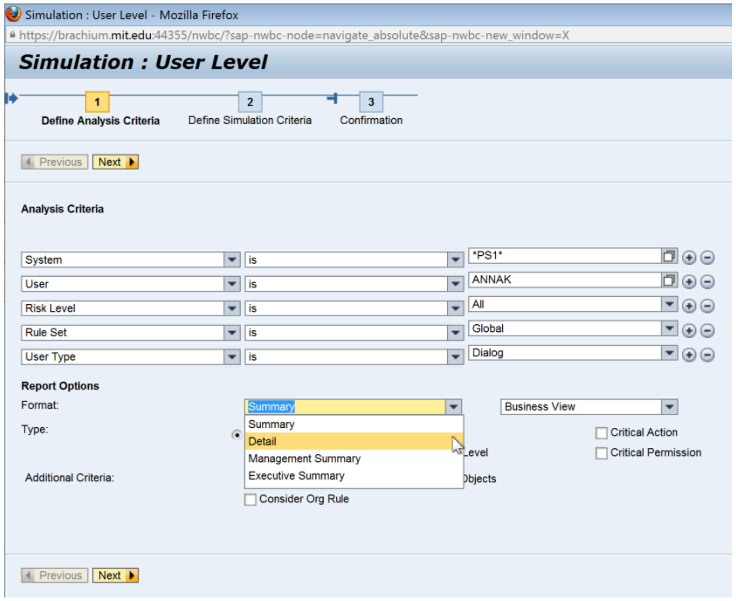
System	is	*PS1*
User	is	ANNAK
Risk Level	is	All
Rule Set	is	Global
User Type	is	Dialog

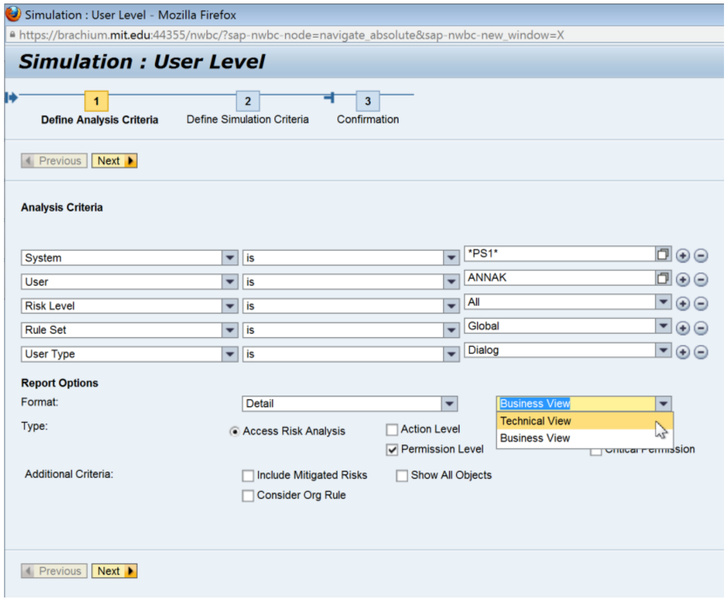
Report Options

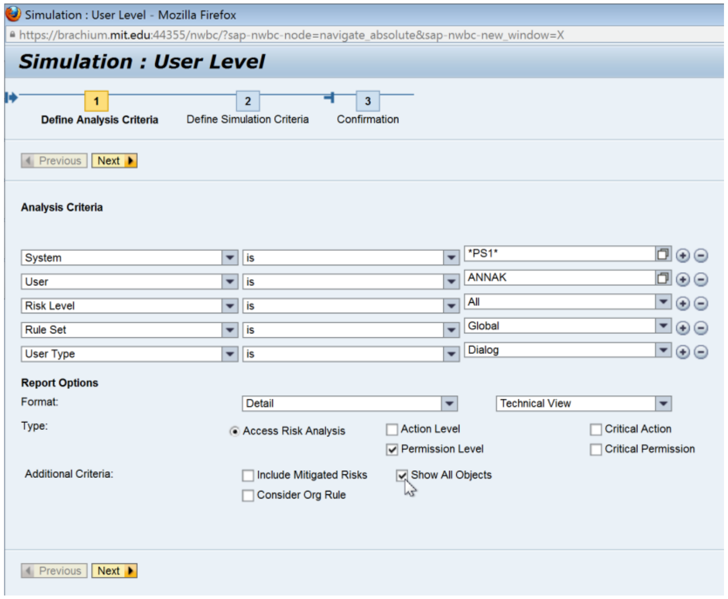
Format: Summary

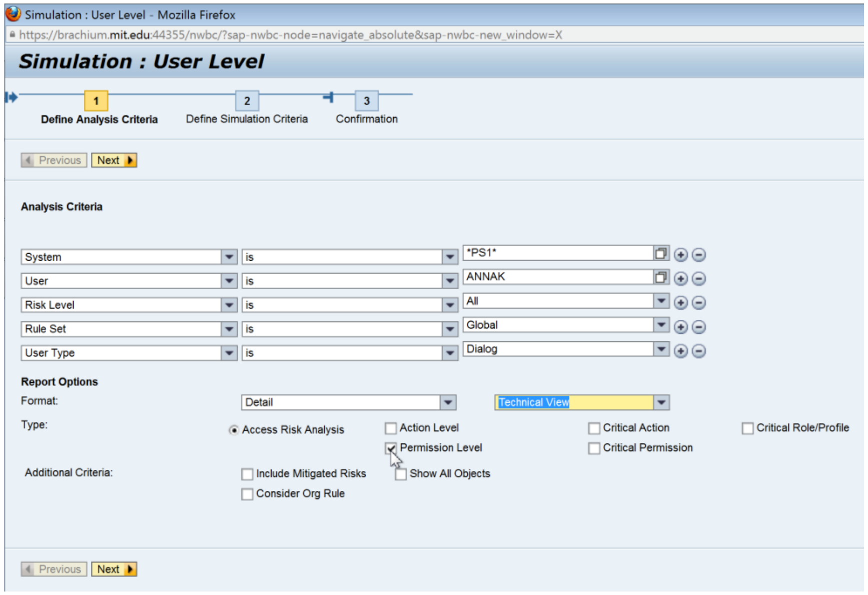
Type: ● Access Risk Analysis □ Action Level ☑ Permission L

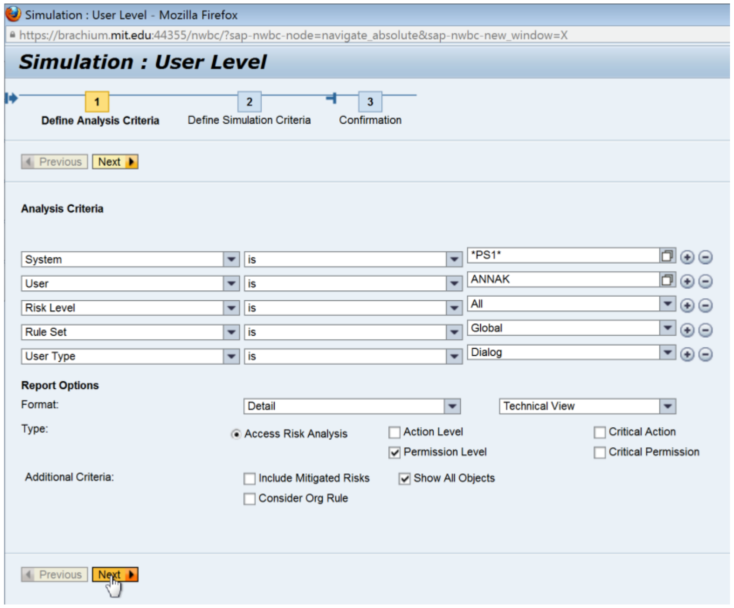
Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule

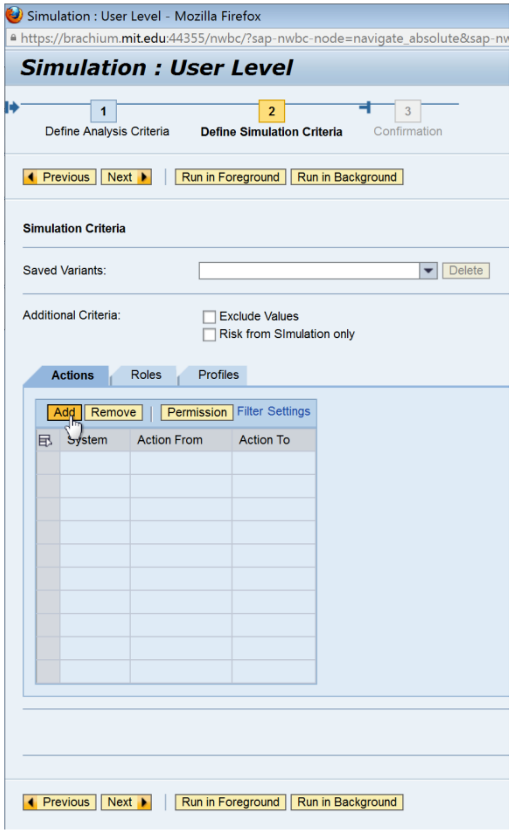
10	In the 'Report Options' section, select the first drop down for 'Format' and select the level of detail at which information is required. In this case, 'Detail' was selected so that the report will show information about why Risks exists.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : User Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next **Analysis Criteria** System · is · *PS1* User · is · ANNAK Risk Level · is · All Rule Set · is · Global User Type · is · Dialog **Report Options** Format: Summary · Business View Summary / Detail / Management Summary / Executive Summary Type: ● · Level · □ Critical Action · □ Critical Permission Additional Criteria: Objects □ Consider Org Rule Previous · Next

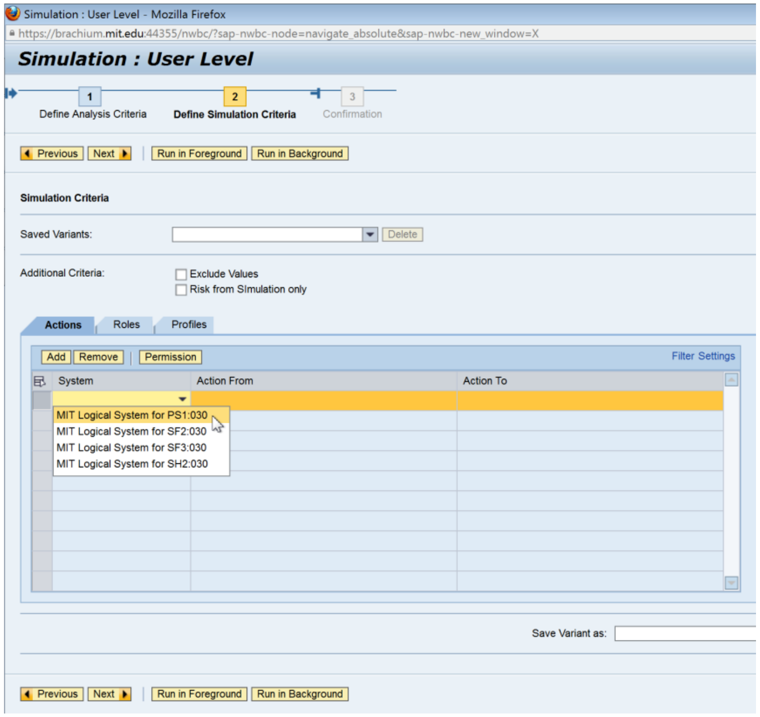
11	In the ‘Report Options’ section, select the second drop down for ‘Format’ and select the type of information that is required. In this case, ‘Technical View’ was selected so that the report will show technical information about why Risks exists.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : User Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next **Analysis Criteria** System · is · *PS1* User · is · ANNAK Risk Level · is · All Rule Set · is · Global User Type · is · Dialog **Report Options** Format: Detail · Business View Technical View Business View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Permission Additional Criteria: □ Include Mitigated Risks · □ Show All Objects · □ Consider Org Rule Previous · Next

12	In the 'Report Options' section, check 'Show All Objects' under 'Additional Criteria'. This will ensure that Users with no violations are explicitly listed as such (i.e. 'No Violations' will be listed as a line item for such users' IDs).	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : User Level 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next Analysis Criteria System · is · *PS1* User · is · ANNAK Risk Level · is · All Rule Set · is · Global User Type · is · Dialog Report Options Format: Detail · Technical View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission Additional Criteria: □ Include Mitigated Risks · □ Consider Org Rule · ☑ Show All Objects Previous · Next

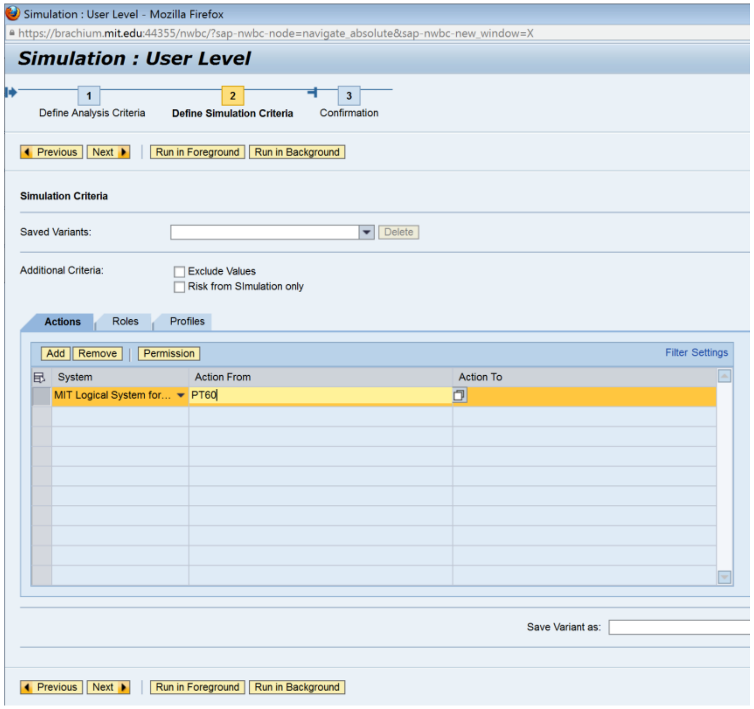
13	Analyze for SODs (excluding false positives). In the 'Report Options' section, select the dial button for 'Access Risk Analysis'. Next, select the type of analysis that is required. The options available are: Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level) Permission Level: SODs at the authorization level Critical Action: Critical transactions that limited/no users should have Critical Permission: Critical authorizations that limited/no users should have Critical Role/Profile: Critical Roles/Profiles that limited/no users should have In this case, 'Permission Level' was selected so that the report will show SODs that exist at the Permission Level.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : User Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next **Analysis Criteria** System · is · *PS1* User · is · ANNAK Risk Level · is · All Rule Set · is · Global User Type · is · Dialog **Report Options** Format: Detail · Technical View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission · □ Critical Role/Profile Additional Criteria: □ Include Mitigated Risks · □ Consider Org Rule · □ Show All Objects Previous · Next

14	The analysis criteria has now been defined. Click on ‘Next’ to define the simulation criteria.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : User Level 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation Previous Next Analysis Criteria System is *PS1* User is ANNAK Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule Previous Next

15A-1	Simulation by Action (transaction). On the ‘Actions’ tab, click on ‘Add’ to define transaction simulation criteria.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nv 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Previous Next Run in Foreground Run in Background Delete Actions Roles Profiles Add Remove Permission Filter Settings **Simulation : User Level** Simulation Criteria Saved Variants: Additional Criteria: □ Exclude Values □ Risk from SImulation only System | Action From | Action To

15A-2	Click the drop down on the ‘System’ field and select the system from which a transaction must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	

Simulation : User Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Simulation : User Level
1 Define Analysis Criteria
2 Define Simulation Criteria
3 Confirmation
Previous
Next
Run in Foreground
Run in Background
Simulation Criteria
Saved Variants:
Delete
Additional Criteria:
□ Exclude Values
□ Risk from Simulation only
Actions
Roles
Profiles
Add
Remove
Permission
Filter Settings
System
Action From
Action To
MIT Logical System for PS1:030
MIT Logical System for SF2:030
MIT Logical System for SF3:030
MIT Logical System for SH2:030
Save Variant as:

15A-3	Add the transaction. In this case, 'PT60' was typed in. The search option can also be used to search for an Action. Please refer to the 'Search for Input Values' reference document (R3) for further information. NOTE: If transactions should be excluded from the User's authorization for the simulation, the 'Exclude Values' box must be checked. Otherwise, any added transactions will be added to the User's authorizations for the simulation.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

1 Define Analysis Criteria — 2 **Define Simulation Criteria** — 3 Confirmation

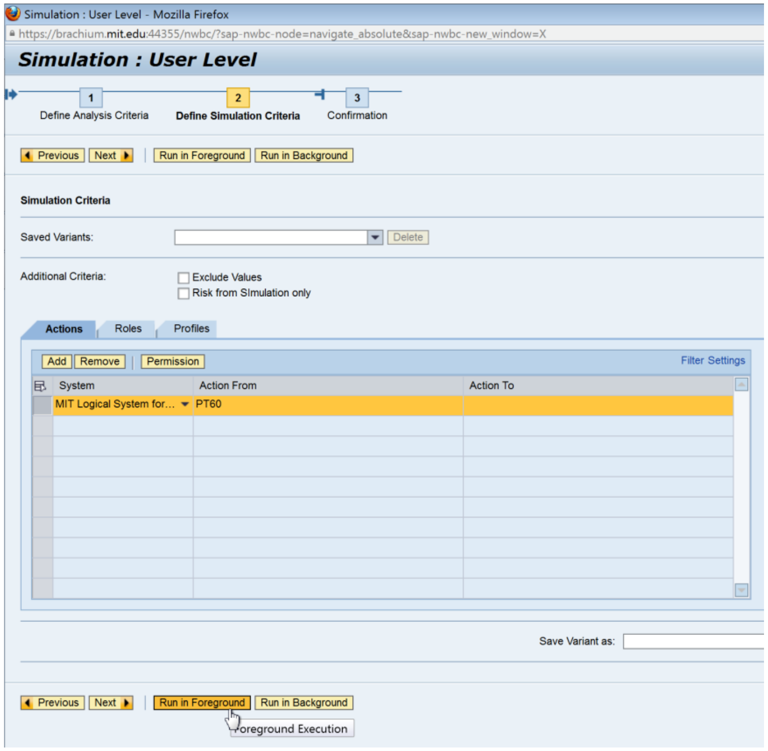
Simulation Criteria

Saved Variants:

Additional Criteria:
□ Exclude Values
□ Risk from Simulation only

System	Action From	Action To
MIT Logical System for...	PT60	

Save Variant as:

15A-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

Simulation Criteria

Saved Variants:

Additional Criteria:
☐ Exclude Values
☐ Risk from Simulation only

System	Action From	Action To
MIT Logical System for...	PT60	

Save Variant as:

15A-5

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

Any orange line items represent risks occuring due to simulation criteria.

User ID: User ID of the user with a Risk that has been mitigated

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Last Executed On: Date of last execution of transaction

Execution Count: Number of times transaction was executed for a specified time period

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

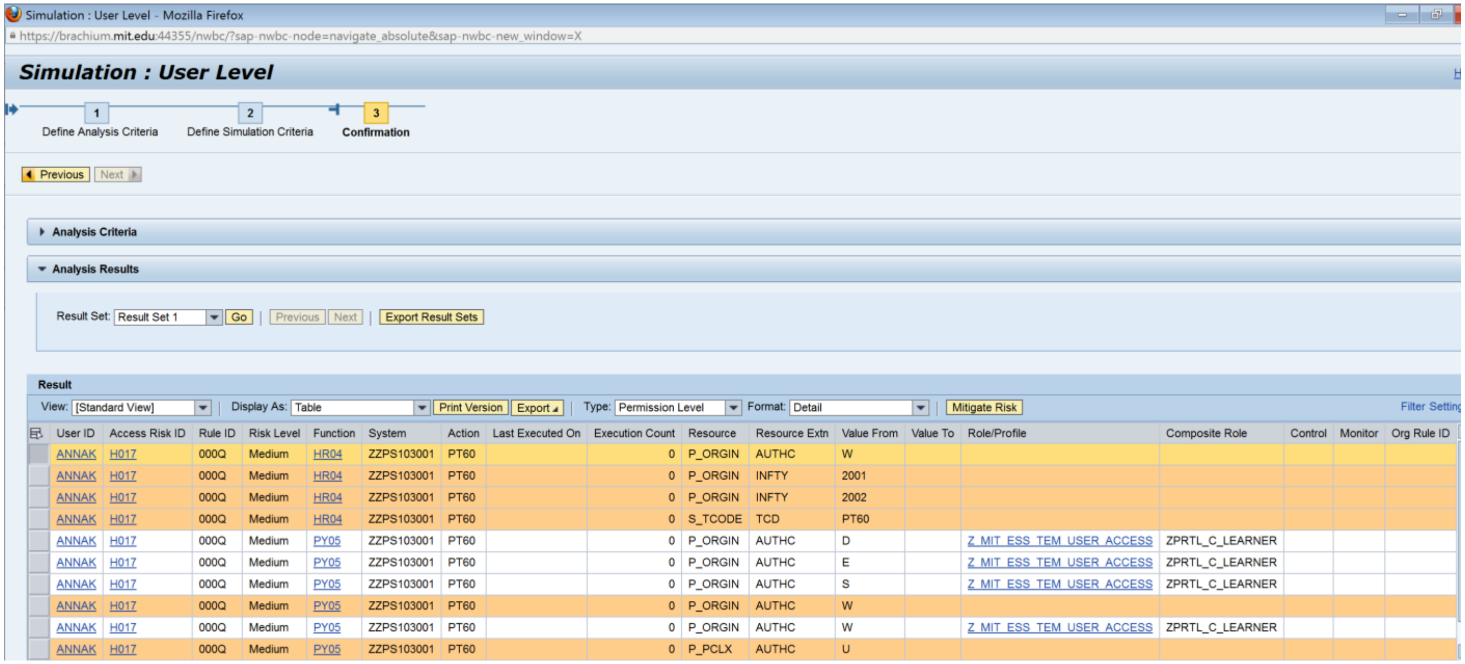
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

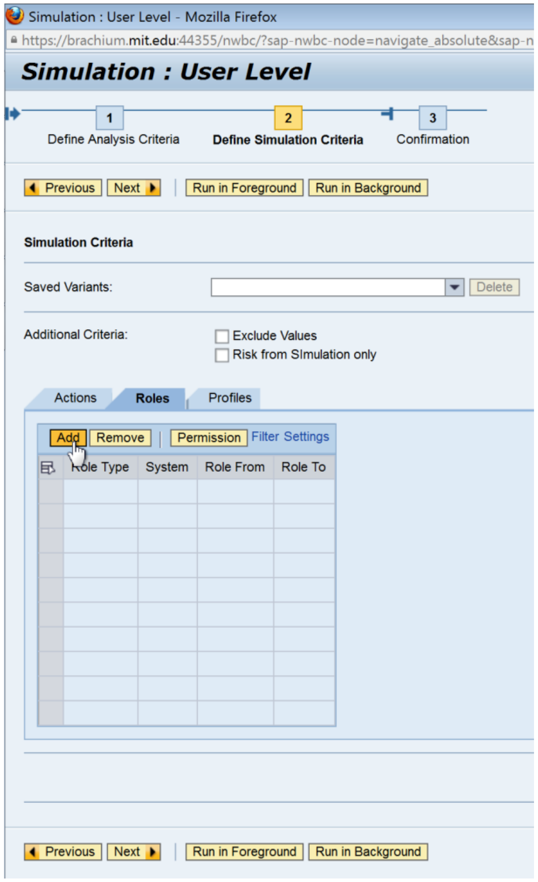
Monitor: The user ID of the Monitor responsible for the Mitigating Control

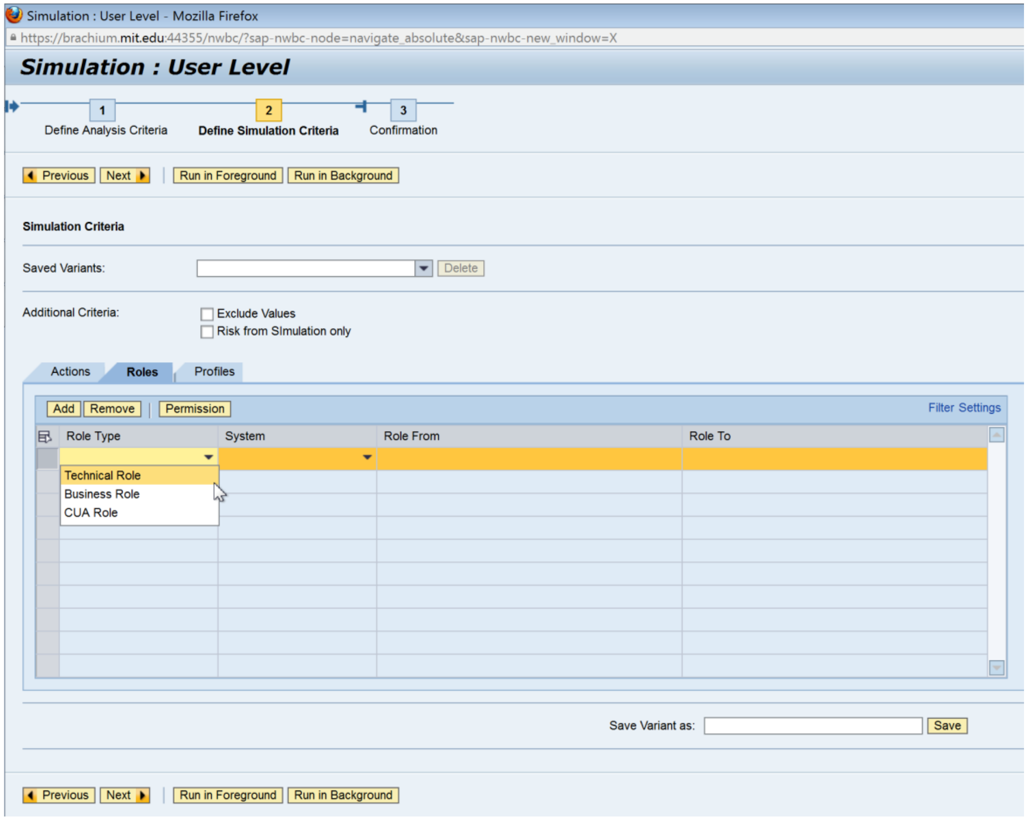


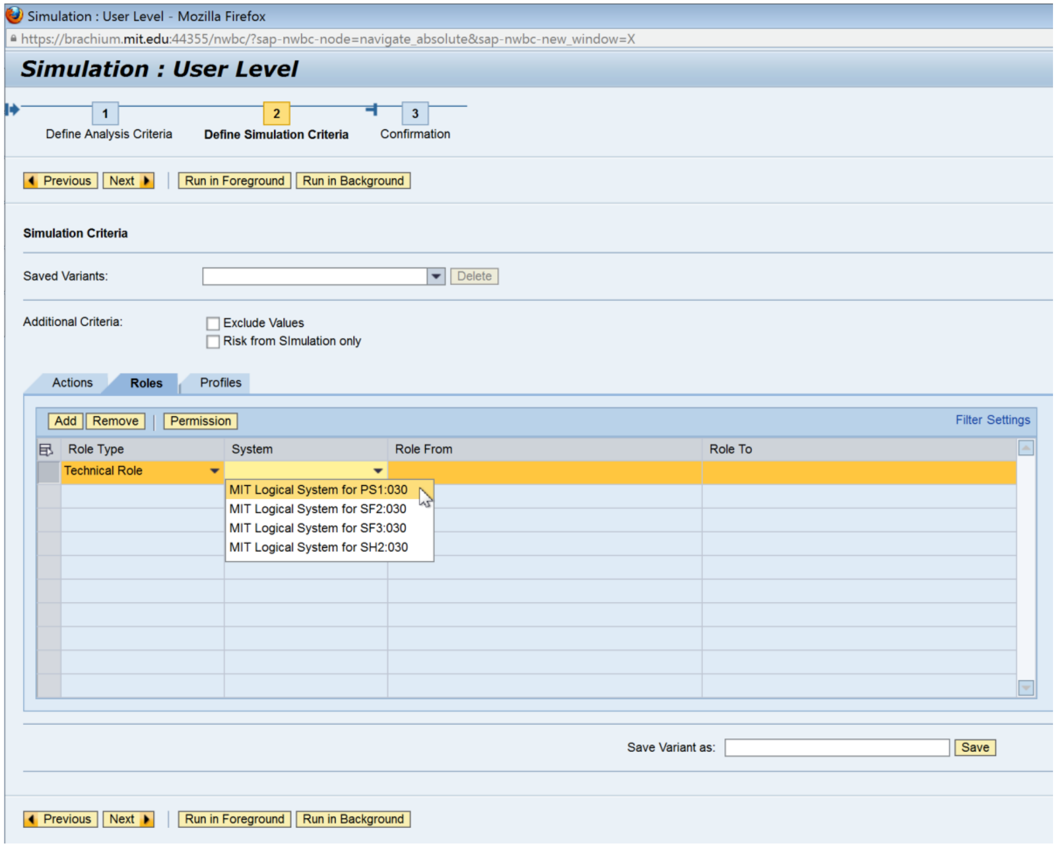
Result Set: Result Set 1

View: [Standard View]
Display As: Table
Type: Permission Level
Format: Detail

User ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
ANNAK	H017	000Q	Medium	HR04	ZZPS103001	PT60		0	P_ORGIN	AUTHC	W						
ANNAK	H017	000Q	Medium	HR04	ZZPS103001	PT60		0	P_ORGIN	INFTY	2001						
ANNAK	H017	000Q	Medium	HR04	ZZPS103001	PT60		0	P_ORGIN	INFTY	2002						
ANNAK	H017	000Q	Medium	HR04	ZZPS103001	PT60		0	S_TCODE	TCD	PT60						
ANNAK	H017	000Q	Medium	PY05	ZZPS103001	PT60		0	P_ORGIN	AUTHC	D		Z_MIT_ESS_TEM_USER_ACCESS	ZPRTL_C_LEARNER			
ANNAK	H017	000Q	Medium	PY05	ZZPS103001	PT60		0	P_ORGIN	AUTHC	E		Z_MIT_ESS_TEM_USER_ACCESS	ZPRTL_C_LEARNER			
ANNAK	H017	000Q	Medium	PY05	ZZPS103001	PT60		0	P_ORGIN	AUTHC	S		Z_MIT_ESS_TEM_USER_ACCESS	ZPRTL_C_LEARNER			
ANNAK	H017	000Q	Medium	PY05	ZZPS103001	PT60		0	P_ORGIN	AUTHC	W						
ANNAK	H017	000Q	Medium	PY05	ZZPS103001	PT60		0	P_ORGIN	AUTHC	W		Z_MIT_ESS_TEM_USER_ACCESS	ZPRTL_C_LEARNER			
ANNAK	H017	000Q	Medium	PY05	ZZPS103001	PT60		0	P_PCLX	AUTHC	U						

15B-1	Simulation by Role. On the ‘Roles’ tab, click on ‘Add’ to define role simulation criteria.	

15B-2	Click the drop down on the ‘Role Type’ field and select ‘Technical Role’. For role-based simulation criteria, unless otherwise advised, the selection will always be ‘Technical Role’.	

15B-3	Click the drop down on the 'System' field and select the system from which a technical role must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

1 Define Analysis Criteria | 2 Define Simulation Criteria | 3 Confirmation

Previous | Next | Run in Foreground | Run in Background

Simulation Criteria

Saved Variants: [ ] Delete

Additional Criteria: □ Exclude Values
□ Risk from Simulation only

Actions | **Roles** | Profiles

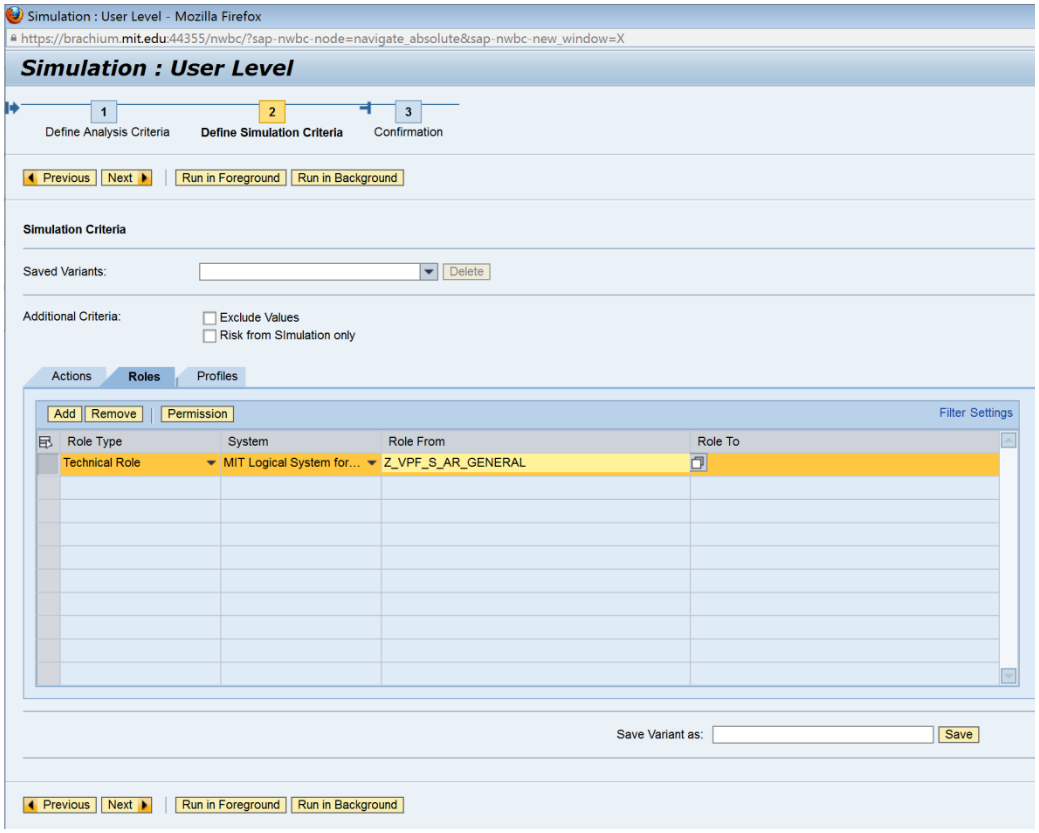
Add | Remove | Permission | Filter Settings

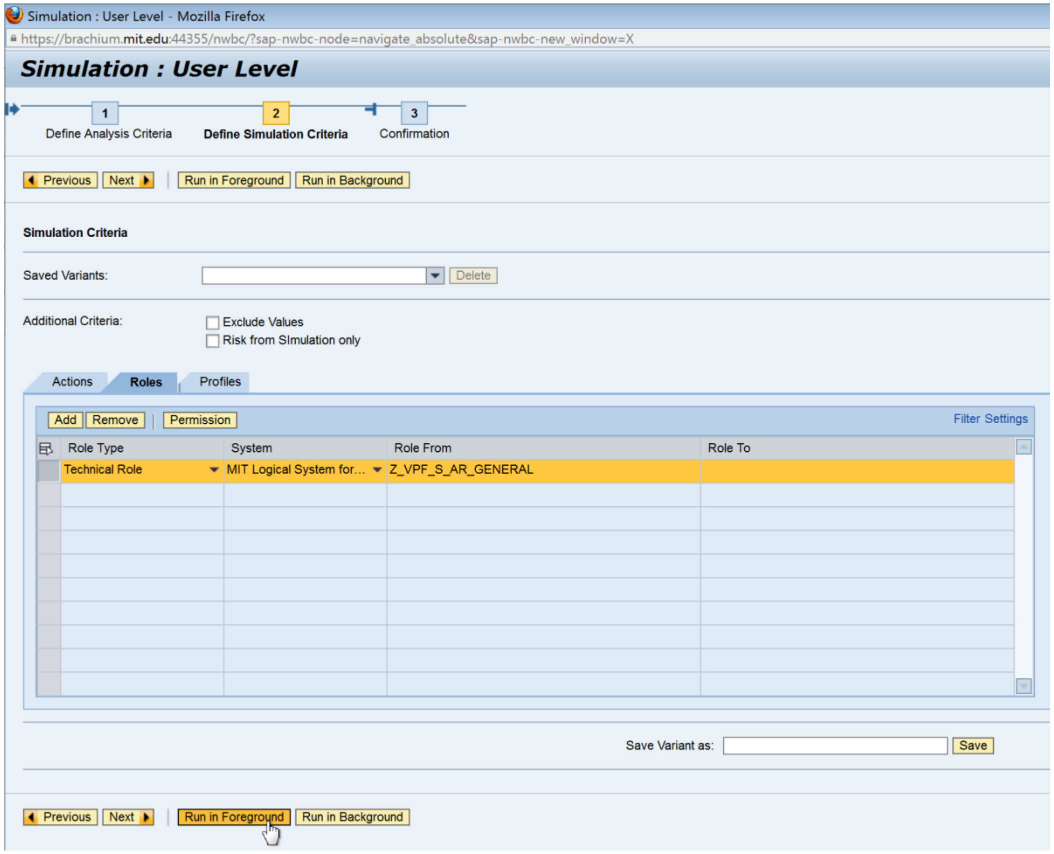
Role Type	System	Role From	Role To
Technical Role			

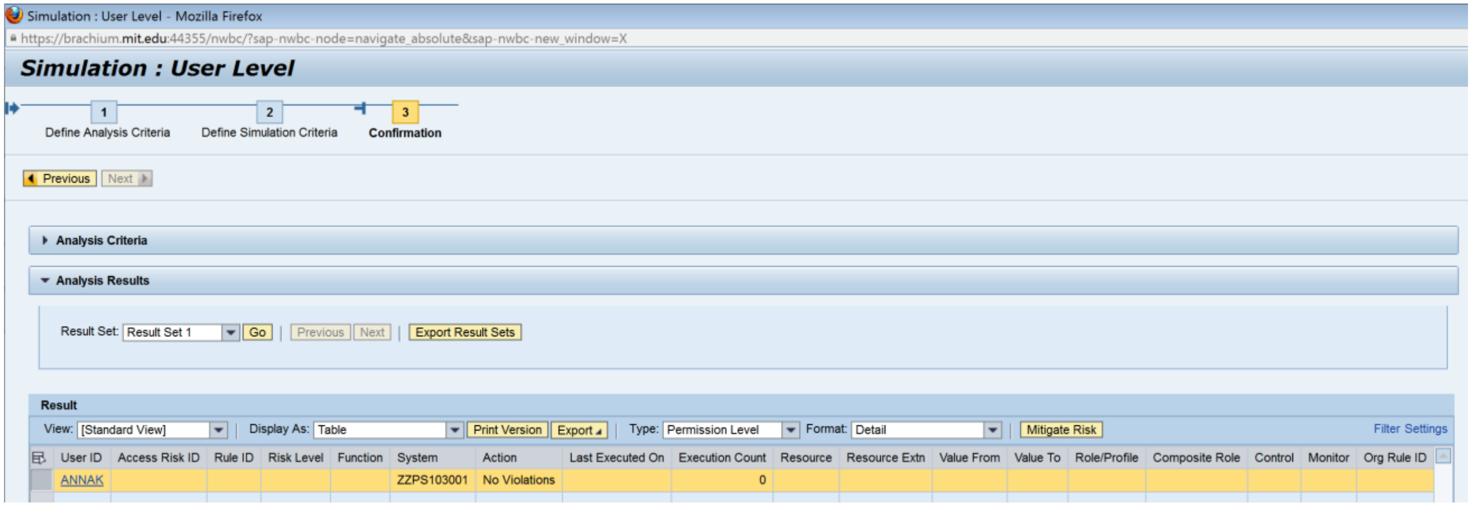
MIT Logical System for PS1:030
MIT Logical System for SF2:030
MIT Logical System for SF3:030
MIT Logical System for SH2:030

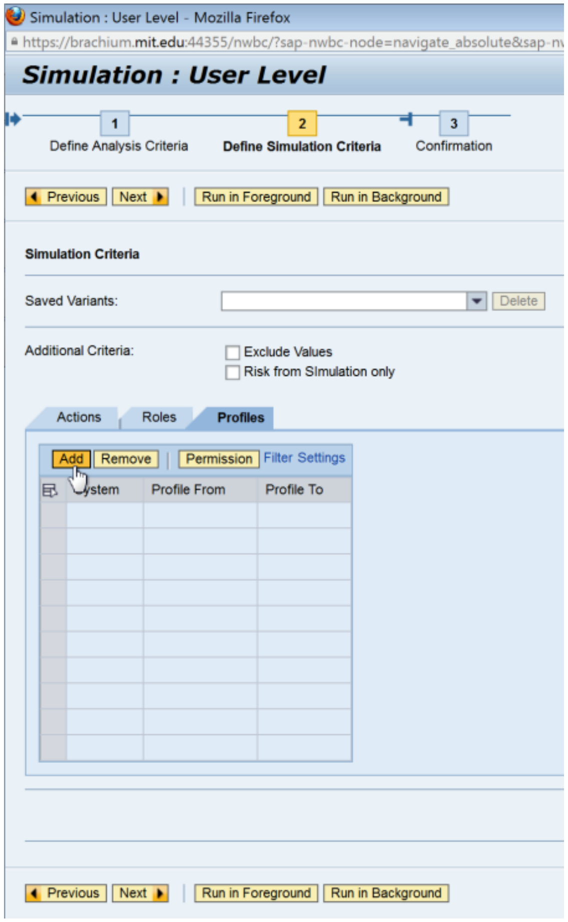
Save Variant as: [ ] Save

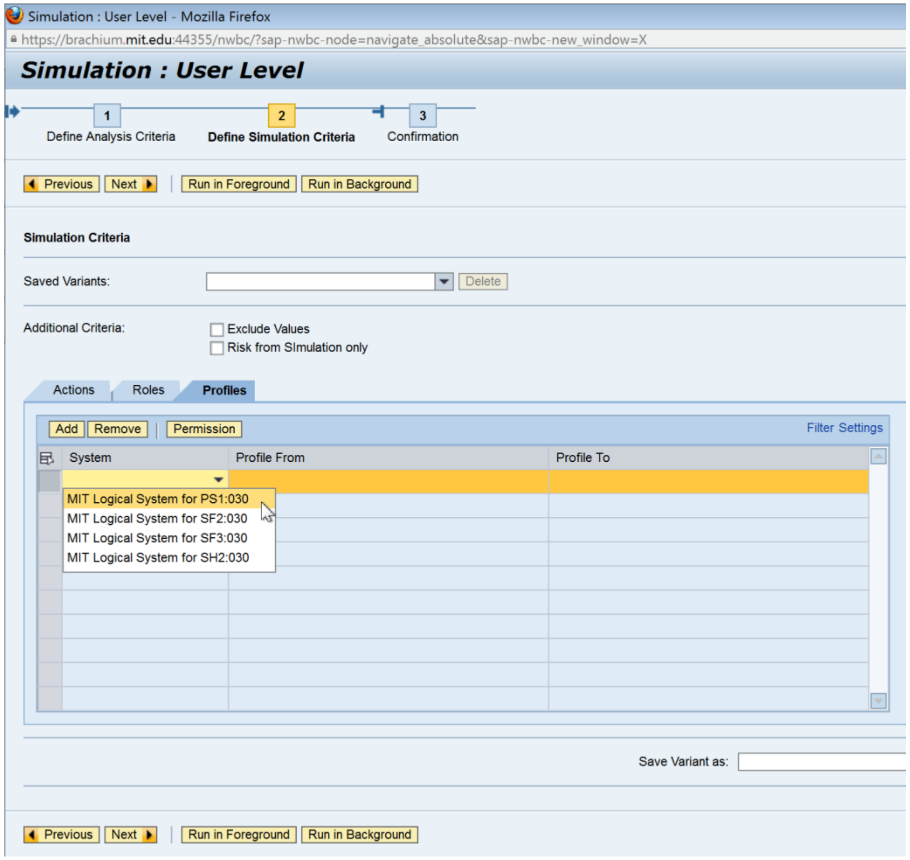
Previous | Next | Run in Foreground | Run in Background

15B-4	Add the role. In this case, 'Z_VPF_S_AR_GENERAL' was typed in. The search option can also be used to search for a Role. Please refer to the 'Search for Input Values' reference document (R3) for further information. NOTE: If roles should be excluded from the User's authorization for the simulation, the 'Exclude Values' box must be checked. Otherwise, any added roles will be added to the User's authorizations for the simulation.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : User Level** 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation Previous Next Run in Foreground Run in Background Simulation Criteria Saved Variants: [ ] Delete Additional Criteria: □ Exclude Values □ Risk from Simulation only Actions **Roles** Profiles Add Remove Permission Filter Settings Role Type | System | Role From | Role To Technical Role | MIT Logical System for... | Z_VPF_S_AR_GENERAL | Save Variant as: [ ] Save Previous Next Run in Foreground Run in Background

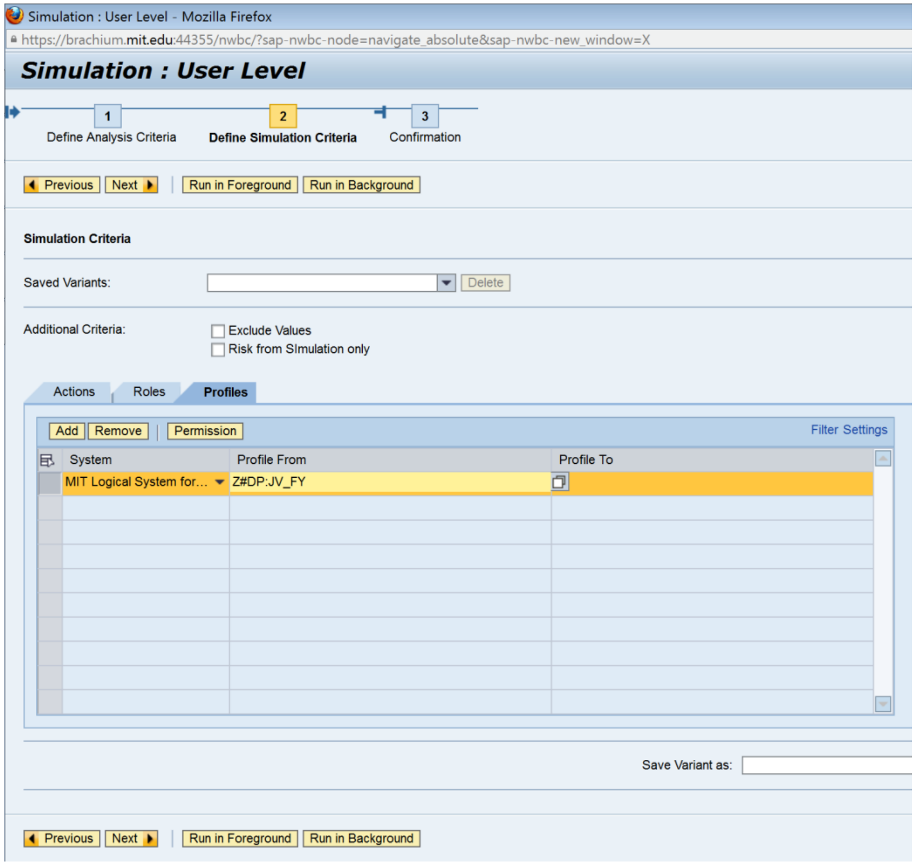
15B-5	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : User Level 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Simulation Criteria Saved Variants: Additional Criteria: ☐ Exclude Values ☐ Risk from Simulation only Role Type | System | Role From | Role To Technical Role | MIT Logical System for... | Z_VPF_S_AR_GENERAL | Save Variant as: Previous Next Run in Foreground Run in Background Delete Actions Roles Profiles Add Remove Permission Filter Settings Save Previous Next Run in Foreground Run in Background

<table>
<tr>
<td>15B-6</td>
<td>Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.
Any orange line items represent risks occuring due to simulation criteria.
User ID: User ID of the user with a Risk that has been mitigated
Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist
Rule ID: The ID representing the particular rule that was triggered for that Risk
Risk Level: The risk level defined for each Access Risk in the standard rule set
Function: The ID representing the particular function that was triggered
System: The system in which the role is assigned to the user
Action: SAP transaction
Last Executed On: Date of last execution of transaction
Execution Count: Number of times transaction was executed for a specified time period
Resource: SAP authorization object
Resource Extn: SAP authorization object field
Value From: SAP authorization object field value (start value for a range)
Value To: SAP authorization object field value (end value for a range)
Role/Profile: The single role/profile causing the SOD
Composite Role: The composite role containing the SOD-causing single role (if any exist)
Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk
Monitor: The user ID of the Monitor responsible for the Mitigating Control</td>
<td>
Simulation : User Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Simulation : User Level
1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation
Previous | Next
Analysis Criteria
Analysis Results
Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets
Result
View: [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Detail | Mitigate Risk | Filter Settings
<table>
<tr><th>User ID</th><th>Access Risk ID</th><th>Rule ID</th><th>Risk Level</th><th>Function</th><th>System</th><th>Action</th><th>Last Executed On</th><th>Execution Count</th><th>Resource</th><th>Resource Extn</th><th>Value From</th><th>Value To</th><th>Role/Profile</th><th>Composite Role</th><th>Control</th><th>Monitor</th><th>Org Rule ID</th></tr>
<tr><td>ANNAK</td><td></td><td></td><td></td><td></td><td>ZZPS103001</td><td>No Violations</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td>
</tr>
</table>

15C-1	Simulation by Profile. On the 'Profiles' tab, click on 'Add' to define profile simulation criteria.	 Simulation : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nv Simulation : User Level 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next · Run in Foreground · Run in Background Simulation Criteria Saved Variants: · Delete Additional Criteria: ☐ Exclude Values ☐ Risk from Simulation only Actions · Roles · Profiles Add · Remove · Permission · Filter Settings System · Profile From · Profile To Previous · Next · Run in Foreground · Run in Background

15C-2	Click the drop down on the 'System' field and select the system from which a profile must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	

Simulation : User Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Simulation : User Level
1 Define Analysis Criteria
2 Define Simulation Criteria
3 Confirmation
Previous
Next
Run in Foreground
Run in Background
Simulation Criteria
Saved Variants:
Delete
Additional Criteria:
□ Exclude Values
□ Risk from SImulation only
Actions
Roles
Profiles
Add
Remove
Permission
Filter Settings
System
Profile From
Profile To
MIT Logical System for PS1:030
MIT Logical System for SF2:030
MIT Logical System for SF3:030
MIT Logical System for SH2:030
Save Variant as:
Previous
Next
Run in Foreground
Run in Background

15C-3	Add the profile. In this case, 'Z#DP:JV_FY' was typed in. The search option can also be used to search for a Profile. Please refer to the 'Search for Input Values' reference document (R3) for further information. NOTE: If profiles should be excluded from the User's authorization for the simulation, the 'Exclude Values' box must be checked. Otherwise, any added profiles will be added to the User's authorizations for the simulation.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

1 Define Analysis Criteria | 2 Define Simulation Criteria | 3 Confirmation

Previous | Next | Run in Foreground | Run in Background

Simulation Criteria

Saved Variants: | Delete

Additional Criteria: □ Exclude Values □ Risk from Simulation only

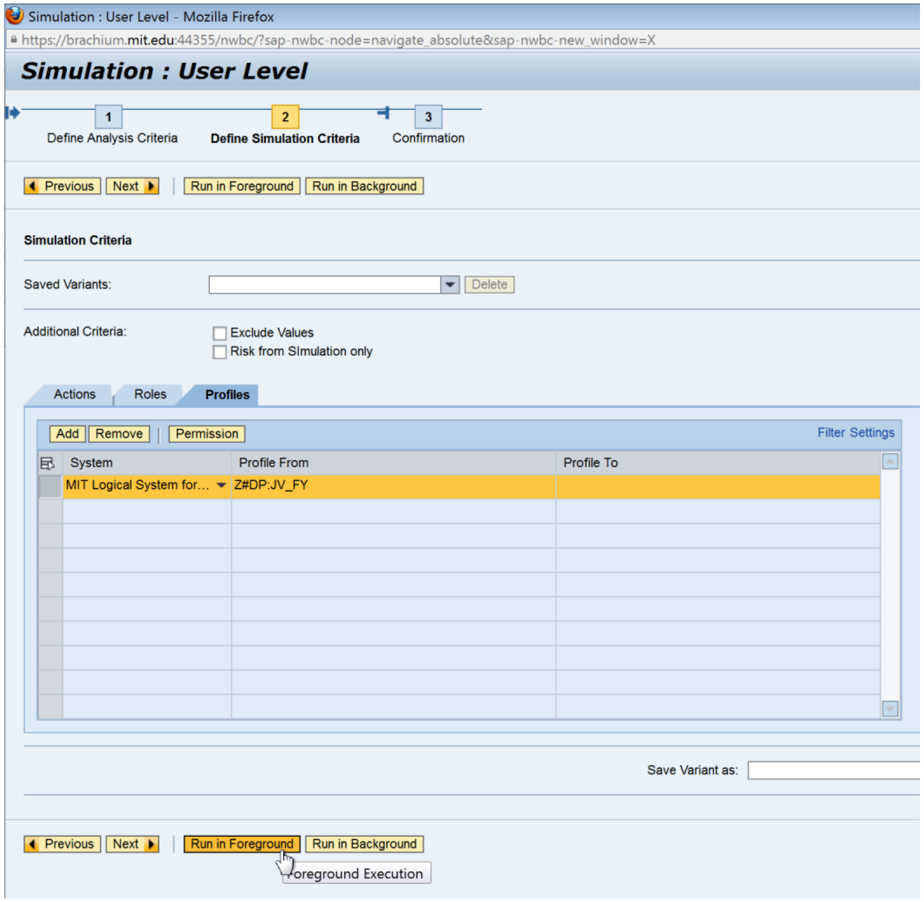
Actions | Roles | Profiles

Add | Remove | Permission | Filter Settings

System	Profile From	Profile To
MIT Logical System for...	Z#DP:JV_FY	

Save Variant as:

Previous | Next | Run in Foreground | Run in Background

15C-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	

Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

◀ Previous | Next ▶ | Run in Foreground | Run in Background

Simulation Criteria

Saved Variants: [ ] Delete

Additional Criteria: □ Exclude Values
 □ Risk from SImulation only

Actions | Roles | **Profiles**

Add | Remove | Permission — Filter Settings

System	Profile From	Profile To
MIT Logical System for...	Z#DP:JV_FY	

Save Variant as:

◀ Previous | Next ▶ | Run in Foreground | Run in Background

Foreground Execution

15C-5

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

Any orange line items represent risks occuring due to simulation criteria.

User ID: User ID of the user with a Risk that has been mitigated

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Last Executed On: Date of last execution of transaction

Execution Count: Number of times transaction was executed for a specified time period

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

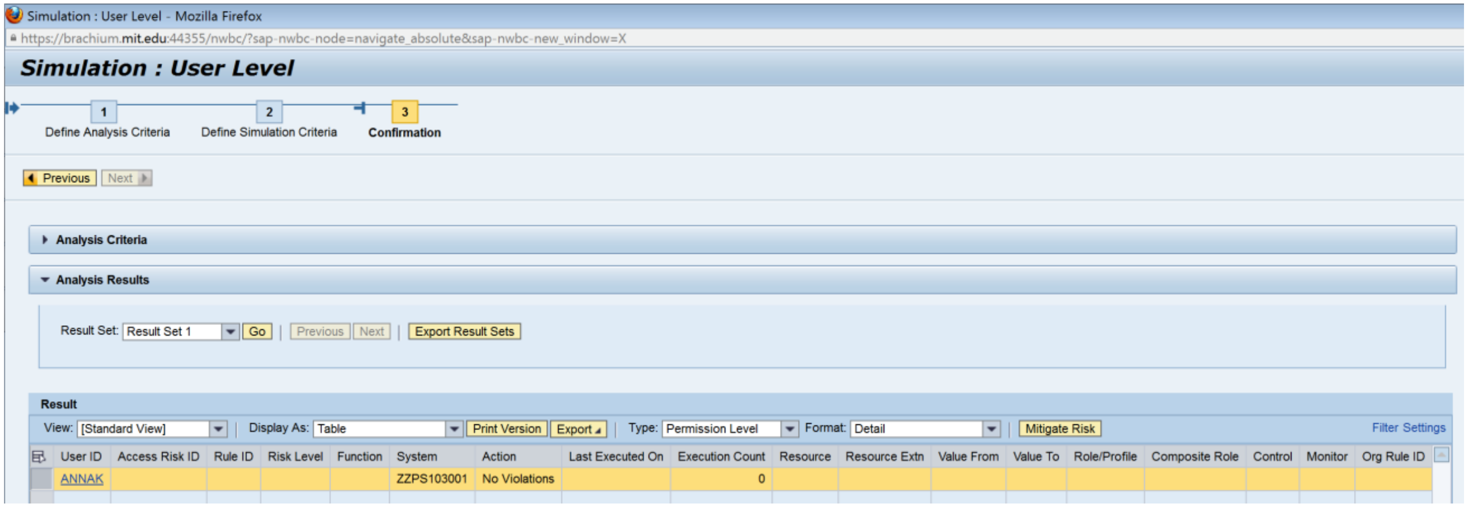
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control



Simulation : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : User Level

1 Define Analysis Criteria

2 Define Simulation Criteria

3 Confirmation

Result Set: Result Set 1

View: [Standard View] | Display As: Table | Type: Permission Level | Format: Detail

User ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
ANNAK					ZZPS103001	No Violations		0									

Job Aid 14 Role Level

USE

This report can be used analyze for risk violations at the role level.

INFORMATION

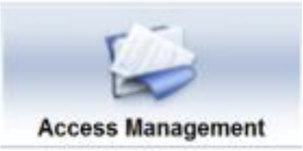
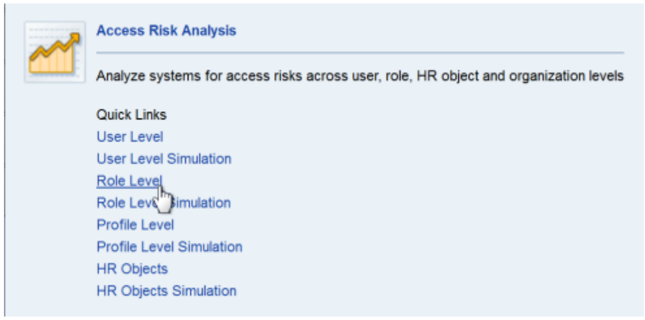
SODs, critical actions or permissions.

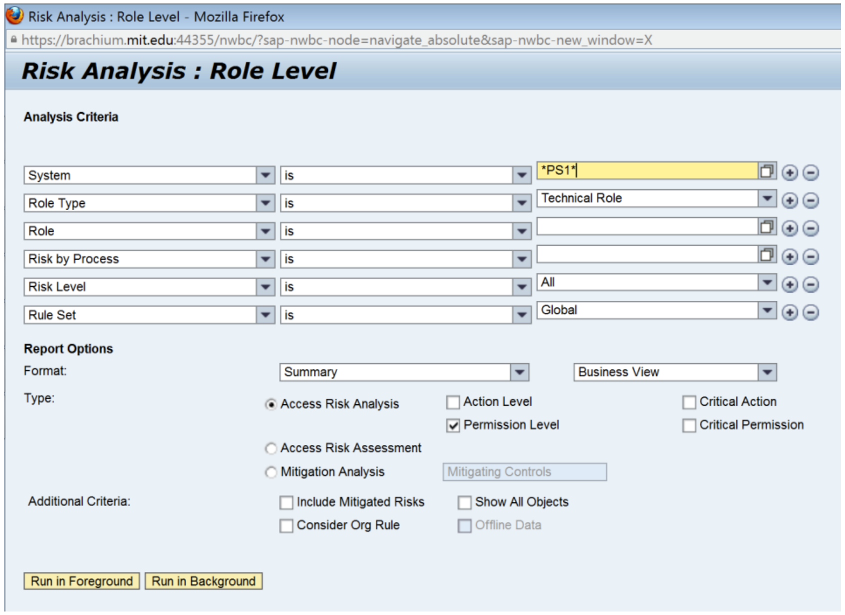
RELATED PROCESSES

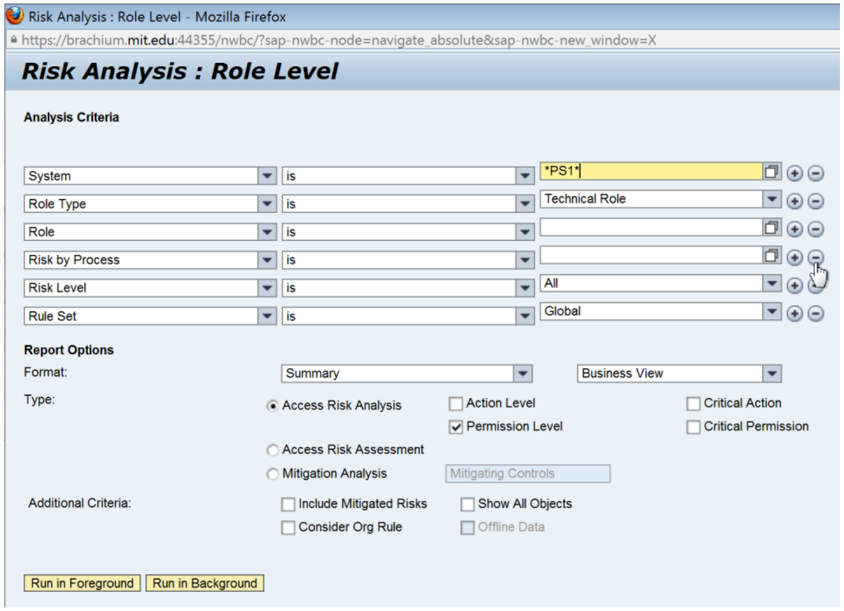
- Process 1: New or Amended Roles
- Process 2: Mitigation Analysis

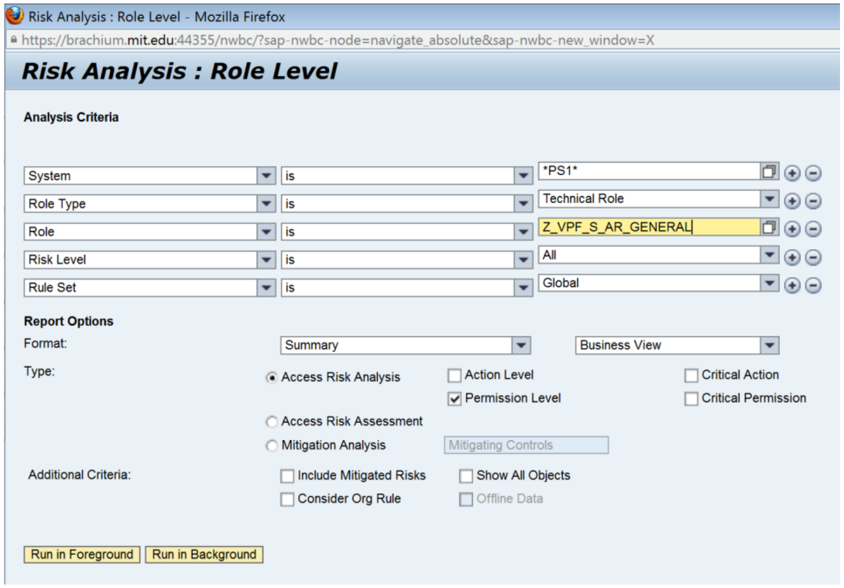
SPECIFIC SCENARIOS

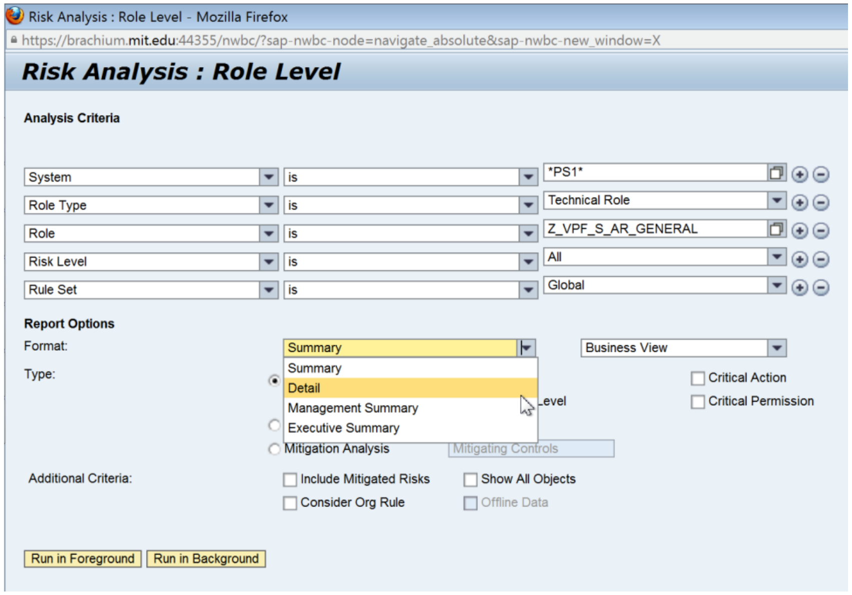
- N/A

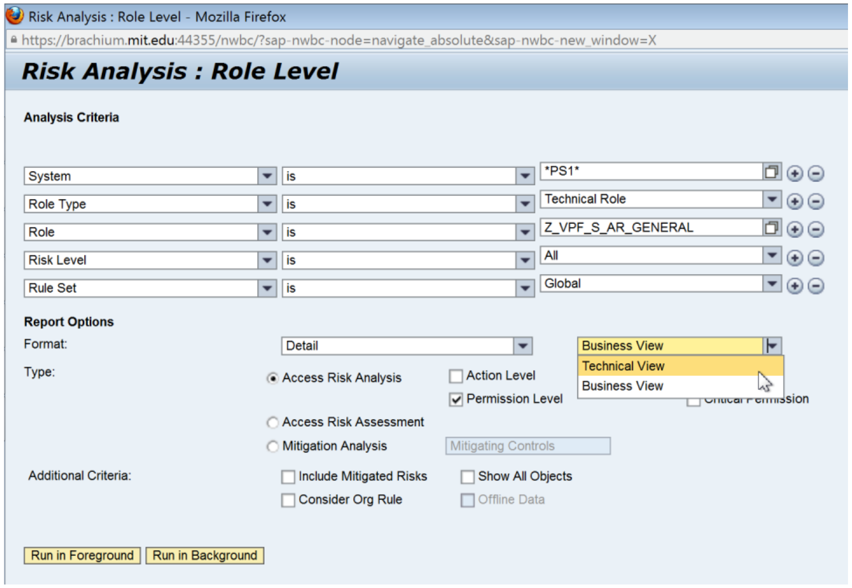
Step	Description	Screenshot
1	Navigate to the 'Access Management' tab.	 Access Management
2	Click on the 'Role Level' report located in the 'Access Risk Analysis' section.	 Access Risk Analysis Analyze systems for access risks across user, role, HR object and organization levels Quick Links User Level User Level Simulation Role Level Role Level Simulation Profile Level Profile Level Simulation HR Objects HR Objects Simulation

3	In the ‘Analysis Criteria’ section, select the System for which information is required. Since the desired selection is PS1 (Production), ‘*PS1*’ was typed in as the system. The search option can also be used to search for the correct system. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Risk Analysis : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : Role Level Analysis Criteria System is *PS1* Role Type is Technical Role Role is Risk by Process is Risk Level is All Rule Set is Global Report Options Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☐ Critical Action ☑ Permission Level ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

4	Analysis for a single techinical role. In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘Risk by Process’ row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Risk Analysis : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Role Level** **Analysis Criteria** System is *PS1* Role Type is Technical Role Role is Risk by Process is Risk Level is All Rule Set is Global **Report Options** Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☐ Critical Action ☑ Permission Level ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

5	Add the Role. In this case, 'Z_VPF_S_AR_GENERAL' was typed in. The search option can also be used to search for a role. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Risk Analysis : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Role Level** **Analysis Criteria** System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk Level is All Rule Set is Global **Report Options** Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

6	In the 'Report Options' section, select the first drop down for 'Format' and select the level of detail at which information is required. In this case, 'Detail' was selected so that the report will show information about why Risks exists.	 Risk Analysis : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : Role Level Analysis Criteria System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk Level is All Rule Set is Global Report Options Format: Summary Business View Summary Detail Management Summary Executive Summary Type: ● Level □ Critical Action □ Critical Permission ○ ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

7	In the 'Report Options' section, select the second drop down for 'Format' and select the type of information that is required. In this case, 'Technical View' was selected so that the report will show technical information about why Risks exists.	

Risk Analysis : Role Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Risk Analysis : Role Level

Analysis Criteria

System	is	*PS1*
Role Type	is	Technical Role
Role	is	Z_VPF_S_AR_GENERAL
Risk Level	is	All
Rule Set	is	Global

Report Options

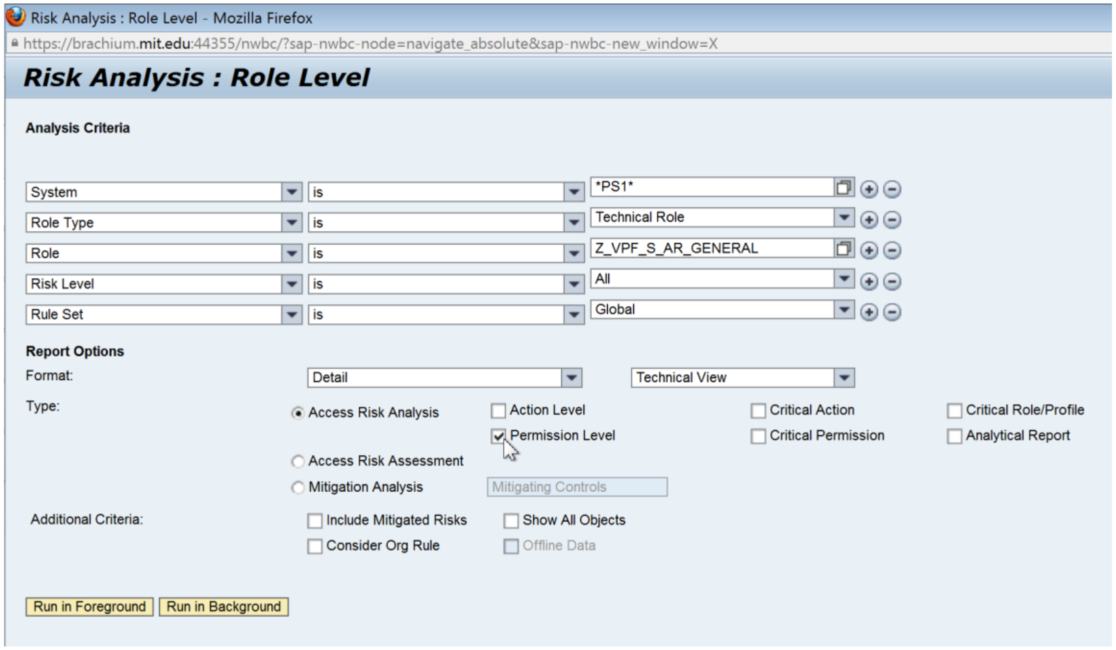
Format: Detail | Business View

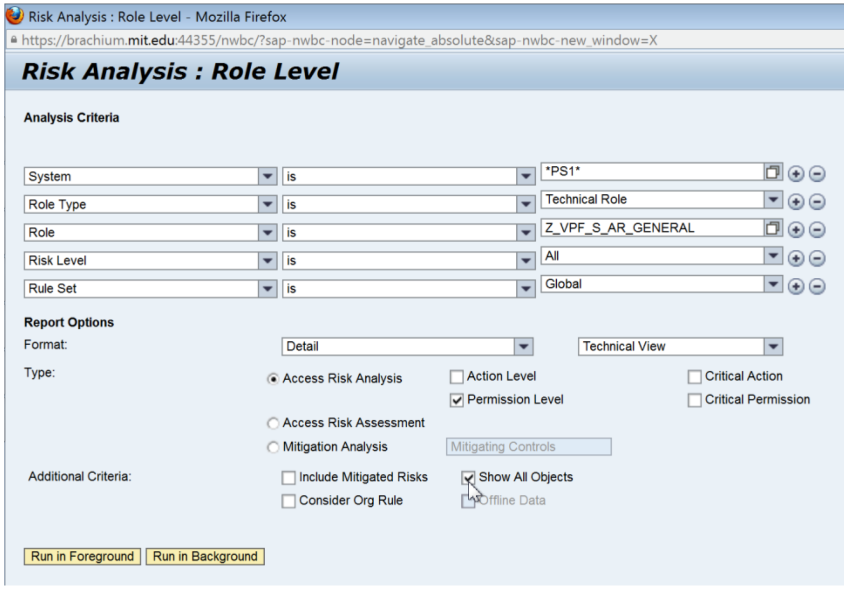
Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Permission

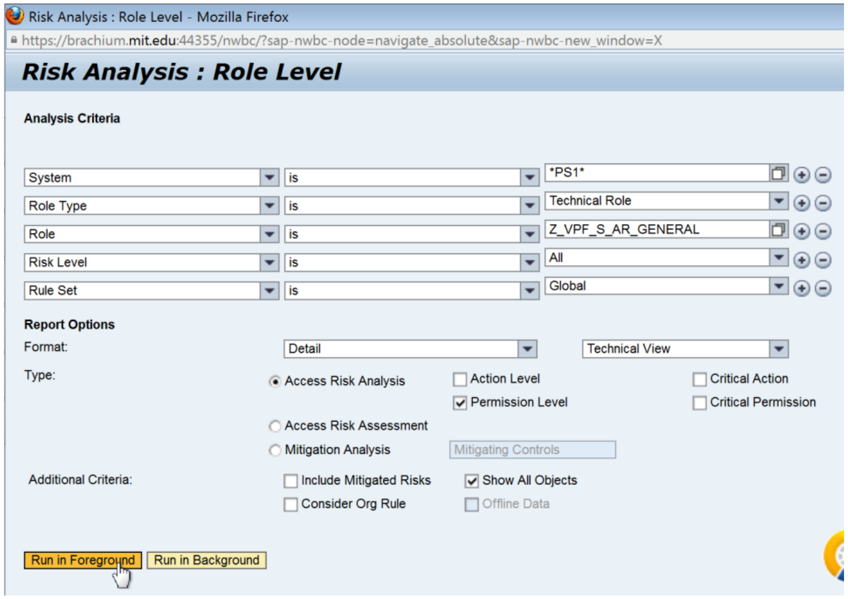
○ Access Risk Assessment

○ Mitigation Analysis Mitigating Controls

Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data

8	Analyze for SODs based on user ID. In the 'Report Options' section, select the first dial button for 'Access Risk Analysis'. Next, select the type of analysis that is required. The options available are: Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level) Permission Level: SODs at the authorization level Critical Action: Critical transactions that limited/no users should have Critical Permission: Critical authorizations that limited/no users should have Critical Role/Profile: Critical Roles/Profiles that limited/no users should have In this case, 'Permission Level' was selected so that the report will show SODs that exist at the Permission Level.	 Risk Analysis : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Role Level** Analysis Criteria System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk Level is All Rule Set is Global Report Options Format: Detail Technical View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission □ Critical Role/Profile □ Analytical Report ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background

9	In the ‘Report Options’ section, check ‘Show All Objects’ under ‘Additional Criteria’. This will ensure that Users with no violations are explicitly listed as such (i.e. ‘No Violations’ will be listed as a line item for such users’ IDs).	 Risk Analysis : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Role Level** **Analysis Criteria** System · is · *PS1* Role Type · is · Technical Role Role · is · Z_VPF_S_AR_GENERAL Risk Level · is · All Rule Set · is · Global **Report Options** Format: Detail · Technical View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis · Mitigating Controls Additional Criteria: □ Include Mitigated Risks · ☑ Show All Objects · □ Consider Org Rule · □ Offline Data Run in Foreground · Run in Background

10	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Risk Analysis : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Role Level** **Analysis Criteria** System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk Level is All Rule Set is Global **Report Options** Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☐ Critical Action ☑ Permission Level ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background

<table>
<tr>
<td>11</td>
<td>Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

Role Name: SAP role name

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Resource: SAP authorization object

Resource Extn: SAP authorization object field

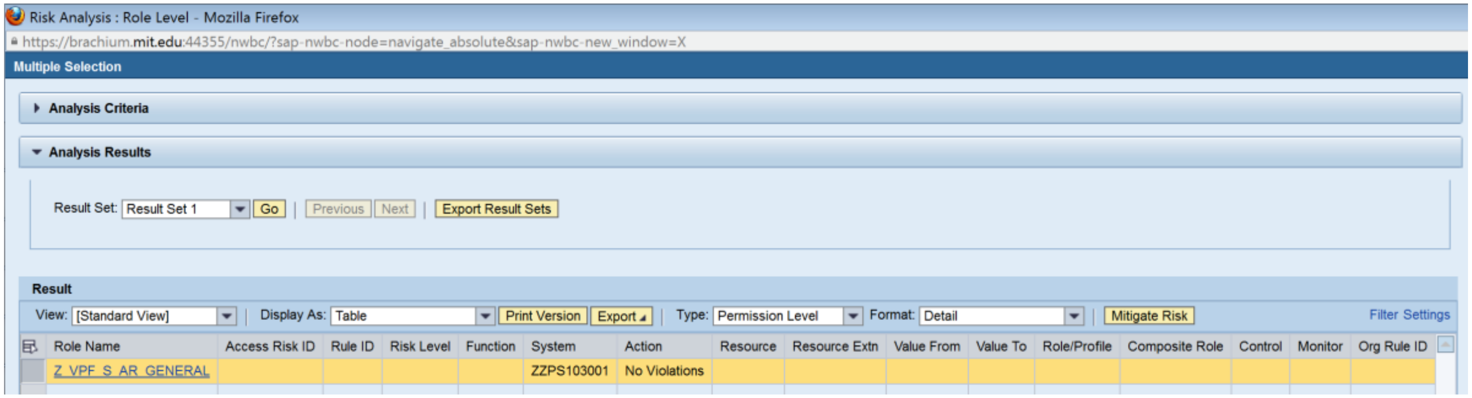
Value From: SAP authorization object field value (start value for a range)

Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control</td>
<td>

Risk Analysis : Role Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Multiple Selection
Analysis Criteria
Analysis Results
Result Set: Result Set 1

Result
View: [Standard View]
Display As: Table

Type: Permission Level
Format: Detail

<table>
<tr><th>Role Name</th><th>Access Risk ID</th><th>Rule ID</th><th>Risk Level</th><th>Function</th><th>System</th><th>Action</th><th>Resource</th><th>Resource Extn</th><th>Value From</th><th>Value To</th><th>Role/Profile</th><th>Composite Role</th><th>Control</th><th>Monitor</th><th>Org Rule ID</th></tr>
<tr><td>Z_VPF_S_AR_GENERAL</td><td></td><td></td><td></td><td></td><td>ZZPS103001</td><td>No Violations</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td>
</tr>
</table>

Job Aid 15 Role Level Simulation

USE

This report can be used carry out simulations at the role level for the purpose of understanding whether the addition or removal of certain access either creates or eliminates SODs and other risks.

INFORMATION

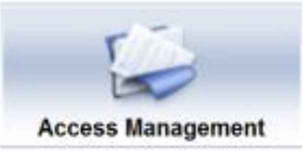
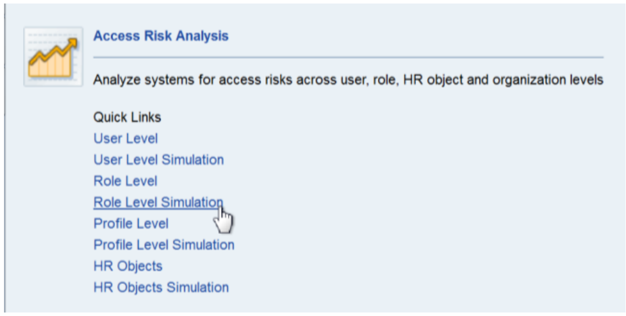
New risk violations that will result due to changes to roles.

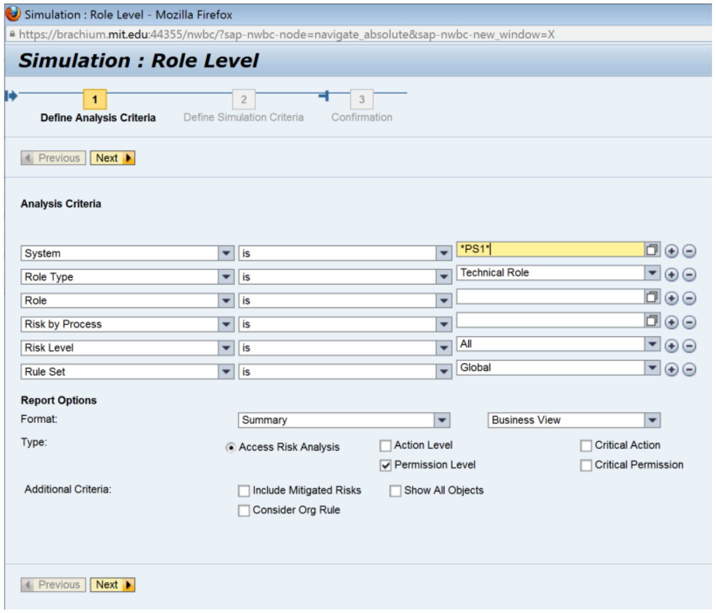
RELATED PROCESSES

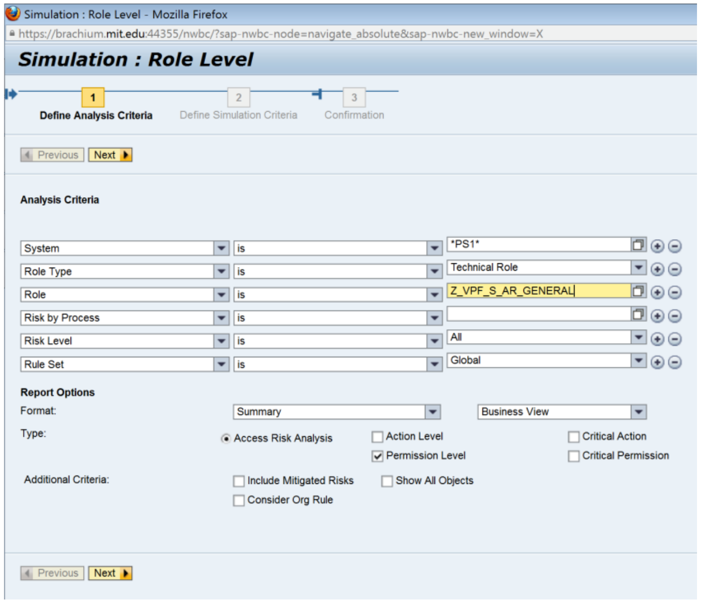
- Process 1: New or Amended Roles
- Process 2: Mitigation Analysis

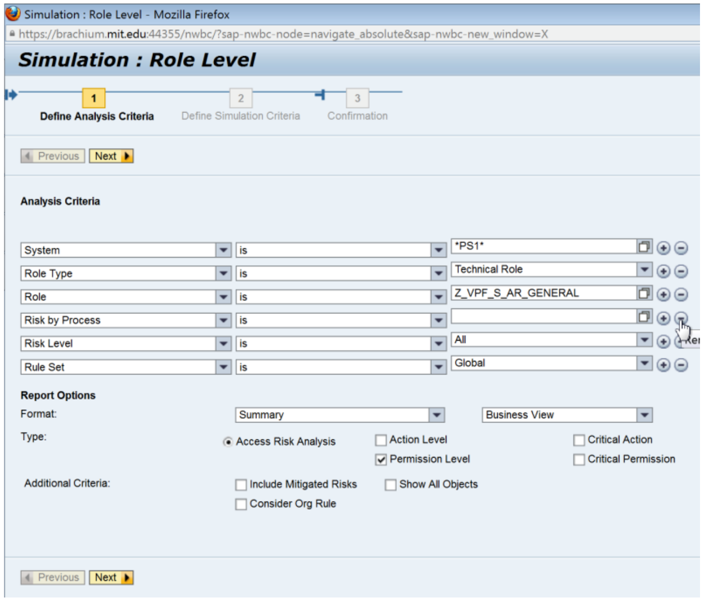
SPECIFIC SCENARIOS

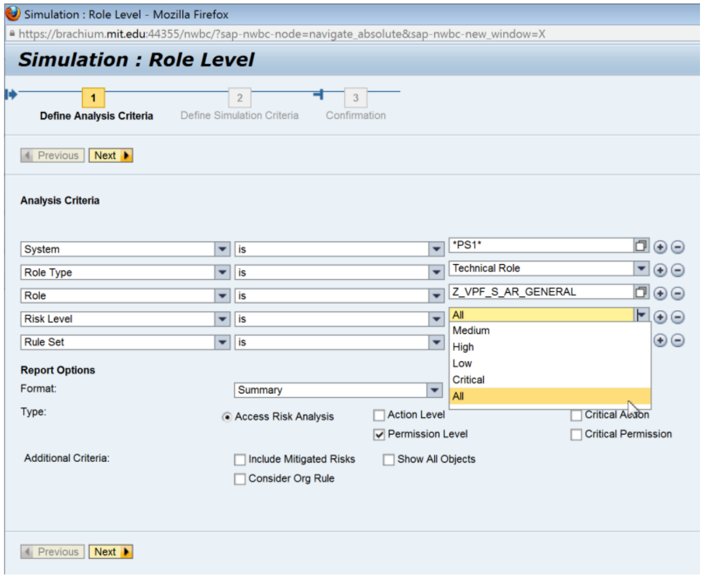
- Step 15A: Simulation by Action (transaction).
- Step 15B: Simulation by Role.
- Step 15C: Simulation by Profile.

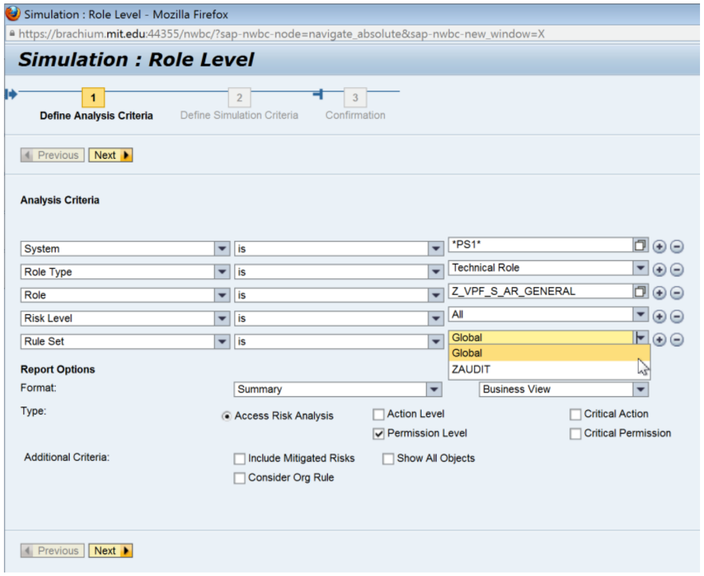
Step	Description	Screenshot
1	Navigate to the 'Access Management' tab.	
2	Click on the 'Role Level Simulation' report located in the 'Access Risk Analysis' section.	 Access Risk Analysis Analyze systems for access risks across user, role, HR object and organization levels Quick Links User Level User Level Simulation Role Level Role Level Simulation Profile Level Profile Level Simulation HR Objects HR Objects Simulation

3	In the 'Analysis Criteria' section, select the System for which information is required. Since the desired selection is PS1 (Production), '*PS1*' was typed in as the system. The search option can also be used to search for the correct system. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next **Analysis Criteria** System · is · *PS1* Role Type · is · Technical Role Role · is · Risk by Process · is · Risk Level · is · All Rule Set · is · Global **Report Options** Format: Summary · Business View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission Additional Criteria: □ Include Mitigated Risks · □ Show All Objects · □ Consider Org Rule Previous · Next

4	Run a simulation for a single Role. Add the Role. In this case, 'Z_VPF_S_AR_GENERAL' was typed in. The search option can also be used to search for an ID. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next **Analysis Criteria** System · is · *PS1* Role Type · is · Technical Role Role · is · Z_VPF_S_AR_GENERAL Risk by Process · is · Risk Level · is · All Rule Set · is · Global **Report Options** Format: · Summary · Business View Type: · ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission Additional Criteria: · □ Include Mitigated Risks · □ Consider Org Rule · □ Show All Objects Previous · Next

5	In the 'Analysis Criteria' section, click on the '-' at the end of the 'Risk by Process' row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : Role Level 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation Previous Next Analysis Criteria System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk by Process is Risk Level is All Rule Set is Global Report Options Format: Summary Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule Previous Next

7	In the 'Analysis Criteria' section, select the 'Risk Level' drop down and select the risk level for which information is required. In this case, 'All' was selected so that the report evaluates for all risk levels.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation ◀ Previous | Next ▶ **Analysis Criteria** System | is | *PS1* Role Type | is | Technical Role Role | is | Z_VPF_S_AR_GENERAL Risk Level | is | All (Medium, High, Low, Critical, All) Rule Set | is **Report Options** Format: Summary Type: ● Access Risk Analysis; □ Action Level; ☑ Permission Level; □ Critical Action; □ Critical Permission Additional Criteria: □ Include Mitigated Risks; □ Show All Objects; □ Consider Org Rule ◀ Previous | Next ▶

8	In the ‘Analysis Criteria’ section, select the ‘Rule Set’ drop down and select the Rule Set against which the report should be executed. In this case, ‘Global’, the MIT Rule Set, was selected. Unless advised otherwise, the selection should always be ‘Global’ for this report.	

Simulation : Role Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Role Level

Analysis Criteria

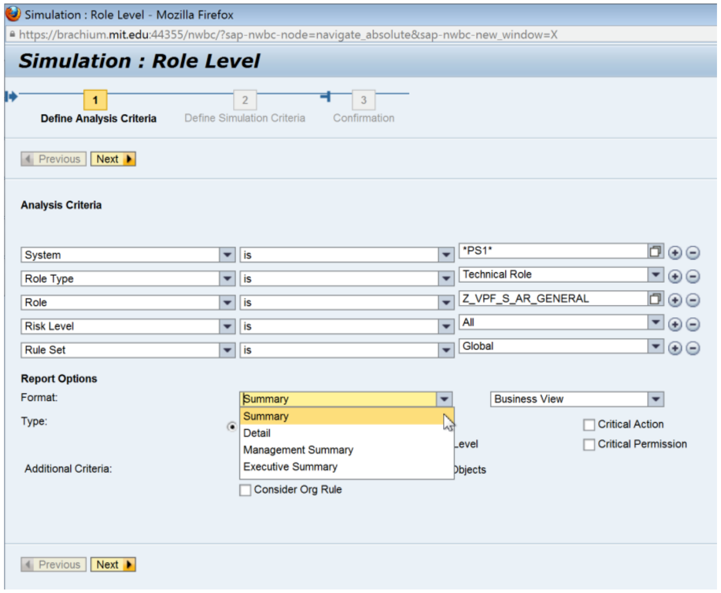
System	is	*PS1*
Role Type	is	Technical Role
Role	is	Z_VPF_S_AR_GENERAL
Risk Level	is	All
Rule Set	is	Global

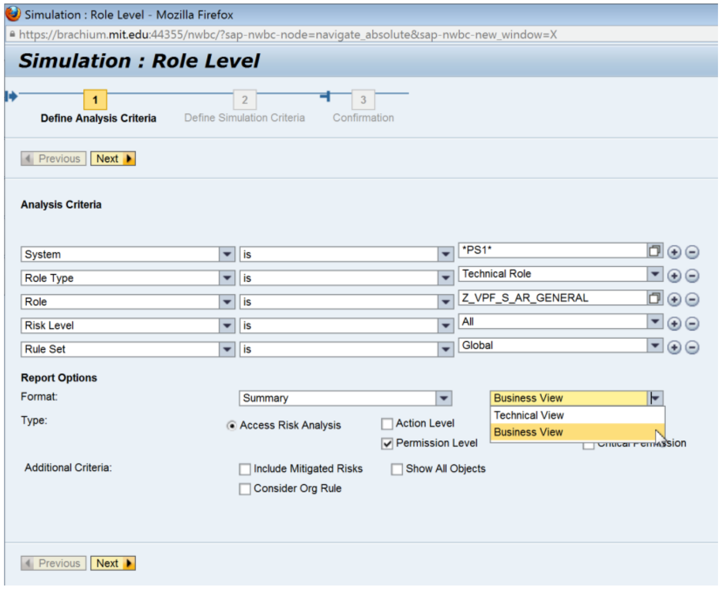
Report Options

Format: Summary | Business View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission

Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule

10	In the ‘Report Options’ section, select the first drop down for ‘Format’ and select the level of detail at which information is required. In this case, the default setting, ‘Summary’, was not changed.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Previous Next **Analysis Criteria** System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk Level is All Rule Set is Global **Report Options** Format: Summary (Summary, Detail, Management Summary, Executive Summary) Business View Type: ● …Level □ Critical Action □ Critical Permission Additional Criteria: …Objects □ Consider Org Rule Previous Next

11	In the 'Report Options' section, select the second drop down for 'Format' and select the type of information that is required. In this case, the default setting, 'Business View', was not changed.	

Simulation : Role Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Role Level

Analysis Criteria

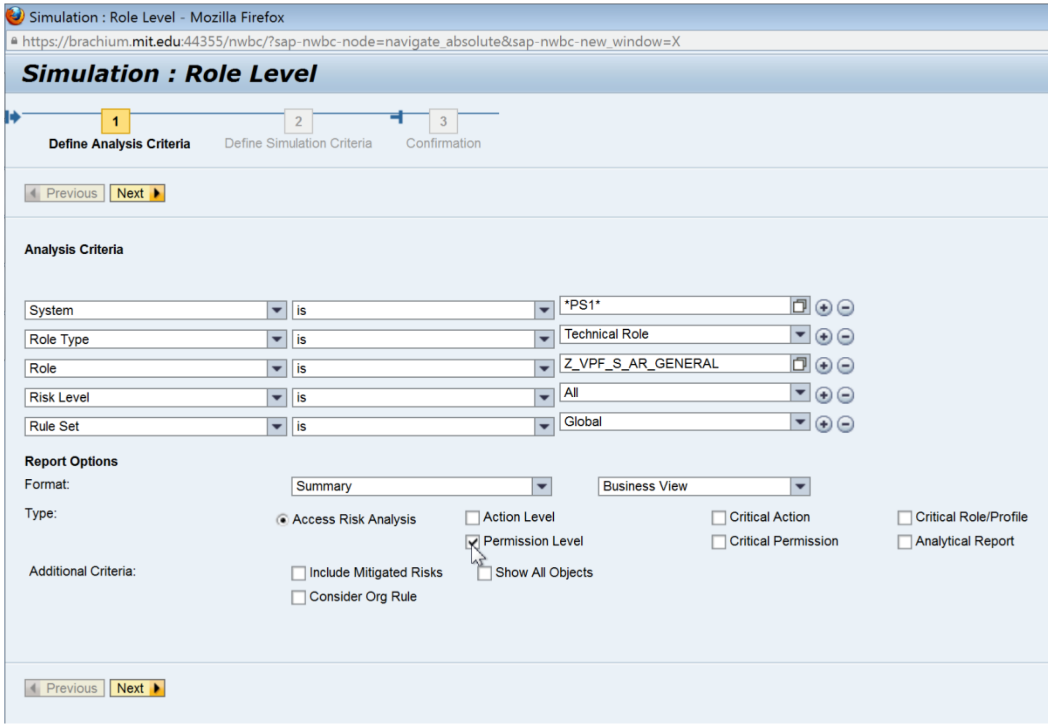
System	is	*PS1*
Role Type	is	Technical Role
Role	is	Z_VPF_S_AR_GENERAL
Risk Level	is	All
Rule Set	is	Global

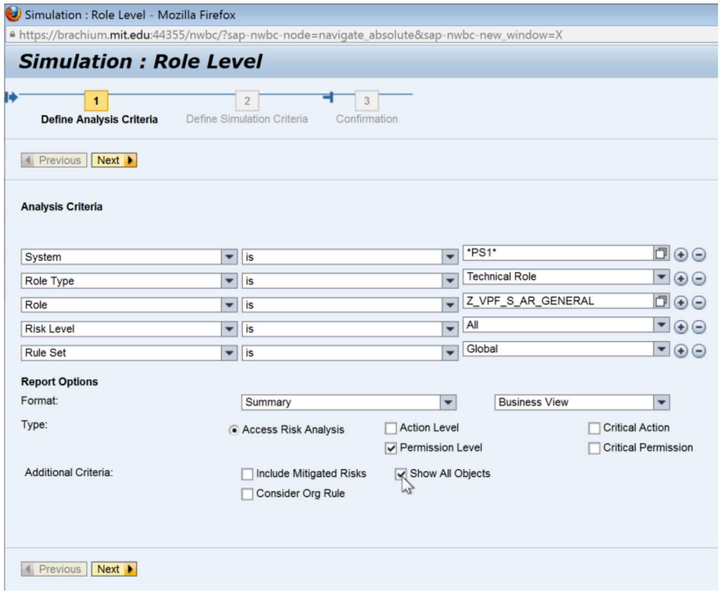
Report Options

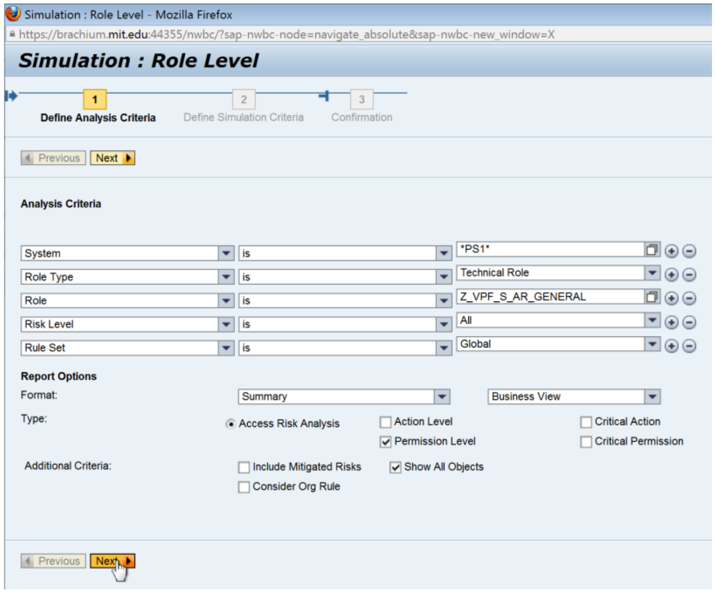
Format: Summary Business View

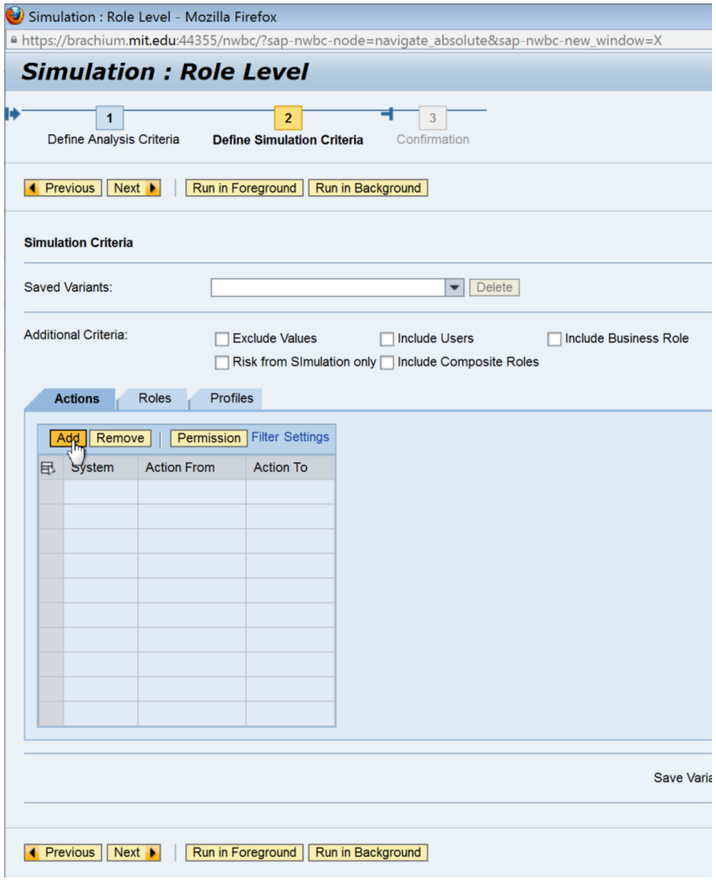
Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Permission

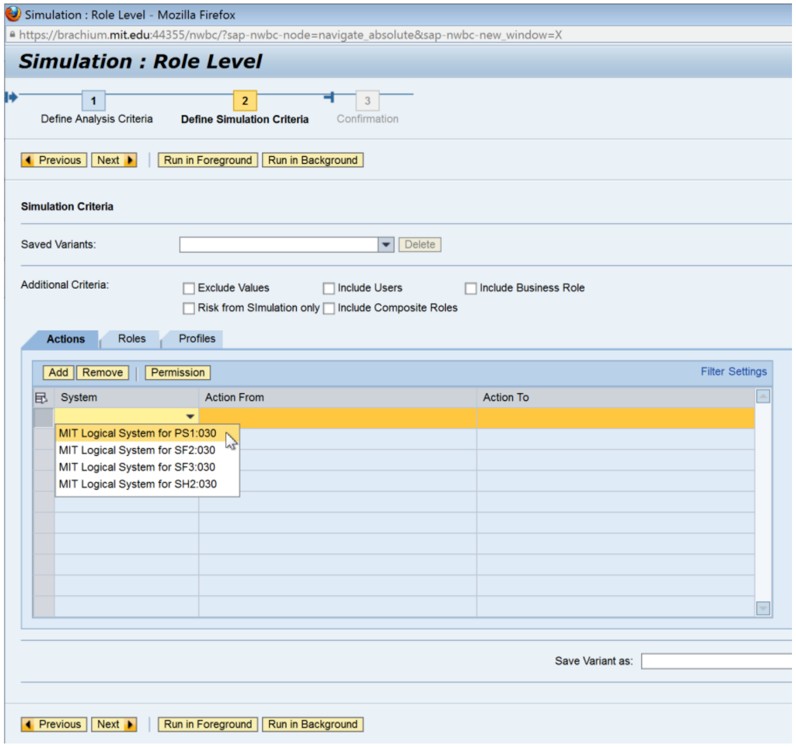
Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule

13	Analyze for SODs (excluding false positives). In the ‘Report Options’ section, select the dial button for ‘Access Risk Analysis’. Next, select the type of analysis that is required. The options available are: Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level) Permission Level: SODs at the authorization level Critical Action: Critical transactions that limited/no users should have Critical Permission: Critical authorizations that limited/no users should have Critical Role/Profile: Critical Roles/Profiles that limited/no users should have In this case, ‘Permission Level’ was selected so that the report will show SODs that exist at the Permission Level.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous Next **Analysis Criteria** System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk Level is All Rule Set is Global **Report Options** Format: Summary, Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ☐ Critical Role/Profile ☐ Analytical Report Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule Previous Next

12	In the ‘Report Options’ section, check ‘Show All Objects’ under ‘Additional Criteria’. This will ensure that Users with no violations are explicitly listed as such (i.e. ‘No Violations’ will be listed as a line item for such users’ IDs).	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous Next **Analysis Criteria** System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk Level is All Rule Set is Global **Report Options** Format: Summary · Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission Additional Criteria: ☐ Include Mitigated Risks ☐ Consider Org Rule ☑ Show All Objects Previous Next

14	The analysis criteria has now been defined. Click on ‘Next’ to define the simulation criteria.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Previous Next Simulation : Role Level Analysis Criteria System is *PS1* Role Type is Technical Role Role is Z_VPF_S_AR_GENERAL Risk Level is All Rule Set is Global Report Options Format: Summary Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule

15A-1	Simulation by Action (transaction). On the ‘Actions’ tab, click on ‘Add’ to define transaction simulation criteria.	

15A-2	Click the drop down on the 'System' field and select the system from which a transaction must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	

Simulation : Role Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Role Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

Previous | Next | Run in Foreground | Run in Background

Simulation Criteria

Saved Variants: Delete

Additional Criteria: □ Exclude Values □ Include Users □ Include Business Role □ Risk from Simulation only □ Include Composite Roles

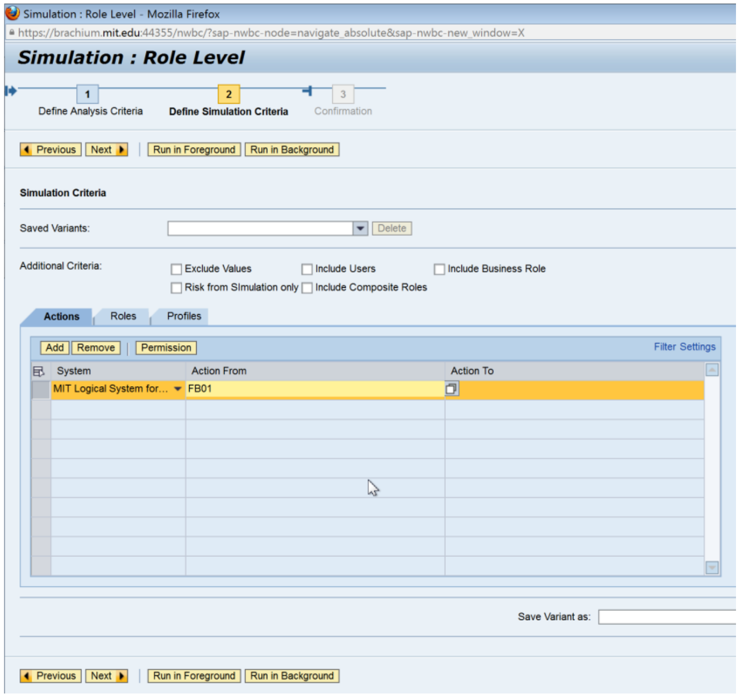
Actions | Roles | Profiles

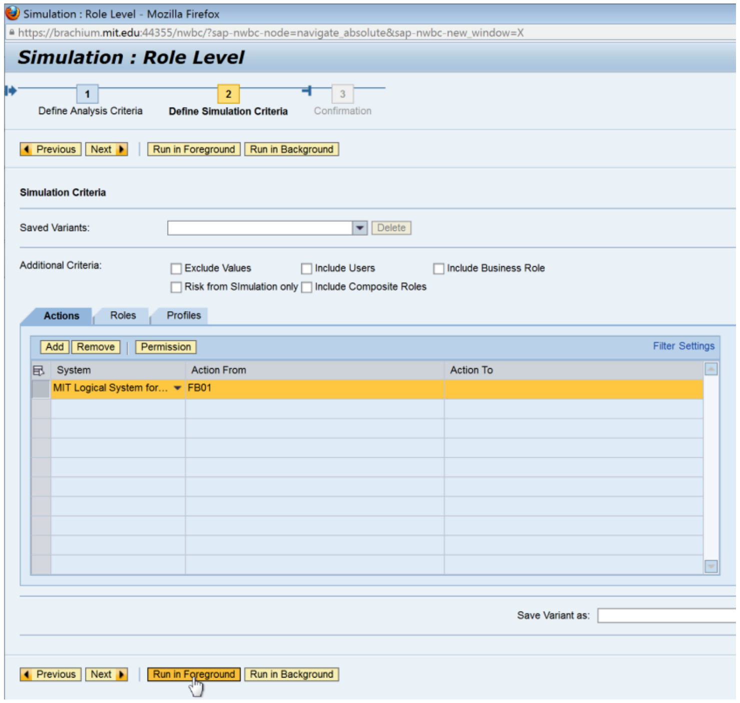
Add | Remove | Permission — Filter Settings

System	Action From	Action To
MIT Logical System for PS1:030 MIT Logical System for SF2:030 MIT Logical System for SF3:030 MIT Logical System for SH2:030		

Save Variant as:

Previous | Next | Run in Foreground | Run in Background

15A-3	Add the transaction. In this case, 'FB01' was typed in. The search option can also be used to search for an Action. Please refer to the 'Search for Input Values' reference document (R3) for further information. NOTE: If transactions should be excluded from the Role for the simulation, the 'Exclude Values' box must be checked. Otherwise, any added transactions will be added to the Role for the simulation.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next · Run in Foreground · Run in Background Simulation Criteria Saved Variants: Delete Additional Criteria: ☐ Exclude Values ☐ Include Users ☐ Include Business Role ☐ Risk from Simulation only ☐ Include Composite Roles Actions · Roles · Profiles Add · Remove · Permission · Filter Settings System: MIT Logical System for... · Action From: FB01 · Action To: Save Variant as: Previous · Next · Run in Foreground · Run in Background

15A-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	

Simulation : Role Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Role Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

Previous | Next | Run in Foreground | Run in Background

Simulation Criteria

Saved Variants: Delete

Additional Criteria: □ Exclude Values □ Include Users □ Include Business Role □ Risk from Simulation only □ Include Composite Roles

Actions | Roles | Profiles

Add | Remove | Permission | Filter Settings

System	Action From	Action To
MIT Logical System for...	FB01	

Save Variant as:

Previous | Next | Run in Foreground | Run in Background

15A-5

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

Any orange line items represent risks occuring due to simulation criteria.

Role Name: SAP role name

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Risk Description: Business description of the Access Risk

System: The system in which the role is assigned to the user

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Action: SAP transaction

Action Description: SAP transaction name

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

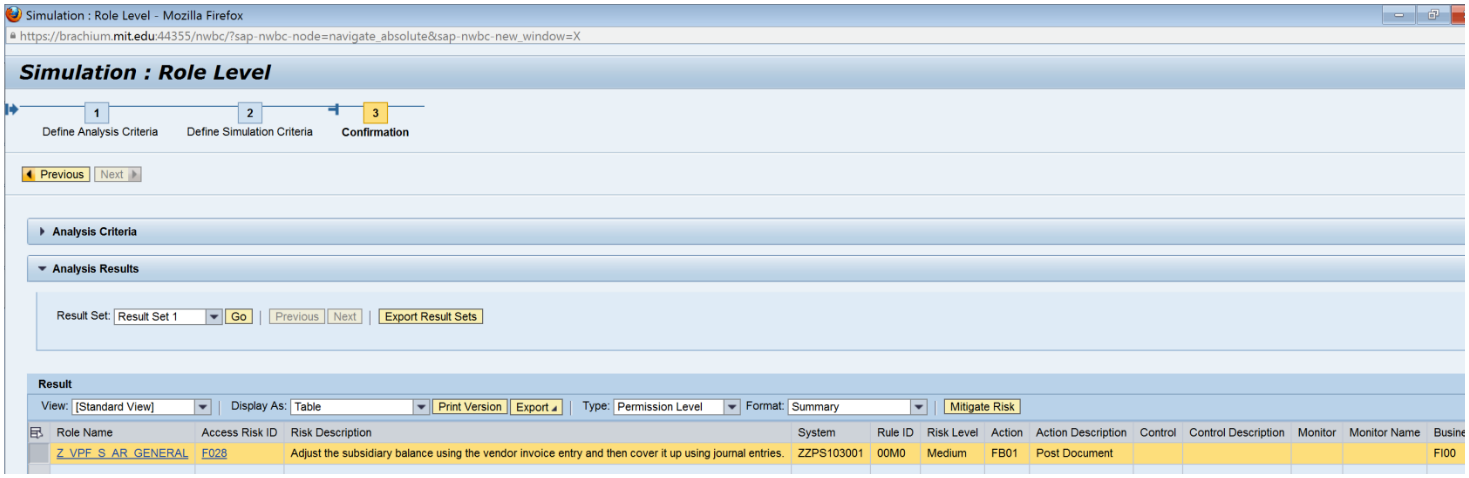
Control Description: Business description of the Mitigating Control

Monitor: The user ID of the Monitor responsible for the Mitigating Control

Monitor Name: Name tied to the user ID of the Monitor

Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set

Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set

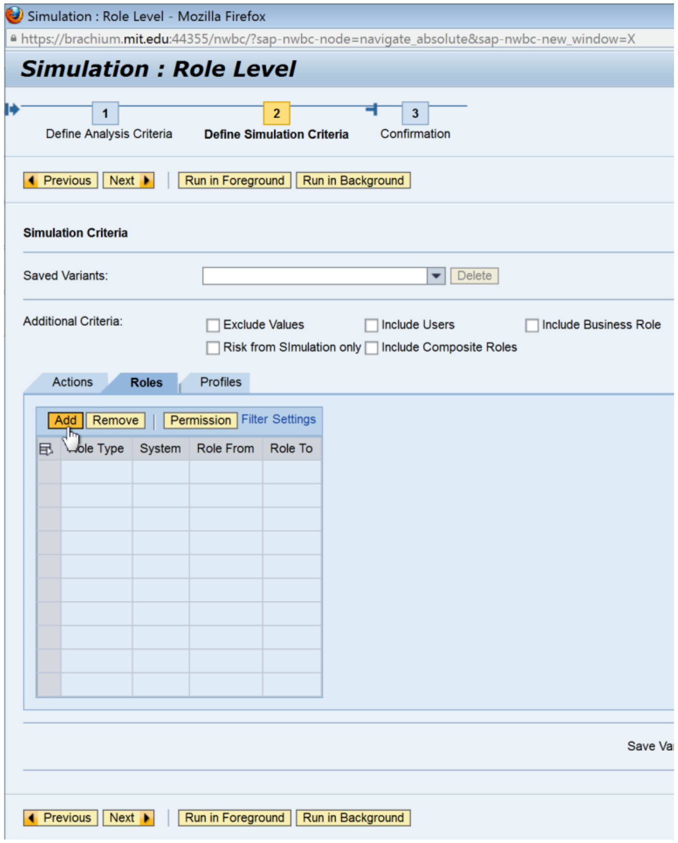

Simulation : Role Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
1
Define Analysis Criteria
2
Define Simulation Criteria
3
Confirmation
Previous
Next
Analysis Criteria
Analysis Results
Go
Previous
Next
Export Result Sets
Result
Print Version
Export
Mitigate Risk

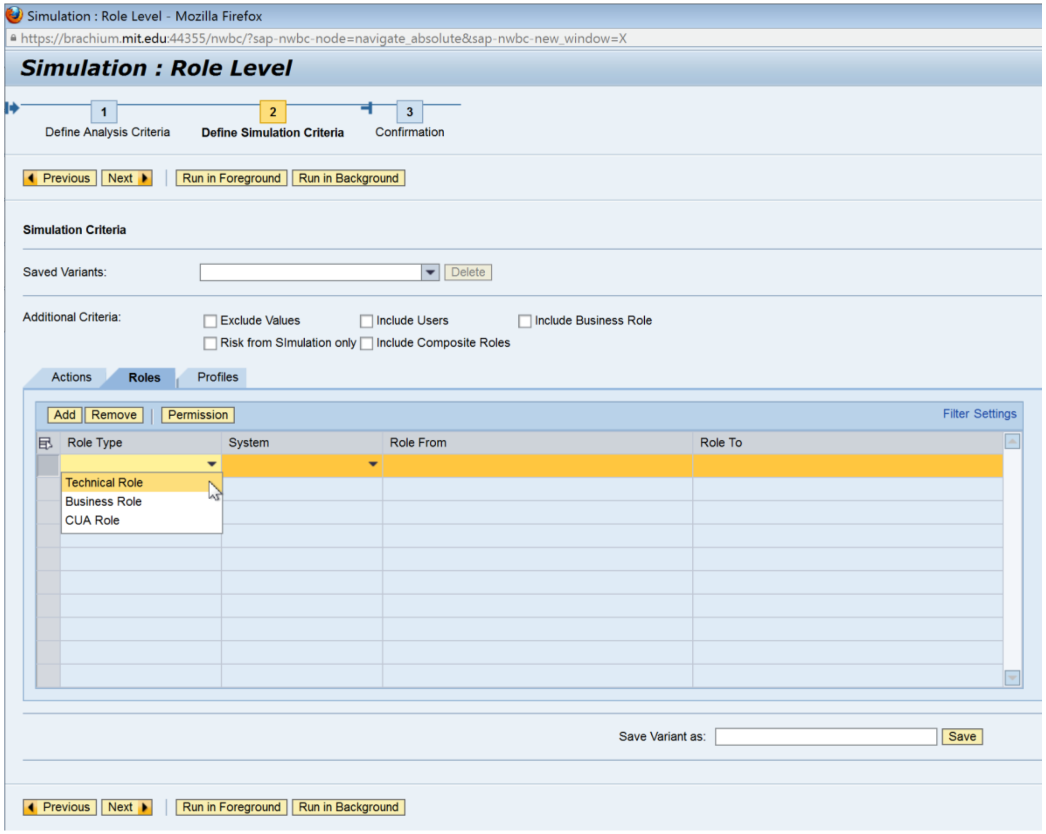
Simulation : Role Level

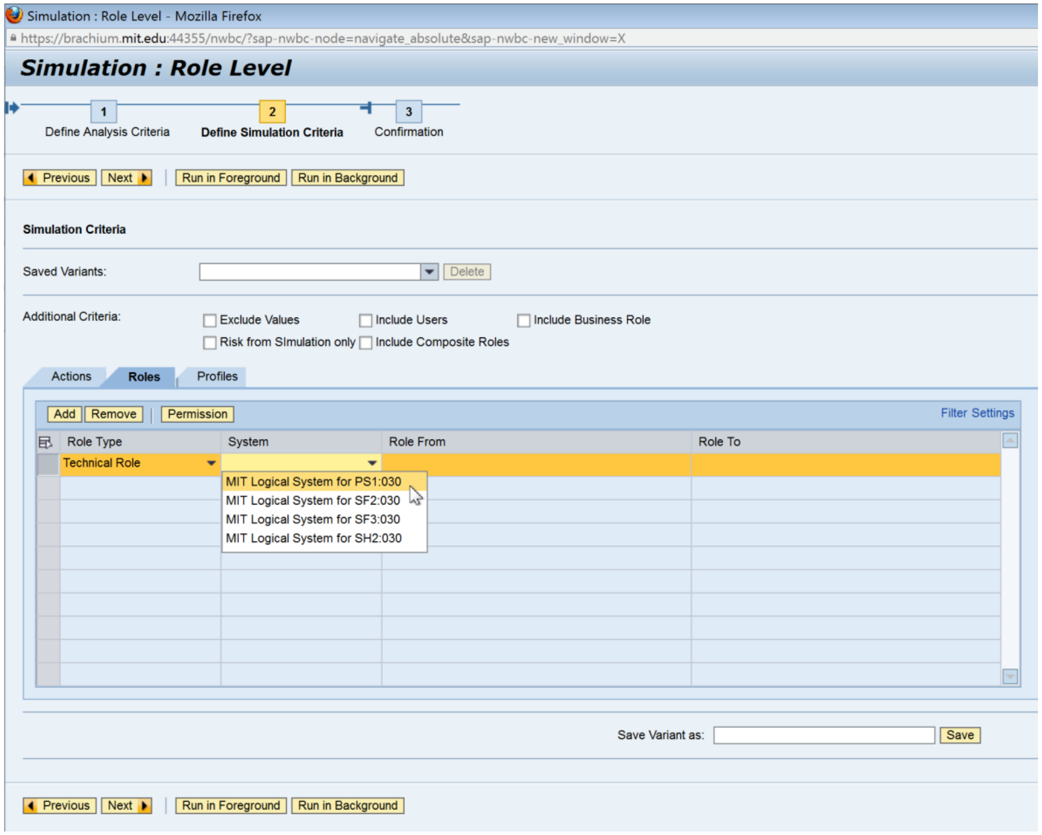
Result Set: Result Set 1

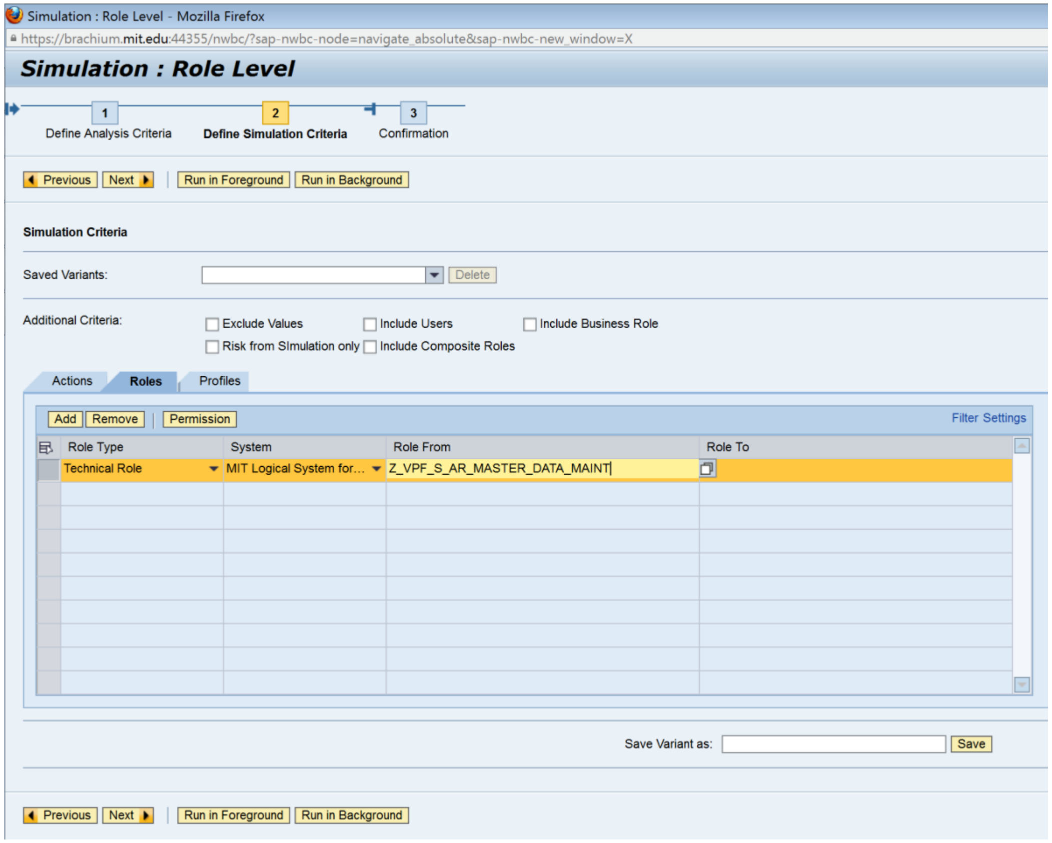
View: [Standard View] Display As: Table Type: Permission Level Format: Summary

Role Name	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action	Action Description	Control	Control Description	Monitor	Monitor Name	Busine
Z_VPF_S_AR_GENERAL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	00M0	Medium	FB01	Post Document					FI00

15B-1	Simulation by Role. On the ‘Roles’ tab, click on ‘Add’ to define role simulation criteria.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next · Run in Foreground · Run in Background **Simulation Criteria** Saved Variants: · Delete Additional Criteria: □ Exclude Values □ Include Users □ Include Business Role □ Risk from Simulation only □ Include Composite Roles Actions · Roles · Profiles Add · Remove · Permission · Filter Settings Role Type · System · Role From · Role To Save Va Previous · Next · Run in Foreground · Run in Background

15B-2	Click the drop down on the 'Role Type' field and select 'Technical Role'. For role-based simulation criteria, unless otherwise advised, the selection will always be 'Technical Role'.	

15B-3	Click the drop down on the ‘System’ field and select the system from which a technical role must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : Role Level 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Previous Next Run in Foreground Run in Background Simulation Criteria Saved Variants: Delete Additional Criteria: □ Exclude Values □ Include Users □ Include Business Role □ Risk from SImulation only □ Include Composite Roles Actions Roles Profiles Add Remove Permission Filter Settings Role Type System Role From Role To Technical Role MIT Logical System for PS1:030 MIT Logical System for SF2:030 MIT Logical System for SF3:030 MIT Logical System for SH2:030 Save Variant as: Save Previous Next Run in Foreground Run in Background

15B-4	Add the role. In this case, 'Z_VPF_S_AR_MASTER_ DATA_MAINT' was typed in. The search option can also be used to search for a Role. Please refer to the 'Search for Input Values' reference document (R3) for further information. NOTE: If the added role's authorizations should be excluded from the original role for the simulation, the 'Exclude Values' box must be checked. Otherwise, authorizations from any added roles will be added to the original role for the simulation.	

Simulation : Role Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Role Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

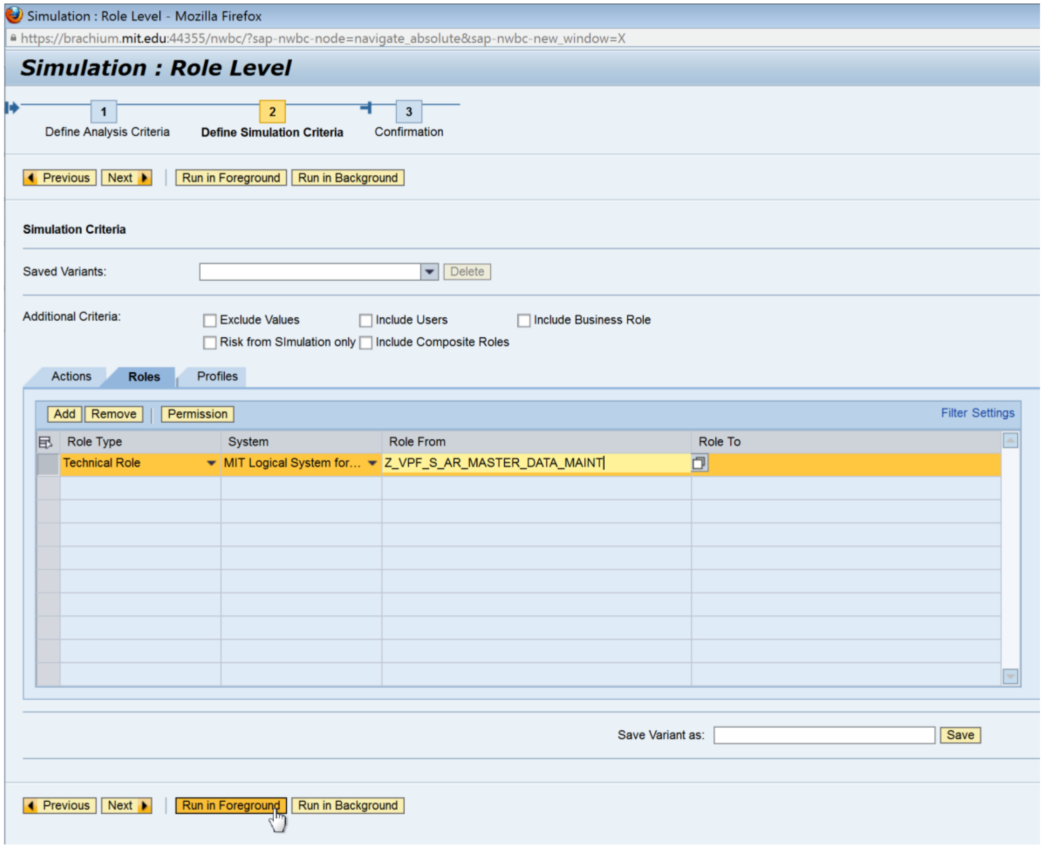
Simulation Criteria

Saved Variants:

Additional Criteria: □ Exclude Values □ Include Users □ Include Business Role □ Risk from Simulation only □ Include Composite Roles

Role Type	System	Role From	Role To
Technical Role	MIT Logical System for...	Z_VPF_S_AR_MASTER_DATA_MAINT	

Save Variant as:

15B-5	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next · Run in Foreground · Run in Background Simulation Criteria Saved Variants: · Delete Additional Criteria: ☐ Exclude Values ☐ Include Users ☐ Include Business Role ☐ Risk from Simulation only ☐ Include Composite Roles Actions · Roles · Profiles Add · Remove · Permission · Filter Settings Role Type: Technical Role · System: MIT Logical System for... · Role From: Z_VPF_S_AR_MASTER_DATA_MAINT · Role To: Save Variant as: · Save Previous · Next · Run in Foreground · Run in Background

15B-6

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

Any orange line items represent risks occuring due to simulation criteria.

Role Name: SAP role name

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Risk Description: Business description of the Access Risk

System: The system in which the role is assigned to the user

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Action: SAP transaction

Action Description: SAP transaction name

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

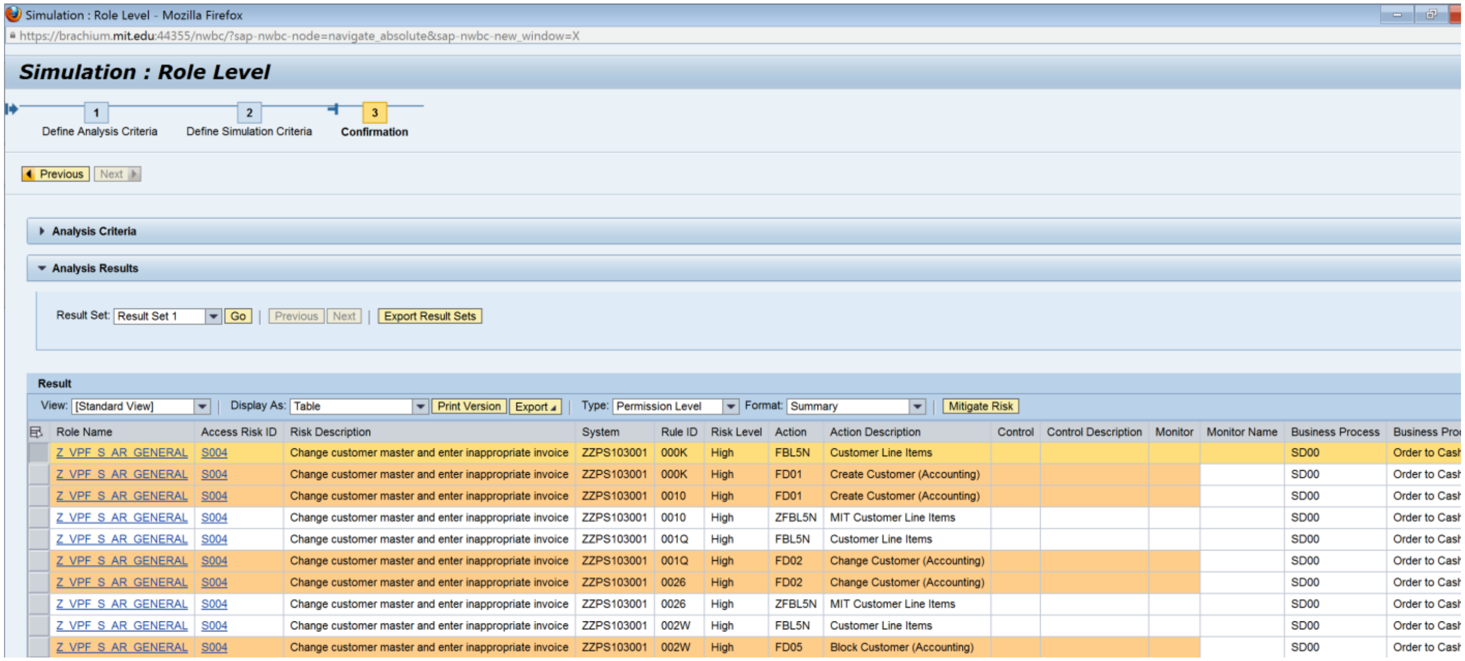
Control Description: Business description of the Mitigating Control

Monitor: The user ID of the Monitor responsible for the Mitigating Control

Monitor Name: Name tied to the user ID of the Monitor

Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set

Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set



Simulation : Role Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Role Level

1 Define Analysis Criteria
2 Define Simulation Criteria
3 Confirmation
Previous
Next
Analysis Criteria
Analysis Results

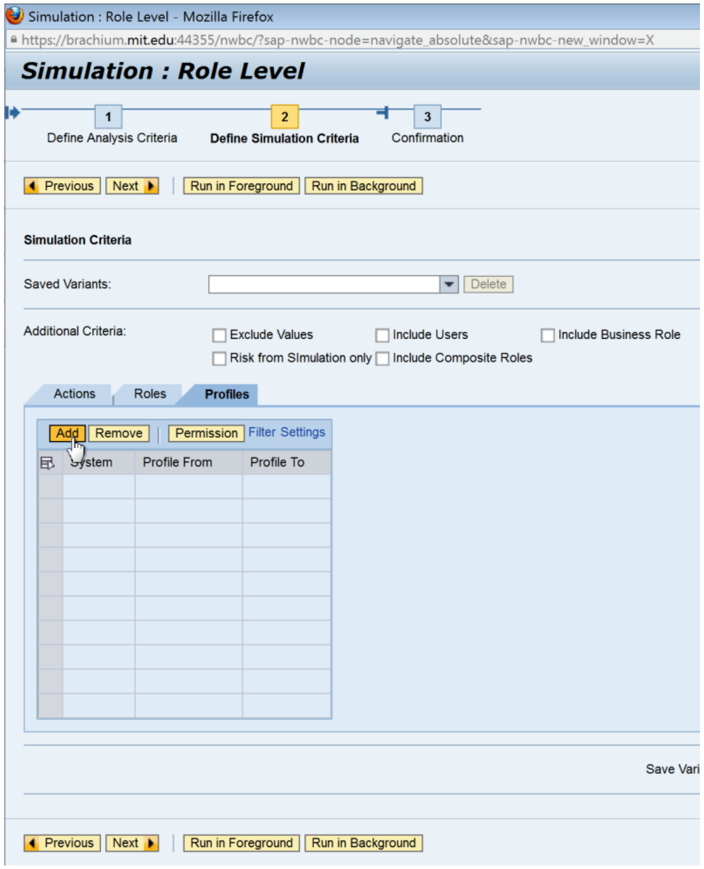
Result Set: Result Set 1

Go
Previous
Next
Export Result Sets
Result

View: [Standard View]   Display As: Table   Type: Permission Level   Format: Summary

Print Version
Export
Mitigate Risk

Role Name	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action	Action Description	Control	Control Description	Monitor	Monitor Name	Business Process	Business Pro
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	000K	High	FBL5N	Customer Line Items					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	000K	High	FD01	Create Customer (Accounting)					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	0010	High	FD01	Create Customer (Accounting)					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	0010	High	ZFBL5N	MIT Customer Line Items					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	001Q	High	FBL5N	Customer Line Items					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	001Q	High	FD02	Change Customer (Accounting)					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	0026	High	FD02	Change Customer (Accounting)					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	0026	High	ZFBL5N	MIT Customer Line Items					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	002W	High	FBL5N	Customer Line Items					SD00	Order to Cash
Z_VPF_S_AR_GENERAL	S004	Change customer master and enter inappropriate invoice	ZZPS103001	002W	High	FD05	Block Customer (Accounting)					SD00	Order to Cash

15C-1	Simulation by Profile. On the ‘Profiles’ tab, click on ‘Add’ to define profile simulation criteria.	

Simulation : Role Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

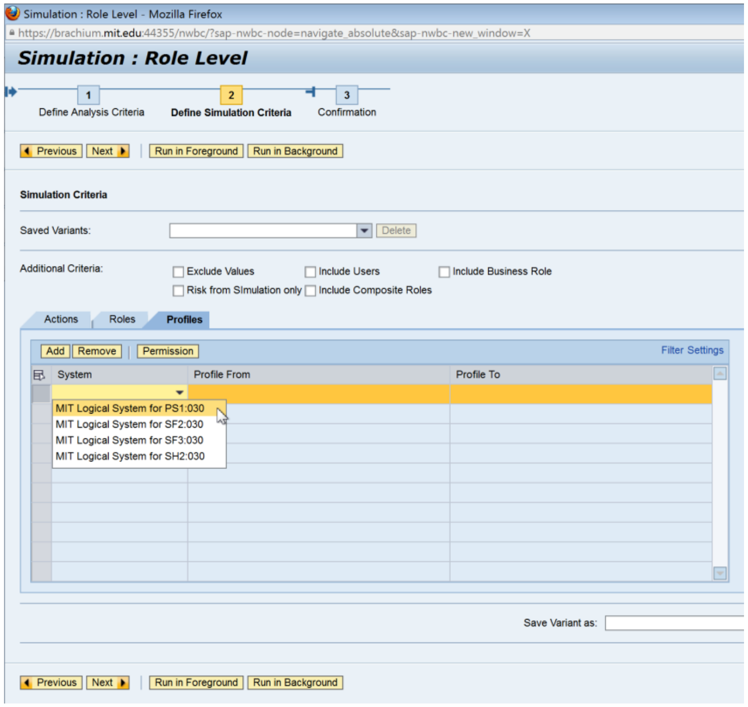
Simulation : Role Level

Simulation Criteria

Saved Variants:

Additional Criteria: ☐ Exclude Values ☐ Include Users ☐ Include Business Role ☐ Risk from Simulation only ☐ Include Composite Roles

System	Profile From	Profile To

15C-2	Click the drop down on the 'System' field and select the system from which a profile must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	

Simulation : Role Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Role Level

1 Define Analysis Criteria — 2 **Define Simulation Criteria** — 3 Confirmation

Simulation Criteria

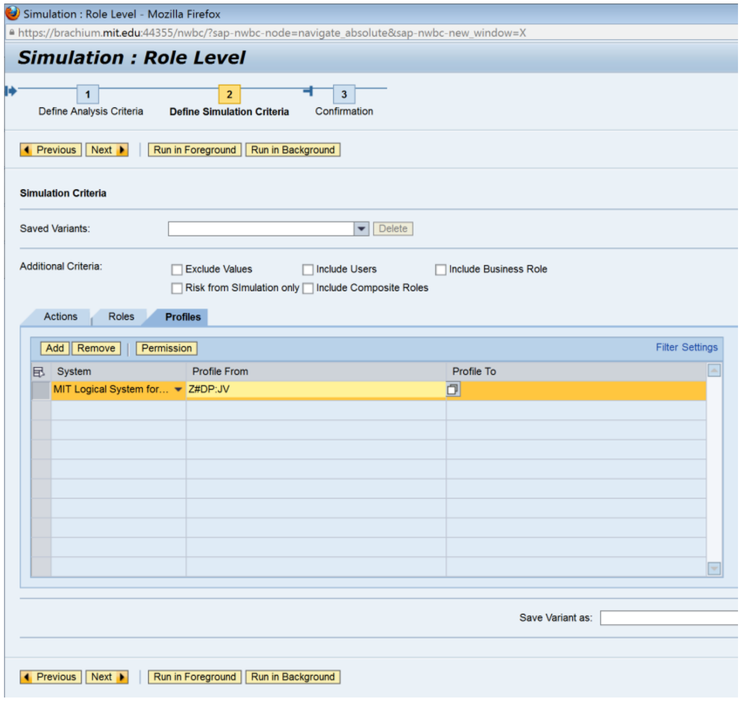
Saved Variants:

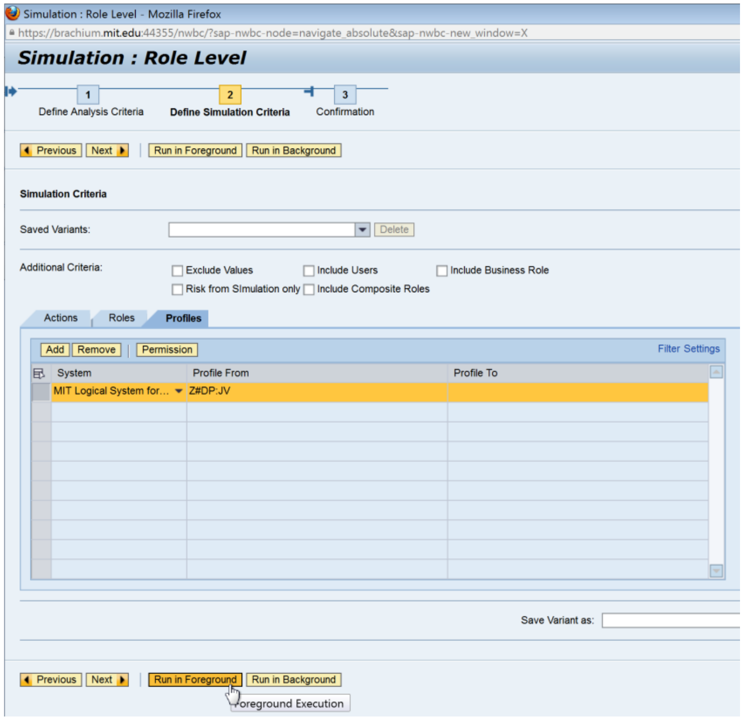
Additional Criteria: □ Exclude Values □ Include Users □ Include Business Role □ Risk from Simulation only □ Include Composite Roles

System	Profile From	Profile To

MIT Logical System for PS1:030
MIT Logical System for SF2:030
MIT Logical System for SF3:030
MIT Logical System for SH2:030

Save Variant as:

15C-3	Add the profile. In this case, ‘Z#DP:JV’ was typed in. The search option can also be used to search for a Profile. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. NOTE: If the added profile’s authorizations should be excluded from the original role for the simulation, the ‘Exclude Values’ box must be checked. Otherwise, authorizations from any added profiles will be added to the original role for the simulation.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : Role Level 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Simulation Criteria Saved Variants: Additional Criteria: □ Exclude Values □ Include Users □ Include Business Role □ Risk from Simulation only □ Include Composite Roles System: MIT Logical System for... · Profile From: Z#DP:JV · Profile To: Save Variant as:

15C-4	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Simulation : Role Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Role Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next · Run in Foreground · Run in Background Simulation Criteria Saved Variants: · Delete Additional Criteria: ☐ Exclude Values ☐ Include Users ☐ Include Business Role ☐ Risk from Simulation only ☐ Include Composite Roles Actions · Roles · Profiles Add · Remove · Permission · Filter Settings System: MIT Logical System for... · Profile From: Z#DP:JV · Profile To: Save Variant as: Previous · Next · Run in Foreground · Run in Background Foreground Execution

15C-5

Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.

Any orange line items represent risks occuring due to simulation criteria.

Role Name: SAP role name

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Risk Description: Business description of the Access Risk

System: The system in which the role is assigned to the user

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: risk level defined for each Access Risk in the standard rule set

Action: SAP transaction

Action Description: SAP transaction name

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

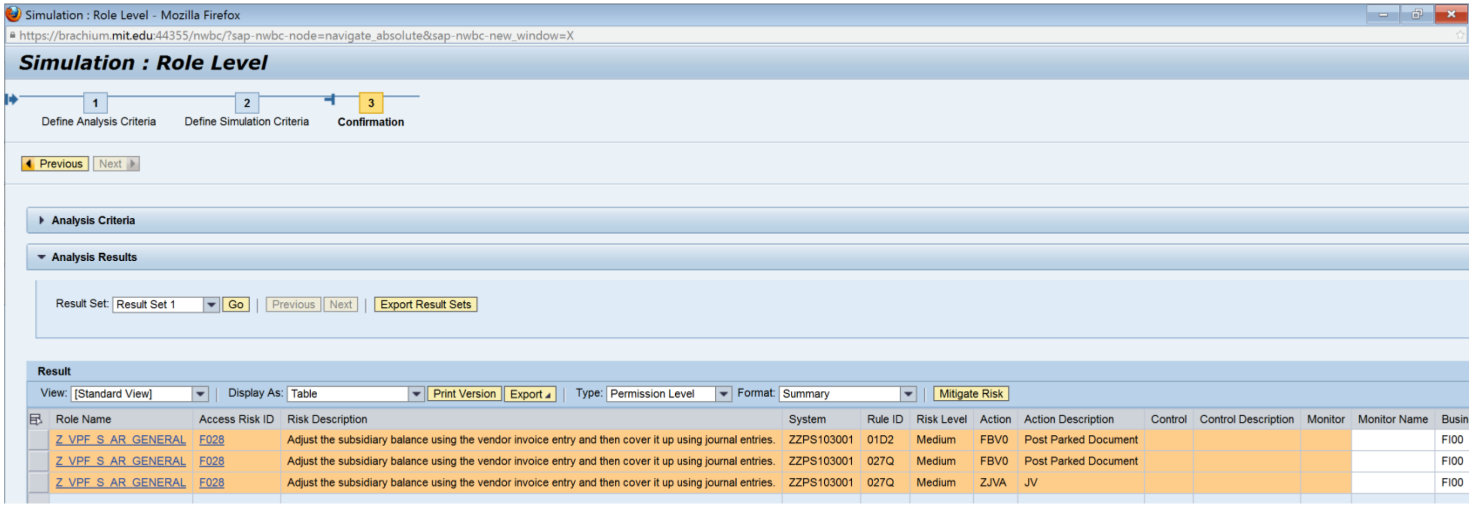
Control Description: Business description of the Mitigating Control

Monitor: The user ID of the Monitor responsible for the Mitigating Control

Monitor Name: Name tied to the user ID of the Monitor

Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set

Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set


Simulation : Role Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Simulation : Role Level
1 Define Analysis Criteria
2 Define Simulation Criteria
3 Confirmation
Previous
Next
Analysis Criteria
Analysis Results
Go
Previous
Next
Export Result Sets
Result
Print Version
Export
Mitigate Risk

Result Set: Result Set 1

View: [Standard View] Display As: Table Type: Permission Level Format: Summary

Role Name	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action	Action Description	Control	Control Description	Monitor	Monitor Name	Busin
Z_VPF_S_AR_GENERAL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	01D2	Medium	FBV0	Post Parked Document					FI00
Z_VPF_S_AR_GENERAL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	027Q	Medium	FBV0	Post Parked Document					FI00
Z_VPF_S_AR_GENERAL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	027Q	Medium	ZJVA	JV					FI00

Job Aid 16 Profile Level

USE

This report can be used analyze for risk violations at the profile level.

INFORMATION

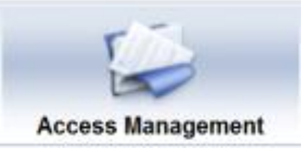
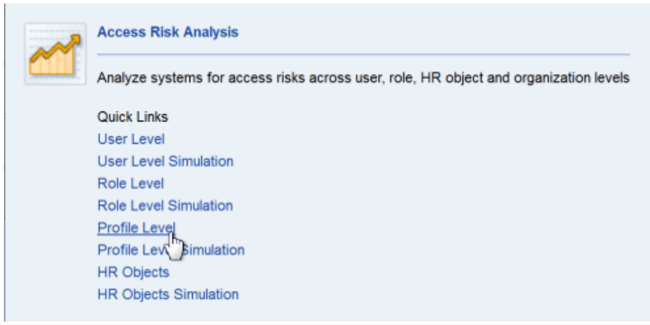
SODs, critical actions or permissions.

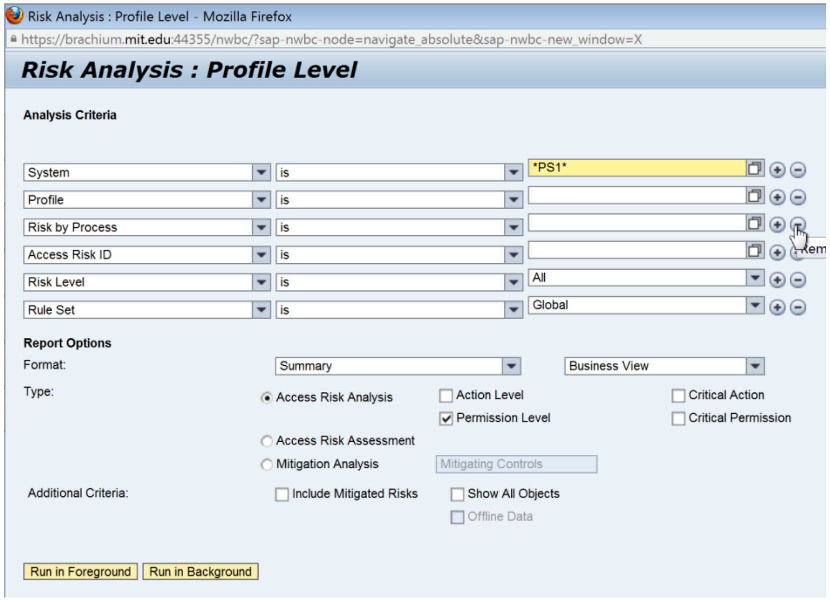
RELATED PROCESSES

- Process 1: New or Amended Roles
- Process 2: Mitigation Analysis

SPECIFIC SCENARIOS

- N/A

Step	Description	Screenshot
1	Navigate to the ‘Access Management’ tab.	
2	Click on the ‘Profile Level’ report located in the ‘Access Risk Analysis’ section.	 Access Risk Analysis Analyze systems for access risks across user, role, HR object and organization levels Quick Links User Level User Level Simulation Role Level Role Level Simulation Profile Level Profile Level Simulation HR Objects HR Objects Simulation

3	In the ‘Analysis Criteria’ section, select the System for which information is required. Since the desired selection is PS1 (Production), ‘*PS1*’ was typed in as the system. The search option can also be used to search for the correct system. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	

Risk Analysis : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Risk Analysis : Profile Level

Analysis Criteria

System	is	*PS1*
Profile	is	
Risk by Process	is	
Access Risk ID	is	
Risk Level	is	All
Rule Set	is	Global

Report Options

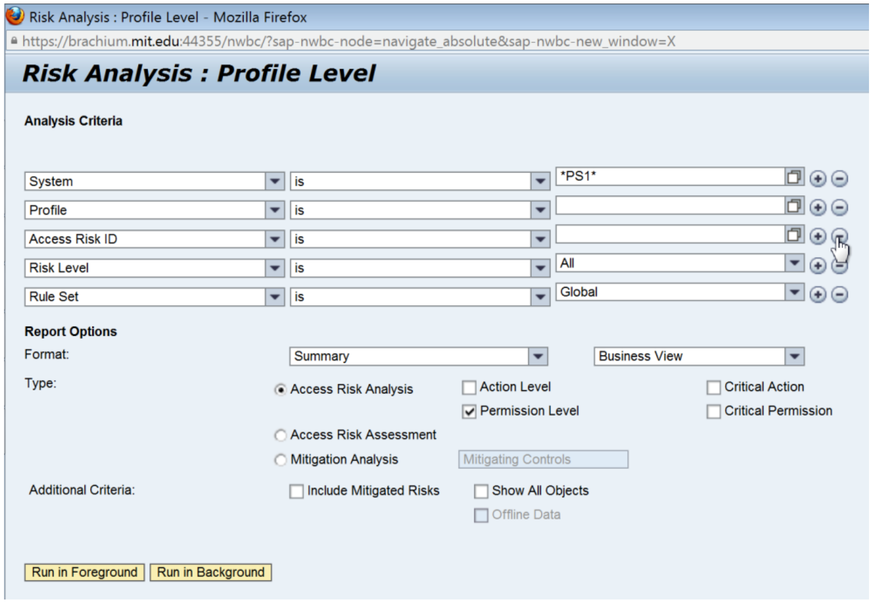
Format: Summary | Business View

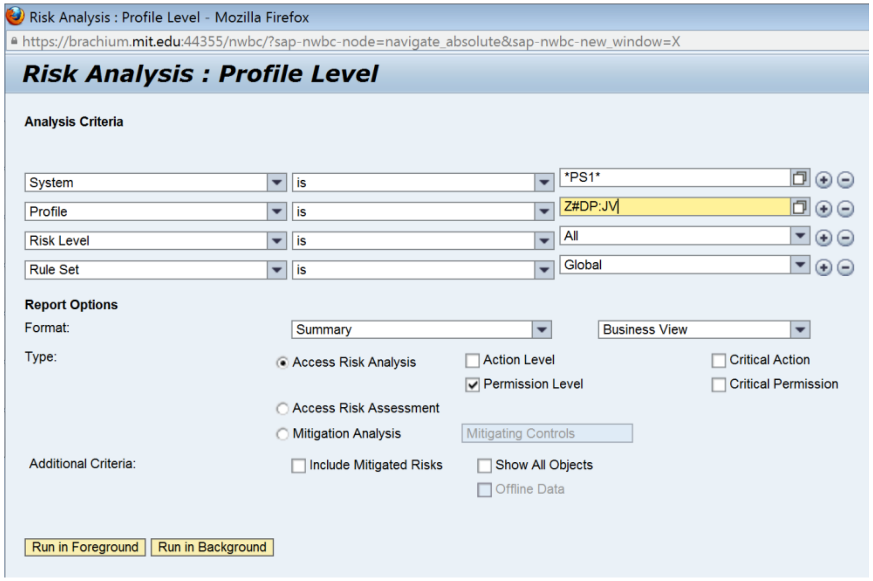
Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission

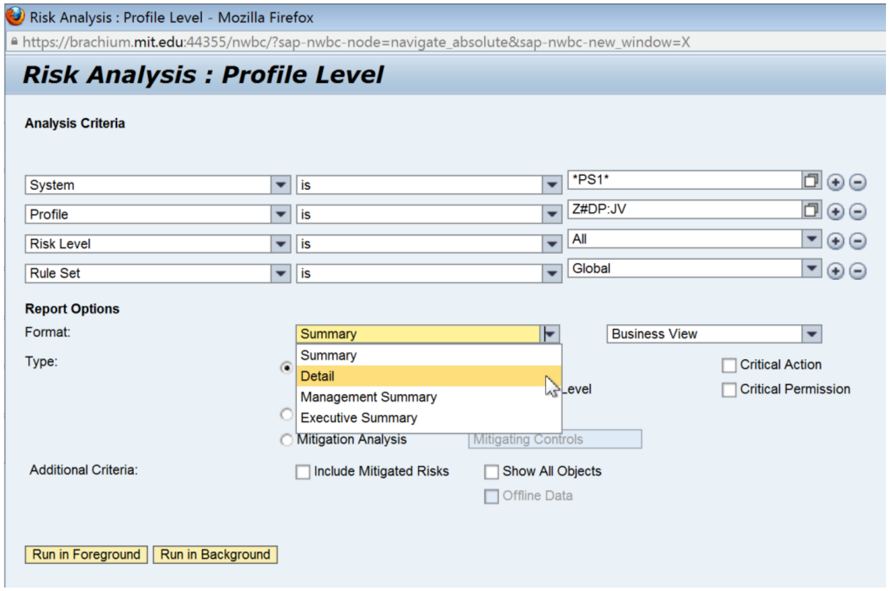
○ Access Risk Assessment

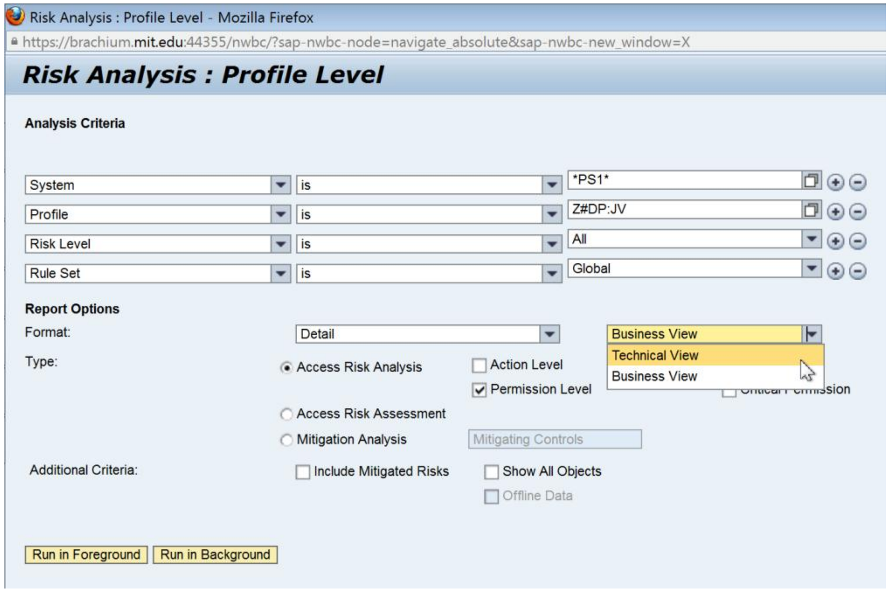
○ Mitigation Analysis Mitigating Controls

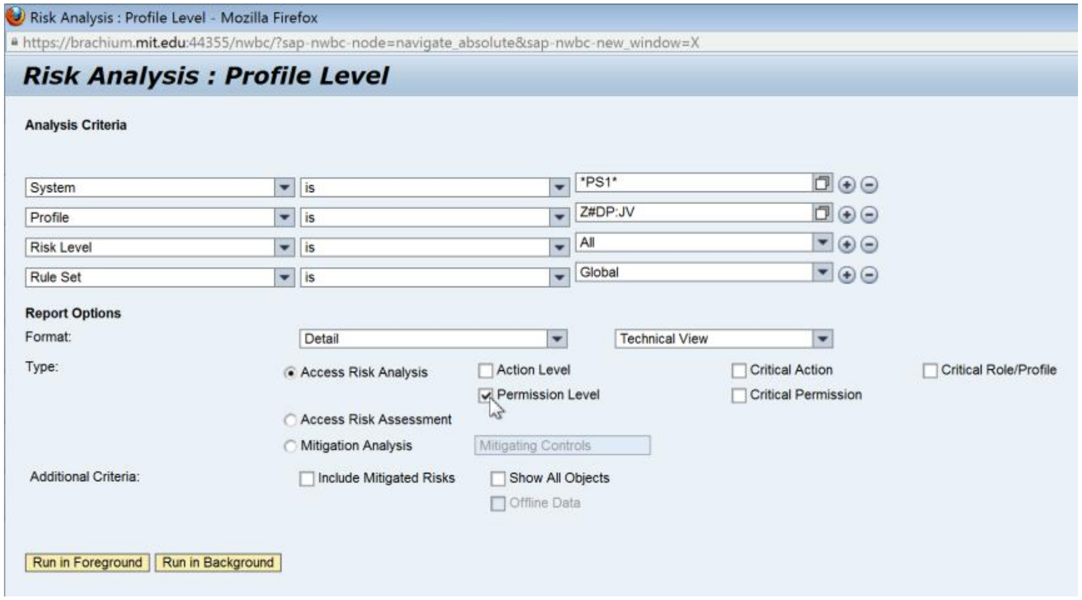
Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Offline Data

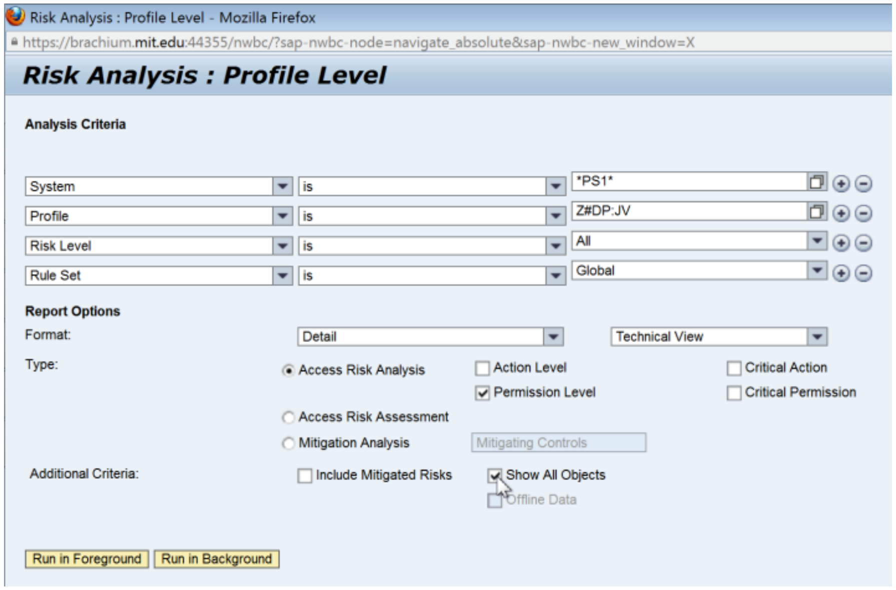
4	Analysis for a single profile. In the 'Analysis Criteria' section, click on the '-' at the end of the 'Access Risk ID' row to remove the row for that search criterion; this criterion is not needed for this scenario.	 Risk Analysis : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Profile Level** **Analysis Criteria** System is *PS1* Profile is Access Risk ID is Risk Level is All Rule Set is Global **Report Options** Format: Summary Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Offline Data Run in Foreground Run in Background

5	Add the Profile. In this case, ‘Z#DP:JV’ was typed in. The search option can also be used to search for a profile. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Risk Analysis : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : Profile Level Analysis Criteria System is *PS1* Profile is Z#DP:JV Risk Level is All Rule Set is Global Report Options Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☐ Critical Action ☑ Permission Level ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Offline Data Run in Foreground Run in Background

6	In the 'Report Options' section, select the first drop down for 'Format' and select the level of detail at which information is required. In this case, 'Detail' was selected so that the report will show information about why Risks exists.	 Risk Analysis : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : Profile Level Analysis Criteria System is *PS1* Profile is Z#DP:JV Risk Level is All Rule Set is Global Report Options Format: Summary — Business View Summary Detail Management Summary Executive Summary Type: ● …Level ○ ○ Mitigation Analysis — Mitigating Controls □ Critical Action □ Critical Permission Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Offline Data Run in Foreground — Run in Background

7	In the 'Report Options' section, select the second drop down for 'Format' and select the type of information that is required. In this case, 'Technical View' was selected so that the report will show technical information about why Risks exists.	 Risk Analysis : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Profile Level** Analysis Criteria System is *PS1* Profile is Z#DP:JV Risk Level is All Rule Set is Global Report Options Format: Detail Business View Technical View Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Offline Data Run in Foreground Run in Background

8	Analyze for SODs based on Profile. In the ‘Report Options’ section, select the first dial button for ‘Access Risk Analysis’. Next, select the type of analysis that is required. The options available are: Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level) Permission Level: SODs at the authorization level Critical Action: Critical transactions that limited/no users should have Critical Permission: Critical authorizations that limited/no users should have Critical Role/Profile: Critical Roles/Profiles that limited/no users should have In this case, ‘Permission Level’ was selected so that the report will show SODs that exist at the Permission Level.	 Risk Analysis : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Profile Level** **Analysis Criteria** System is *PS1* Profile is Z#DP:JV Risk Level is All Rule Set is Global **Report Options** Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ☐ Critical Role/Profile ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Offline Data Run in Foreground Run in Background

9	In the ‘Report Options’ section, check ‘Show All Objects’ under ‘Additional Criteria’. This will ensure that a Profile with no violations is explicitly listed as such (i.e. ‘No Violations’ will be listed as a line item for such Profiles).	

Risk Analysis : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Risk Analysis : Profile Level

Analysis Criteria

System	is	*PS1*
Profile	is	Z#DP:JV
Risk Level	is	All
Rule Set	is	Global

Report Options

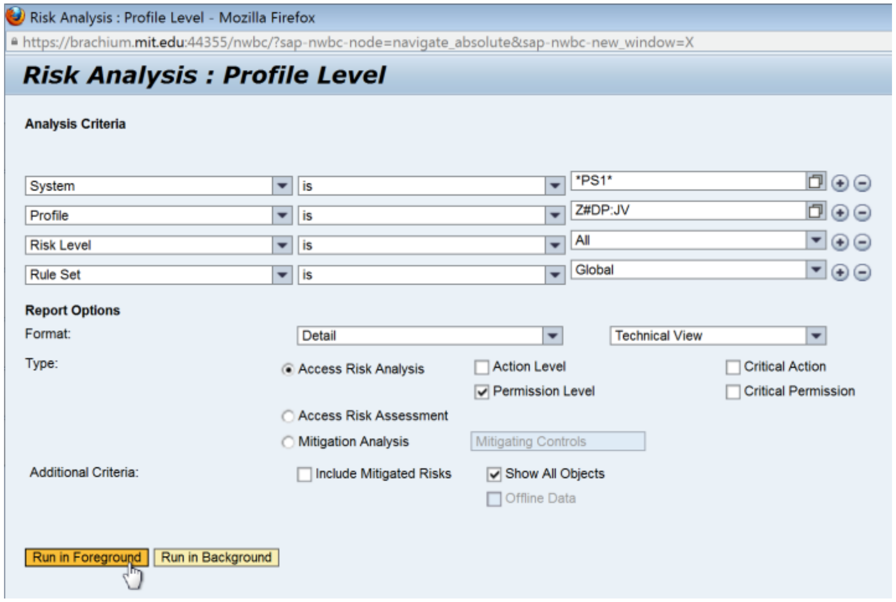
Format: Detail | Technical View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission

○ Access Risk Assessment

○ Mitigation Analysis | Mitigating Controls

Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Offline Data

10	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	 Risk Analysis : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : Profile Level** **Analysis Criteria** System · is · *PS1* Profile · is · Z#DP:JV Risk Level · is · All Rule Set · is · Global **Report Options** Format: Detail · Technical View Type: ● Access Risk Analysis · ☐ Action Level · ☑ Permission Level · ☐ Critical Action · ☐ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis · Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks · ☑ Show All Objects · ☐ Offline Data Run in Foreground · Run in Background

11

Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information.

Profile ID: SAP profile name

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

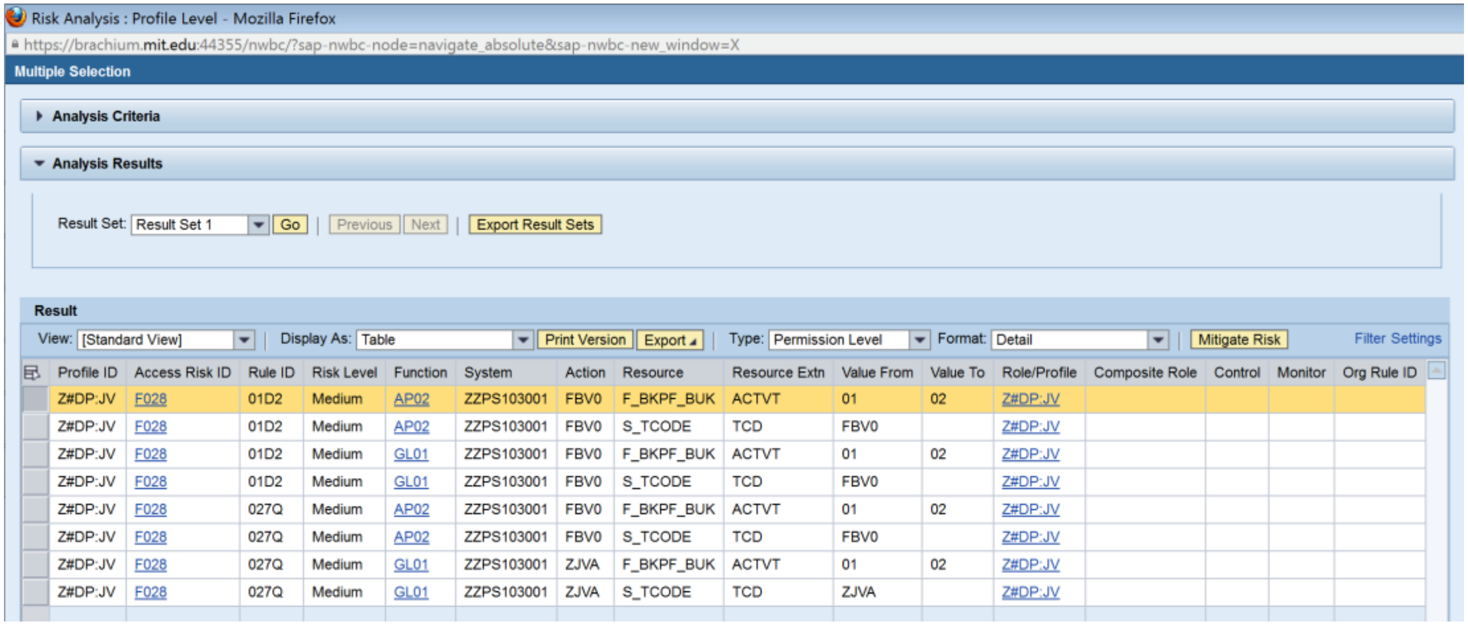
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control


Risk Analysis : Profile Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Multiple Selection
Analysis Criteria
Analysis Results
Go
Previous
Next
Export Result Sets
Result
Print Version
Export
Mitigate Risk
Filter Settings

Result Set: Result Set 1

View: [Standard View]

Display As: Table

Type: Permission Level

Format: Detail

Profile ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
Z#DP:JV	F028	01D2	Medium	AP02	ZZPS103001	FBV0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV				
Z#DP:JV	F028	01D2	Medium	AP02	ZZPS103001	FBV0	S_TCODE	TCD	FBV0		Z#DP:JV				
Z#DP:JV	F028	01D2	Medium	GL01	ZZPS103001	FBV0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV				
Z#DP:JV	F028	01D2	Medium	GL01	ZZPS103001	FBV0	S_TCODE	TCD	FBV0		Z#DP:JV				
Z#DP:JV	F028	027Q	Medium	AP02	ZZPS103001	FBV0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV				
Z#DP:JV	F028	027Q	Medium	AP02	ZZPS103001	FBV0	S_TCODE	TCD	FBV0		Z#DP:JV				
Z#DP:JV	F028	027Q	Medium	GL01	ZZPS103001	ZJVA	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV				
Z#DP:JV	F028	027Q	Medium	GL01	ZZPS103001	ZJVA	S_TCODE	TCD	ZJVA		Z#DP:JV				

Job Aid 17 Profile Level Simulation

USE

This report can be used carry out simulations at the profile level for the purpose of understanding whether the addition or removal of certain access either creates or eliminates SODs and other risks.

INFORMATION

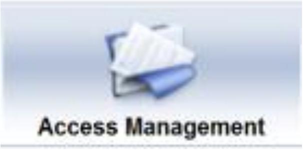
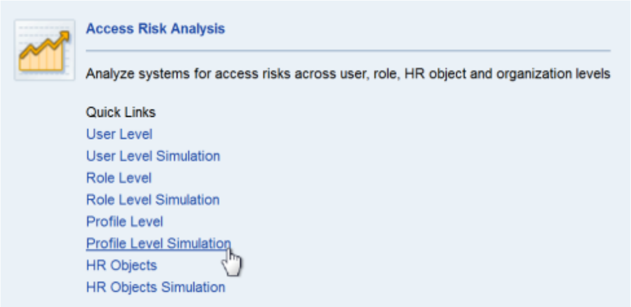
New risk violations that will result due to changes to profiles.

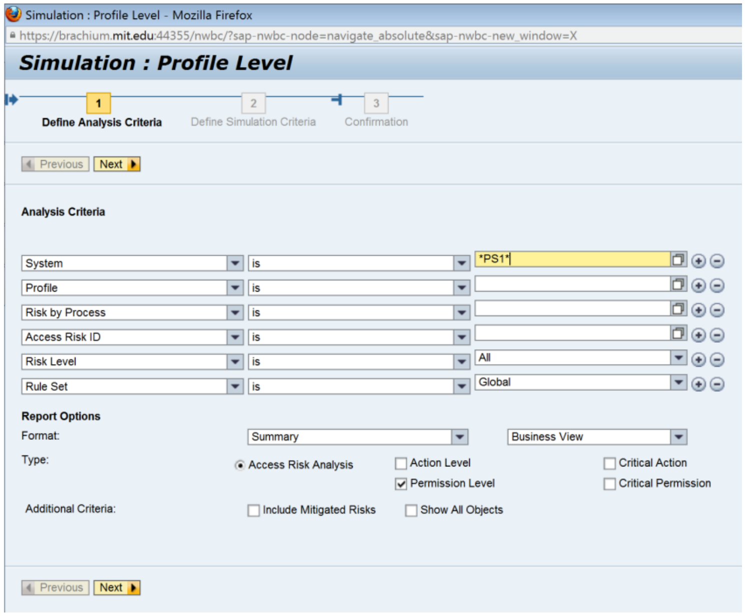
RELATED PROCESSES

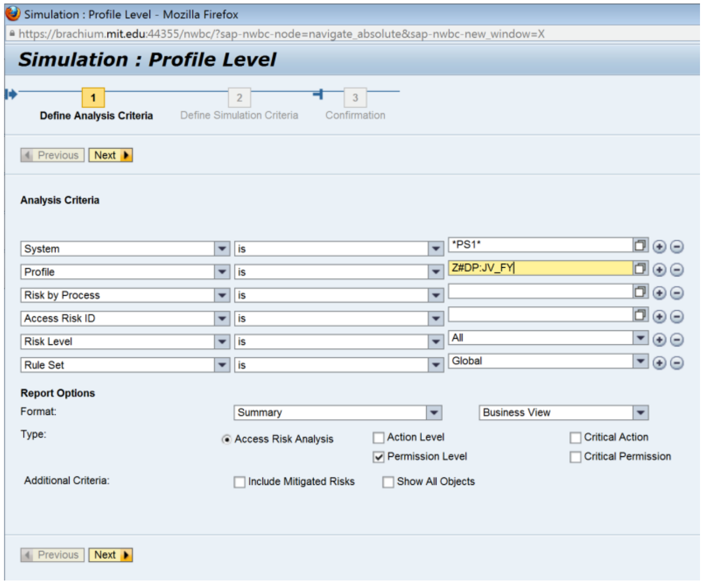
- Process 1: New or Amended Roles
- Process 2: Mitigation Analysis

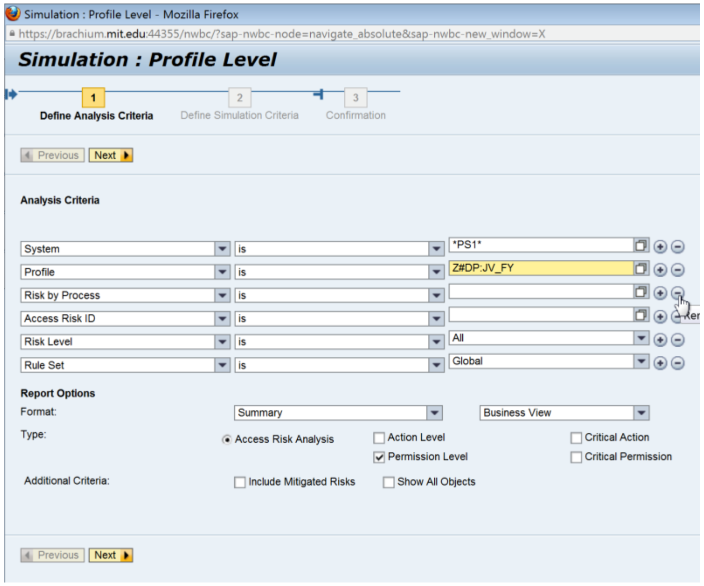
SPECIFIC SCENARIOS

- 14A: Simulation by Action (transaction).
- 14B: Simulation by Role.
- 14C: Simulation by Profile.

Step	Description	Screenshot
1	Navigate to the 'Access Management' tab.	
2	Click on the 'Role Level Simulation' report located in the 'Access Risk Analysis' section.	 Access Risk Analysis Analyze systems for access risks across user, role, HR object and organization levels Quick Links User Level User Level Simulation Role Level Role Level Simulation Profile Level Profile Level Simulation HR Objects HR Objects Simulation

3	In the 'Analysis Criteria' section, select the System for which information is required. Since the desired selection is PS1 (Production), '*PS1*' was typed in as the system. The search option can also be used to search for the correct system. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Profile Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next **Analysis Criteria** System · is · *PS1* Profile · is · Risk by Process · is · Access Risk ID · is · Risk Level · is · All Rule Set · is · Global **Report Options** Format: Summary · Business View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission Additional Criteria: □ Include Mitigated Risks · □ Show All Objects Previous · Next

4	Run a simulation for a single Profile. Add the Profile. In this case, ‘Z#DP:JV_FY’ was typed in. The search option can also be used to search for a profile. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : Profile Level 1 Define Analysis Criteria – 2 Define Simulation Criteria – 3 Confirmation Previous Next Analysis Criteria System is *PS1* Profile is Z#DP:JV_FY Risk by Process is Access Risk ID is Risk Level is All Rule Set is Global Report Options Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects Previous Next

5	In the 'Analysis Criteria' section, click on the '-' at the end of the 'Risk by Process' row to remove the row for that search criterion; this criterion is not needed for this scenario.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

Analysis Criteria

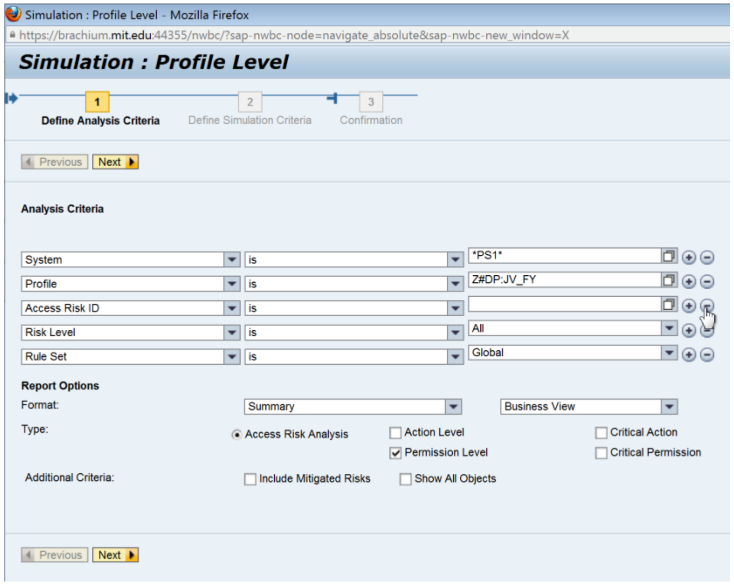
System	is	*PS1*
Profile	is	Z#DP:JV_FY
Risk by Process	is	
Access Risk ID	is	
Risk Level	is	All
Rule Set	is	Global

Report Options

Format: Summary Business View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission

Additional Criteria: □ Include Mitigated Risks □ Show All Objects

6	In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘Access Risk ID’ row to remove the row for that search criterion; this criterion is not needed for this scenario.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

Previous | Next

Analysis Criteria

System	is	*PS1*
Profile	is	Z#DP:JV_FY
Access Risk ID	is	
Risk Level	is	All
Rule Set	is	Global

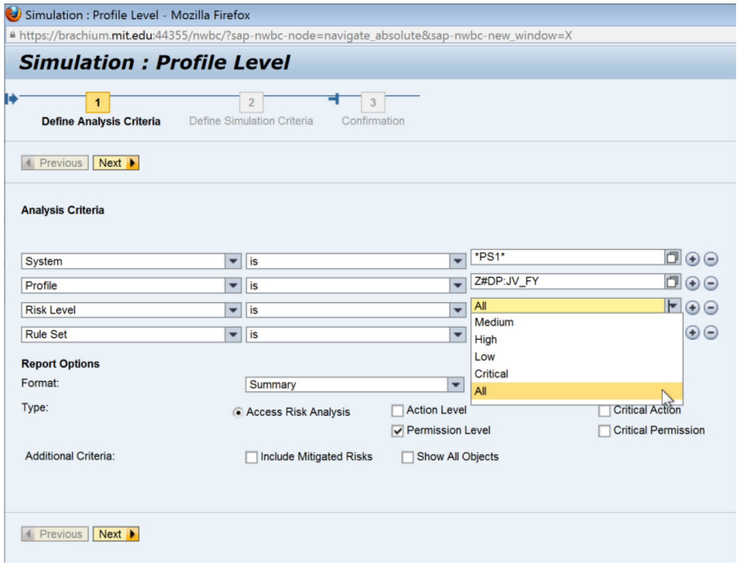
Report Options

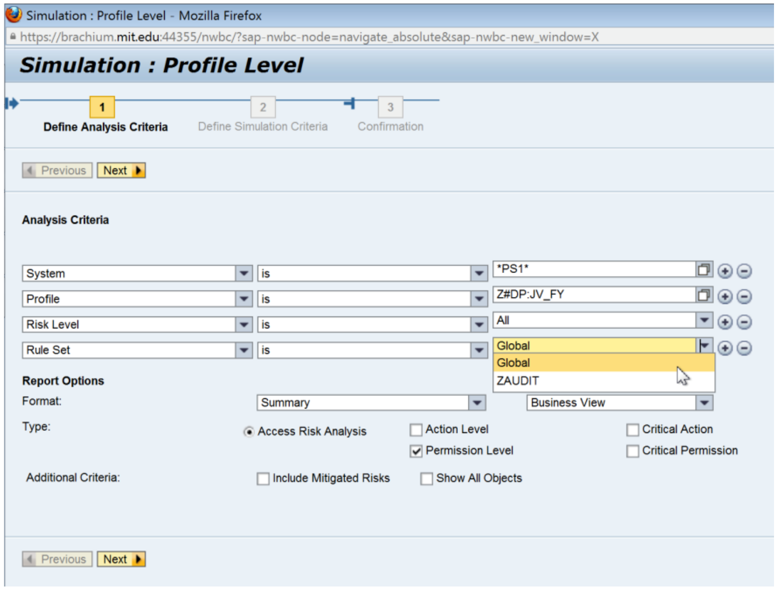
Format: Summary | Business View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission

Additional Criteria: □ Include Mitigated Risks □ Show All Objects

Previous | Next

7	In the 'Analysis Criteria' section, select the 'Risk Level' drop down and select the risk level for which information is required. In this case, 'All' was selected so that the report evaluates for all risk levels.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : Profile Level 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Analysis Criteria System is *PS1* Profile is Z#DP:JV_FY Risk Level is All Rule Set is Report Options Format: Summary Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission Additional Criteria: □ Include Mitigated Risks □ Show All Objects Previous Next Medium High Low Critical All

8	In the 'Analysis Criteria' section, select the 'Rule Set' drop down and select the Rule Set against which the report should be executed. In this case, 'Global', the MIT Rule Set, was selected. Unless advised otherwise, the selection should always be 'Global' for this report.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

Analysis Criteria

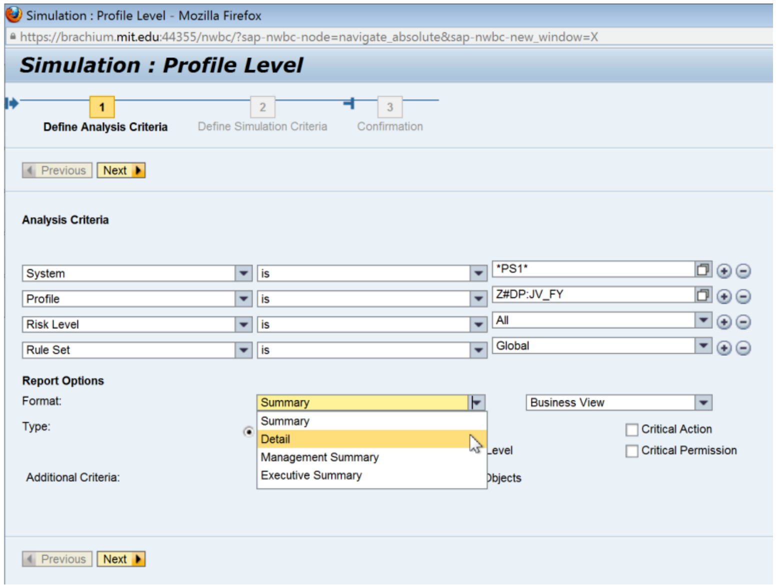
System	is	*PS1*
Profile	is	Z#DP:JV_FY
Risk Level	is	All
Rule Set	is	Global

Report Options

Format: Summary — Business View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission

Additional Criteria: □ Include Mitigated Risks □ Show All Objects

9	In the ‘Report Options’ section, select the first drop down for ‘Format’ and select the level of detail at which information is required. In this case, ‘Detail’ was selected so that the report will show information about why Risks exists.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

Analysis Criteria

System	is	*PS1*
Profile	is	Z#DP:JV_FY
Risk Level	is	All
Rule Set	is	Global

Report Options

Format: Summary

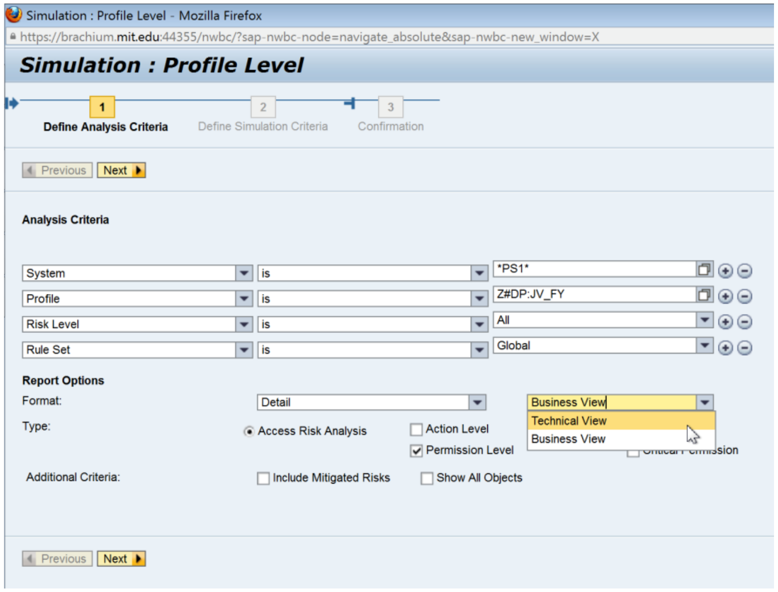
Business View

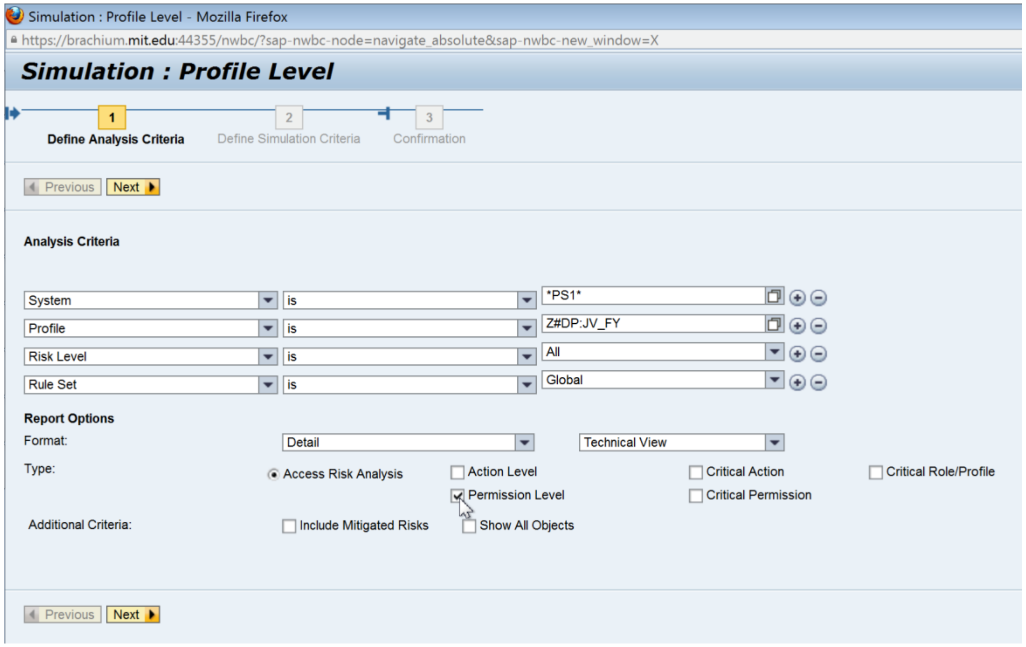
Type:

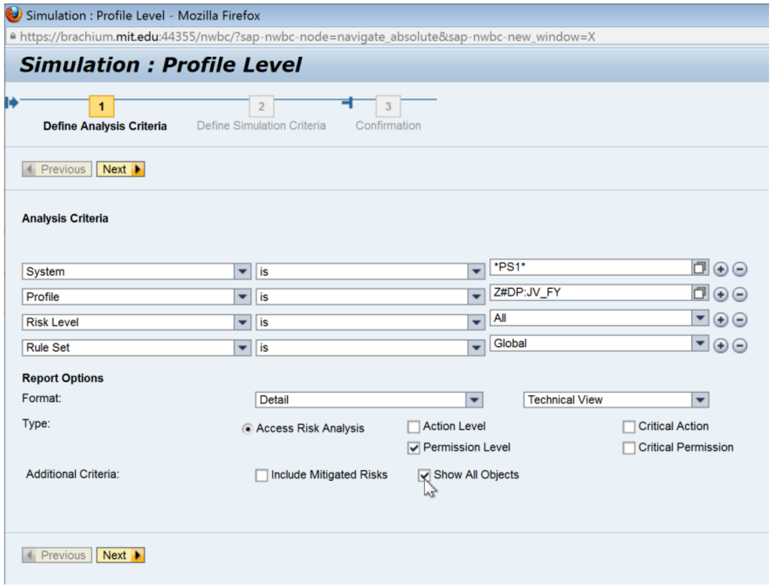
☐ Critical Action

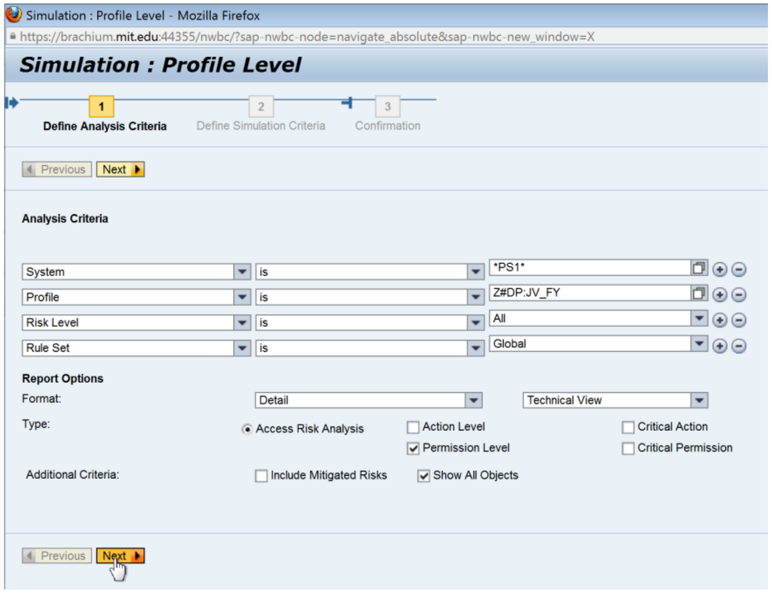
☐ Critical Permission

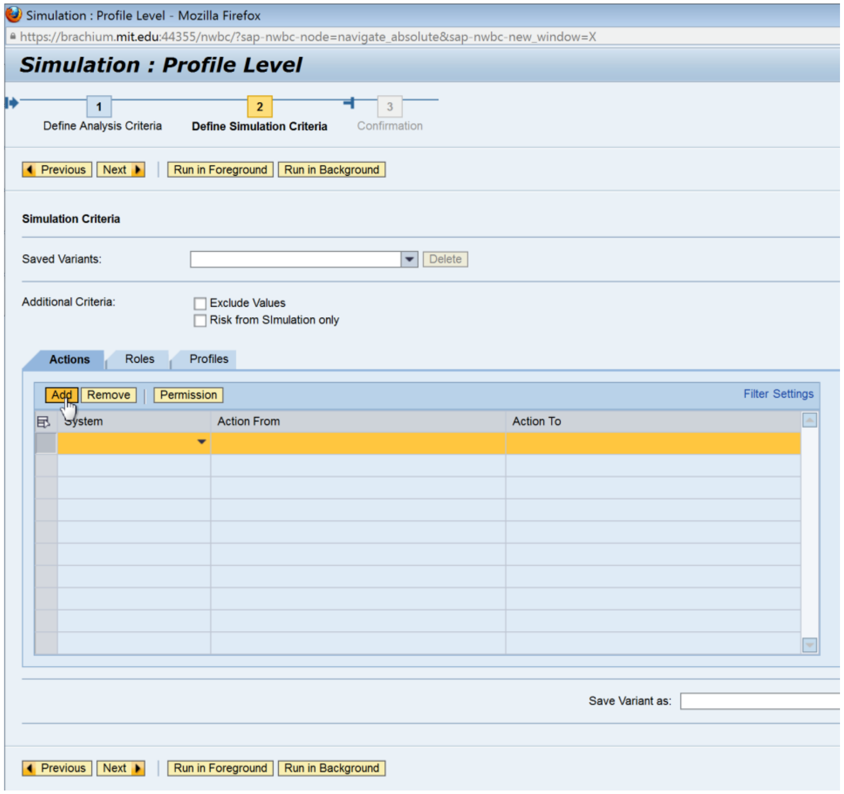
Additional Criteria:

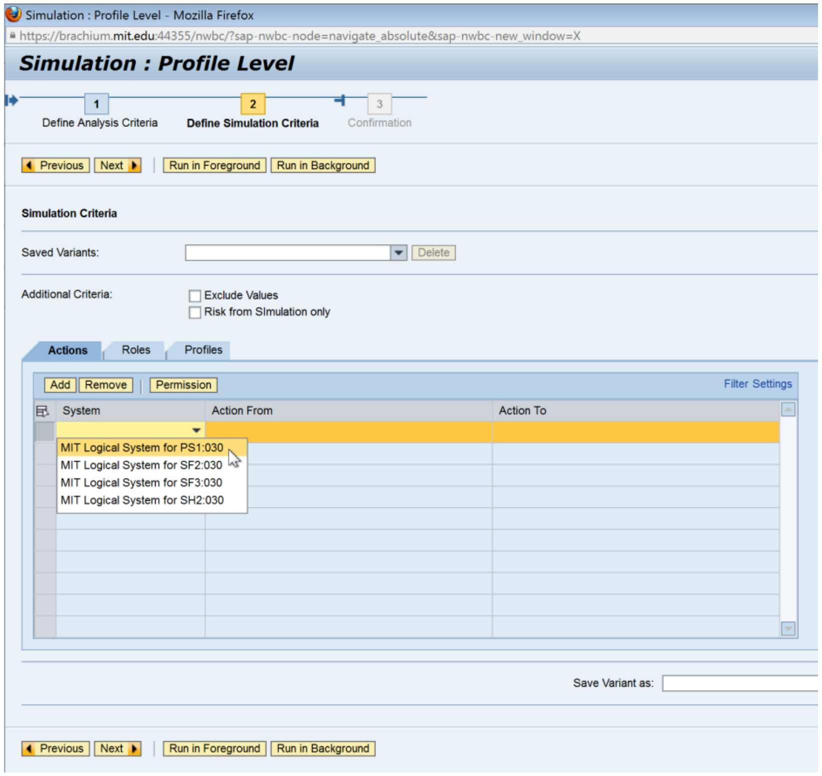
10	In the ‘Report Options’ section, select the second drop down for ‘Format’ and select the type of information that is required. In this case, ‘Technical View’ was selected so that the report will show technical information about why Risks exists.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : Profile Level 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation Previous Next Analysis Criteria System is *PS1* Profile is Z#DP:JV_FY Risk Level is All Rule Set is Global Report Options Format: Detail Business View Technical View Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Permission Additional Criteria: □ Include Mitigated Risks □ Show All Objects Previous Next

11	Analyze for SODs (excluding false positives). In the 'Report Options' section, select the dial button for 'Access Risk Analysis'. Next, select the type of analysis that is required. The options available are: Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level) Permission Level: SODs at the authorization level Critical Action: Critical transactions that limited/no users should have Critical Permission: Critical authorizations that limited/no users should have Critical Role/Profile: Critical Roles/Profiles that limited/no users should have In this case, 'Permission Level' was selected so that the report will show SODs that exist at the Permission Level.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Profile Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next **Analysis Criteria** System · is · *PS1* Profile · is · Z#DP:JV_FY Risk Level · is · All Rule Set · is · Global **Report Options** Format: Detail · Technical View Type: ● Access Risk Analysis · □ Action Level · ☑ Permission Level · □ Critical Action · □ Critical Permission · □ Critical Role/Profile Additional Criteria: □ Include Mitigated Risks · □ Show All Objects Previous · Next

12	In the 'Report Options' section, check 'Show All Objects' under 'Additional Criteria'. This will ensure that Profiles with no violations are explicitly listed as such (i.e. 'No Violations' will be listed as a line item for such Profiles).	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Profile Level** 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation Previous Next **Analysis Criteria** System is *PS1* Profile is Z#DP:JV_FY Risk Level is All Rule Set is Global **Report Options** Format: Detail Technical View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects Previous Next

13	The analysis criteria has now been defined. Click on 'Next' to define the simulation criteria.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Profile Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next **Analysis Criteria** System · is · *PS1* Profile · is · Z#DP:JV_FY Risk Level · is · All Rule Set · is · Global **Report Options** Format: Detail · Technical View Type: ● Access Risk Analysis · ☐ Action Level · ☑ Permission Level · ☐ Critical Action · ☐ Critical Permission Additional Criteria: ☐ Include Mitigated Risks · ☑ Show All Objects Previous · Next

14A-1	Simulation by Action (transaction). On the 'Actions' tab, click on 'Add' to define transaction simulation criteria.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Profile Level** 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation ◀ Previous | Next ▶ | Run in Foreground | Run in Background Simulation Criteria Saved Variants: [▾] Delete Additional Criteria: □ Exclude Values □ Risk from Simulation only Actions | Roles | Profiles Add | Remove | Permission — Filter Settings System | Action From | Action To Save Variant as: ◀ Previous | Next ▶ | Run in Foreground | Run in Background

14A-2	Click the drop down on the 'System' field and select the system from which a transaction must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

Simulation Criteria

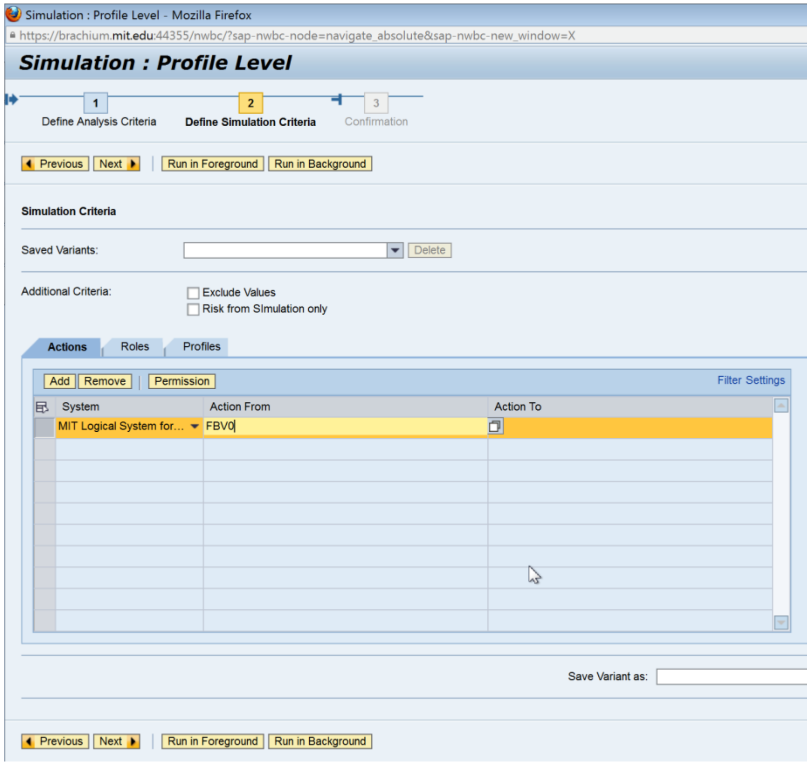
Saved Variants:

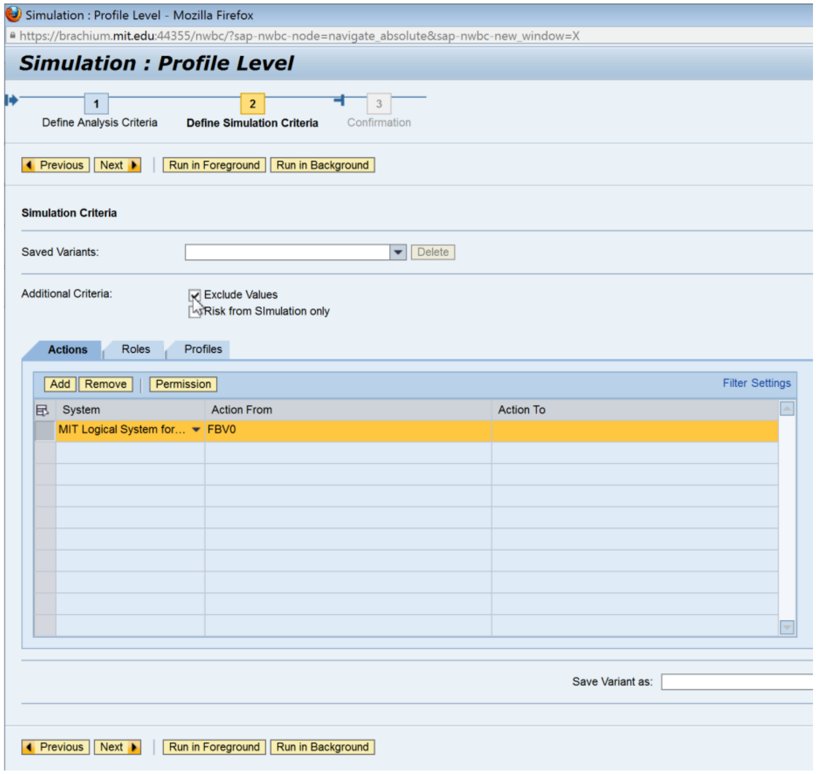
Additional Criteria: □ Exclude Values □ Risk from Simulation only

System	Action From	Action To

Save Variant as:

1 Define Analysis Criteria
2 Define Simulation Criteria
3 Confirmation
Previous
Next
Run in Foreground
Run in Background
Delete
Actions
Roles
Profiles
Add
Remove
Permission
Filter Settings
MIT Logical System for PS1:030
MIT Logical System for SF2:030
MIT Logical System for SF3:030
MIT Logical System for SH2:030
Previous
Next
Run in Foreground
Run in Background

14A-3	Add the transaction. In this case, ‘FBV0’ was typed in. The search option can also be used to search for an Action. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Profile Level** 1 Define Analysis Criteria · 2 Define Simulation Criteria · 3 Confirmation Previous · Next · Run in Foreground · Run in Background Simulation Criteria Saved Variants: · Delete Additional Criteria: ☐ Exclude Values ☐ Risk from Simulation only Actions · Roles · Profiles Add · Remove · Permission · Filter Settings System: MIT Logical System for... · Action From: FBV0 · Action To: Save Variant as: Previous · Next · Run in Foreground · Run in Background

14A-4	If transactions should be excluded from the Profile for the simulation, the 'Exclude Values' box must be checked. Otherwise, any added transactions will be added to the Profile for the simulation. The 'Exclude Values' box is checked in this example.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

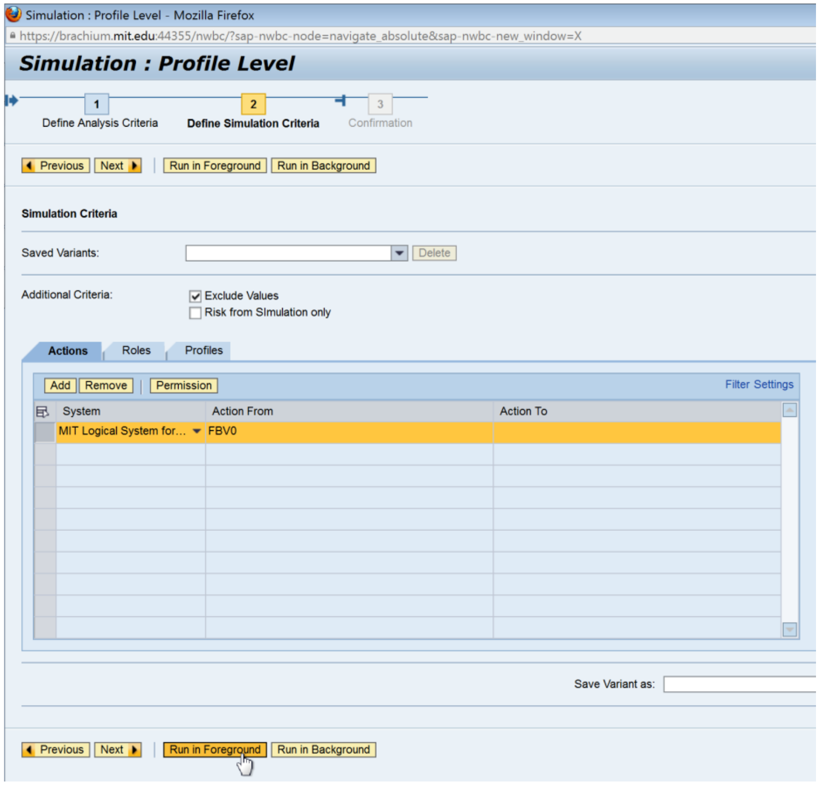
Simulation Criteria

Saved Variants:

Additional Criteria: ☑ Exclude Values ☐ Risk from Simulation only

System	Action From	Action To
MIT Logical System for...	FBV0	

Save Variant as:

14A-5	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : Profile Level 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Simulation Criteria Saved Variants: Additional Criteria: ☑ Exclude Values ☐ Risk from Simulation only Actions / Roles / Profiles System: MIT Logical System for... Action From: FBV0 Action To: Save Variant as: Previous Next Run in Foreground Run in Background Delete Add Remove Permission Filter Settings Previous Next Run in Foreground Run in Background

14A-6

Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information.

Any orange line items represent risks occuring due to simulation criteria.

Profile ID: SAP profile name

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

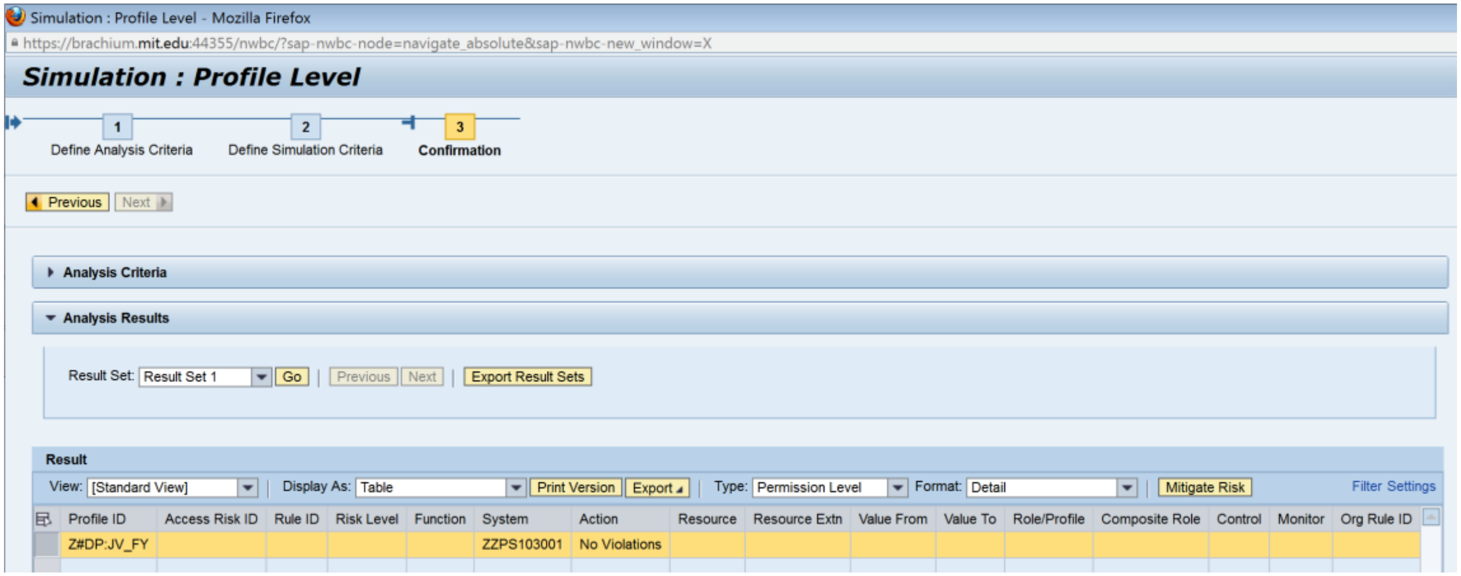
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control



Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

1 Define Analysis Criteria | 2 Define Simulation Criteria | 3 Confirmation

Previous | Next

Analysis Criteria

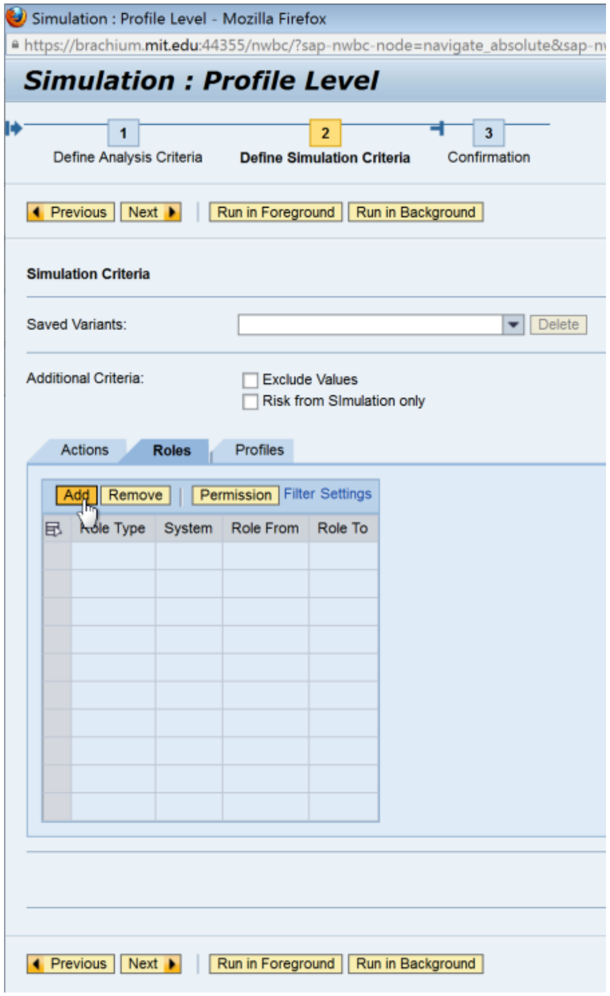
Analysis Results

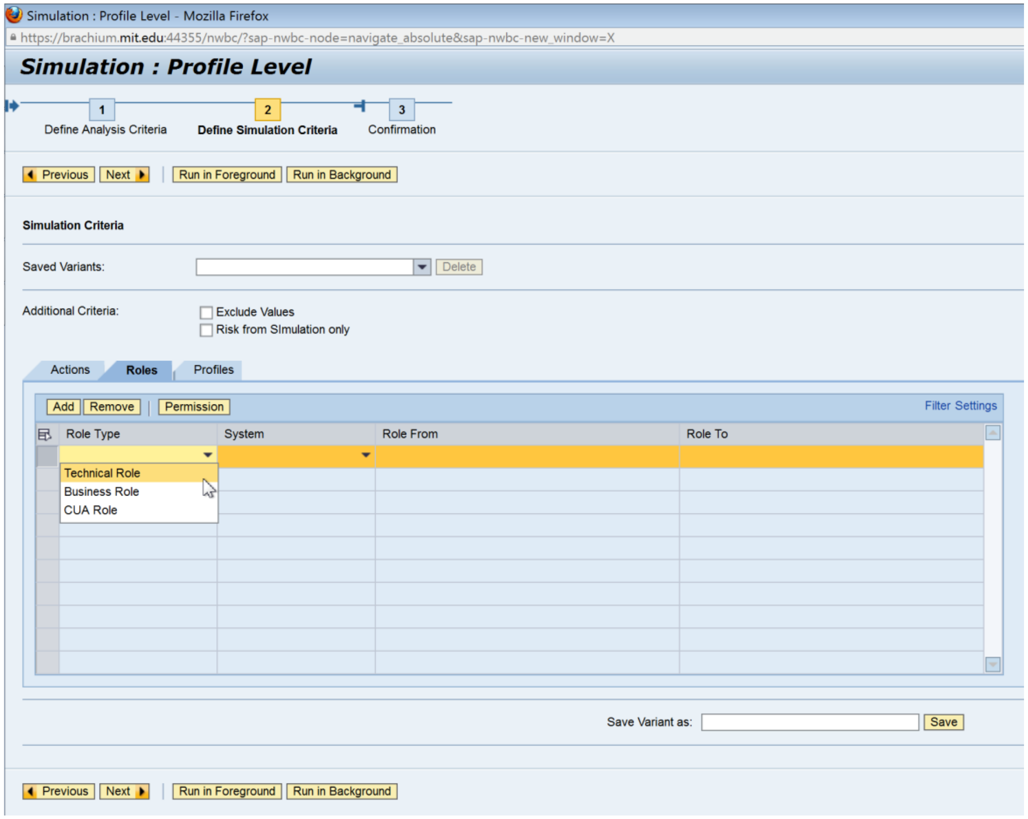
Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets

Result

View: [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Detail | Mitigate Risk | Filter Settings

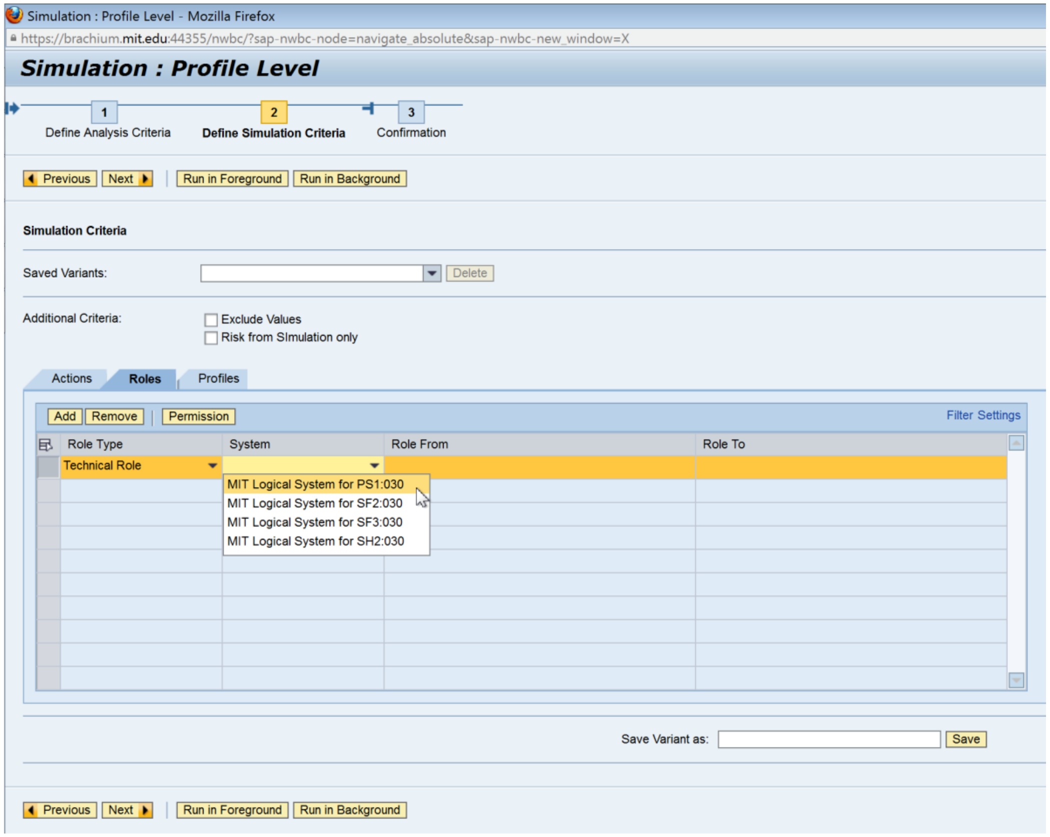
Profile ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
Z#DP:JV_FY					ZZPS103001	No Violations									

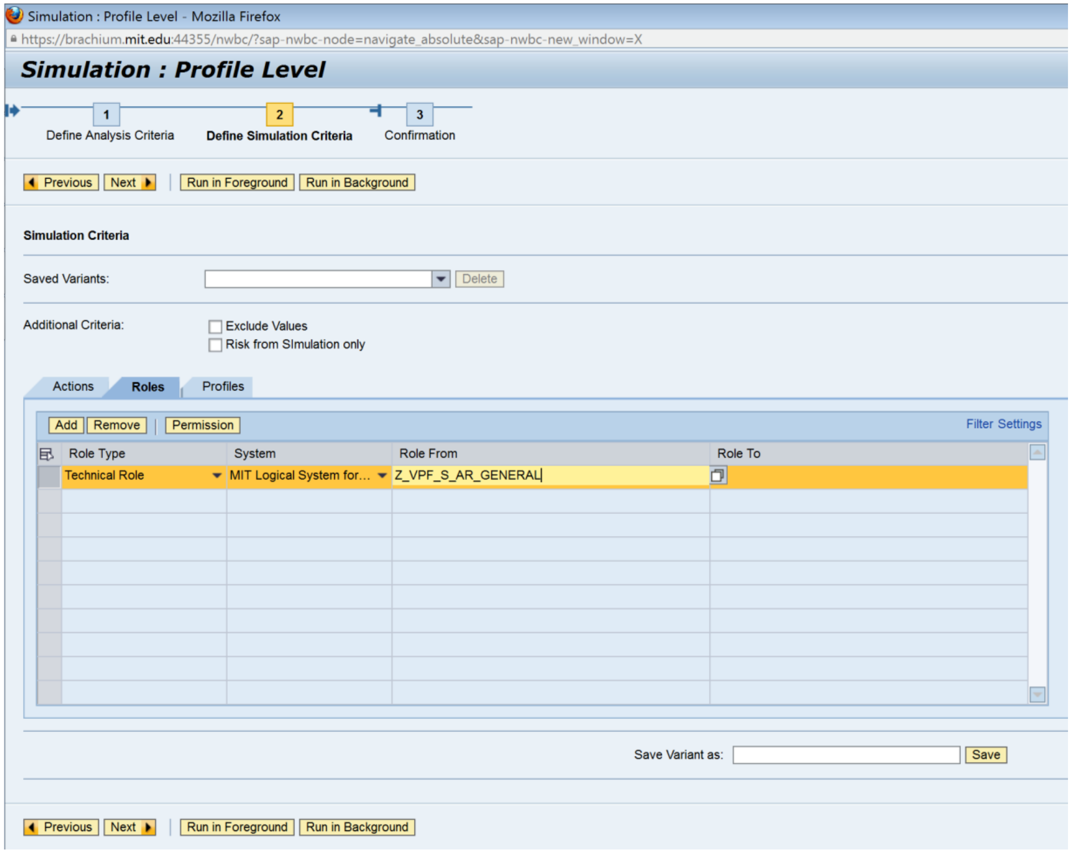
14B-1	Simulation by Role. On the ‘Roles’ tab, click on ‘Add’ to define role simulation criteria.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-n Simulation : Profile Level 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Previous Next Run in Foreground Run in Background Simulation Criteria Saved Variants: Delete Additional Criteria: □ Exclude Values □ Risk from Simulation only Actions Roles Profiles Add Remove Permission Filter Settings Role Type System Role From Role To Previous Next Run in Foreground Run in Background

14B-2	Click the drop down on the ‘Role Type’ field and select ‘Technical Role’. For role-based simulation criteria, unless otherwise advised, the selection will always be ‘Technical Role’.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

14B-3	Click the drop down on the 'System' field and select the system from which a technical role must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Simulation : Profile Level 1 Define Analysis Criteria 2 Define Simulation Criteria 3 Confirmation Previous Next Run in Foreground Run in Background Simulation Criteria Saved Variants: Delete Additional Criteria: □ Exclude Values □ Risk from SImulation only Actions Roles Profiles Add Remove Permission Filter Settings Role Type System Role From Role To Technical Role MIT Logical System for PS1:030 MIT Logical System for SF2:030 MIT Logical System for SF3:030 MIT Logical System for SH2:030 Save Variant as: Save Previous Next Run in Foreground Run in Background

14B-4	Add the role. In this case, 'Z_VPF_S_AR_GENERAL' was typed in. The search option can also be used to search for a Role. Please refer to the 'Search for Input Values' reference document (R3) for further information. NOTE: If the added role's authorizations should be excluded from the original Profile for the simulation, the 'Exclude Values' box must be checked. Otherwise, authorizations from any added roles will be added to the original Profile for the simulation.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

Previous | Next | Run in Foreground | Run in Background

Simulation Criteria

Saved Variants: [ ] Delete

Additional Criteria: □ Exclude Values
□ Risk from Simulation only

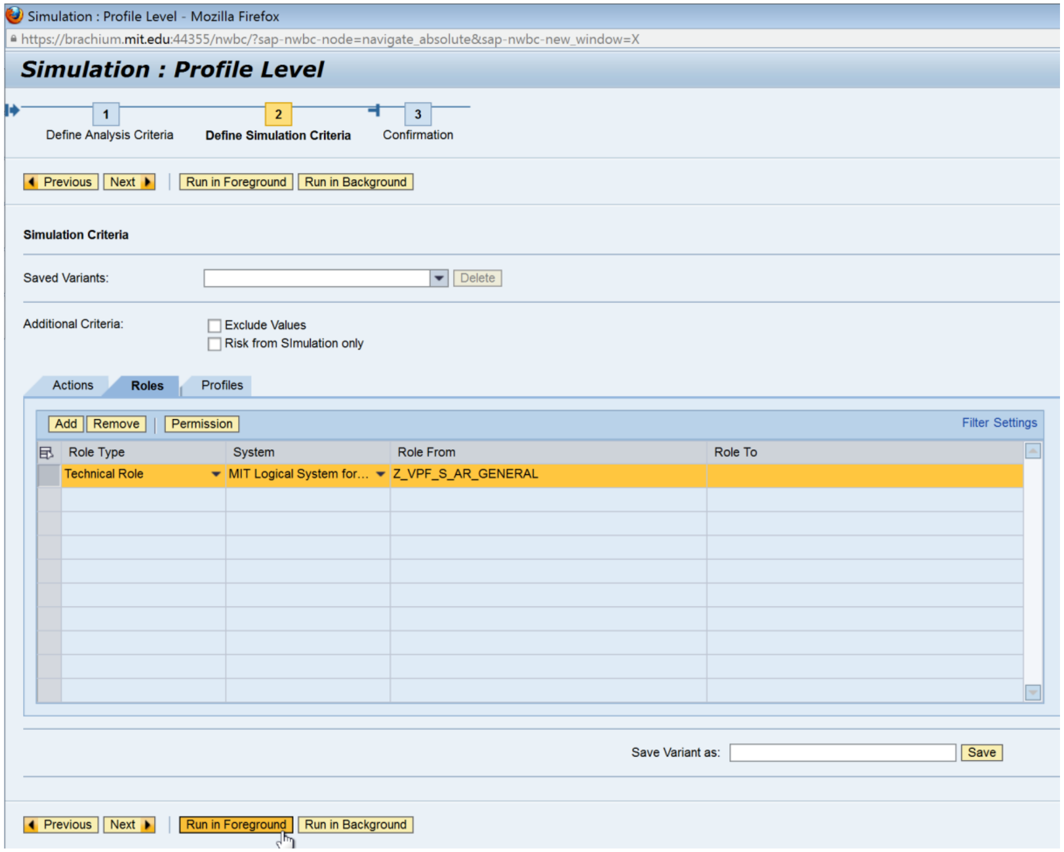
Actions | Roles | Profiles

Add | Remove | Permission — Filter Settings

Role Type	System	Role From	Role To
Technical Role	MIT Logical System for...	Z_VPF_S_AR_GENERAL	

Save Variant as: [ ] Save

Previous | Next | Run in Foreground | Run in Background

14B-5	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

Previous | Next | Run in Foreground | Run in Background

Simulation Criteria

Saved Variants: Delete

Additional Criteria:
☐ Exclude Values
☐ Risk from Simulation only

Actions | Roles | Profiles

Add | Remove | Permission | Filter Settings

Role Type	System	Role From	Role To
Technical Role	MIT Logical System for...	Z_VPF_S_AR_GENERAL	

Save Variant as: Save

Previous | Next | Run in Foreground | Run in Background

14B-6

Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information.

Any orange line items represent risks occuring due to simulation criteria.

Profile ID: SAP profile name

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

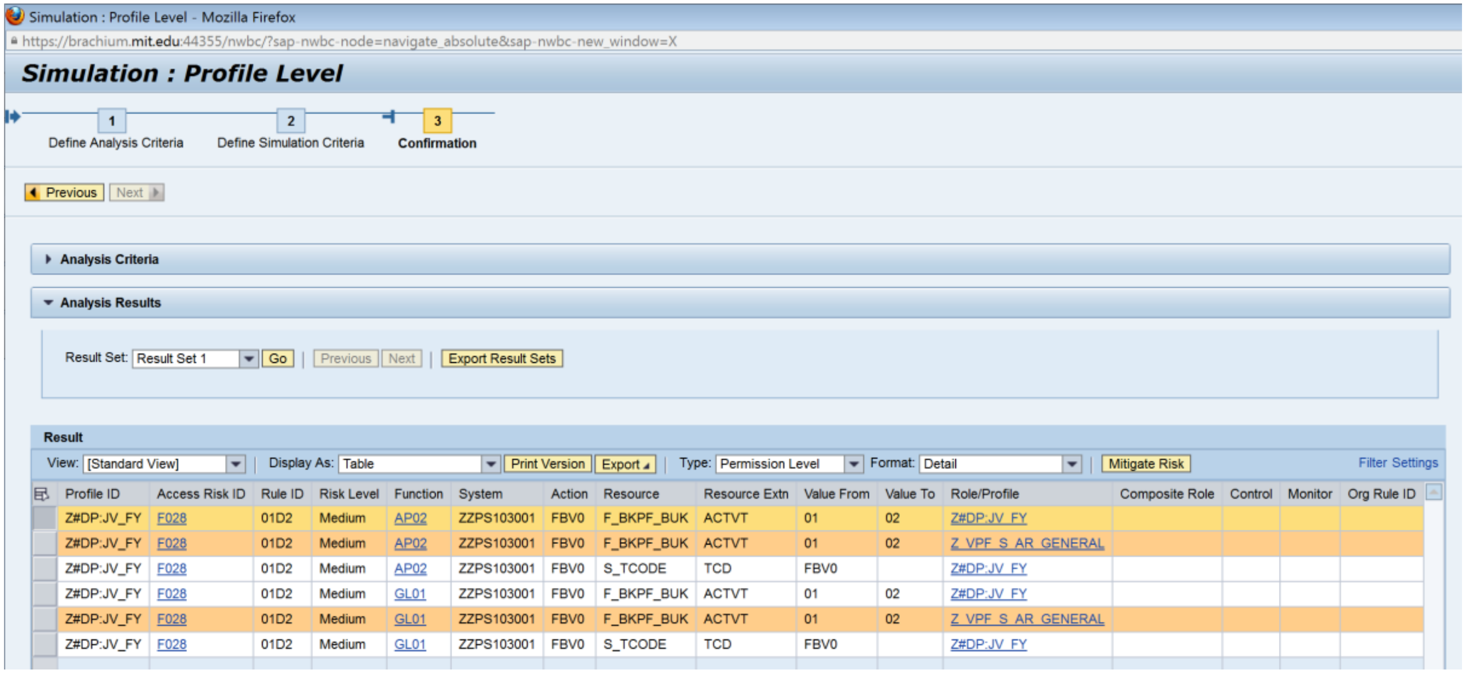
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control



Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

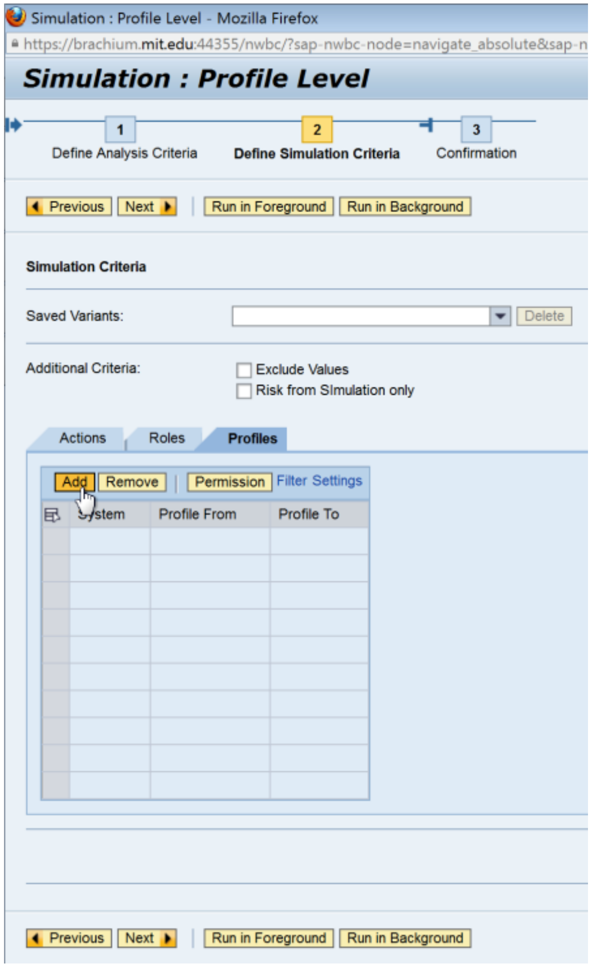
Simulation : Profile Level

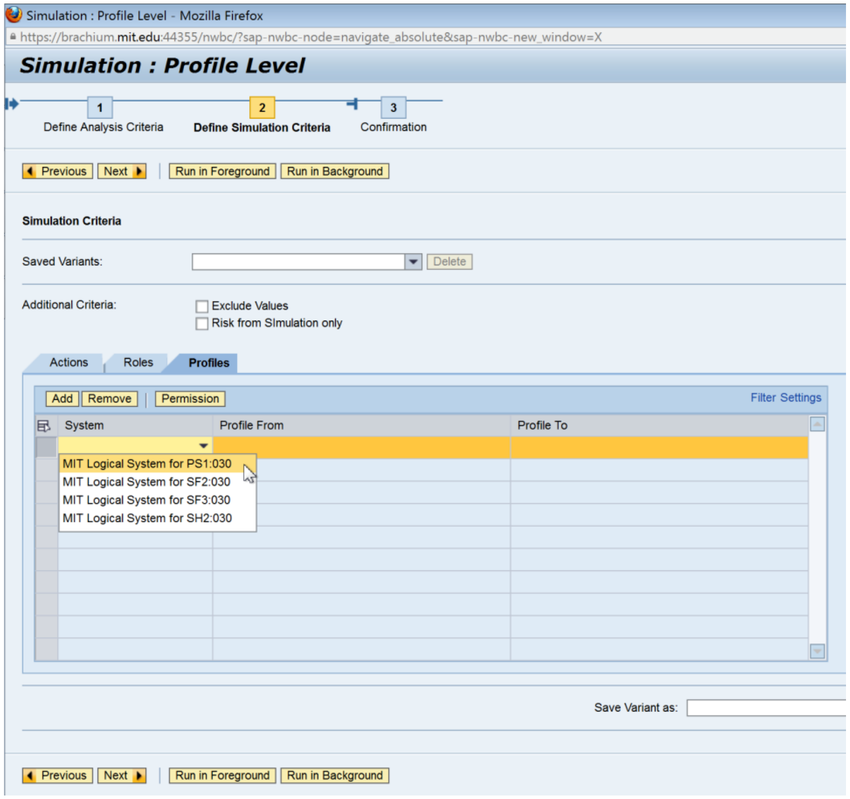
Result Set: Result Set 1

Result

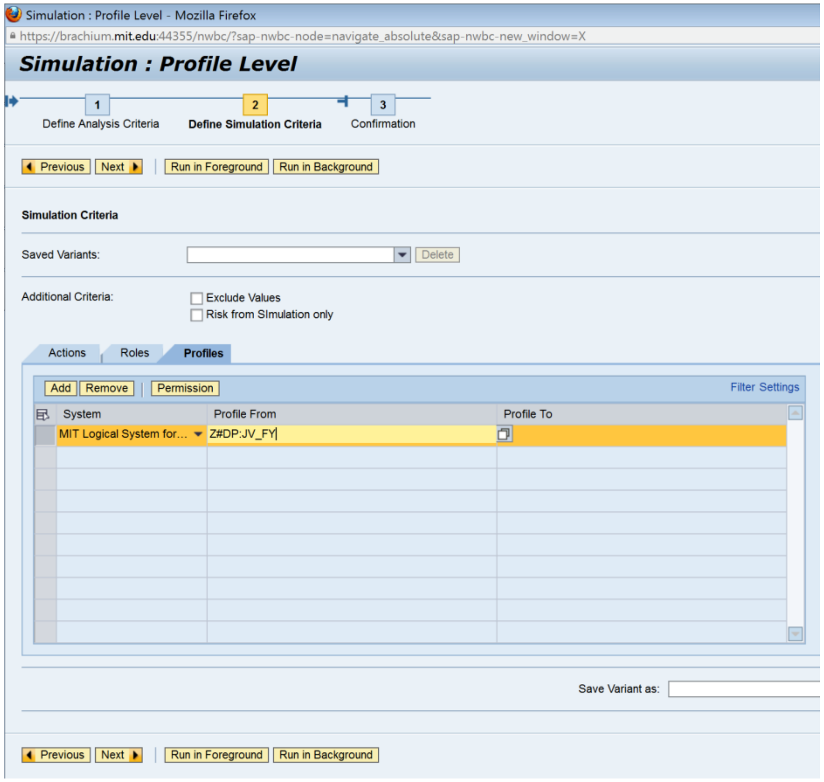
View: [Standard View] Display As: Table Type: Permission Level Format: Detail

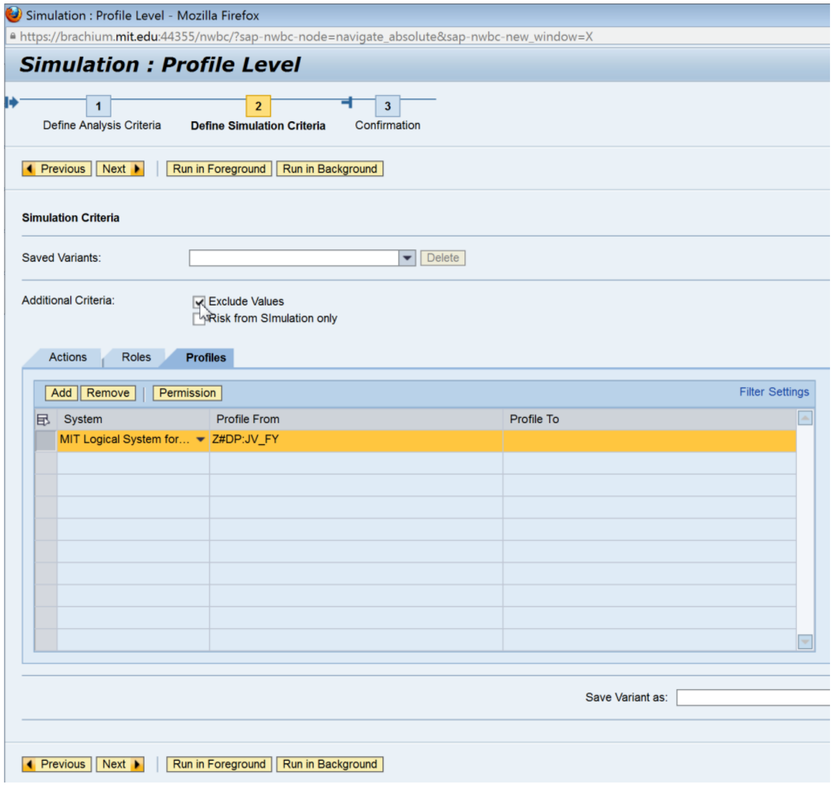
Profile ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
Z#DP:JV_FY	F028	01D2	Medium	AP02	ZZPS103001	FBV0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV_FY				
Z#DP:JV_FY	F028	01D2	Medium	AP02	ZZPS103001	FBV0	F_BKPF_BUK	ACTVT	01	02	Z_VPF_S_AR_GENERAL				
Z#DP:JV_FY	F028	01D2	Medium	AP02	ZZPS103001	FBV0	S_TCODE	TCD	FBV0		Z#DP:JV_FY				
Z#DP:JV_FY	F028	01D2	Medium	GL01	ZZPS103001	FBV0	F_BKPF_BUK	ACTVT	01	02	Z#DP:JV_FY				
Z#DP:JV_FY	F028	01D2	Medium	GL01	ZZPS103001	FBV0	F_BKPF_BUK	ACTVT	01	02	Z_VPF_S_AR_GENERAL				
Z#DP:JV_FY	F028	01D2	Medium	GL01	ZZPS103001	FBV0	S_TCODE	TCD	FBV0		Z#DP:JV_FY				

14C-1	Simulation by Profile. On the ‘Profiles’ tab, click on ‘Add’ to define profile simulation criteria.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-n Simulation : Profile Level Simulation Criteria Saved Variants: Additional Criteria: □ Exclude Values □ Risk from Simulation only

14C-2	Click the drop down on the ‘System’ field and select the system from which a profile must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected.	

Simulation : Profile Level - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
Simulation : Profile Level
1 Define Analysis Criteria
2 Define Simulation Criteria
3 Confirmation
Previous
Next
Run in Foreground
Run in Background
Simulation Criteria
Saved Variants:
Delete
Additional Criteria:
Exclude Values
Risk from Simulation only
Actions
Roles
Profiles
Add
Remove
Permission
Filter Settings
System
Profile From
Profile To
MIT Logical System for PS1:030
MIT Logical System for SF2:030
MIT Logical System for SF3:030
MIT Logical System for SH2:030
Save Variant as:
Previous
Next
Run in Foreground
Run in Background

14C-3	Add the profile. In this case, 'Z#DP:JV_FY' was typed in. The search option can also be used to search for a Profile. Please refer to the 'Search for Input Values' reference document (R3) for further information.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Profile Level** 1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation Previous Next Run in Foreground Run in Background **Simulation Criteria** Saved Variants: Delete Additional Criteria: □ Exclude Values □ Risk from Simulation only Actions Roles **Profiles** Add Remove Permission Filter Settings System: MIT Logical System for... — Profile From: Z#DP:JV_FY — Profile To: Save Variant as: Previous Next Run in Foreground Run in Background

14C-4	If authorizations from any added Profiles should be excluded from the Profile for the simulation, the ‘Exclude Values’ box must be checked. Otherwise, authorizations from any added Profiles will be added to the Profile for the simulation. The ‘Exclude Values’ box is checked in this example.	

Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

1 Define Analysis Criteria — **2 Define Simulation Criteria** — 3 Confirmation

Previous | Next | Run in Foreground | Run in Background

Simulation Criteria

Saved Variants: [ ] Delete

Additional Criteria: ☑ Exclude Values ☐ Risk from SImulation only

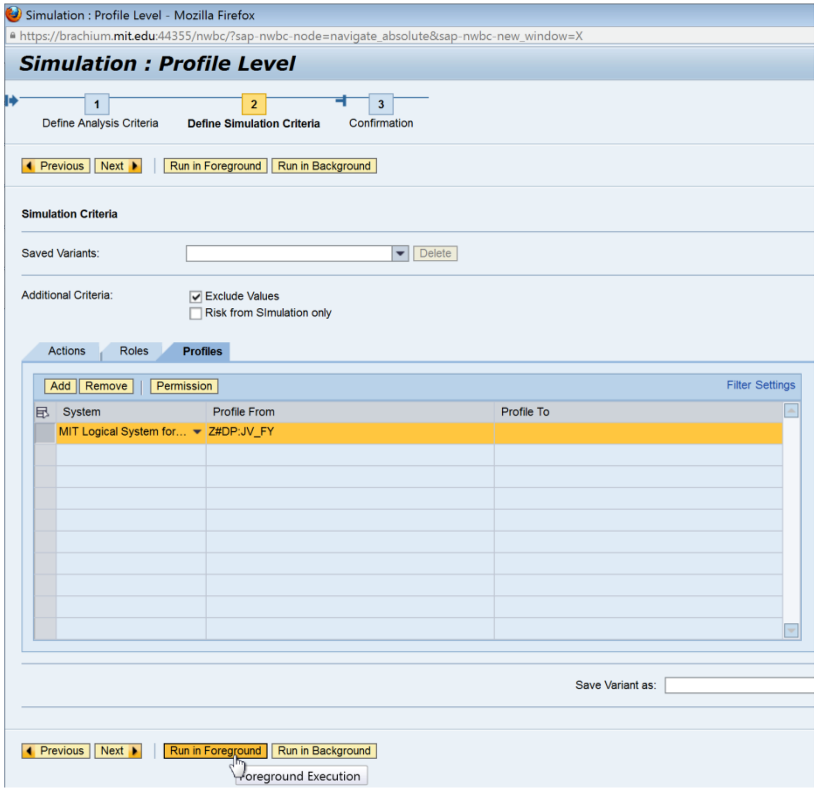
Actions | Roles | **Profiles**

Add | Remove | Permission — Filter Settings

System	Profile From	Profile To
MIT Logical System for...	Z#DP:JV_FY	

Save Variant as:

Previous | Next | Run in Foreground | Run in Background

14C-5	Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the 'Execute a Background Job' reference document (R5) for further information.	 Simulation : Profile Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Simulation : Profile Level** 1 Define Analysis Criteria – 2 **Define Simulation Criteria** – 3 Confirmation **Simulation Criteria** Saved Variants: Additional Criteria: ☑ Exclude Values ☐ Risk from Simulation only Actions / Roles / **Profiles** System | Profile From | Profile To MIT Logical System for... | Z#DP:JV_FY | Save Variant as: Previous Next Run in Foreground Run in Background Delete Add Remove Permission Filter Settings Foreground Execution

14C-6

Analyze the data. This data can also be exported. See the 'Export Data from GRC' reference document (R8) for further information.

Any orange line items represent risks occuring due to simulation criteria.

Profile ID: SAP profile name

Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist

Rule ID: The ID representing the particular rule that was triggered for that Risk

Risk Level: The risk level defined for each Access Risk in the standard rule set

Function: The ID representing the particular function that was triggered

System: The system in which the role is assigned to the user

Action: SAP transaction

Resource: SAP authorization object

Resource Extn: SAP authorization object field

Value From: SAP authorization object field value (start value for a range)

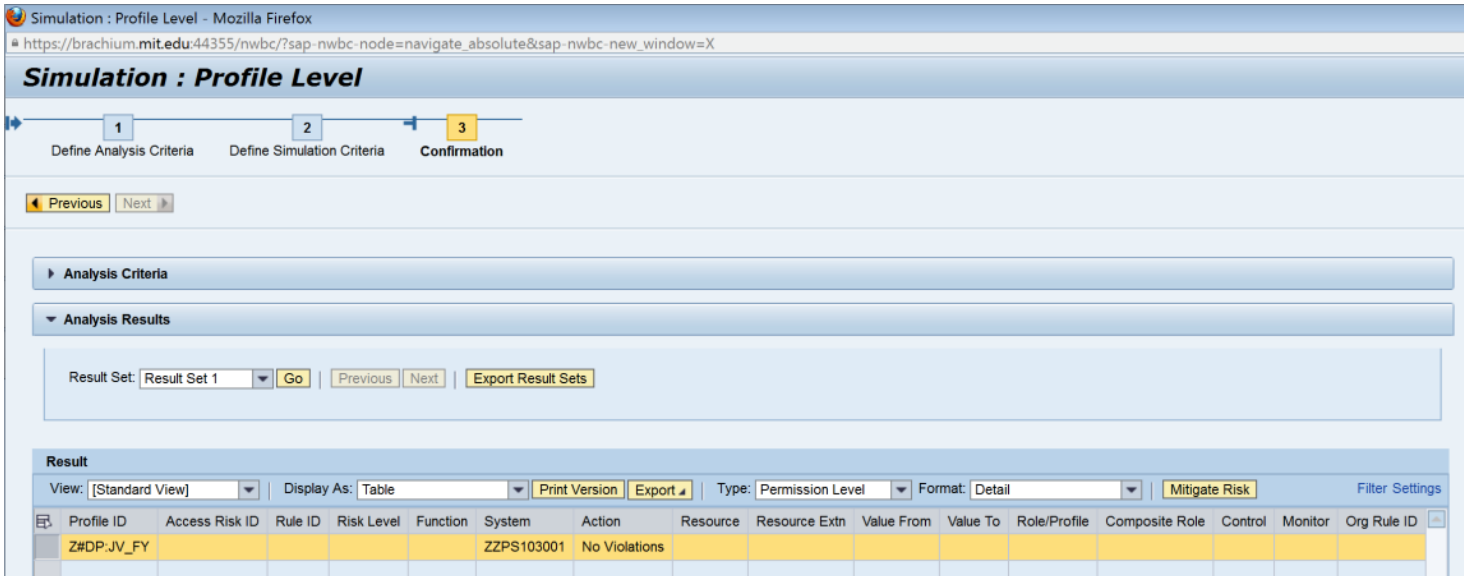
Value To: SAP authorization object field value (end value for a range)

Role/Profile: The single role/profile causing the SOD

Composite Role: The composite role containing the SOD-causing single role (if any exist)

Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk

Monitor: The user ID of the Monitor responsible for the Mitigating Control



Simulation : Profile Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Simulation : Profile Level

1 Define Analysis Criteria — 2 Define Simulation Criteria — 3 Confirmation

Result Set: Result Set 1

Result

View: [Standard View] Display As: Table Type: Permission Level Format: Detail

Profile ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
Z#DP:JV_FY					ZZPS103001	No Violations									

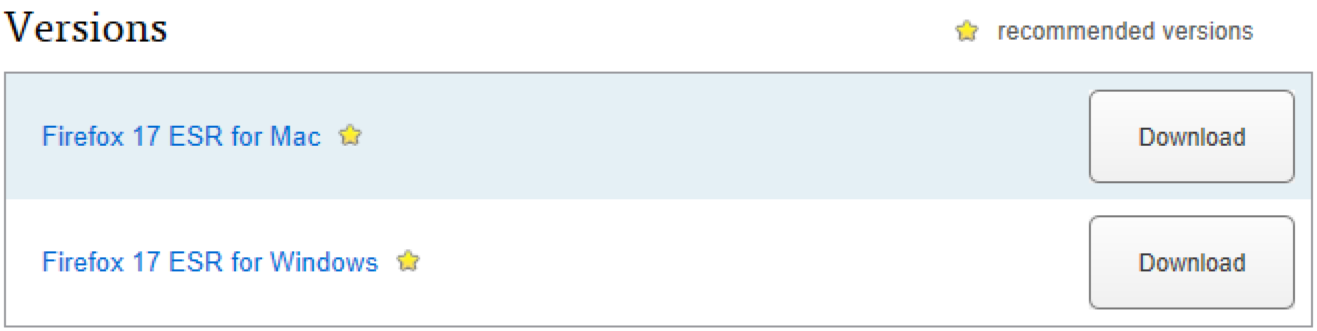
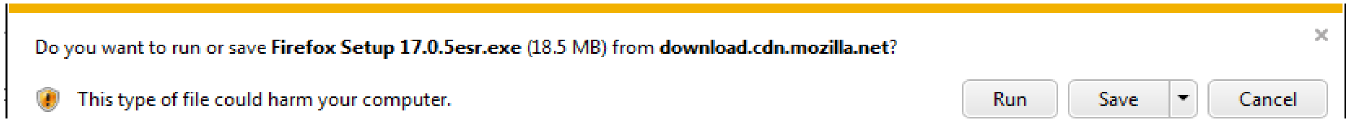
Reference Aids

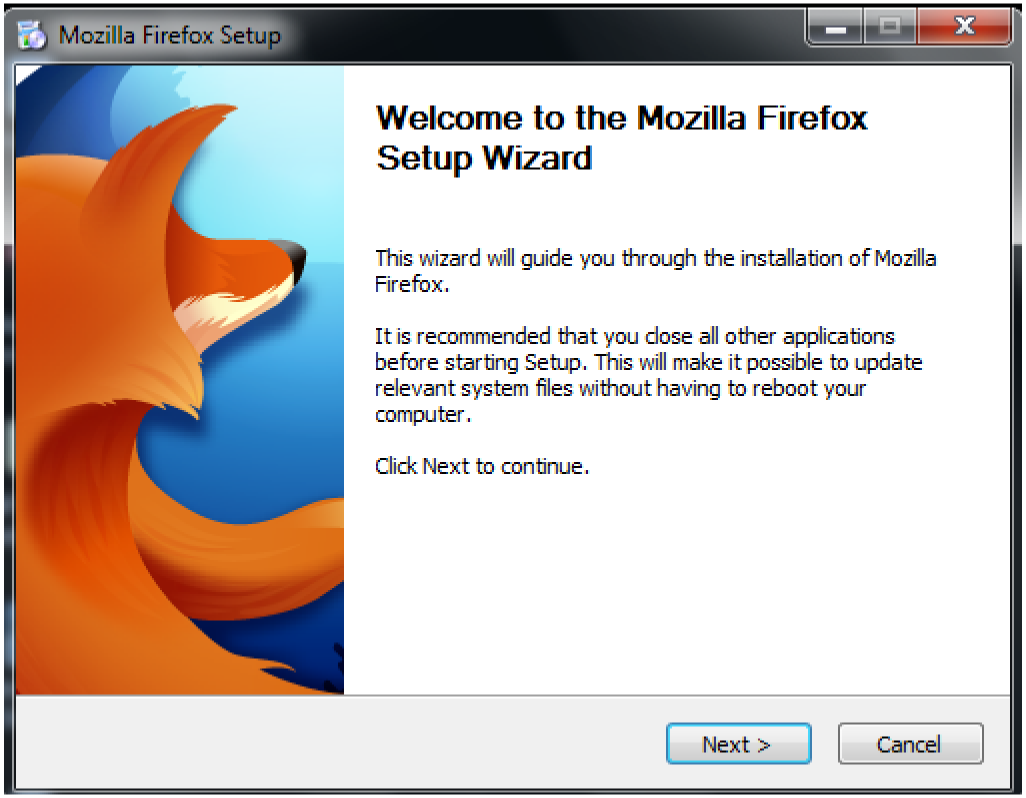
PURPOSE OF THIS DOCUMENT

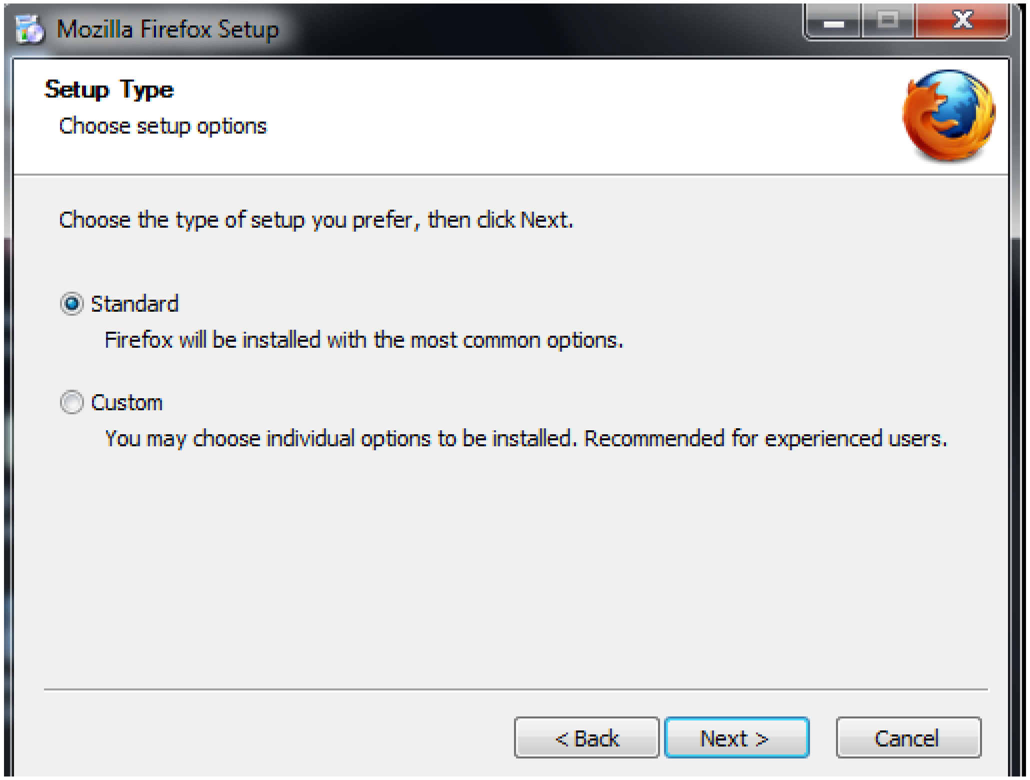
Procedures on repetitive tasks and actions related to GRC Reports are documented in reporting Reference Aids. Each Reference Aid provides details on execution for a particular repeated action.

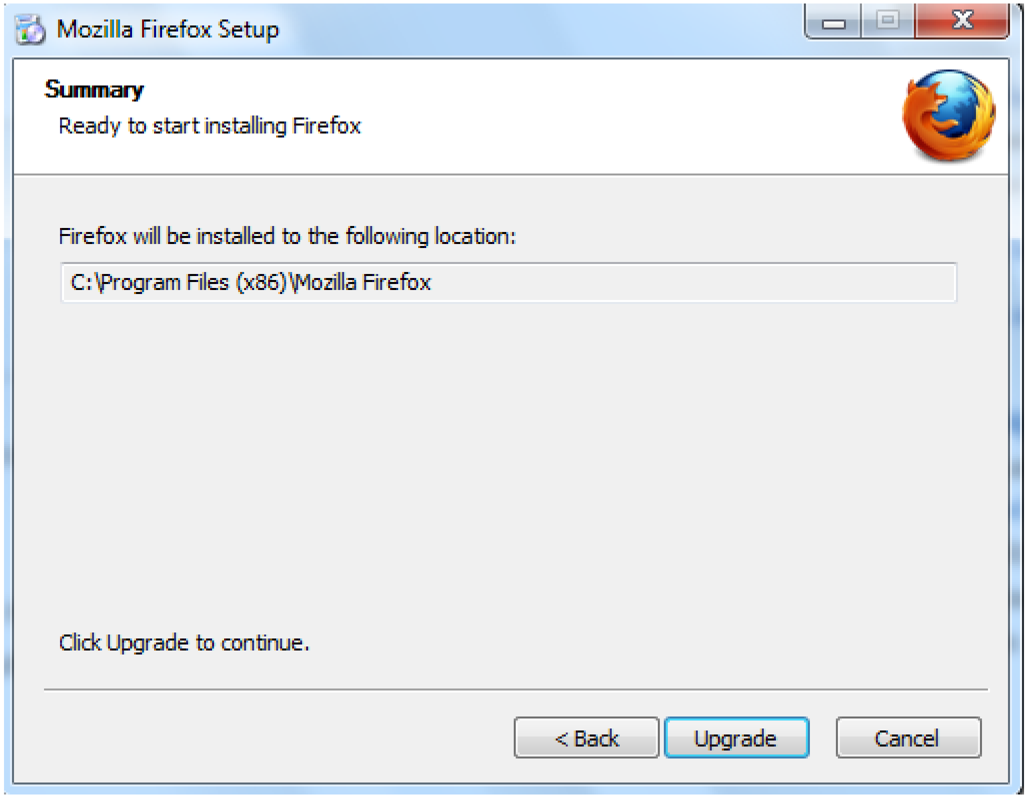
CONTENTS

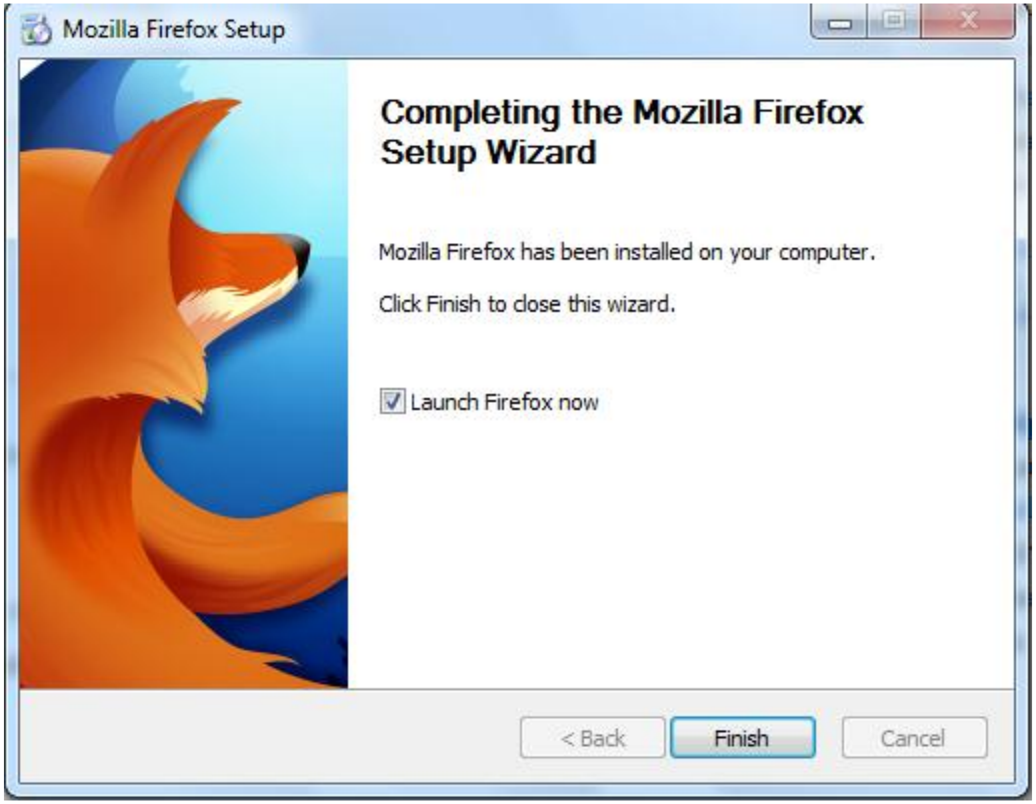
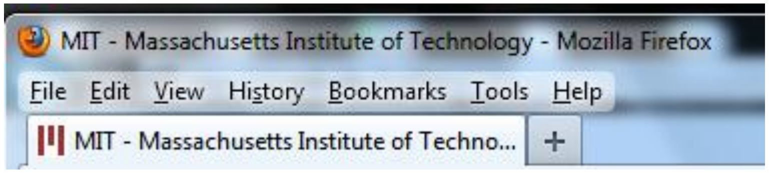
Reference R1 Access GRC Reporting

Step	Description	Screenshot
1	Install Mozilla Firefox ESR (Extended Support Release) 17 by pressing Ctrl + Click on the link.	http://ist.mit.edu/firefox
2	Click the Download button next to Firefox 17 ESR for Windows.	 Versions recommended versions Firefox 17 ESR for Mac Download Firefox 17 ESR for Windows Download
3	You will see a pop-up message. Click the *Run* button.	 Do you want to run or save **Firefox Setup 17.0.5esr.exe** (18.5 MB) from **download.cdn.mozilla.net**? This type of file could harm your computer.

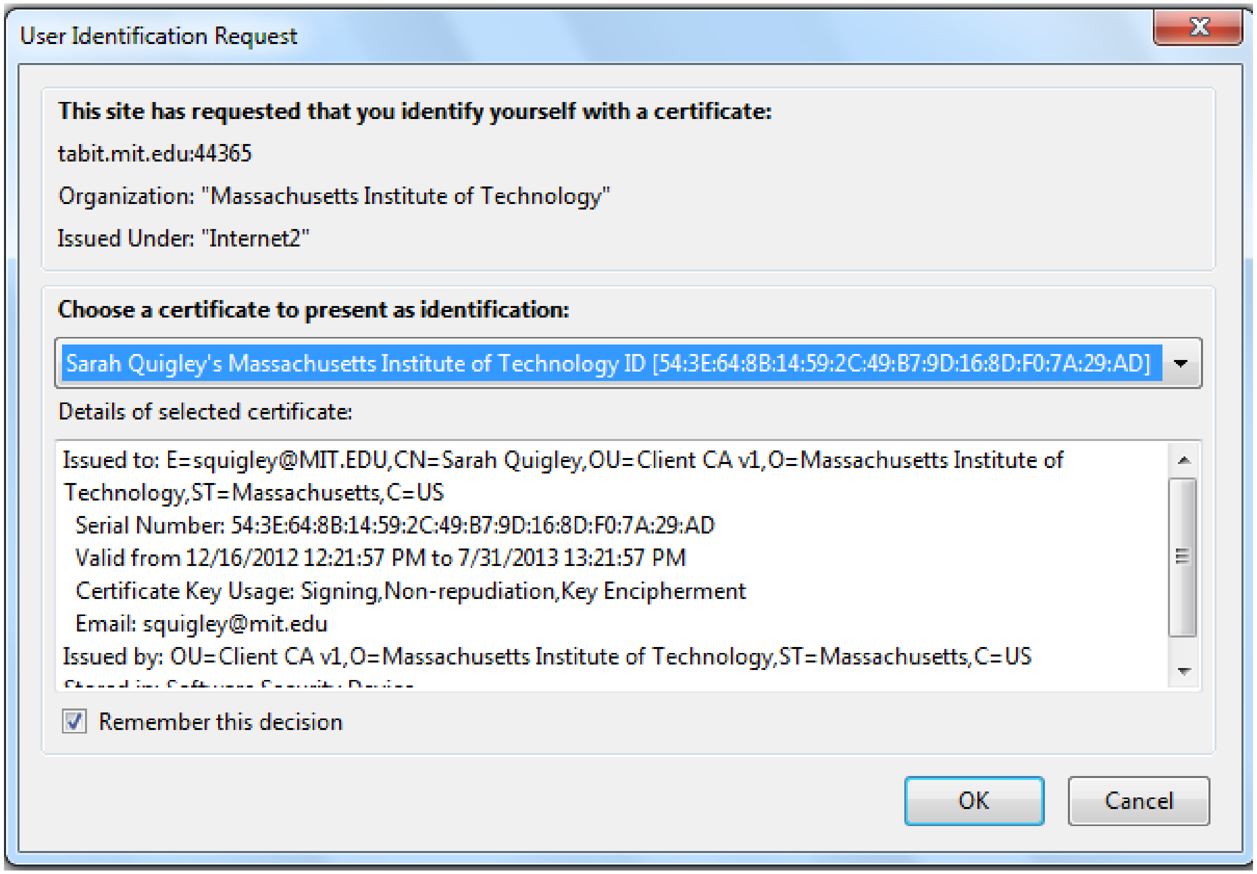
4	A '*Running Security Scan'* message will appear at the bottom of the screen. Then the Mozilla Firefox Setup Window will appear. Click *Next.*	 **Welcome to the Mozilla Firefox Setup Wizard** This wizard will guide you through the installation of Mozilla Firefox. It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer. Click Next to continue.

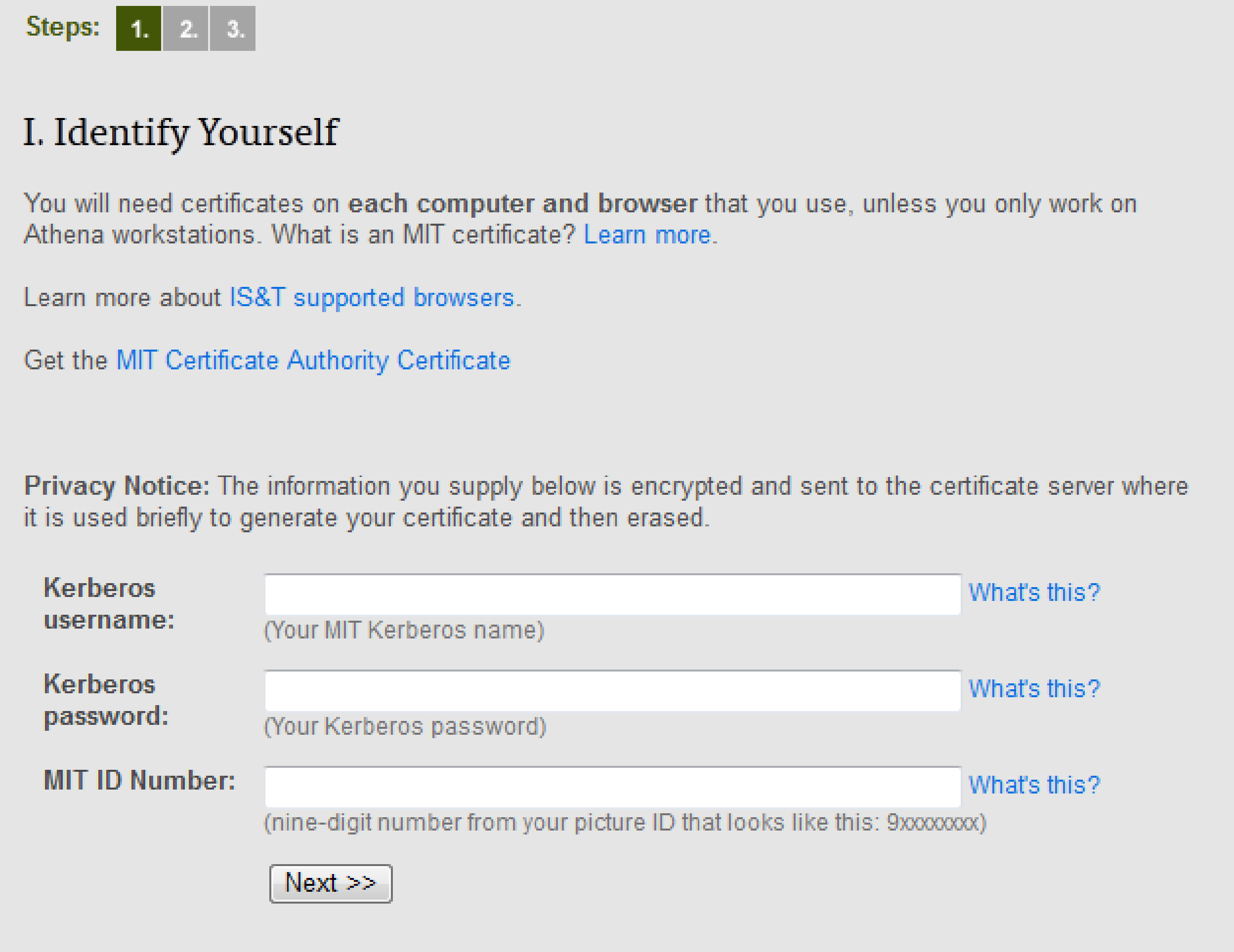
5	Leave the Setup Type option as *Standard*, which is the default. Click *Next.*	 **Setup Type** Choose setup options Choose the type of setup you prefer, then click Next. ● Standard Firefox will be installed with the most common options. ○ Custom You may choose individual options to be installed. Recommended for experienced users.

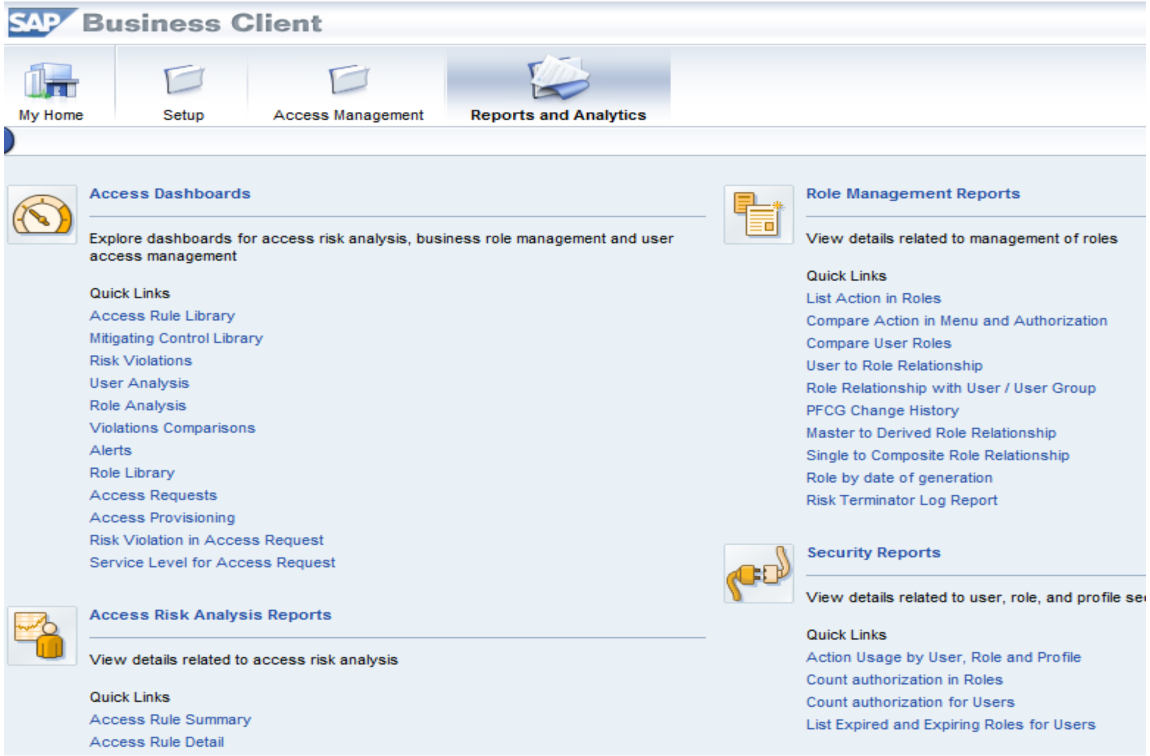
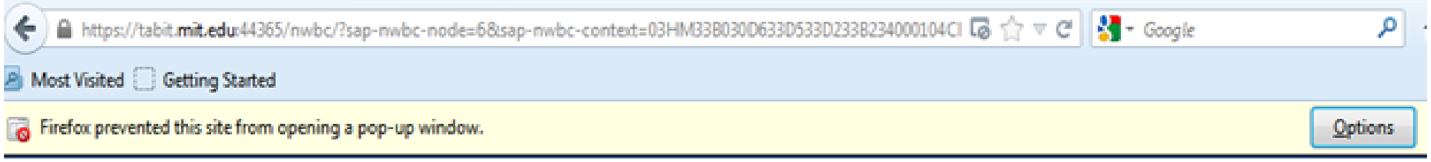
6	A screen with the installation location on the C drive will appear. Click the *Upgrade* or *Install* button.	 Mozilla Firefox Setup **Summary** Ready to start installing Firefox Firefox will be installed to the following location: C:\Program Files (x86)\Mozilla Firefox Click Upgrade to continue.

7	The Firefox Installation will run for a few seconds. Leave the *Launch Firefox Now button* selected. Click the Finish button.	 Mozilla Firefox Setup **Completing the Mozilla Firefox Setup Wizard** Mozilla Firefox has been installed on your computer. Click Finish to close this wizard. ☑ Launch Firefox now
8	The installation will complete, and you will should the Mozilla Firefox icon in the upper left corner of the MIT homepage.	 MIT - Massachusetts Institute of Technology - Mozilla Firefox File Edit View History Bookmarks Tools Help MIT - Massachusetts Institute of Techno... +

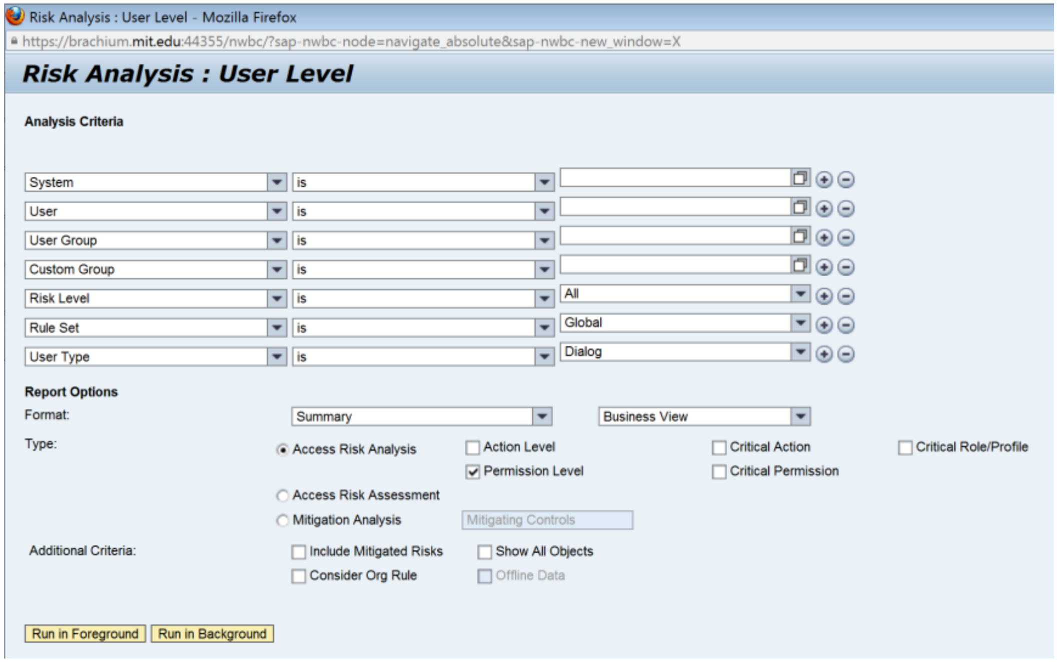
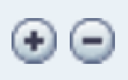
9	If you do not see the Firefox icon there, go to Start/Programs/Firefox, or double-click on the Firefox icon on the taskbar.	
10	Paste the URL for NetWeaver Business Client (NWBC) for GRC Test/QA into your Firefox browser.	https://tabit.mit.edu:44365/nwbc/?sap-client=330&sap-language=EN&sap-nwbc-node=root

11	You will see a pop-up message requesting you select your certificate for the browser. Click OK.	 User Identification Request **This site has requested that you identify yourself with a certificate:** tabit.mit.edu:44365 Organization: "Massachusetts Institute of Technology" Issued Under: "Internet2" **Choose a certificate to present as identification:** Sarah Quigley's Massachusetts Institute of Technology ID [54:3E:64:8B:14:59:2C:49:B7:9D:16:8D:F0:7A:29:AD] Details of selected certificate: Issued to: E=squigley@MIT.EDU,CN=Sarah Quigley,OU=Client CA v1,O=Massachusetts Institute of Technology,ST=Massachusetts,C=US Serial Number: 54:3E:64:8B:14:59:2C:49:B7:9D:16:8D:F0:7A:29:AD Valid from 12/16/2012 12:21:57 PM to 7/31/2013 13:21:57 PM Certificate Key Usage: Signing,Non-repudiation,Key Encipherment Email: squigley@mit.edu Issued by: OU=Client CA v1,O=Massachusetts Institute of Technology,ST=Massachusetts,C=US Stored in: Software Security Device ☑ Remember this decision

12	**Please Note**: If you receive an error related to not having a valid certificate for Firefox, enter the URL below into your browser. https://ca.mit.edu/ca/ In the fields under **Identify Yourself**, enter your Name, Kerberos ID, and Employee ID. Click Next. You will see your Certificate appear. Click OK.	 Steps: 1. 2. 3. I. Identify Yourself You will need certificates on **each computer and browser** that you use, unless you only work on Athena workstations. What is an MIT certificate? Learn more. Learn more about IS&T supported browsers. Get the MIT Certificate Authority Certificate **Privacy Notice:** The information you supply below is encrypted and sent to the certificate server where it is used briefly to generate your certificate and then erased. **Kerberos username:** (Your MIT Kerberos name) What's this? **Kerberos password:** (Your Kerberos password) What's this? **MIT ID Number:** (nine-digit number from your picture ID that looks like this: 9xxxxxxxx) What's this? Next >>

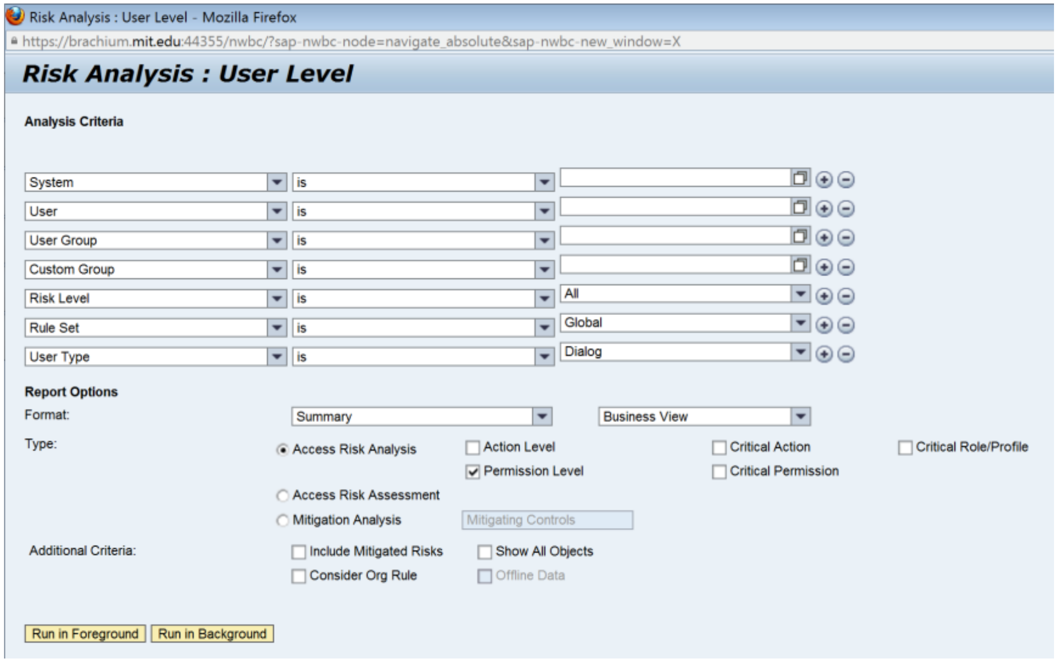
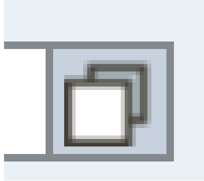
13	The NetWeaver Business Client (NWBC) screen will open. Select the *Reports and Analytics* Tab at the top. This is where we will start running GRC Reports during GRC training class.	 SAP Business Client My Home Setup Access Management Reports and Analytics **Access Dashboards** Explore dashboards for access risk analysis, business role management and user access management Quick Links Access Rule Library Mitigating Control Library Risk Violations User Analysis Role Analysis Violations Comparisons Alerts Role Library Access Requests Access Provisioning Risk Violation in Access Request Service Level for Access Request **Access Risk Analysis Reports** View details related to access risk analysis Quick Links Access Rule Summary Access Rule Detail **Role Management Reports** View details related to management of roles Quick Links List Action in Roles Compare Action in Menu and Authorization Compare User Roles User to Role Relationship Role Relationship with User / User Group PFCG Change History Master to Derived Role Relationship Single to Composite Role Relationship Role by date of generation Risk Terminator Log Report **Security Reports** View details related to user, role, and profile se Quick Links Action Usage by User, Role and Profile Count authorization in Roles Count authorization for Users List Expired and Expiring Roles for Users
14	If you see a message in the upper left corner of the NWBC screen at any time which says ‘*Firefox prevented this site from opening a pop-up window,*’ click the *Options* button in the upper right corner, and select *Always allow* for the site tabit.mit.edu.	 https://tabit.mit.edu:44365/nwbc/?sap-nwbc-node=6&sap-nwbc-context=03HM33B030D633D533D233B234000104CI Firefox prevented this site from opening a pop-up window.

Reference R2 Add or Remove Search Lines to a Report

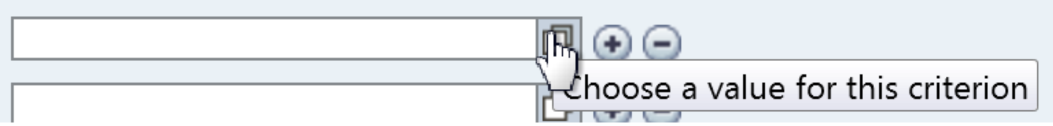
Step	Description	Screenshot
1	Execute a report containing Analysis Criteria.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Summary Business View Type: ● Access Risk Analysis □ Action Level □ Critical Action □ Critical Role/Profile ☑ Permission Level □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Show All Objects □ Consider Org Rule □ Offline Data Run in Foreground Run in Background
2	Note the '+' and '-' signs at the end of each Analysis Criteria row.	

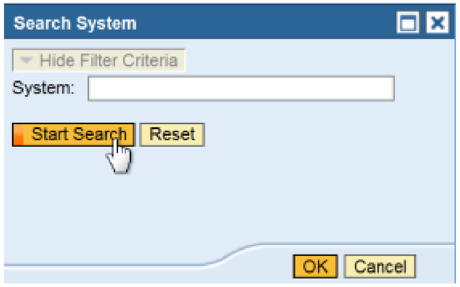
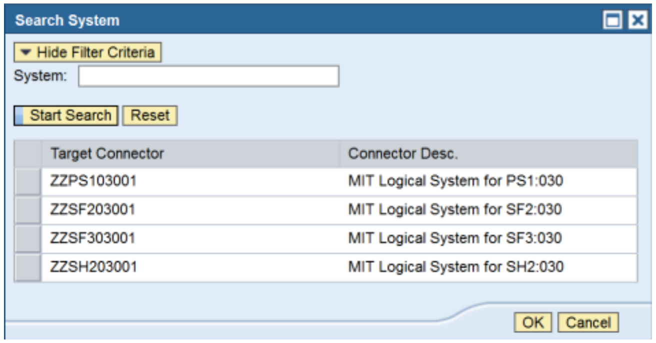
3	Click on the '-' sign to remove an Analysis Criteria row. NOTE: If a row is not being used, it should be removed to ensure the report executes correctly.	⊖
4	Click on the '+' sign to add an Analysis Criteria row. NOTE: If a row is added, the criterion category for that row can be changed using the drop down in the first column. Similarly, the operand for the criterion can be changed using the drop down in the second column.	⊕

Reference R3 Search for Input Values

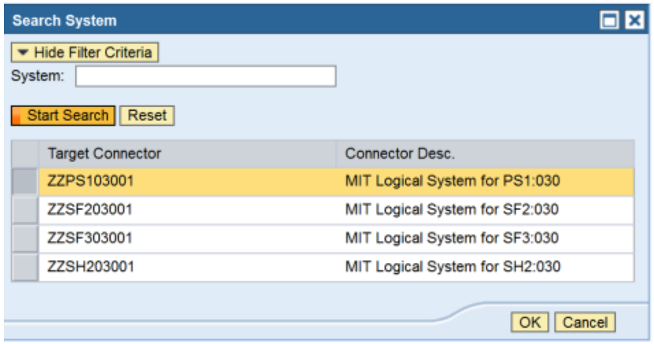
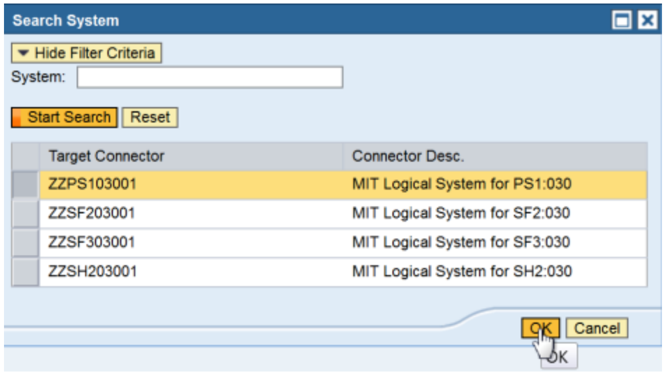
Step	Description	Screenshot
1	Execute a report containing Analysis Criteria.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ☐ Critical Role/Profile ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☐ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background
2	Note the input icon in the last column of some Analysis Criteria rows. Input values can only be searched for criteria rows with this icon	

<table>
<tr><td>3</td><td>Click on the input icon to search for a value.

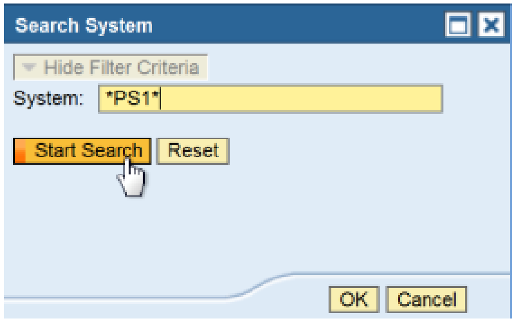
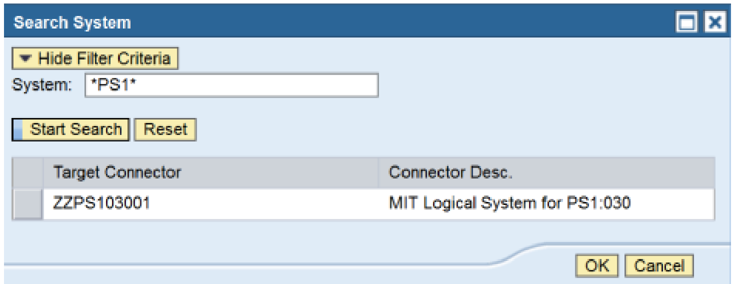
In this example, the input icon for the ‘System’ row was clicked.</td><td>
</td></tr>
<tr><td>4A-1</td><td>Click on ‘Start Search’ to carry out an open search.

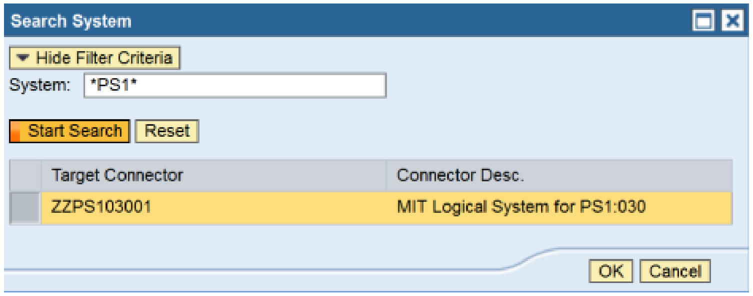
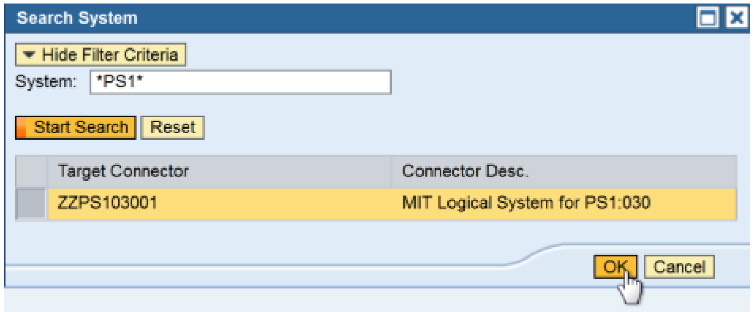
NOTE: If there are a large number of input values available, an open search is NOT recommended.</td><td>
</td></tr>
<tr><td>4A-2</td><td>A set of possible input values will be returned.</td><td>

<table>
<tr><th>Target Connector</th><th>Connector Desc.</th></tr>
<tr><td>ZZPS103001</td><td>MIT Logical System for PS1:030</td></tr>
<tr><td>ZZSF203001</td><td>MIT Logical System for SF2:030</td></tr>
<tr><td>ZZSF303001</td><td>MIT Logical System for SF3:030</td></tr>
<tr><td>ZZSH203001</td><td>MIT Logical System for SH2:030</td></tr>
</table>
</td></tr>
</table>

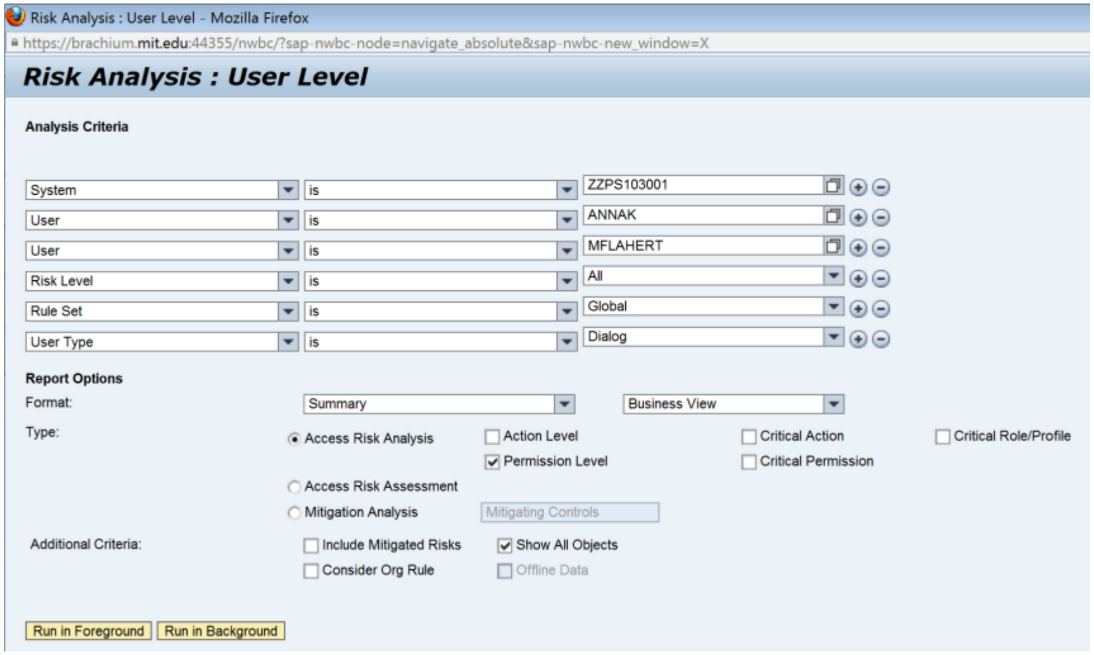
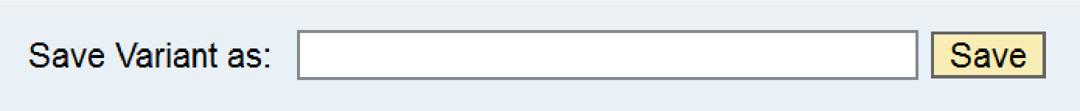
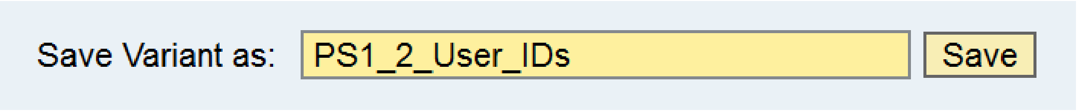
4A-3	Click on the required input value.	 Search System Hide Filter Criteria System: Start Search Reset OK Cancel Target Connector — Connector Desc. ZZPS103001 — MIT Logical System for PS1:030 ZZSF203001 — MIT Logical System for SF2:030 ZZSF303001 — MIT Logical System for SF3:030 ZZSH203001 — MIT Logical System for SH2:030
4A-4	Click ‘OK’ to enter the selected input value as your search criteria for that row.	 Search System Hide Filter Criteria System: Start Search Reset OK Cancel OK Target Connector — Connector Desc. ZZPS103001 — MIT Logical System for PS1:030 ZZSF203001 — MIT Logical System for SF2:030 ZZSF303001 — MIT Logical System for SF3:030 ZZSH203001 — MIT Logical System for SH2:030

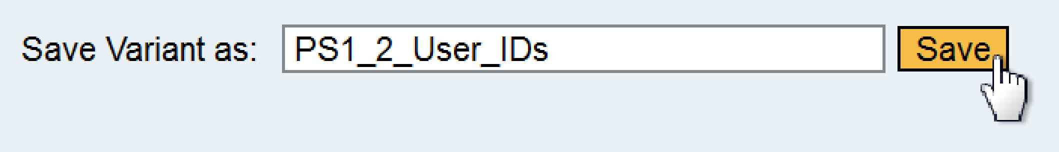
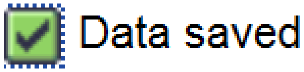
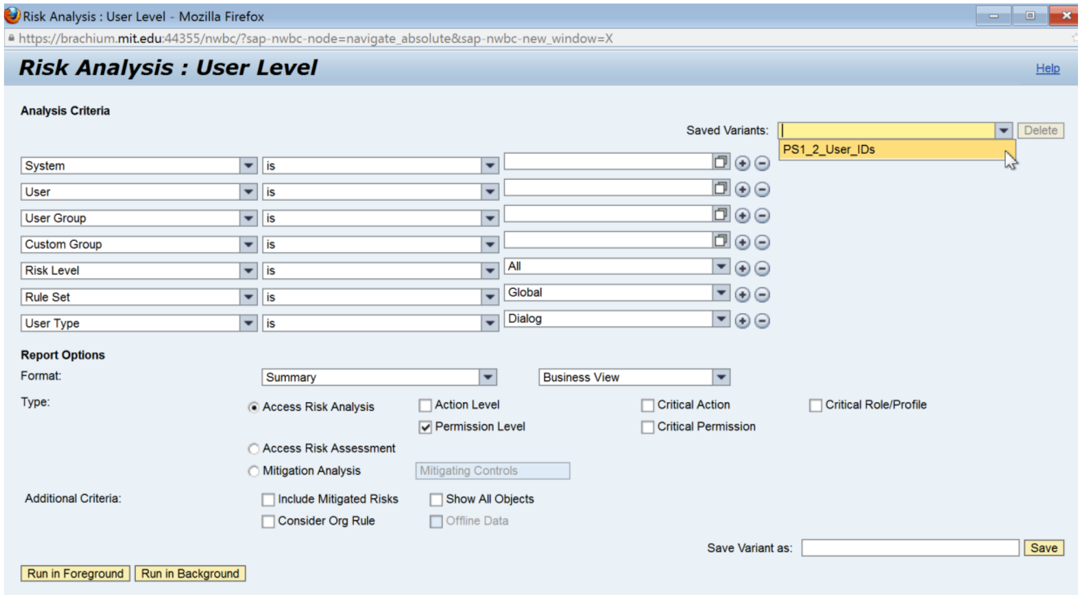
<table>
<tr>
<td>4B-1</td>
<td>Enter a search value and click on ‘Start Search’ to carry out an open search. In this case ‘*PS1*’ was entered.

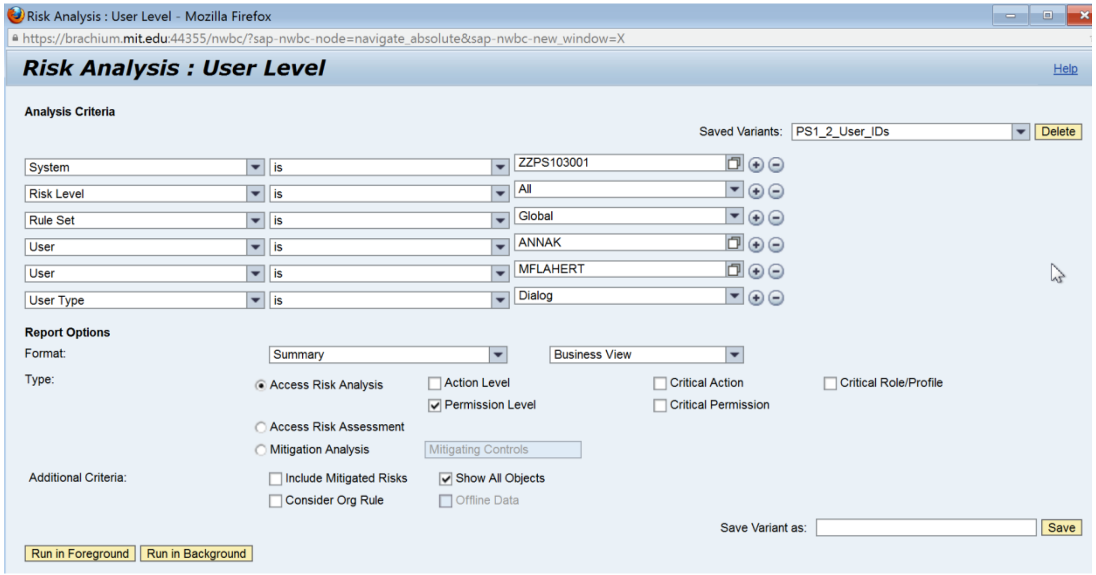
NOTE: For some searches, such as that for a particular user or role, a system will have to be defined to limit the search. In such cases, the system name with surrounding asteriks (i.e. *PS1*) is the recommended entry.</td>
<td>
System: *PS1*</td>
</tr>
<tr>
<td>4B-2</td>
<td>A set of possible input values will be returned.</td>
<td>
System: *PS1*
<table><tr><th>Target Connector</th><th>Connector Desc.</th></tr><tr><td>ZZPS103001</td><td>MIT Logical System for PS1:030</td></tr></table></td>
</tr>
</table>

4B-3	Click on the required input value.	 Search System System: *PS1* Target Connector: ZZPS103001 Connector Desc.: MIT Logical System for PS1:030 Hide Filter Criteria Start Search Reset OK Cancel
4B-4	Click 'OK' to enter the selected input value as your search criteria for that row.	 Search System System: *PS1* Target Connector: ZZPS103001 Connector Desc.: MIT Logical System for PS1:030 Hide Filter Criteria Start Search Reset OK Cancel

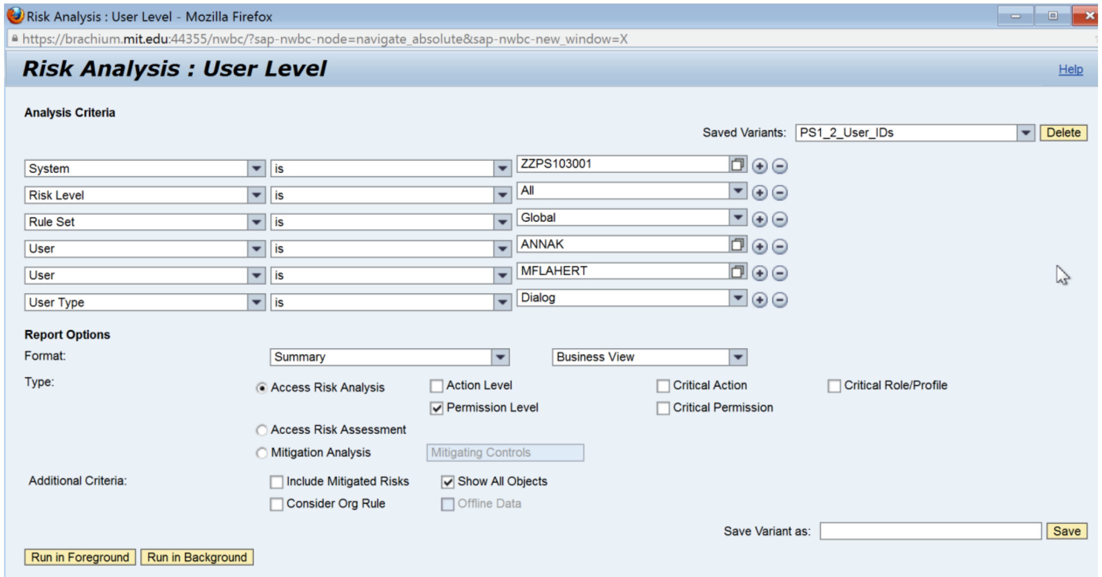
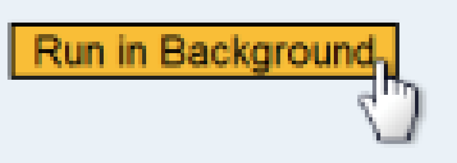
Reference R4 Save a Variant

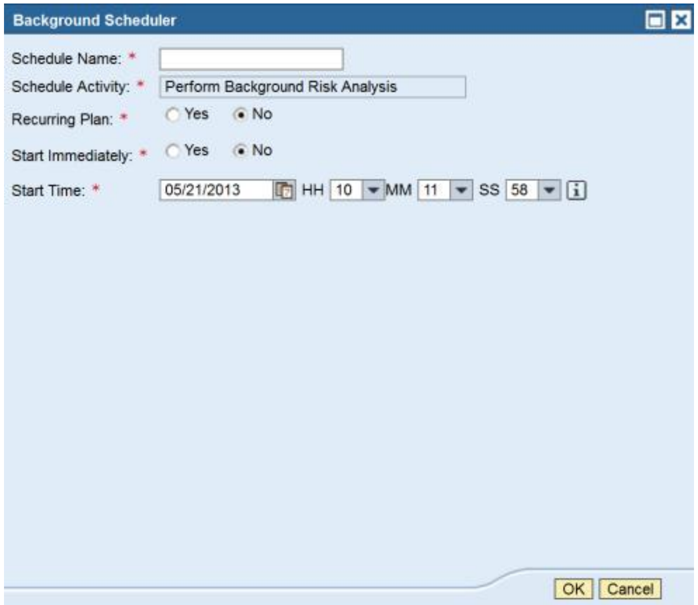
Step	Description	Screenshot
1	Execute a report and define the Analysis Criteria and Report Options required for the variant.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** **Analysis Criteria** System is ZZPS103001 User is ANNAK User is MFLAHERT Risk Level is All Rule Set is Global User Type is Dialog **Report Options** Format: Summary Business View Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ☐ Critical Role/Profile ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects ☐ Consider Org Rule ☐ Offline Data Run in Foreground Run in Background
2	Note the 'Save Variant as' bar on the bottom right of the report screen.	 Save Variant as: Save
3	Input a name for the report variant.	 Save Variant as: PS1_2_User_IDs Save

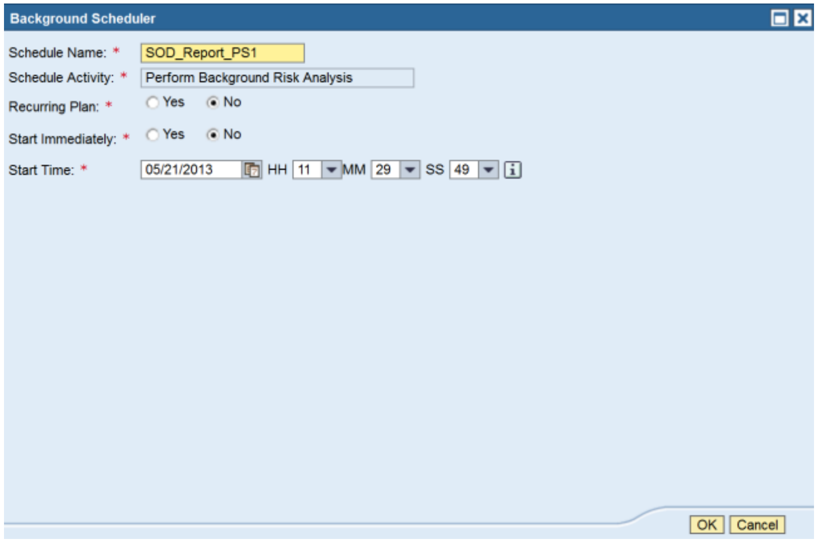
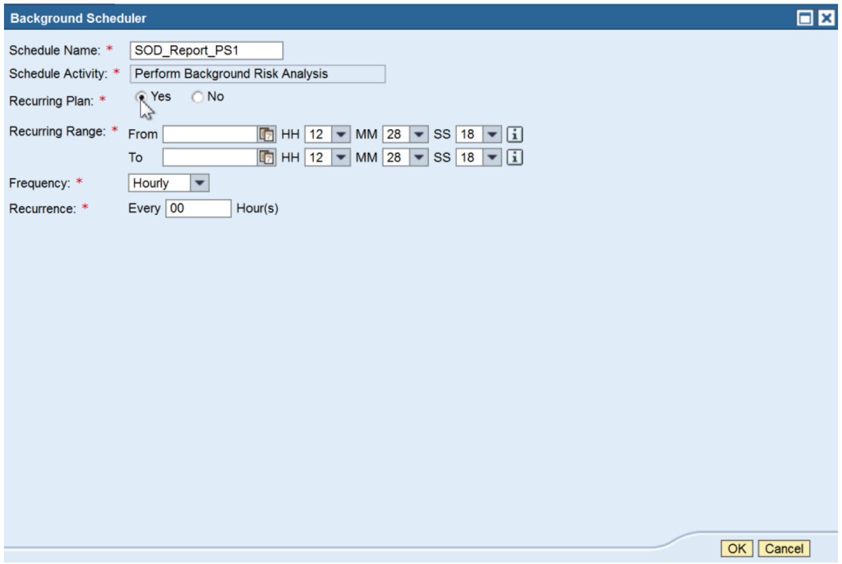
4	Click on 'Save' to save the variant.	 Save Variant as: PS1_2_User_IDs
5	A 'Data saved' message will appear	 ✓ Data saved
6	Next time the report is executed, note the 'Saved Variants' bar on the top right of the report screen. Click on the drop down menu and select the required variant.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Help Risk Analysis : User Level Analysis Criteria Saved Variants: PS1_2_User_IDs System is User is User Group is Custom Group is Risk Level is All Rule Set is Global User Type is Dialog Report Options Format: Summary Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission □ Critical Role/Profile ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Consider Org Rule □ Show All Objects □ Offline Data Save Variant as:

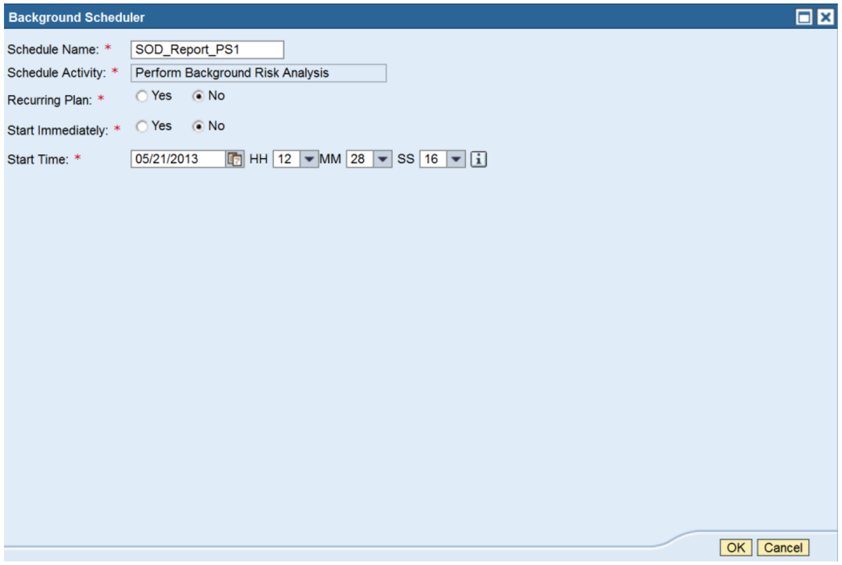
7	The Analysis Criteria and Report Options defined for the variant will appear in the report.	Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X **Risk Analysis : User Level** Help **Analysis Criteria** Saved Variants: PS1_2_User_IDs Delete System is ZZPS103001 Risk Level is All Rule Set is Global User is ANNAK User is MFLAHERT User Type is Dialog **Report Options** Format: Summary Business View Type: ● Access Risk Analysis □ Action Level □ Critical Action □ Critical Role/Profile ☑ Permission Level □ Critical Permission ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks ☑ Show All Objects □ Consider Org Rule □ Offline Data Save Variant as: Save Run in Foreground Run in Background

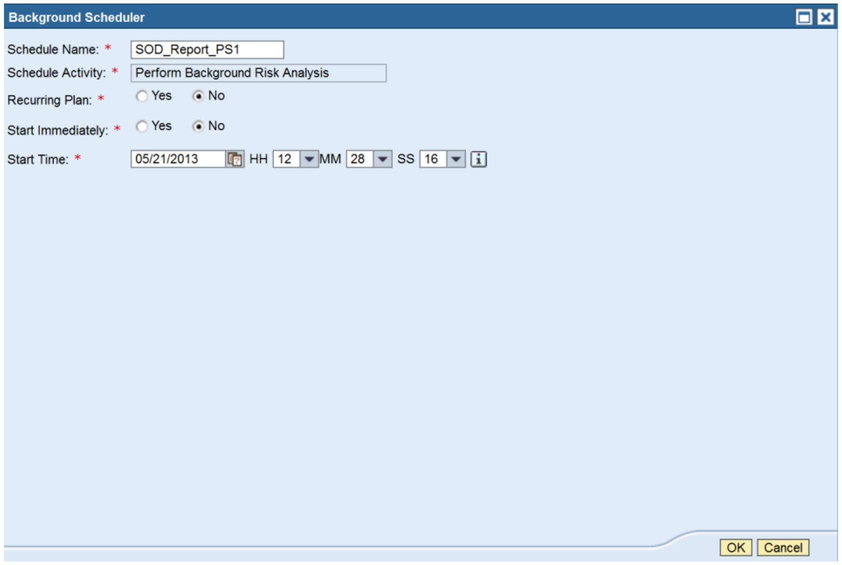
Reference R5 Execute a Background Job

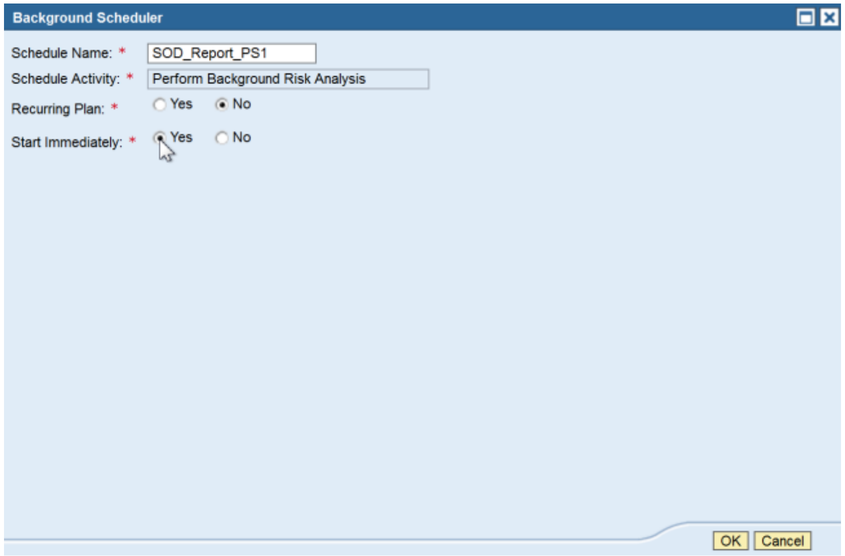
Step	Description	Screenshot
1	Execute a report and define the Analysis Criteria and Report Options required for the job.	 Risk Analysis : User Level - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Risk Analysis : User Level Help Analysis Criteria Saved Variants: PS1_2_User_IDs Delete System is ZZPS103001 Risk Level is All Rule Set is Global User is ANNAK User is MFLAHERT User Type is Dialog Report Options Format: Summary Business View Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission □ Critical Role/Profile ○ Access Risk Assessment ○ Mitigation Analysis Mitigating Controls Additional Criteria: □ Include Mitigated Risks □ Consider Org Rule ☑ Show All Objects □ Offline Data Save Variant as: Save Run in Foreground Run in Background
2	Click on the ‘Run in Background’ button on the bottom left of the report.	 Run in Background

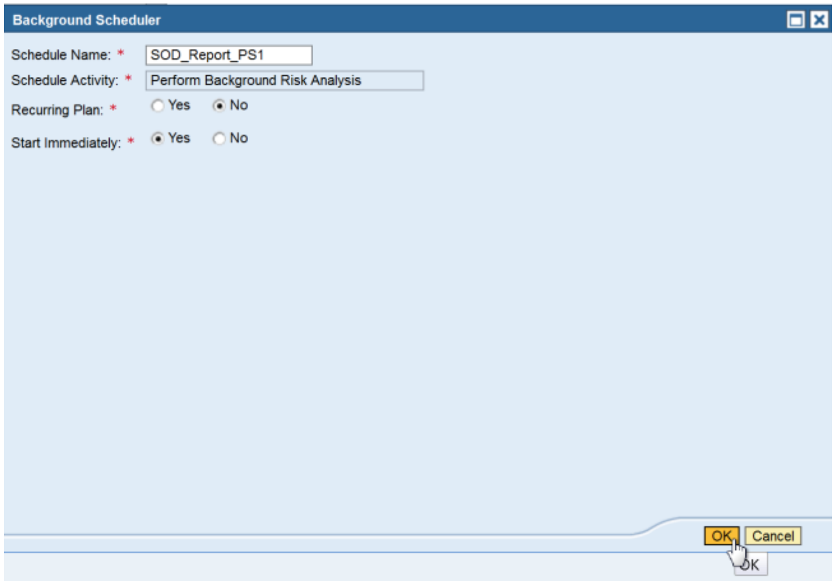
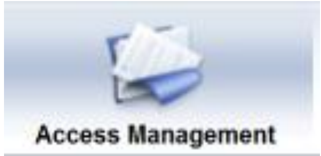
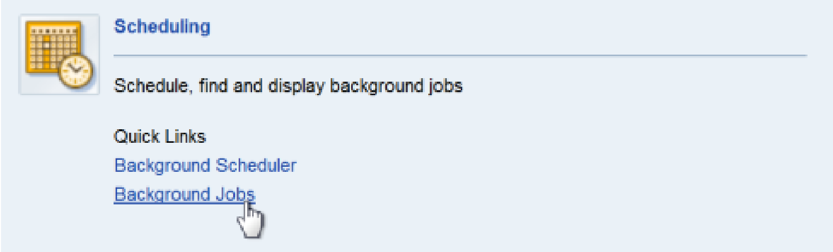
3	A 'Background Scheduler' window will appear.	 Background Scheduler Schedule Name: * Schedule Activity: * Perform Background Risk Analysis Recurring Plan: * ○ Yes ● No Start Immediately: * ○ Yes ● No Start Time: * 05/21/2013 HH 10 MM 11 SS 58 OK Cancel

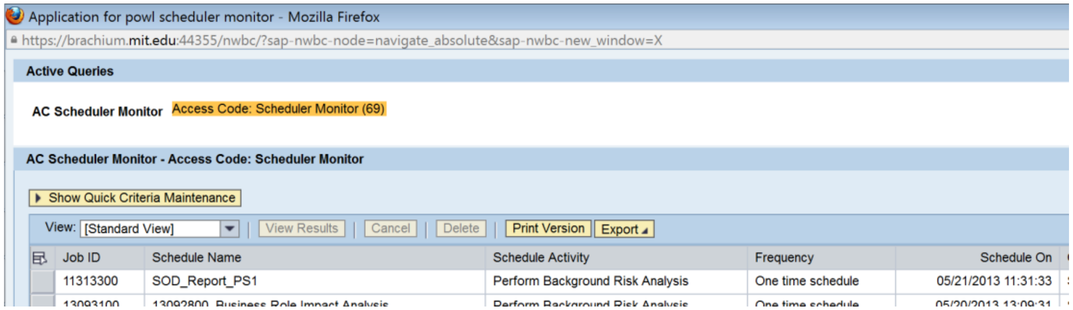
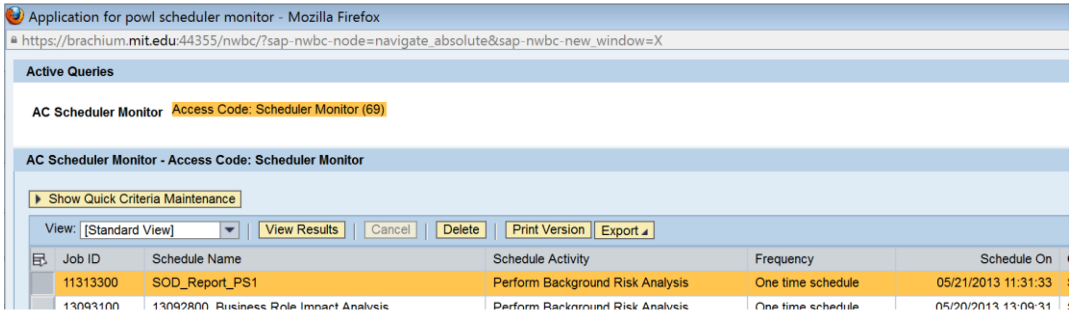
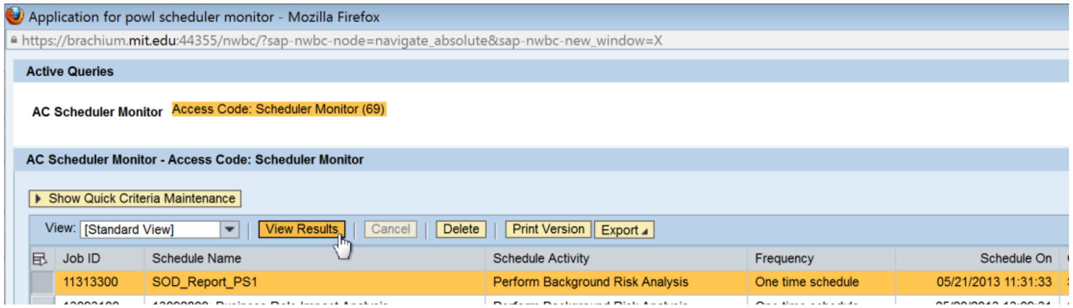
4	Enter in the name of the background job. In this case, 'SOD_Report_PS1' was entered.	 Background Scheduler Schedule Name: * SOD_Report_PS1 Schedule Activity: * Perform Background Risk Analysis Recurring Plan: * ○ Yes ● No Start Immediately: * ○ Yes ● No Start Time: * 05/21/2013 HH 11 MM 29 SS 49
5	If the job will be a recurring job, click on the 'Yes' dial button next to 'Recurring Plan'. Define the Recurrance Range, Frequency and Recurrance criteria.	 Background Scheduler Schedule Name: * SOD_Report_PS1 Schedule Activity: * Perform Background Risk Analysis Recurring Plan: * ● Yes ○ No Recurring Range: * From HH 12 MM 28 SS 18 To HH 12 MM 28 SS 18 Frequency: * Hourly Recurrence: * Every 00 Hour(s)

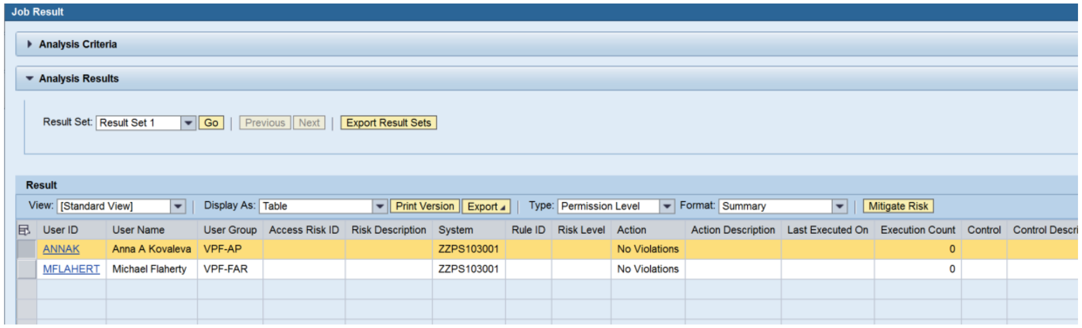
6	If the job must only be executed once, click on the ‘No’ dial button next to ‘Recurring Plan’.	 Background Scheduler Schedule Name: * SOD_Report_PS1 Schedule Activity: * Perform Background Risk Analysis Recurring Plan: * ○ Yes ● No Start Immediately: * ○ Yes ● No Start Time: * 05/21/2013 HH 12 MM 28 SS 16

7	If the job must be scheduled for a later date or time, click on the 'No' dial button next to 'Start Immediately' and enter the required 'Start Time' details.	 Background Scheduler Schedule Name: * SOD_Report_PS1 Schedule Activity: * Perform Background Risk Analysis Recurring Plan: * ○ Yes ● No Start Immediately: * ○ Yes ● No Start Time: * 05/21/2013 HH 12 MM 28 SS 16

8	If the job can be started immediately, click on the 'Yes' dial button next to 'Start Immediately' and enter the required 'Start Time' details.	 Background Scheduler Schedule Name: * SOD_Report_PS1 Schedule Activity: * Perform Background Risk Analysis Recurring Plan: * ○ Yes ● No Start Immediately: * ● Yes ○ No

9	Once all background job criteria have been entered, click on 'OK'.	 Background Scheduler Schedule Name: * SOD_Report_PS1 Schedule Activity: * Perform Background Risk Analysis Recurring Plan: * ○ Yes ● No Start Immediately: * ● Yes ○ No
10	Navigate to the 'Access Management' tab.	
11	Click on the 'Background Jobs' link located in the 'Scheduling' section.	 Scheduling Schedule, find and display background jobs Quick Links Background Scheduler Background Jobs

12	A list of all background jobs executed by the ID that is logged in will be displayed.	 Application for powl scheduler monitor - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Active Queries AC Scheduler Monitor Access Code: Scheduler Monitor (69) AC Scheduler Monitor - Access Code: Scheduler Monitor Show Quick Criteria Maintenance View: [Standard View] View Results Cancel Delete Print Version Export Job ID | Schedule Name | Schedule Activity | Frequency | Schedule On 11313300 | SOD_Report_PS1 | Perform Background Risk Analysis | One time schedule | 05/21/2013 11:31:33 13093100 | 13092800_Business Role Impact Analysis | Perform Background Risk Analysis | One time schedule | 05/20/2013 13:09:31
13	Select the background job for which information is required.	 Application for powl scheduler monitor - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Active Queries AC Scheduler Monitor Access Code: Scheduler Monitor (69) AC Scheduler Monitor - Access Code: Scheduler Monitor Show Quick Criteria Maintenance View: [Standard View] View Results Cancel Delete Print Version Export Job ID | Schedule Name | Schedule Activity | Frequency | Schedule On 11313300 | SOD_Report_PS1 | Perform Background Risk Analysis | One time schedule | 05/21/2013 11:31:33 13093100 | 13092800_Business Role Impact Analysis | Perform Background Risk Analysis | One time schedule | 05/20/2013 13:09:31
14	Click on ‘View Results’.	 Application for powl scheduler monitor - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X Active Queries AC Scheduler Monitor Access Code: Scheduler Monitor (69) AC Scheduler Monitor - Access Code: Scheduler Monitor Show Quick Criteria Maintenance View: [Standard View] View Results Cancel Delete Print Version Export Job ID | Schedule Name | Schedule Activity | Frequency | Schedule On 11313300 | SOD_Report_PS1 | Perform Background Risk Analysis | One time schedule | 05/21/2013 11:31:33

15	The results for the report that was executed in the background will be displayed.	

Job Result

Analysis Criteria

Analysis Results

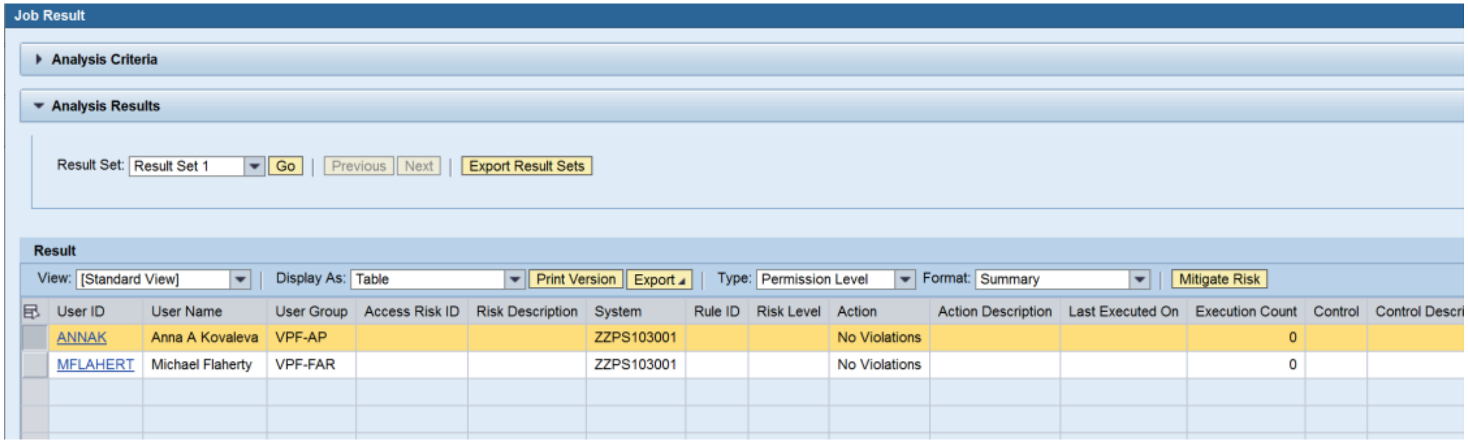
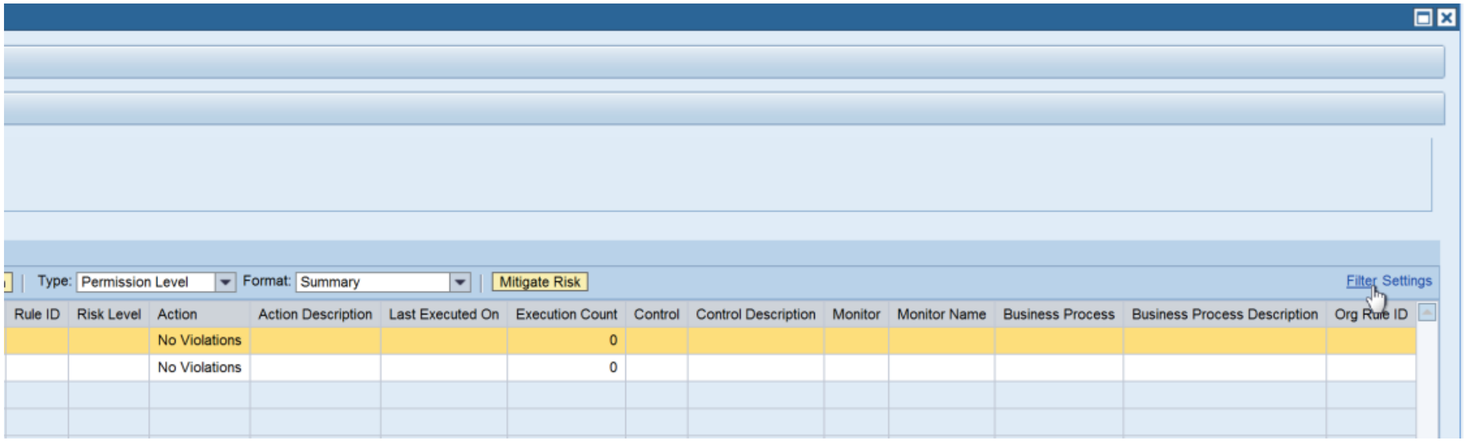
Result Set: Result Set 1 Go | Previous Next | Export Result Sets

Result

View: [Standard View] | Display As: Table Print Version Export | Type: Permission Level Format: Summary | Mitigate Risk

User ID	User Name	User Group	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action	Action Description	Last Executed On	Execution Count	Control	Control Descri
ANNAK	Anna A Kovaleva	VPF-AP			ZZPS103001			No Violations			0		
MFLAHERT	Michael Flaherty	VPF-FAR			ZZPS103001			No Violations			0		

Reference R6 Filter a Report

Step	Description	Screenshot
1	Execute a report in the foreground or background and view the results.	
2	Scroll to the right side of the report and click on the ‘Filter’ link on the top right of the report.	

Step 1 screenshot:

Job Result

Analysis Criteria

Analysis Results

Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets

Result

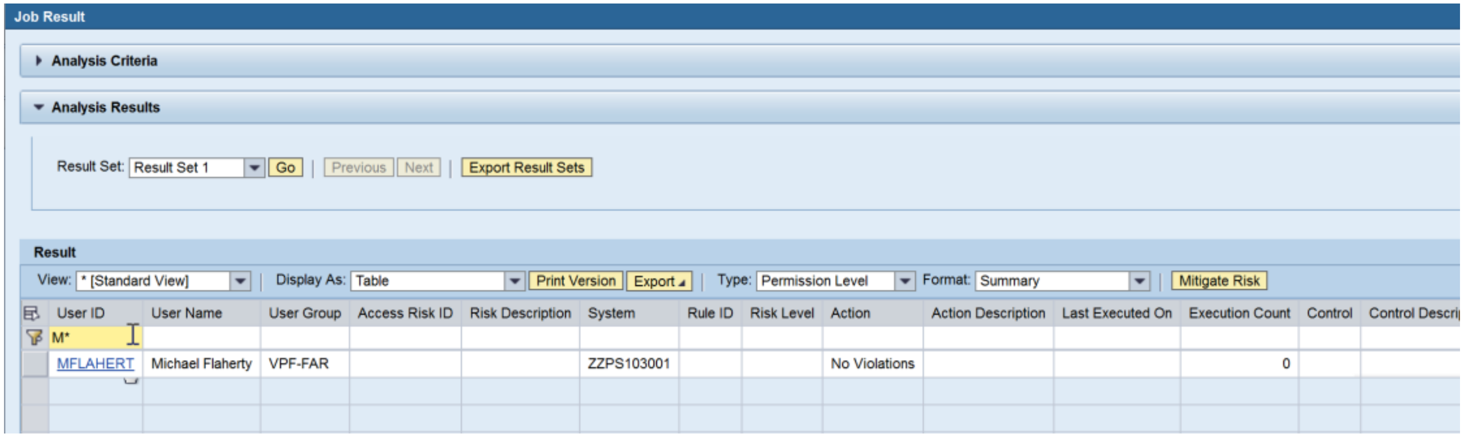
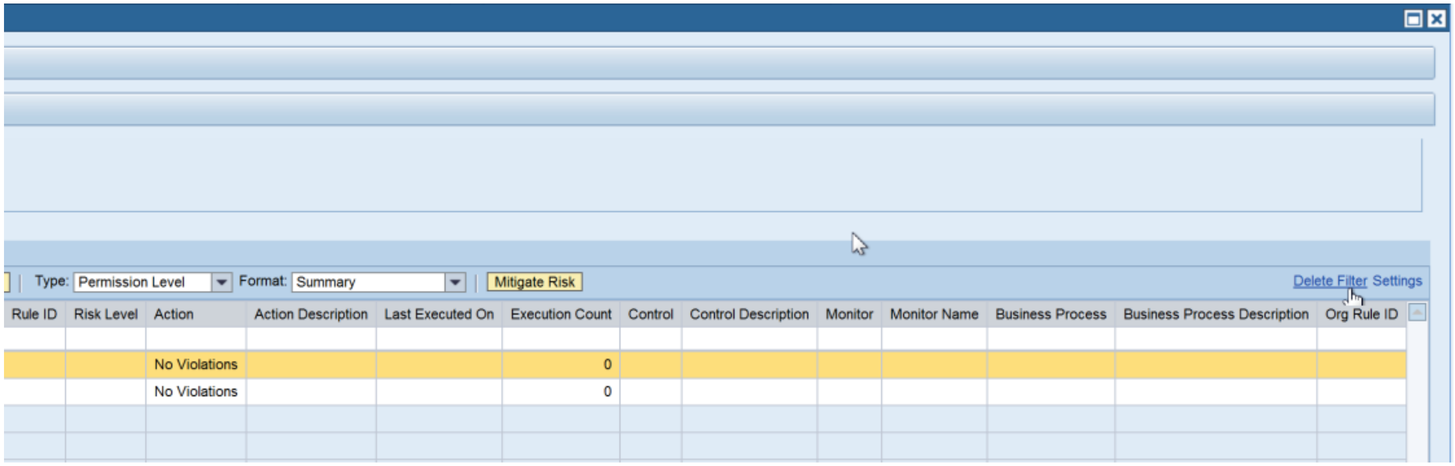
View: [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Summary | Mitigate Risk

User ID	User Name	User Group	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action	Action Description	Last Executed On	Execution Count	Control	Control Descri
ANNAK	Anna A Kovaleva	VPF-AP			ZZPS103001			No Violations			0		
MFLAHERT	Michael Flaherty	VPF-FAR			ZZPS103001			No Violations			0		

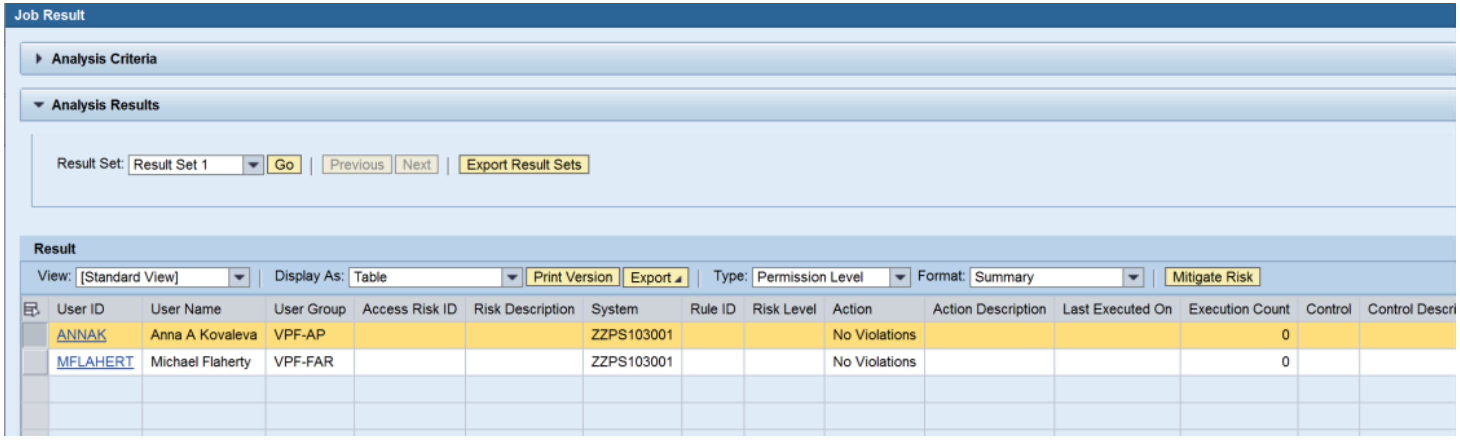
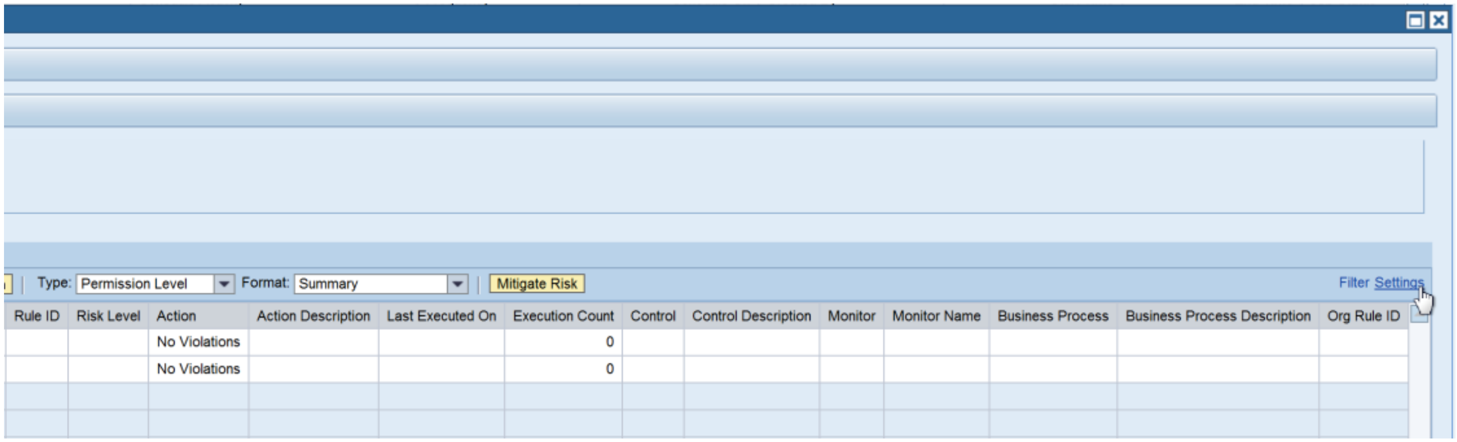
Step 2 screenshot:

Type: Permission Level | Format: Summary | Mitigate Risk | Filter Settings

Rule ID	Risk Level	Action	Action Description	Last Executed On	Execution Count	Control	Control Description	Monitor	Monitor Name	Business Process	Business Process Description	Org Rule ID
		No Violations			0							
		No Violations			0							

3	A filter row will appear at the top of the report. Enter filter criteria. Asteriks may be used.	 Job Result Analysis Criteria Analysis Results Result Set: Result Set 1 Go | Previous Next | Export Result Sets Result View: * [Standard View] | Display As: Table Print Version Export | Type: Permission Level Format: Summary | Mitigate Risk User ID | User Name | User Group | Access Risk ID | Risk Description | System | Rule ID | Risk Level | Action | Action Description | Last Executed On | Execution Count | Control | Control Descri M* MFLAHERT | Michael Flaherty | VPF-FAR | | | ZZPS103001 | | | No Violations | | | 0 | |
4	Remove the filter by clicking on the 'Delete Filter' link on the top right of the report.	 Type: Permission Level | Format: Summary | Mitigate Risk | Delete Filter Settings Rule ID | Risk Level | Action | Action Description | Last Executed On | Execution Count | Control | Control Description | Monitor | Monitor Name | Business Process | Business Process Description | Org Rule ID | | No Violations | | | 0 | | | | | | | | | No Violations | | | 0 | | | | | | |

Reference R7 Change Your Report View

Step	Description	Screenshot
1	Execute a report in the foreground or background and view the results.	
2	Scroll to the right side of the report and click on the 'Settings' link on the top right of the report.	

Step 1 screenshot:

Job Result

Analysis Criteria

Analysis Results

Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets

Result

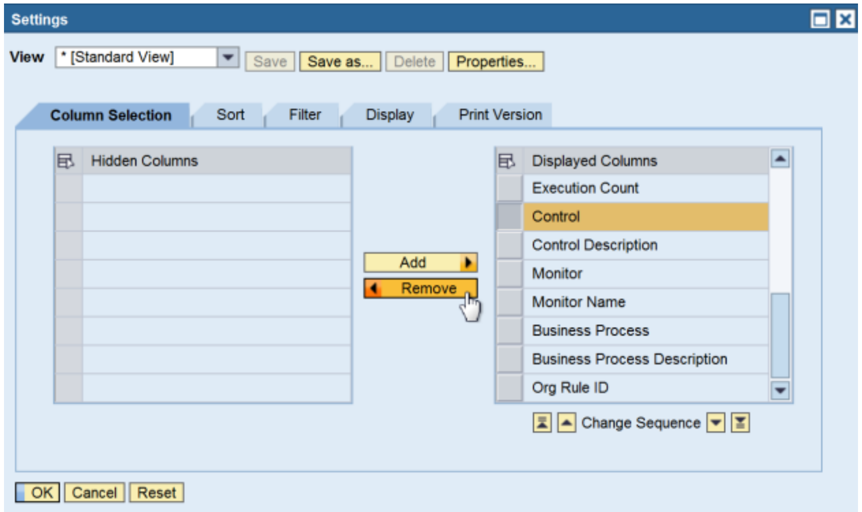
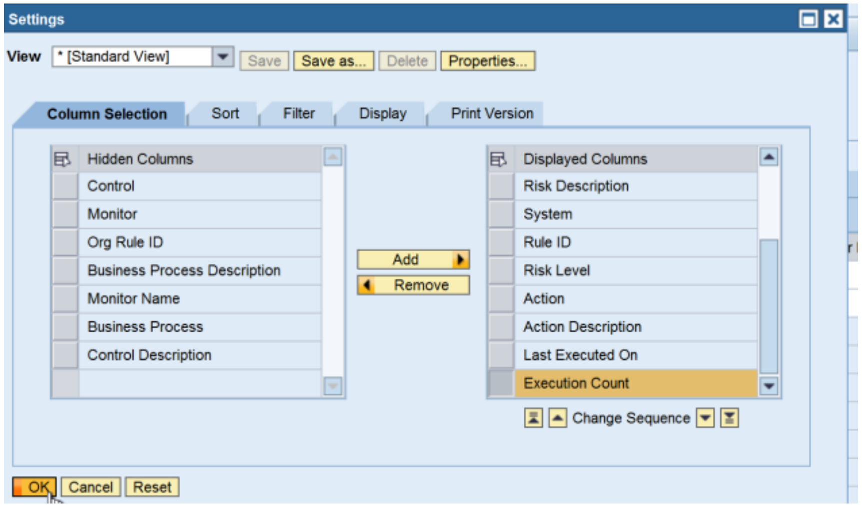
View: [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Summary | Mitigate Risk

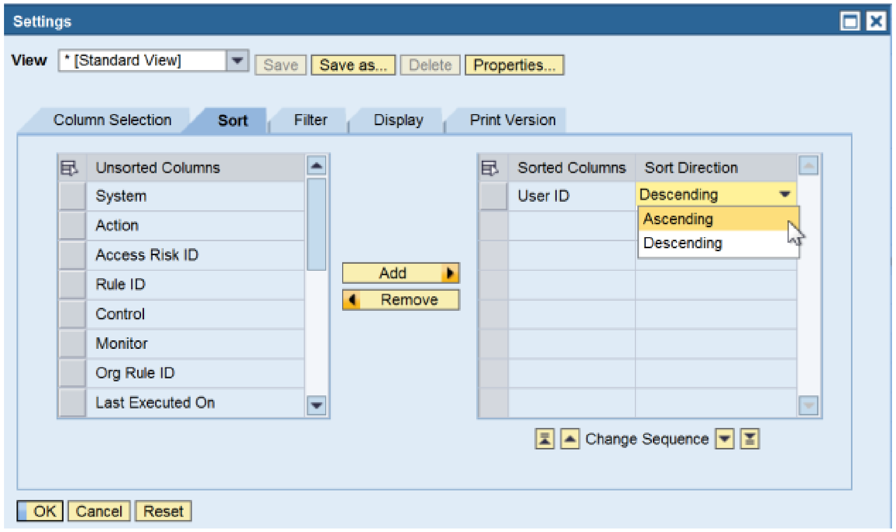
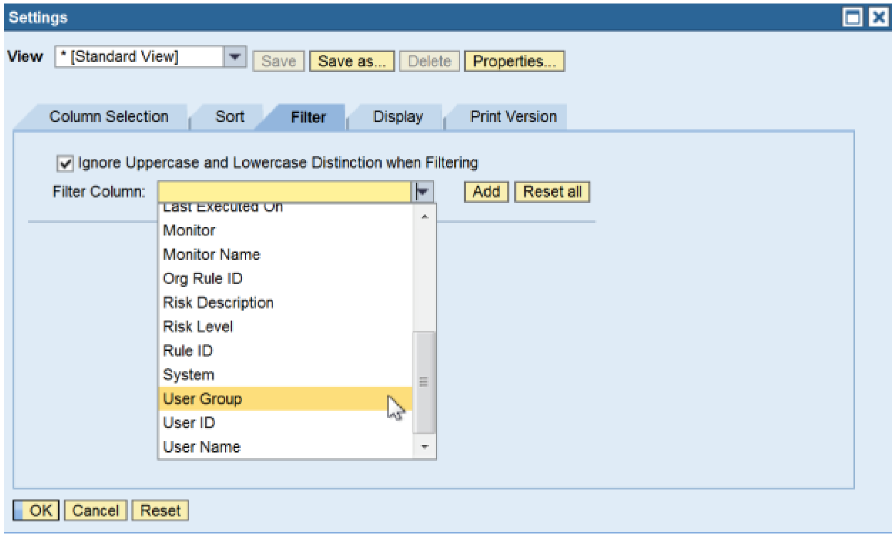
User ID	User Name	User Group	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action	Action Description	Last Executed On	Execution Count	Control	Control Descri
ANNAK	Anna A Kovaleva	VPF-AP			ZZPS103001			No Violations			0		
MFLAHERT	Michael Flaherty	VPF-FAR			ZZPS103001			No Violations			0		

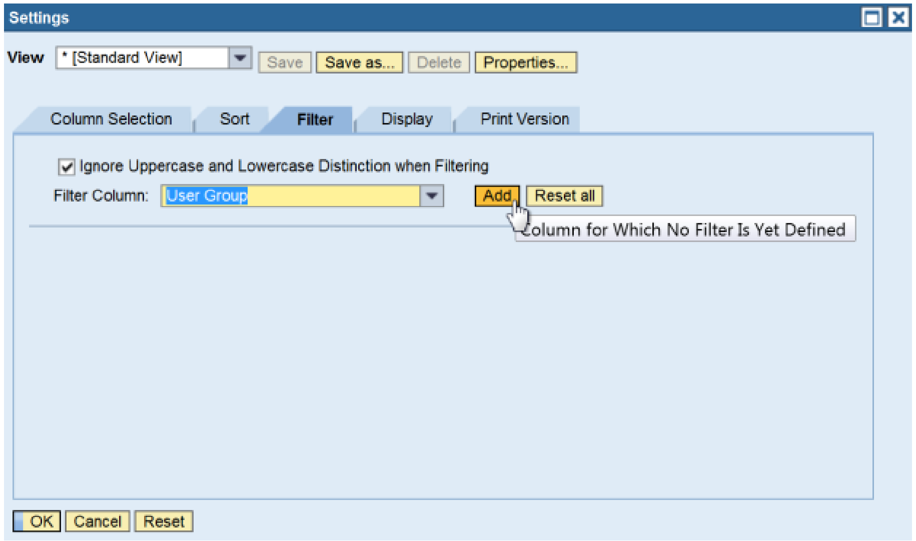
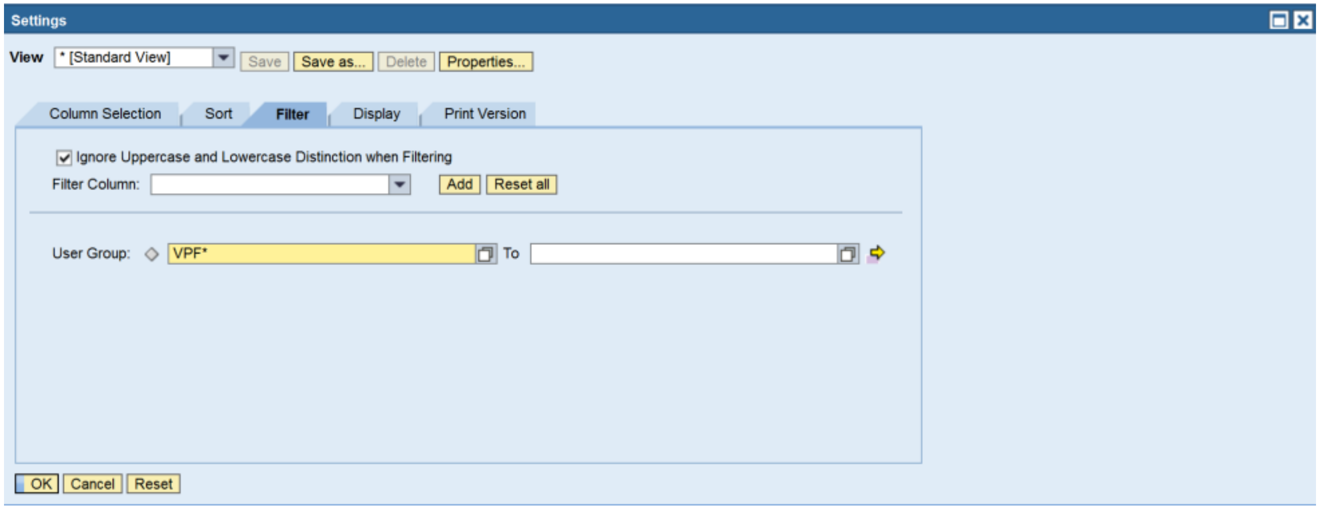
Step 2 screenshot:

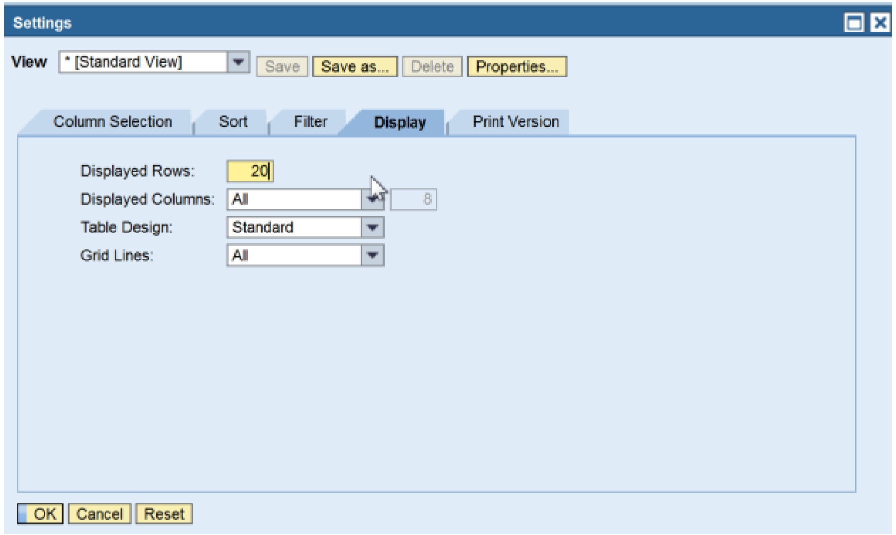
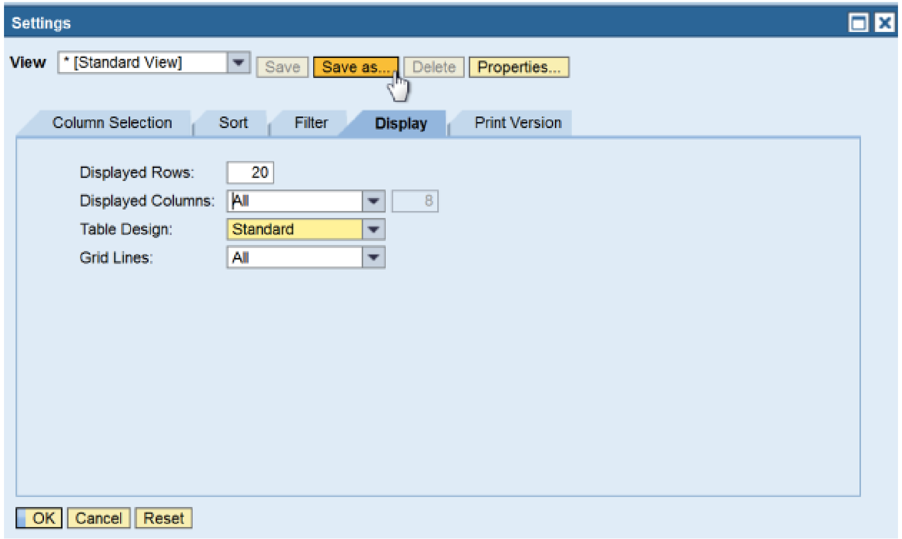
Type: Permission Level | Format: Summary | Mitigate Risk | Filter Settings

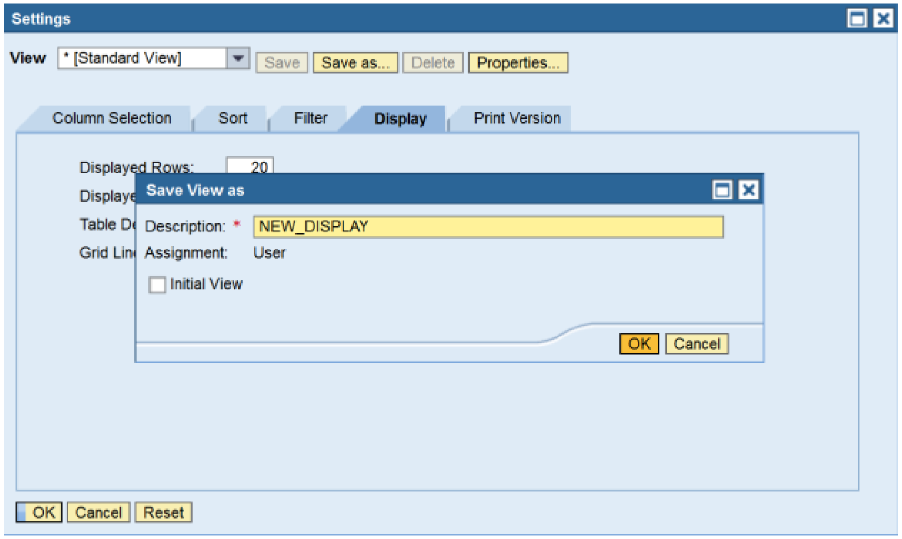
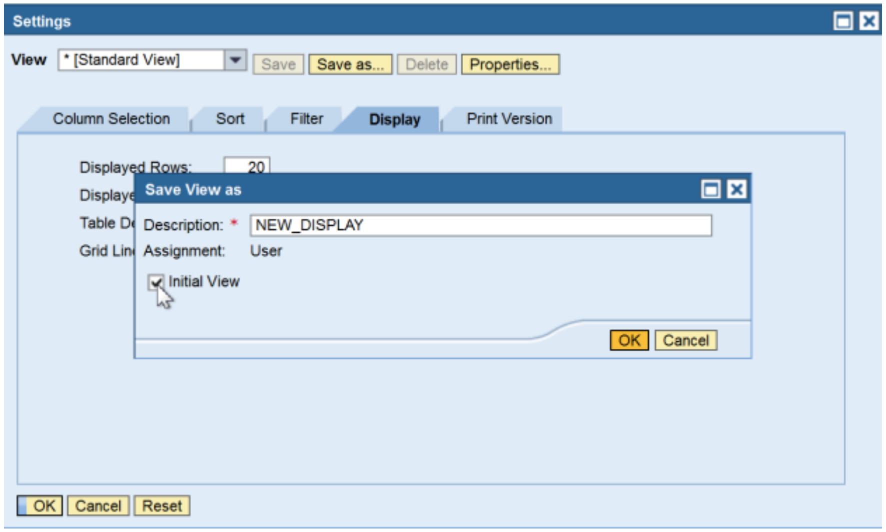
Rule ID	Risk Level	Action	Action Description	Last Executed On	Execution Count	Control	Control Description	Monitor	Monitor Name	Business Process	Business Process Description	Org Rule ID
		No Violations			0							
		No Violations			0							

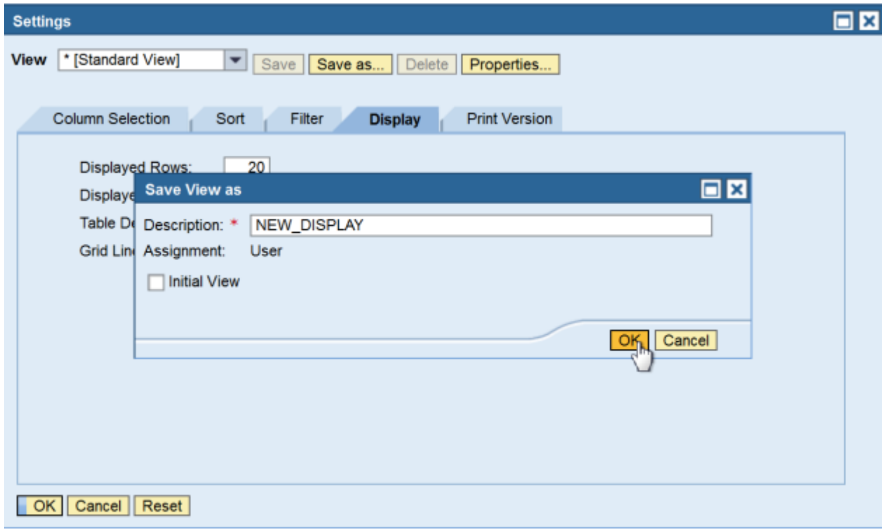
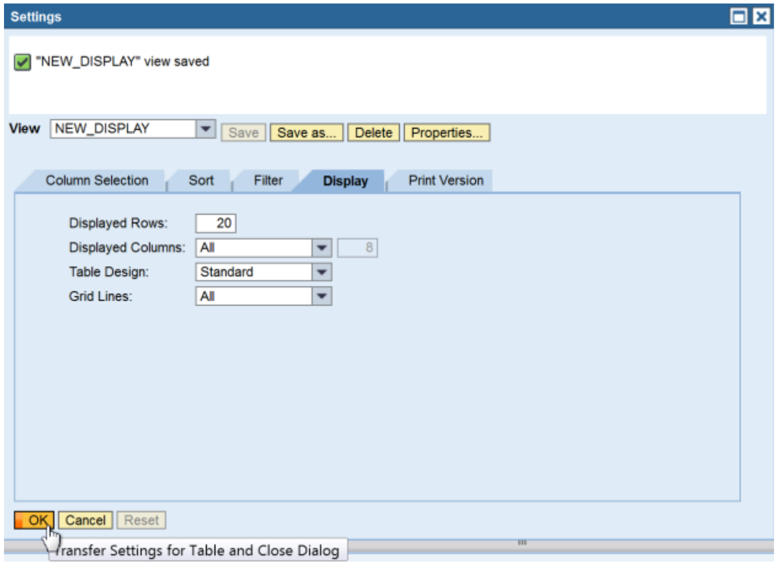
3	A ‘Settings’ window will appear where different view settings can be defined. Click on the ‘Column Selection’ tab to add/remove columns to/from the report.	 Settings View * [Standard View] Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version Hidden Columns Displayed Columns Execution Count Control Control Description Monitor Monitor Name Business Process Business Process Description Org Rule ID Add Remove Change Sequence OK Cancel Reset
4	Use the icons below the ‘Displayed Columns’ list to change the order in which columns are displayed.	 Settings View * [Standard View] Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version Hidden Columns Control Monitor Org Rule ID Business Process Description Monitor Name Business Process Control Description Displayed Columns Risk Description System Rule ID Risk Level Action Action Description Last Executed On Execution Count Add Remove Change Sequence OK Cancel Reset

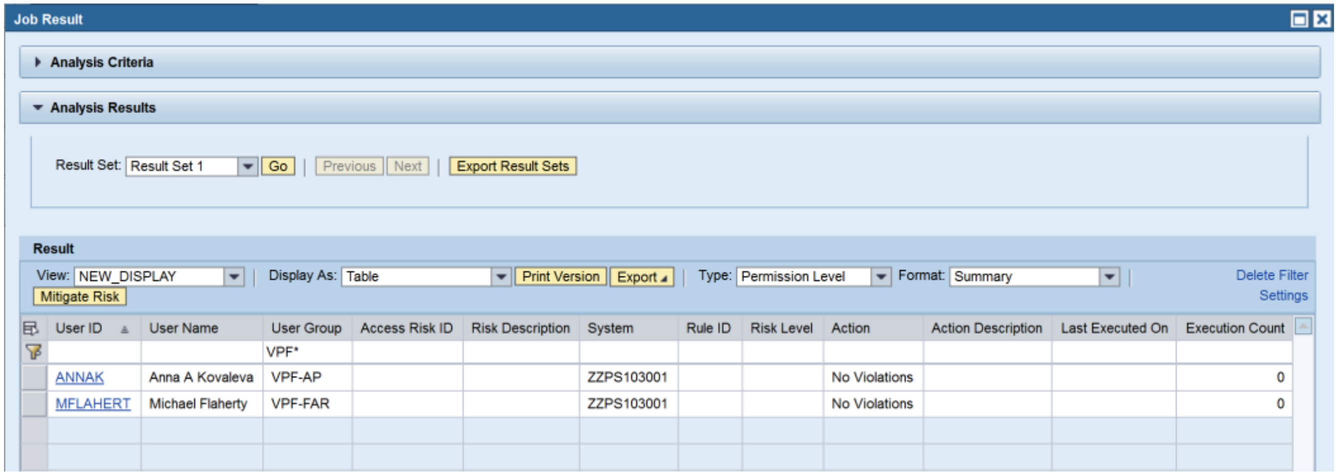
5	Click on the 'Sort' tab to define which columns in the report should be sorted, and how they should be sorted.	 Settings View * [Standard View] Unsorted Columns System Action Access Risk ID Rule ID Control Monitor Org Rule ID Last Executed On Sorted Columns | Sort Direction User ID | Descending Ascending Descending Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version Add Remove Change Sequence OK Cancel Reset
6	Click on the 'Filter' tab to define any columns that should be filtered. Click on the 'Filter Column' drop down and select a column.	 Settings View * [Standard View] ☑ Ignore Uppercase and Lowercase Distinction when Filtering Filter Column: Last Executed On Monitor Monitor Name Org Rule ID Risk Description Risk Level Rule ID System User Group User ID User Name Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version Add Reset all OK Cancel Reset

7	Once the column is selected, click on 'Add'.	 Settings Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version Add Reset all OK Cancel Reset View * [Standard View] ☑ Ignore Uppercase and Lowercase Distinction when Filtering Filter Column: User Group Column for Which No Filter Is Yet Defined
8	For the column that was added, in this case, 'User Group', enter the filter that should be used. In this example, 'VPF*' is entered to restrict the report to user groups that begin with 'VPF'.	 Settings Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version Add Reset all OK Cancel Reset View * [Standard View] ☑ Ignore Uppercase and Lowercase Distinction when Filtering Filter Column: User Group: ◇ VPF* To

9	Click on the 'Display' tab to change the table display settings for the report.	 Settings Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version OK Cancel Reset View: * [Standard View] Displayed Rows: 20 Displayed Columns: All 8 Table Design: Standard Grid Lines: All
10	To save the settings as a view variant, click on the 'Save as…' button.	 Settings Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version OK Cancel Reset View: * [Standard View] Displayed Rows: 20 Displayed Columns: All 8 Table Design: Standard Grid Lines: All

11	Enter a name for the view variant in the 'Description' field. In this case, 'NEW_DISPLAY' is entered.	 Settings View: * [Standard View] Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version Displayed Rows: 20 Save View as Description: * NEW_DISPLAY Assignment: User □ Initial View OK Cancel OK Cancel Reset
12	To make the new view variant the default initial view for the report, check the 'Initial View' box.	 Settings View: * [Standard View] Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version Displayed Rows: 20 Save View as Description: * NEW_DISPLAY Assignment: User ☑ Initial View OK Cancel OK Cancel Reset

13	Click on 'OK' to save.	 Settings View * [Standard View] Displayed Rows: 20 Save View as Description: * NEW_DISPLAY Assignment: User □ Initial View Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version OK Cancel OK Cancel Reset
14	A message will appear to confirm the view settings have been saved.	 Settings ✓ "NEW_DISPLAY" view saved View NEW_DISPLAY Displayed Rows: 20 Displayed Columns: All 8 Table Design: Standard Grid Lines: All Transfer Settings for Table and Close Dialog Save Save as... Delete Properties... Column Selection Sort Filter Display Print Version OK Cancel Reset

15	The next time the report is run, it will default to the view that was defined and set as the ‘Initial View’.	

Job Result

▸ Analysis Criteria

▾ Analysis Results

Result Set: Result Set 1 ▾ Go | Previous Next | Export Result Sets

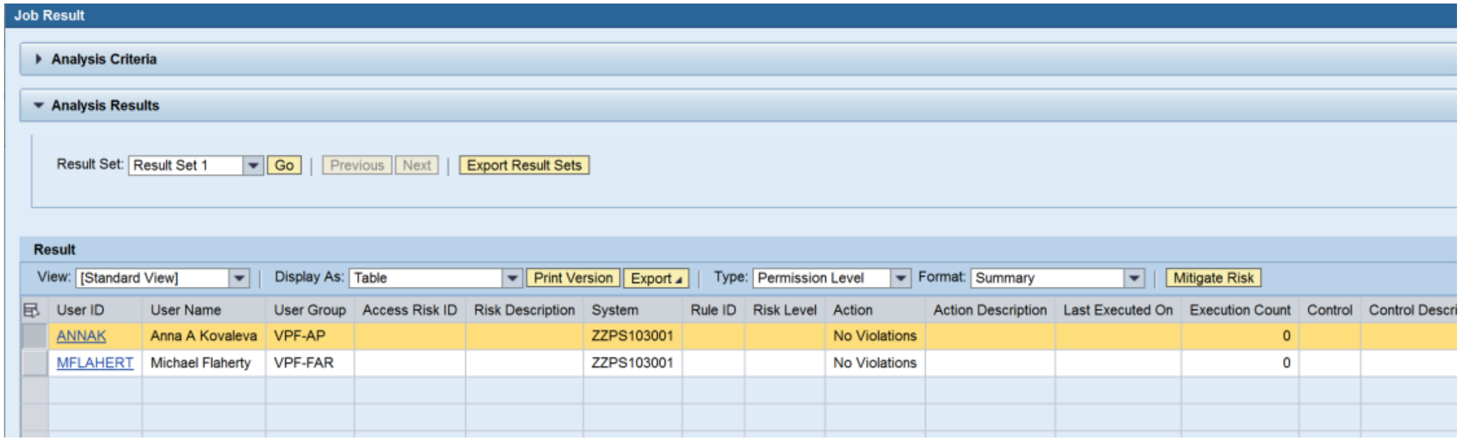
Result

View: NEW_DISPLAY ▾ | Display As: Table ▾ Print Version Export ▴ | Type: Permission Level ▾ Format: Summary ▾ | Delete Filter Settings

Mitigate Risk

User ID	User Name	User Group	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action	Action Description	Last Executed On	Execution Count
		VPF*									
ANNAK	Anna A Kovaleva	VPF-AP			ZZPS103001			No Violations			0
MFLAHERT	Michael Flaherty	VPF-FAR			ZZPS103001			No Violations			0

Reference R8 Export Data from GRC

<table>
<tr><th>Step</th><th>Description</th><th>Screenshot</th></tr>
<tr><td>1</td><td>Execute a report in the foreground or background and view the results.</td><td>

Job Result

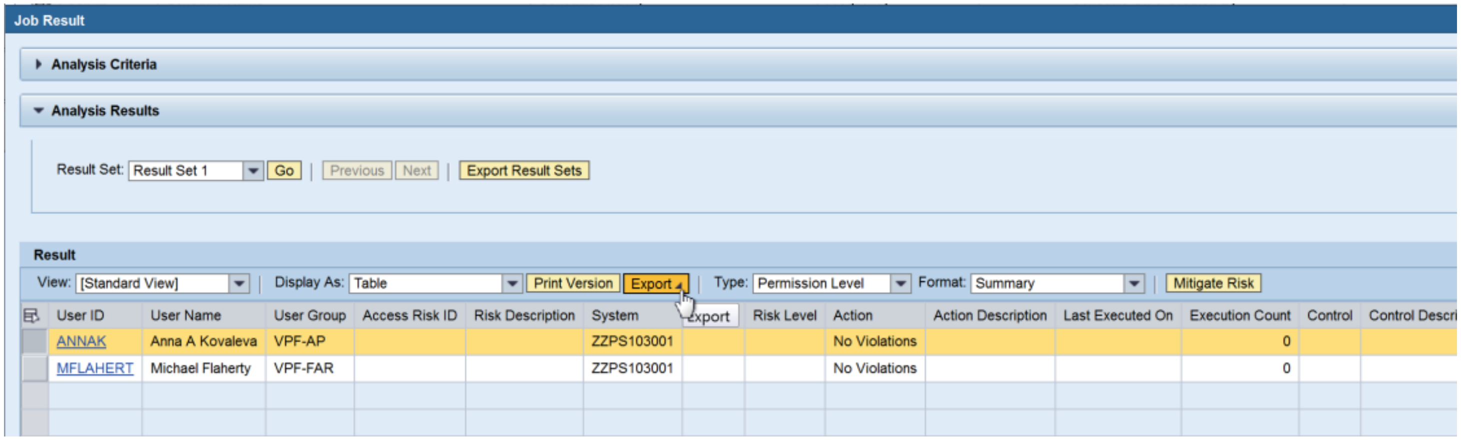
Analysis Criteria

Analysis Results

Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets

Result

View: [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Summary | Mitigate Risk

<table>
<tr><th>User ID</th><th>User Name</th><th>User Group</th><th>Access Risk ID</th><th>Risk Description</th><th>System</th><th>Rule ID</th><th>Risk Level</th><th>Action</th><th>Action Description</th><th>Last Executed On</th><th>Execution Count</th><th>Control</th><th>Control Descri</th></tr>
<tr><td>ANNAK</td><td>Anna A Kovaleva</td><td>VPF-AP</td><td></td><td></td><td>ZZPS103001</td><td></td><td></td><td>No Violations</td><td></td><td></td><td>0</td><td></td><td></td></tr>
<tr><td>MFLAHERT</td><td>Michael Flaherty</td><td>VPF-FAR</td><td></td><td></td><td>ZZPS103001</td><td></td><td></td><td>No Violations</td><td></td><td></td><td>0</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td>Click on the ‘Export’ button to export the report from GRC.</td><td>

Job Result

Analysis Criteria

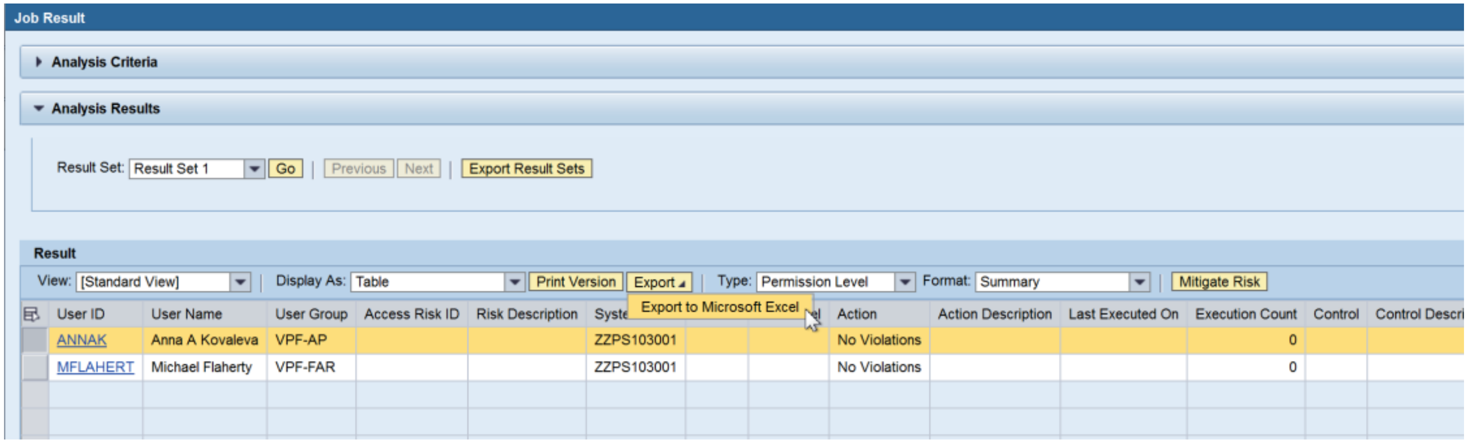
Analysis Results

Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets

Result

View: [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Summary | Mitigate Risk

<table>
<tr><th>User ID</th><th>User Name</th><th>User Group</th><th>Access Risk ID</th><th>Risk Description</th><th>System</th><th></th><th>Risk Level</th><th>Action</th><th>Action Description</th><th>Last Executed On</th><th>Execution Count</th><th>Control</th><th>Control Descri</th></tr>
<tr><td>ANNAK</td><td>Anna A Kovaleva</td><td>VPF-AP</td><td></td><td></td><td>ZZPS103001</td><td></td><td></td><td>No Violations</td><td></td><td></td><td>0</td><td></td><td></td></tr>
<tr><td>MFLAHERT</td><td>Michael Flaherty</td><td>VPF-FAR</td><td></td><td></td><td>ZZPS103001</td><td></td><td></td><td>No Violations</td><td></td><td></td><td>0</td><td></td><td></td></tr>
</table></td></tr>
</table>

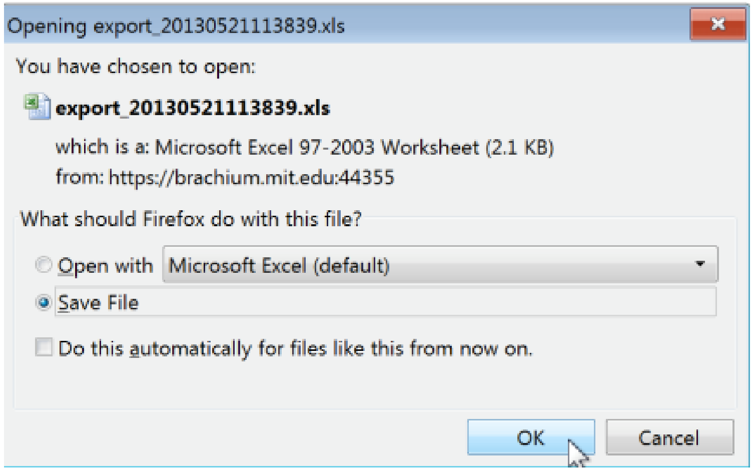
<table>
<tr>
<td>3</td>
<td>An ‘Export to Microsoft Excel’ button will appear. Click on the button to continue the export.</td>
<td>


Result Set: Result Set 1 ▾ Go | Previous | Next | Export Result Sets

Result

View: [Standard View] ▾ | Display As: Table ▾ Print Version Export ▴ | Type: Permission Level ▾ Format: Summary ▾ | Mitigate Risk

Export to Microsoft Excel
<table>
<tr><th>User ID</th><th>User Name</th><th>User Group</th><th>Access Risk ID</th><th>Risk Description</th><th>Syste</th><th></th><th>el</th><th>Action</th><th>Action Description</th><th>Last Executed On</th><th>Execution Count</th><th>Control</th><th>Control Descri</th></tr>
<tr><td>ANNAK</td><td>Anna A Kovaleva</td><td>VPF-AP</td><td></td><td></td><td>ZZPS103001</td><td></td><td></td><td>No Violations</td><td></td><td></td><td>0</td><td></td><td></td></tr>
<tr><td>MFLAHERT</td><td>Michael Flaherty</td><td>VPF-FAR</td><td></td><td></td><td>ZZPS103001</td><td></td><td></td><td>No Violations</td><td></td><td></td><td>0</td><td></td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td>4</td>
<td>The Firefox browser will open a download window. Select the required option and click ‘OK’.

If ‘Save File’ is selected, the file will be saved to the directory defined in Firefox. Otherwise, the file will open.</td>
<td>

Opening export_20130521113839.xls

You have chosen to open:

export_20130521113839.xls

which is a: Microsoft Excel 97-2003 Worksheet (2.1 KB)

from: https://brachium.mit.edu:44355

What should Firefox do with this file?

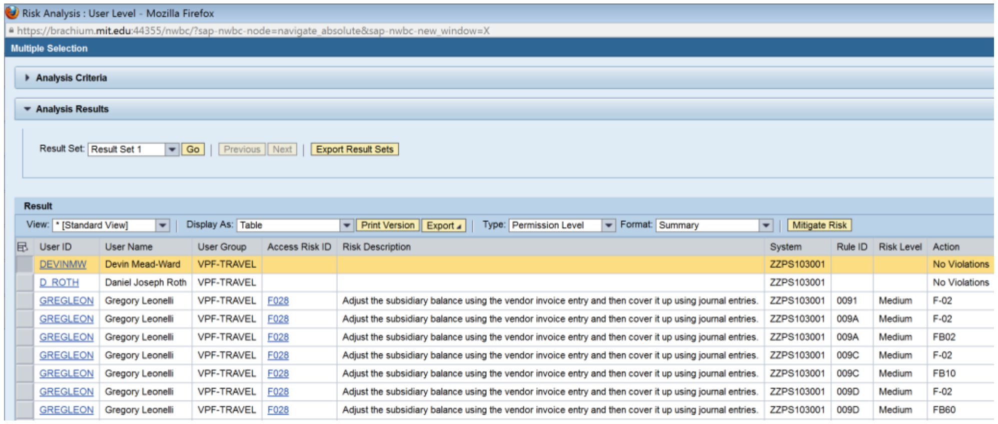
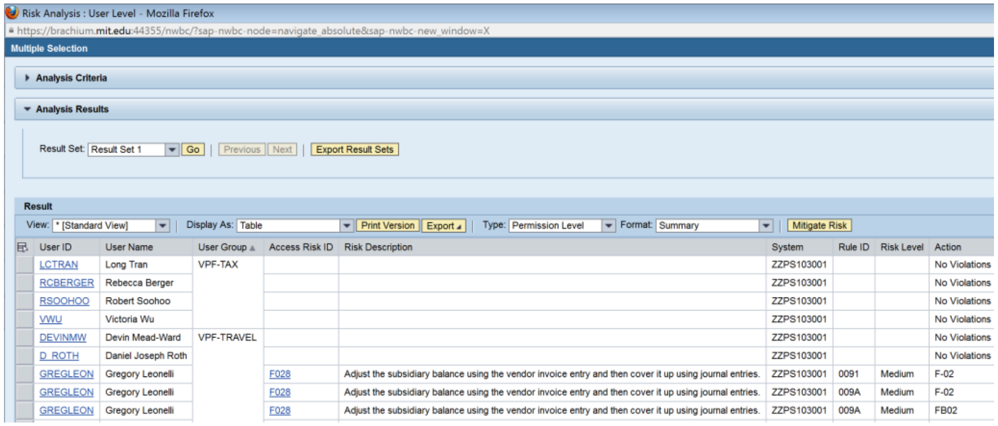
○ Open with Microsoft Excel (default) ▾

● Save File

□ Do this automatically for files like this from now on.

OK Cancel
</td>
</tr>
</table>

Reference R9 Simple Sort

Step	Description	Screenshot
1	Execute a report in the foreground or background and view the results.	
2	Click on the column header for the column which must be sorted. Click on the header once for an 'Ascending' sort and twice for a 'Descending' sort. In this example, the 'User Group' header was clicked once.	

Risk Analysis : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Multiple Selection

Analysis Criteria

Analysis Results

Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets

Result

View: * [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Summary | Mitigate Risk

User ID	User Name	User Group	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action
DEVINMW	Devin Mead-Ward	VPF-TRAVEL			ZZPS103001			No Violations
D_ROTH	Daniel Joseph Roth	VPF-TRAVEL			ZZPS103001			No Violations
GREGLEON	Gregory Leonelli	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	0091	Medium	F-02
GREGLEON	Gregory Leonelli	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	009A	Medium	F-02
GREGLEON	Gregory Leonelli	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	009A	Medium	FB02
GREGLEON	Gregory Leonelli	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	009C	Medium	F-02
GREGLEON	Gregory Leonelli	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	009C	Medium	FB10
GREGLEON	Gregory Leonelli	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	009D	Medium	F-02
GREGLEON	Gregory Leonelli	VPF-TRAVEL	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	009D	Medium	FB60

Risk Analysis : User Level - Mozilla Firefox

https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Multiple Selection

Analysis Criteria

Analysis Results

Result Set: Result Set 1 | Go | Previous | Next | Export Result Sets

Result

View: * [Standard View] | Display As: Table | Print Version | Export | Type: Permission Level | Format: Summary | Mitigate Risk

User ID	User Name	User Group ▲	Access Risk ID	Risk Description	System	Rule ID	Risk Level	Action
LCTRAN	Long Tran	VPF-TAX			ZZPS103001			No Violations
RCBERGER	Rebecca Berger				ZZPS103001			No Violations
RSOOHOO	Robert Soohoo				ZZPS103001			No Violations
VWU	Victoria Wu				ZZPS103001			No Violations
DEVINMW	Devin Mead-Ward	VPF-TRAVEL			ZZPS103001			No Violations
D_ROTH	Daniel Joseph Roth				ZZPS103001			No Violations
GREGLEON	Gregory Leonelli		F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	0091	Medium	F-02
GREGLEON	Gregory Leonelli		F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	009A	Medium	F-02
GREGLEON	Gregory Leonelli		F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	ZZPS103001	009A	Medium	FB02

GRC Terminology

Term	Short term	Source	Meaning	Example
Action		GRC	A business function step, usually an SAP ECC transaction code.	FB01 Post an FI Document F-65 Park an FI Document ME21 Create a Purchase Order
Action Level		GRC	Term for analysis of risks at the SAP transaction code level, without looking at additional permissions (R/3 authorizations) which could otherwise eliminate the risk.	
Access Risk	Risk	GRC	A GRC Access Risk is a description of a unique situation – a Critical Action /Role or a Segregation of Duties (SOD) breakdown. • The system has a delivered set of critical technical actions (like SE16, SM30 to amend database files) and roles, and these can be added to. • The SOD risk will always have two parts, like Create Fictitious Vendor and Enter a fictitious Invoice. Each SOD Access Risk can be assigned a Risk level and can be activated / deactivated. There is a pre-defined list of 454 SOD risks - each has a combination of conflicting GRC Functions assigned, or a critical action and its related permission.	**SOD Risk H0164** is the combination of : **Function HR03** Modify Employee Payroll Data **AND** **Function HR14** Enter time data
Access Risk Analysis	ARA	GRC	The part of the GRC package which is used to analyze for access risks - specifically access to powerful / critical transactions and Segregation of Duties (SOD) breakdowns.	

Term	Short term	Source	Meaning	Example
Access Rule	Rule	GRC	A system-generated object with a single pair of tcodes & related permissions, based on the combination of GRC Functions which were defined as the Access Risk. Each Access Risk has one or more Access Rules generated for it.	Access Risk F028 is defined as having access to both Function AP02 (47 tcodes) AND Function GL01 (69 tcodes) together. So Access Risk F028 has over 3200 generated Access Rules.
Access Rule set	Rule set	GRC	A pre-defined set of : • Access Risks and assigned Function combinations, against which a User or Role can be checked for potential SOD breakdown issues. • Critical roles, critical profiles and critical actions – mostly focused on semi-technical system access. A system may have several rule sets, e.g. SAP-delivered, External Audit, MIT modified, and the risk analysis reports can be run using any one rule set at a time. Also, rule sets can be compared to each other for differences.	GLOBAL ZAUDIT
Authorization Profiles	Profiles	SAP	In earlier SAP releases, a user's access was defined through creating and assigning manually created Authorization Profiles. The current SAP release defines user access by having job-related "Roles" from which the R/3 Security Profile Generator then generates a large Profile (for each Role). Thus, when a Role is assigned to a user, the corresponding Profile is also assigned and the system uses this to determine the user's authorized access. At MIT, the process of creating Authorization Profiles without an associated Role has to be continued for those parts of SAP R/3 access which are provisioned from the RolesDB system.	SAP_ALL Z#:JV_FY

Term	Short term	Source	Meaning	Example
Business Analyst	BA	MIT	The VPF Business Analyst (BA) is a member of the VPF Financial Systems and Data team who helps in the operational management of financial systems, processes, reporting, and data. Also, the BA supports the GRC/SOD review process by validating the business access requirements in the area they support.	
Business End User	End User	MIT	An SAP system user for whom access needs to be provided.	
Business Process		GRC	A very high level categorization which is used to group Access Rules.	Accounts Payable, HR & Payroll
Business System Analyst	BSA	MIT	IS&T Business System Analyst – IS&T's counterpart to the VPF Business Analyst – providing more technical support, or can be both the BA and BSA support in areas where there is no designated BA. Also, now supports the GRC/SOD review process in terms of simulations and action/permission knowledge.	
Composite Role		SAP	This is type of R/3 Security Role which is a combination of other Roles and can be assigned to one or more users. A typical MIT composite Role will have several different shared Roles and one or more unique ones as well, creating a unique combination of access authorizations. These composite Roles more closely match one or more users' complete access requirements, making Role provisioning easier as it can mostly be done at the Composite role level, reducing the complexity for the Role Owner. Note: authorization profiles provisioned from the MIT Roles Database system are in addition to those from the composite Roles, so GRC-Access Risk Analysis always needs to be performed at the User level to get a complete analysis. Naming convention: Z_DDD_C_X where DDD is the MIT department, "C" indicates it is a composite role, and X is descriptive of the role (see example to the right).	Z_VPF_C_ADMIN_COMMON

Term	Short term	Source	Meaning	Example
Critical Role Critical Profile Critical Action	Critical	GRC	Roles, Profiles and Transaction Codes (GRC Actions / Permissions) can be tagged as "critical" to ensure inclusion in access reviews (compliance and technical). If required, Mitigation Controls can be assigned to the critical risk.	Role = SAP_ALL Tcode/Action = FB01 with Permission 01 (Post)
Custom User Group	User Group	GRC	GRC has a “Custom User Group” for use in filtering reports. This is in addition to the SAP R/3 user‘s “User Group” field.	VPF
ESS	ESS	SAP	Web-based portal for Employee Self Service functionality	
Exception Access Rules		GRC	Reporting exceptions can be defined : e.g. Organization / Access risk	Not currently used at MIT.
FireFighter logs	Logs	GRC	Action logs recorded in SAP R/3 when a user checks-in to the GRC FFID.	
Firefighter Role	Role	SAP	An SAP R/3 Security Role assigned to the FireFighter R/3 Users. Different types of FireFighter need different access and Roles.	
FireFighter R/3 User	FireFighter	SAP	A special SAP R/3 business user provisioned with the SAP R/3 Security FireFighter Role. There are several different types of FireFighter : • **Business User** – where the FF role is limited to back-up actions, or special actions that would otherwise have created an SOD issue if combined with a user’s existing role. • **VPF Business Analyst** - broad access for emergency VPF Financial Systems support • **IS&T Business System Analyst** – broad access for emergency IS&T support • **IST&T Basis** –additional technical access not usually needed. FireFighter R/3 User naming convention: FF_XXX_NN where XXX = the business area letters and NN is a sequential number. The User Type = SERVICE and so cannot be used directly in SAP; instead it is called up from GRC-EAM.	

Term	Short term	Source	Meaning	Example
Firefighter ID	FFID	GRC-EAM	A GRC-EAM identifier used to manage access to the Firefighter R/3 User : • each GRC FFID is assigned to a Firefighter R/3 User (and so indirectly to the assigned R/3 access role). • regular SAP users are assigned to the GRC FFID, when they have been approved as having a back-up or a support function that requires FireFighter access. The Firefighter R/3 User can only be entered / checked into via the GRC-EAM system, and an R/3 user only has access to the FFIDs they have been assigned to. When finished their work, the user "checks-out" of the FFID in GRC system. When a FireFighter Id is used, an email is sent to its assigned FFID Controller and the FireFighter's actions in R/3 are logged for review.	
Firefighter ID Controller	FFID Controller	GRC-EAM	An MIT person (currently only in VPF or IS&T) who performs the process of monitoring FireFighter usage – both the checking-in activity and the review of action logs.	
Firefighter ID Owner		GRC-EAM	Not currently made use of by MIT – but is a required assignment for a FFID. At MIT, this will be the same as the FFID Controller.	
Function		GRC	A GRC Function identifies a medium-level business process and will have one or many transaction codes (GRC Actions) assigned, with additional permission level definitions where appropriate. Also, a transaction code may be assigned to several functions, if it has the implied business flexibility. GRC has approximately 200 pre-delivered functions that are used to define the mostly SOD-related Access Risks.	PR02 Maintain Purchase Order - with permissions to create or change. HR04 Enter Employee Time Data.
GRC Power User	Power User	MIT	BSAs, BAs and some Role owners will use most of the reports in GRC - so they are known as the "Power Users" in respect of the report usage and training requirements.	

Term	Short term	Source	Meaning	Example
GRC system GRC-ARA GRC-EAM	GRC	GRC	SAP's "Governance, Risk and Compliance" software system – MIT is currently using the following components. **GRC-ARA :** Access Risk Analysis – this analyzes access in SAP ECC Security Profiles, Roles and Users – to see if there are (a) any "critical" features (transactions, roles, profiles) and (b) any potential Segregation of Duties breakdowns, as well as reporting details of user access and role / profile assignments. • GRC-ARA also has a what-if simulation reporting capabilities, to analyze risks for proposed role / user changes. **GRC-EAM:** Emergency Access Management – also known as FireFighter user management. See entries under "FireFighter".	
MIT Roles Database	RolesDB		MIT's custom system for managing some of the cross-system access, including some SAP access. SAP access is provisioned through an automated process, mapping RolesDB rules to SAP R/3 Security profiles, which are then assigned to the R/3 User.	
Mitigation Control	Mitigation	GRC	The Mitigation Control object contains an explanation of how a specific Access Risk (SOD or Critical risk) has been mitigated. Each Mitigation Control has a unique id. • At MIT, the same access risk can exist in different areas but may be mitigated differently, so there is a separate Mitigation Control for each Risk / User Group combination, where the User group may be VPF-Property, or VPF-Accounts Payable. • Where the same risk is mitigated the same was across all of MIT user community, the same Mitigation Control can be used for all users. The Mitigation Control identifier is assigned to the appropriate combination of Access Risk and User to whom it applies.	**General MIT business control**: bank reconciliation performed by VPF independent of VPF AR Cashiers. **New SOD mitigation reports** (for otherwise unmitigated access): VPF AP report xxxx.

Term	Short term	Source	Meaning	Example
Permission Level	Permissions	GRC	In standard SAP Security, the transaction-level checks may include an additional check of an "Authorization" which is like an MIT "Qualifier" - to restrict that user to by Company Code, or types of Customers, or FI Document Types – and additionally allows access restriction by system activity, like create, change and display, where the transaction itself can allow access to all activities if not restricted by the authorization. In GRC these lower-level authorization are called "Permissions". The Access Risk Analysis reports should be executed at this level, as this will reduce the number of risks reported compared to the "Action" level reporting, where the permission distinguished between create, change and display.	Action / Transaction Code : FS00 Maintain GL Account Master (Allows : Create, Change, Display, Lock, Delete) Permission / Authorization: only given Activity = 03 (Display). No access to Activity = 01 (Create) or 02 (Change) etc.
Profile Generator	PFCG	SAP	SAP ECC access management tool used to generate access roles and the Authorization Profiles based on roles.	
Provisioning			The process whereby system access is provided to users. Specifically for SAP this encompasses the procedures for requesting, analyzing risk, approving and executing changes to roles, profiles and their assignment to users. Three systems are involved: SAP ECC, MIT RolesDB, and SAP GRC.	
Risk Level		GRC	For each defined GRC Risk, an associated risk level is assigned - high, medium or low. This is used in Dashboard and other GRC report filtering.	
Risk Owner			For each business area at MIT, the Risk Owner is the person who has the responsibility for ensuring the business system controls are in place and functioning, and any and all appropriate follow-up actions are taken. In the GRC/SOD context this includes periodic reviews of system access, SOD analysis as well as any SOD-related mitigation controls.	
Risk Violations	Violations	GRC	Access risk - can be analyzed at User, Role or Profile level.	

Term	Short term	Source	Meaning	Example
Role		SAP	An SAP access control object used to group together actions (transaction codes) and permissions (authorizations) to represent all or part of a business job role. MIT has several roles per user, e.g. those which are: common to all MIT users, common to all business area (e.g. VPF-FAR) users, common to a group within the business area (e.g. Cashier), or finally a role specific to only one job duty for only one or a few users. See also "Composite Role" definition.	Z_VPF_S_AR_MANAGER Z_VPF_S_DOCUMENT_REVERSE
Role Owner			For each business area at MIT, the Role Owner is the person who has the responsibility for managing the SAP access roles specific for their area: requesting role changes and role / user reassignments.	
Roles Database	RolesDB	MIT	An MIT custom system to manage access across many of MIT's computer systems, including SAP. The SAP access focus relates to provisioning common Roles and related Profiles (with common actions and permissions) and additional "qualifier" profiles – the latter relates to controlling access at organizational levels or other SAP system attributes. The "qualifier" provisioning is managed by the MIT business users who have provisioning rights. Currently, some RolesDB common Roles are blocked for the SAP users who have already had their Roles in SAP re-engineered as part of the SOD project.	
SAP Access Control SAP Authorization	SAP R/3 Security	SAP	SAP's core system access control functionality using: Users, Roles, Profiles and Authorizations.	
SAP ECC SAP Core SAP 6.0			The SAP software used by MIT for Financial Accounting, Procurement and HR/Payroll. "ECC" stands for Enterprise Core Component, and 6.0 is the software release level.	

Term	Short term	Source	Meaning	Example
SAP User Group	User Group	SAP	Each SAP R/3 user is defined in the SAP system. One of the SAP User's attributes is the "User Group" field which MIT is using to identify a group of users for analysis. Some GRC-ARA reports make use of this "User Group" for selection. Additionally, GRC has a "Custom User Group".	VPF-FAR
Segregation of Duties	SOD	GRC	System access is expected to support the business requirement that no single user should have end-to-end business process access, otherwise there is risk of internal fraud occurring. In some high risk areas, access to only several steps in a process are enough to cause a Segregation of Duties breakdown.	Ability to create a Vendor Master and any one of: create a Purchase order, post an invoice, generate a payment.
Simulation	Simulation	GRC	The GRC-ARA simulation tool is a "what if" access risk analysis - it simulates adding more access (actions and permissions) to existing Users, Roles or Profiles. The simulation can also specify access to be removed – e.g. what if transaction FCH9 Void Check were removed from a user who currently has it.	What if tcode ME21N (Create a Purchase Order) is added to User FREDX, or to Role Z_VPF_S_AR_MANAGER.
SOD Coordinator		MIT	A person in VPF who has been designated to coordinate several of the GRC-related processes.	
SUIM	SUIM	SAP	An SAP R/3 transaction which calls up a menu of authorization-related reports of Users, Roles, Profiles, Authorizations. Note: each item on the menu requires access to be granted, as it links to a different SAP transaction code – like S_BCE_68001421 – which in turn call up the related RSUSRxxx program.	
Transaction code	tcode	SAP	The SAP ECC system users "transaction code" for each business action - usually all menu lines have a transaction code behind them to call up the dialog (online) function. In GRC, these are called Actions.	FB01 Post an FI Document FB02 Change an FI Document FB03 Display an FI Document

Term	Short term	Source	Meaning	Example
User Master	User	SAP	This is the SAP system user master record or Logon Id – the naming convention at MIT is to match the MIT Kerberos Id, based on the user's name.	PAMELAS DALET VACHA
Workflow – ECC			In SAP ECC, "workflow" is automated for some financial postings/documents. Users enter financial transactions and they are "work flowed" in custom MIT programming to approvers' inboxes.	
Workflow – GRC			GRC functionality for approving access change requests - currently not implemented.	

GRC Roles & Responsibilities

ROLE	RESPONSIBILITY	ACCESS-RELATED ACTIONS	FORM/REPORT USE
RISK OWNER Gerry O'Toole Basil Stewart Tricia Sullivan Mullen James Walsh Allen Marcum Bart Dahlstrom	• Provide guidance on **- Simon** ○ acceptable level of risk related to SODs and critical access ○ adequacy of compensating (mitigating) controls • Ensure control processes are in place : **- Karon** ○ Regular access review ○ Mitigation processes, including specific reports. • Final approval on new/amended Mitigation Control definitions and assignment to Risk / User combinations. **- Simon** • Approve recertification of mitigating controls – supported by Role Owner and Compliance Officer. **- New**	• Review high-level GRC-ARA reporting • Monitor the execution of the access-related business control processes	High level GRC Dashboard reports Final sign-off on Mitigation Control change request form.

ROLE	RESPONSIBILITY	ACCESS-RELATED ACTIONS	FORM/REPORT USE
ROLE OWNER John Larkin Donna Cairns Eileen DesRosiers James Walsh Chris Durham Sara Malconian Long Tran Kathy McGrath Kevin Miligan Pamela Schickling Jo Anne Chute Tricia Sullivan Mullen Ann Harvey Danielle Khoury Jo Lynn Whitlock Siobhan Cunningham Frank Quern Ron Parker Wai Ming Li	• Identify potential access changes, aligned to the business area's functions, organization and Segregation of Duties requirements. **- George** ○ New or amended role definition. ○ User assignments to new or amended roles • Assist the SOD Coordinator with the assessment of new risks associated with proposed changes **- Simon** • Formally request Production access changes (role activation and user/role assignment) when the GRC risk analysis is completed and documented. **- New** • Manage changes to SAP access from the RolesDB, where appropriate. Note: there is usually no SAP Security Admin involvement in this step. **- George** • Request assignment of users to Firefighter roles in GRC **– Siobhan, Sandy** • Advise SAP Security of any Transfer Out / Termination **- New** • Conduct regular reviews of : **- New** ○ Roles for the business area – who has them ○ Users per business area – what roles they have ○ Users per business area – what Risk/ Mitigation combinations are assigned ○ GRC-ARA (SOD) analysis ○ Assignment of Business Back-up FireFighter roles to Users • Monitor access logs for business user "FireFighter" and IS&T Support role usage - **New**	• Initiate change requests – SAP access • Initiate change requests – GRC mitigations • Keep Risk Owner aware of all proposed changes and status • Review SOD Risk simulation results provided by BA/BSA for proposed role changes • Perform Role and User level access analysis – with support from BA and/or BSA.	**FORM** : Access Change Request **FORM** : Mitigation Control request form – Risk/User assignment Various GRC reports – may be a GRC "Super User" SAP ECC SUIM reports - limited use.

ROLE	RESPONSIBILITY	ACCESS-RELATED ACTIONS	FORM/REPORT USE
BUSINESS ANALYST (BA) Mirella Villa Leslie Wright Scott Ball Lody Petriv	• Assist the Role Owner and Risk Owner with : **- Simon** ○ Analysis of changes to risks due to changes in roles or user/role assignments ○ Redesign of Role in terms of business-relevant information ○ Understanding the Risk as reported by GRC-ARA – i.e. why there is a potential SOD issue. • Document Mitigation Control and send to GRC team, after approval of Role Owner and Risk Owner **- Simon** • Testing new/changed access **– BA/BSA**	• Perform GRC-ARA simulations or review simulation results • Perform Role and User level access analysis in GRC • Create/update SAP Access Role design documents.	**FORM** : Mitigation Control request– initial definition and creation GRC Power User reporting SAP ECC SUIM reports
BUSINESS SYSTEM ANALYST (BSA) Ken Levie Kristen Hann Bob Casey Keyur Patel Sandeep Nadendla And others	Essentially the same as the Business Analyst, **<u>plus</u>** providing assistance with : • Alternatives for Actions (tcodes) or Permissions (Authorizations) **- BSA** • Categorizing “”Z” transactions **- BSA** • Prepare mini-specs for any additional mitigation system development (configuration, enhancements or reports) **- BSA** • Manage transports for any development technical objects. **- BSA**	Same as Business Analyst, **<u>plus</u>** : ○ More use of SUIM??? ○ Access to use SU56 on Production users and run “Z” auth reports	GRC “Super User” SAP ECC SUIM reports
SAP END USER All VPF users	○ Test new/amended access **- same** ○ Report missing authorization**- same** ○ Report access in excess of job requirements**- same** ○ Report breakdown of mitigating controls – e.g. user finds they can approve own Requisitions above the limit, or can approve own JVs. **- same**	Email to Role Owner any issues.	N/Av

ROLE	**RESPONSIBILITY**	**ACCESS-RELATED ACTIONS**	**FORM/REPORT USE**
SOD COORDINATOR Lody Petriv **On Demand Epiuse AMS Remote Consulting (Simon & Suman) for 6-12 months under current contract hours**	• Coordinate monthly SOD Analysis reviews **- Karon** • Coordinate Quarterly User Access reviews **- Karon** • **Business lead for GRC, including :** • **VPF Roles : for new/amended roles, coordinate SOD Issue resolution – involving Risk Owner, Role Owner, Audit, as well as support from BA / BSA** ○ **Also, identify any additional mitigation controls required if new risks are to be accepted.** • Ensure mitigation controls are in place before user / role access change is effective. **- Simon** • Support the Risk Owner and Role Owner by providing information from GRC system **– Suman, JD** • Support the process for recertification of mitigating controls. **- New**	• Run GRC and SUIM reports	GRC Power User reporting
BSA Manager = IS&T Role Owner Siobhan Cunningham Frank Quern	• Advise SAP Security Admin, GRC Team and Director of Financial Systems and Data- when there are new or amended IS&T Support users **- Siobhan, Frank**	• Request user assignments to Support roles	**FORM** : Access change request
GRC ADMIN **Sara Quigley** Ron Parker George Petrowsky Rich Katkowski Quian Kang	• Manage rulesets, including adding "Z" transactions **- Sarah** • Manage Mitigation Controls and their related Risk/User assignments **- Sarah** • Manage access to GRC functionality and reports**- Sarah** • Manage GRC updates **- Sara** • Manage "Fire Fighter" to User assignments. **- Sarah** • Provide information on reporting, report results and GRC ruleset contents as requested. **- Sarah**	No access-related actions as such, but provide : ○ Confirmation to Role Owner that a Mitigation Control is assigned to the users as requested. ○ Risk and Function definition information on request ○ Explain results from any GRC Dashboard or detailed report.	Potentially any report from GCR

ROLE	RESPONSIBILITY	ACCESS-RELATED ACTIONS	FORM/REPORT USE
SAP SECURITY ADMIN TEAM Ron Parker **George Petrowsky** Rich Katkowski Quian Kang Sara Quigley	• Execute properly approved SAP User Access change requests : **Admin Team** ○ Amend Roles ○ Amend User / Role assignment ○ Amend Profiles ○ Amend RolesDB / SAP interface ○ Amend Firefighter Roles ○ Provide User Aliases for testing new/amended roles **Admin Team** • Redesign Roles for efficiency or to separate functions which were bundled. May be in conjunction with RoleDB changes. **Admin Team**	○ Confirm SAP access changes to Role Owner ○ Move access through Development, QA and Production landscape ○ Advise Role Owners when any "technical" role redesign / clean-up is performed – as user access testing will be required.	Any report from SAP Reporting from GRC?
MIT Audit	• Periodic reviews of **- MIT Audit** ○ SOD risk mitigation controls ○ SAP access change process controls ○ User access		Power User of GRC reports
Ongoing Oversight Committee – Chair Gerry O'Toole Basil Stewart Tricia Sullivan Mullen Bart Dahlstrom James Walsh Allen Marcum	• SOD / GRC Champion • Speaks to overall approach with PWC Audit		

GRC SOD Analysis Steps

PURPOSE OF THIS DOCUMENT

This document sets out the steps required to understand the Segregation of Duties risks and their actual impact within the specific business environment. The details here support the high-level GRC Process 2 Flowchart presented during GRC training.

The details below describe the users (BA, BSA, Risk Owner, Role Owner, SOD Coordinator, SAP Security Admin) who will be involved in each step. The steps are broken down into phases of the task :

• Phase A	Steps 1 – 7	Risk understanding
• Phase B	Step 8	Role redesign and SOD analysis
• Phase C	Steps 9 – 11	Mitigation Strategy

DETAILED STEPS – USERS INVOLVED AND ACTIONS

INFORMATION INPUT	ROLE DESIGN / REDESIGN STEPS
PHASE A	**PREPARATION (1 – 7)**
Audit Business Analyst Business Systems Analyst	**1. Understand the business operations :** a. Business activities, scope, value, volume, risk. b. Business systems , including manual steps outside the computerized systems and any automated processes c. Any Key Performance Indicators affecting employee remuneration. d. Business events which involve employees with access to MIT resources and business processes which could be subject to misappropriation / fraudulent activities: • Cash and Treasury • Stores inventory • Equipment and Fixed Assets • Req-to-check/payment : inwards goods/services consumption • Order-to-cash : outwards goods/services • Service provided internally • HCM : HR and time data affecting Payroll e. Where relevant, any external legal / regulatory requirements for fiscal reporting, trade restrictions, privacy / data protection, disclosures etc.

INFORMATION INPUT	ROLE DESIGN / REDESIGN STEPS
Audit Risk Owner GRC system	**2. Business Risks and related Control Objectives** a. High level control objectives for completeness, accuracy, authorization, timeliness, quality, privacy etc b. Identification of major risk areas relevant to the MIT business area, including the GRC Ruleset – with its "Risk" definitions. c. Determine if there are any Audit findings (internal & external) which are still unaddressed.
Business Management HR IS&T	**3. Organizational Structures relevant to the processes** a. Business Organization Chart b. System Org hierarchies and system approval structures and limits c. Current job incumbents and vacancies and temporary staffing d. Reality Check : the actual supervision / management in place
Business Management HR	**4. Job Descriptions relevant to the business processes** a. Identify the business process steps the user is currently responsible for. b. Identify any requirements for confidentiality (personal data, financial data, contract bidding, etc) relating to the user / job position. c. Reality Check : shared UserIds d. Reality Check : multiple UserIds (not at MIT due to unique Kerberos Id).
Business Management Audit	**5. Published Policies and Procedures** a. Identify procedures requiring control and what the control procedure is. b. For each procedure, summarize into bullet points in process step sequence, with system / person / action c. Reality Check : make sure the procedure is still in use.
	6. Actual users and system usage
IS&T - Security Business Analyst Business Systems Analyst (Role Owner to an extent)	a. List of current users, by User Group (matching the MIT business area) b. List of transaction codes executed by SAP UserId over a 1 or 2 year period. (Job changes will make this less useful). Review the list of business process identified for the users and • assign any major action tcodes for data maintenance, logistics/financials postings / approvals, and • identify remaining tcodes not associated with a business process. c. Identification of any Emergency Access the user has - managed in GRC or

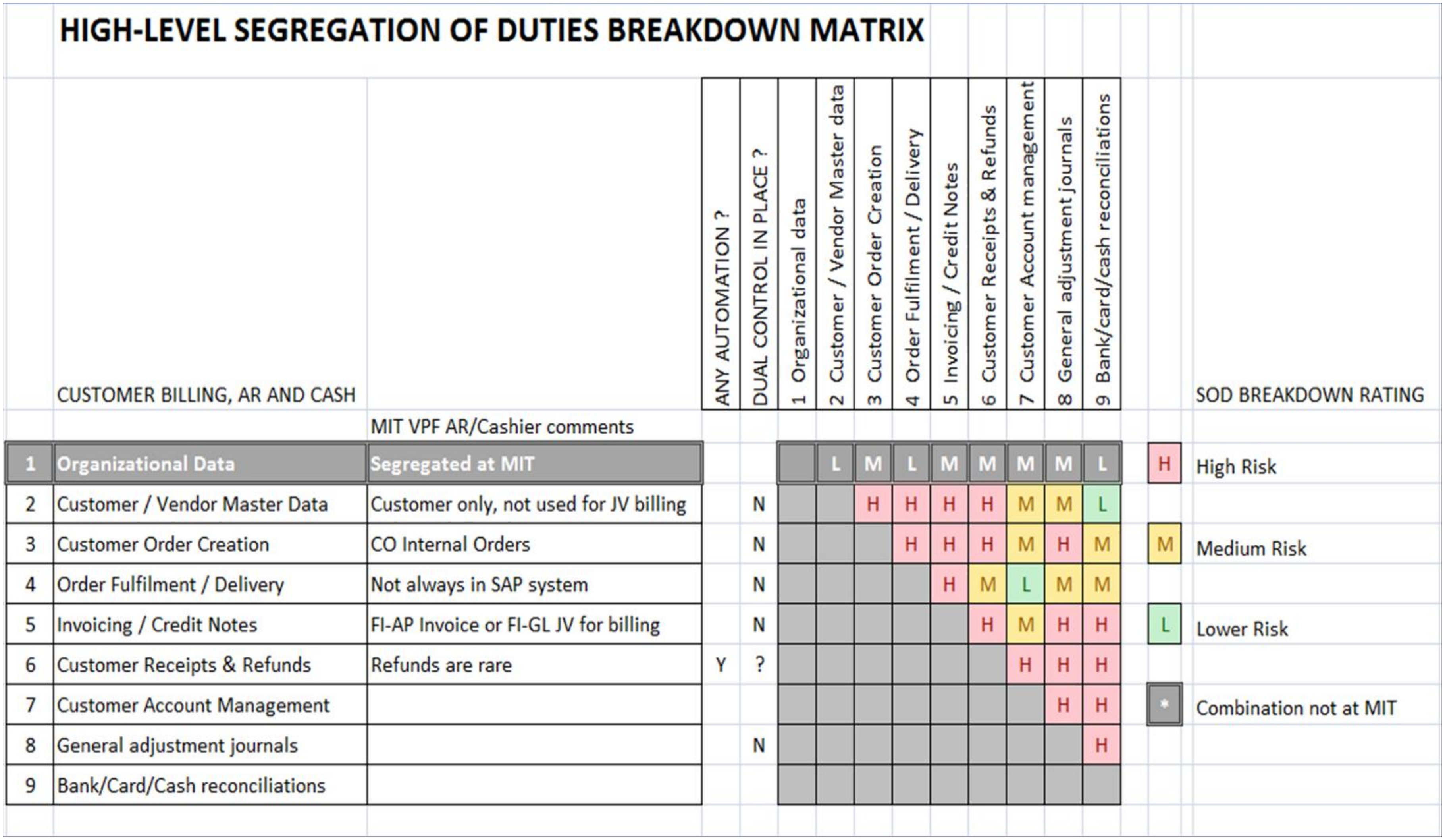
INFORMATION INPUT	ROLE DESIGN / REDESIGN STEPS
	in any other way. d. List of roles / composite roles assigned to the users e. Additional Authorizations used to restrict access by organizational, functional, or business classification. • This may include authorizations provisioned through the MIT custom Rules Database • Once a role is created, the Profile Generator requires values for the Authorization Objects used by the tcodes in the role. f. Additionally, IS&T can list the Authorization Objects called for a transaction code.
	7. Business Controls and Risk Mitigation
Audit Business Analyst	a. Dual actions required by procedures or in use – e,g. entry & independent approval of entered data (master data and financially-relevant transactions). b. Any organizational "segregation of duties" – e.g. Master Data users are a separate group of users from the Financial Transaction Entry users. c. The usual business procedures for reconciling business activity – e.g. cash receipts, check stationery, warehouse physical inventory, fixed assets inventory. d. Detective, like independent review of reports - and who performs the review. Often there are "exception" reports which focus on specific risks for the users. e. Configured or programmed system restrictions.
Audit IS&T	f. Activity logs and reviews, and the data being reviewed is protected from change / deletion. Typically reports of master data changes, financial transactions, overdue open items, unblocked invoices).
Audit Business Analyst Business System Analyst	g. Additional access restrictions - e.g. users activity is limited to specific GL Accounts, Vendors / Customers, FI Document Types or dollar amounts – which may reduce the risk.
PHASE B	**ROLE REDESIGN– Role Build and SOD Analysis (8)**
	8. Analysis of actual Segregation Of Duties
All of the above GRC Risks definition	a. Understand the expected / best practices SOD requirements for the SAP UserIds, based on the actual business area being reviewed and the actual business systems in place . b. Use Standard SOD rulesets for identifying Risks and Function-level

INFORMATION INPUT	ROLE DESIGN / REDESIGN STEPS
	definitions – the function level clash is usually like Vendor Master + Invoice Entry. c. Understand the “High Risk” or Critical activties in GRC.
IS&T Business Management	d. Redesign of SAP Roles and UserIds • Remove all unused SAP transaction codes and other SAP Authorizations from the roles • Match additional Authorizations to any restriction requirements (organizational and accounting restrictions) • Identify and set up any new users (if there is additional staffing to help with maintaining SOD). • Assignment of all expected roles to a user - check tcodes match actual job duties, no more and no less • This is mostly managed at MIT with Composite Roles – so several single roles are assigned to a Composite role. • In smaller operational areas there may be one Composite Role per user, reflecting a unique mix of job duties per user.
Business Analyst Business Systems Analyst	e. Review of redesigned SAP Roles (preliminary review per Role, and then per User with all roles and Roles Database profiles assigned) for any SOD Issues • SOD breakdowns reviewed – identify real risk / processing scenario for the SOD in the specific environment. • Uses Standard SOD rulesets for identifying activity-level (tcode) and permission-level SOD breakdown.
Business Management IS&T Security	f. Consider remediation possibilities - looking at either side of the function clash for the SOD risk : • Adjusting several roles / job duties to avoid an SOD • Move one or more of the tcodes to a “FireFighter” role • Have another business area manage a function • Use alternative tcodes which do not have the same risk.
Audit Business Management	g. Review of total physical business environment, including business processes across systems where SAP is not the only system in the business process. • There may be an SOD where the user performs two actions, one in each system, which would be reported as an SOD if both actions were managed in SAP.

INFORMATION INPUT	**ROLE DESIGN / REDESIGN STEPS**
PHASE C	**MITIGATION STRATEGY (9 – 11)**
Audit Business Analyst Business Systems Analyst	9. Understand the exact scenario possible for the reported Risk a. Look at the exact tcode combinations reported for the Risk. Each Risk has two conflicting functions – and each function can have several tcodes. - Where there are a large number of combinations, they can usually be grouped to simplify the analysis. - Look at the tcode combination in conjunction with the GRC Risk description, it sometimes helps to focus on a specific issue. b. Check if the GRC system already has a Mitigation Control defined for this Risk. If there is one, make sure the same tcode combinations were involved. If there is a major difference in the conflicting tcodes, the Mitigation Control may not be valid for the new users under analysis. c. Determine if any of the combinations are not a significant risk for MIT. For the combinations remaining, outline the process steps needed for the user, with no collusion, to benefit from the potential SOD. d. In some cases a multi-step scenario is needed, and a mitigating control at any one step may be adequate. e. Double check with Audit if the issue has been reported and/or already addressed or risk is formally accepted by management to be within acceptable levels.
Information gathered above Audit Business Analyst Business Systems Analyst	10. **Review of SOD issues and any effective “mitigating” control processes already in place.** This may include a. workflowed approvals, independent “release” or “activation” processes, or dual control master data b. workflowed / emailed notifications of activity c. regular business post-facto report review, including “reconciliations” , activity reporting and exception reporting d. other SAP Authorizations (GL/Customer/Vendor accounts, document types, Fixed Assets, organizational, table access) e. transactional value limits f. configured restrictions (document types, field restrictions) g. programmed restrictions, including validations or upload program checks.
	11. Recommendations for addressing remaining SOD issues :
Audit	a. Improved SOD within SAP user business roles – potential for business

INFORMATION INPUT	**ROLE DESIGN / REDESIGN STEPS**
Business Management	user role changes – but not always possible.
Audit Business Analyst	b. Improved procedural controls – e.g. detective report reviews
Business Analyst Business Systems Analyst IS&T Development	c. Additional lower-level preventative / limiting controls such as : • Authorizations – e.g. restricted access based on account assignments (GL Accounts, Vendors, Customers, Plants, FI Document Types etc) • Configuration / Enhancements – like • Data Entry validations • FI Document Type settings • SAP dual control activations • Workflows
Business Analyst Business Systems Analyst IS&T Development	d. Custom processes / enhancements with inbuilt restrictions preventing or limiting the SOD issue : • Screen variants for restricting and/or forcing data and options • Functionality limitations • Specific data tables or data • Special checks – like prevent entering invoices for Vendors created by the same user.
Risk Owner	e. Ensure controls are in place – has to be evidenced and testable.

Example of a Sales related SOD risk matrix, showing conflicting functions. Risk rating (High, Medium, Low) is for illustration purposes only.



HIGH-LEVEL SEGREGATION OF DUTIES BREAKDOWN MATRIX

	CUSTOMER BILLING, AR AND CASH		ANY AUTOMATION ?	DUAL CONTROL IN PLACE ?	1 Organizational data	2 Customer / Vendor Master data	3 Customer Order Creation	4 Order Fulfilment / Delivery	5 Invoicing / Credit Notes	6 Customer Receipts & Refunds	7 Customer Account management	8 General adjustment journals	9 Bank/card/cash reconciliations		SOD BREAKDOWN RATING
		MIT VPF AR/Cashier comments													
1	Organizational Data	Segregated at MIT				L	M	L	M	M	M	M	L	H	High Risk
2	Customer / Vendor Master Data	Customer only, not used for JV billing		N			H	H	H	H	M	M	L		
3	Customer Order Creation	CO Internal Orders		N				H	H	H	M	H	M	M	Medium Risk
4	Order Fulfilment / Delivery	Not always in SAP system		N					H	M	L	M	M		
5	Invoicing / Credit Notes	FI-AP Invoice or FI-GL JV for billing		N						H	M	H	H	L	Lower Risk
6	Customer Receipts & Refunds	Refunds are rare	Y	?							H	H	H		
7	Customer Account Management											H	H	*	Combination not at MIT
8	General adjustment journals			N									H		
9	Bank/Card/Cash reconciliations														

GRC Forms

Example Form A: GRC Mitigation Control Change Request

Massachusetts Institute of Technology

GRC MITIGATION CONTROL CHANGE REQUEST

Please use this form to request changes to the SAP GRC Mitigation Controls – for new / amended descriptions, and for new / amended assignments to Risk/User combinations.

ACTION REQUIRED ***- check with "Y" all applicable***					
□	**New Mitigation Control ?**	□	**Amend the MC description ?**		**GRC ADMIN STATUS**
□	**New Risk/User assignments ?**	□	**Amend Risk/User assignments ?**		
□	Document to be attached ? ➢ .				**DEV** *DD/MM/YY*
□	Hyperlinks to be attached ? ➢ .				**TEST** *DD/MM/YY*
	Date Required in Production MM / DD / YY Coordinated with other SAP R/3 Production transports Y/N ?				**PROD** *DD/MM/YY*

MITIGATING CONTROL : GENERAL INFORMATION	
GRC MC ID	Use format MC-XXX-12 where XXX is VPF Business Area ➢
GRC MC CONTROLLER	➢ *MC Controller Name :* ______________________________ ➢ *SAP User Id :* ______________________________
SHORT DESCRIPTION	*Short description (max. 25 characters)* ➢
LONG DESCRIPTION	*Long description in attached document ? If not, enter below :* ➢

Massachusetts
Institute of
Technology

GRC MITIGATION CONTROL CHANGE REQUEST

RISK / USER ASSIGNMENT – to be added or removed ?				
ADD	REMOVE	GRC RISK ID	SAP USER ID	User Name

ROLE OWNER - PROPOSER			
Name	Telephone #	Kerberos Id	Date
RISK OWNER – APPROVER			
Name	Telephone #	Kerberos Id	Date

Example Form B: GRC FireFighter Change Request

Massachusetts
Institute of
Technology

GRC FIREFIGHTER CHANGE REQUEST

Please use this form to request changes to the SAP GRC FireFighter assignments for existing or new FFIDs

ACTION REQUIRED *- check with "Y" all applicable*						
□	Amend assignment - FFID User	□	Amend assignment - FF ID Controller	□	Amend assignment - FF ID Owner	**GRC ADMIN STATUS**
□	New FF ID and R/3 User and Role ?	□	Add / Remove GRC EAM report user ?			**PROD** *DD/MM/YY*
□	Coordinate with other SAP R/3 Production transports ? Date Required in Production > *MM / DD / YY*					

FIREFIGHTER CHANGES : GENERAL INFORMATION	
RT TICKET ID	➢
RT TICKET TITLE	➢
RT TICKET – ISSUE TYPE	➢ *GRC FIREFIGHTER CHANGES*
REQUESTER	➢ *Name :*
BUSINESS PROCESS OWNER / BA	➢ *Name :*
IS&T BSA	➢ *Name :*
REQUIREMENT / JUSTIFICATION	➢
RELATED R/3 TRANSPORTS	➢

Massachusetts Institute of Technology

GRC FIREFIGHTER CHANGE REQUEST

GRC FFID ASSIGNMENTS – to be added or removed

NEW FFID	Existing FFID	GRC FF ID	SAP USER KERBEROS ID	FFID USER	FFID CONTROLLER	FFID OWNER
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove
□	□			□ Add □ Remove	□ Add □ Remove	□ Add □ Remove

FIREFIGHTER ROLE OWNER - APPROVER

Name	Telephone #	Kerberos Id	Date

Example Form C: SAP User or Role Change Checklist

Massachusetts Institute of Technology

SAP PS1 SECURITY CHANGE CHECKLIST

Please use this form to request or document changes to the SAP R/3 Security in Production (PS1) –for changes to Roles and for Role assignment to Users (pages 1 -3), FireFighter Users and roles (page 3) and for User administrative data changes including lock/unlock and reset password (page 4).

For new Composite Roles or new FireFighter Users, please use one Change Request form per role or user.

ACTION REQUIRED *- check with "X" all applicable*						
□	LOCK / UNLOCK USER (Page 4)	□	RESET PASSWORD (Page 4)			
□	COMPOSITE ROLE NEW	□	SINGLE ROLE NEW	□	NEW USER – role assignment	**ADMIN STATUS**
□	COMPOSITE ROLE CHANGE	□	SINGLE ROLE CHANGE	□	EXISTING USER – role change	
□	Coordinate with other SAP R/3 Production transports ?					
□	Coordinate with Roles Database changes ?					
□	Coordinate with GRC FireFighter changes ?					
	Date Required in Production > *MM / DD / YY*					**PROD UPDATED** *DD/MM/YY*

R/3 ROLE AND ROLE ASSIGNMENT CHANGES : GENERAL INFORMATION	
RT TICKET ID	➢
RT TICKET TITLE	➢
RT TICKET – ISSUE TYPE	➢ *R/3 SECURITY ADMIN*
REQUESTER / ROLE OWNER	➢ *Name :*
BUSINESS PROCESS OWNER / BA	➢ *Name :*
IS&T BSA	➢ *Name :*
REQUIREMENT / JUSTIFICATION	➢
RELATED R/3 TRANSPORTS	➢

SAP PS1 SECURITY CHANGE CHECKLIST

COMPOSITE ROLE CHANGES

COMPOSITE ROLE	NEW ROLE	ADD SINGLE	REMOVE SINGLE	SINGLE ROLE	GRC ARA ROLE	GRC ARA USERS
	□	□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			

SINGLE ROLE CHANGES (USER AND FIREFIGHTER)	
SINGLE ROLE (s) -	*The role(s) to be changed.* ➢ . ➢ .
ROLE DESIGN DOCUMENT **(required for new roles)**	*File name and location of Role Design document* ➢
LIST OF CHANGES TO EXISTING ROLE	*Description of Transaction Codes (added or removed) and/or Authorizations (to be added, removed or amended)* ➢
GRC Risk Analysis – Role ?	➢ *Simulation Provided / Needs to be run ?*
GRC Risk Analysis – Users ?	➢ *Simulation Provided / Needs to be run ?*

NEW FIREFIGHTER USER	
USER	➢ *FF-XXX-NN*
ROLE DESIGN DOCUMENT	*File name and location of Role Design document (optional)* ➢
FFID SET UP COMPLETED IN GRC ?	➢ *Date / Time :*

ROLE OWNER - APPROVER (USER ROLES AND FIREFIGHTER ROLES)			
Name	**Telephone #**	**Kerberos Id**	**Date**
GRC Verification – SOD Coordinator (USER ROLES ONLY)			
Name	**Telephone #**	**Kerberos Id**	**Date**

SAP PS1 SECURITY CHANGE CHECKLIST

USER STATUS : CHANGES	
USER ID	➢
PASSWORD RESET	➢ *Date / Time :*
LOCK USER	➢ *Date / Time :* ➢ *Reason :*
UNLOCK USER	➢ *Date / Time :* ➢ *Reason :*

USER IDENTIFICATION DATA : CHANGES	
USER ID	➢
USER GROUP	➢
GRC CUSTOM USER GROUP	➢
NAME	➢
WORKCENTER	➢ *Department :* ➢ *Building :* ➢ *Room :*
LOCATION	➢
COMMUNICATION DETAILS	➢ *Phone :* ➢ *Fax :* ➢ *Email :* ➢ .
ACCOUNT NUMBER	➢

USER MANAGER - APPROVER			
Name	Telephone #	Kerberos Id	Date

GRC Change Events

Massachusetts Institute of Technology

MIT BUSINESS EVENTS TRIGGERING SAP/RDB AUTH CHANGES AND THE IMPACT ON GRC

Event triggering change	Type of change	SAP UserId and Auth changes	MIT Roles Database (RDB) changes	GRC changes, SOD Risk Analysis impact, FireFighter	Mitigation Signoff	Process Flowchart
The business event which triggers a change in Users, User Access, Role Design, Mitigation Requirements, GCR assignments (Mitigations and FireFighters).	The type of change that is triggered, in business terms.	Exactly what SAP R/3 objects needs to be amended and the type of amendment – add, remove, reassign, create, change etc.	Any changes that are expected in the MIT Roles Database system. This is mostly managed by the user's management – but may sometimes also have a technical change component.	The actions and changes which will be needed in the GRC system – for Mitigation analysis, Mitigation Control assignment and for FireFighter management.. In some cases Validity Period can be used instead of de-assignment.		1. Roles Maintenance 2. Mitigation 3. Role Provisioning to Users 4. FireFighter 5. Compliance reviews
Departmental reorganization	Job duty changes – may be substantial changes	• Role / composite role changes • User role combinations changed • Probably an existing User Group, but may be a new one.	• Probably a few RDB changes • If user role redesigned for the first time under new process, update the RDB user list so that some of the old common profiles are not exported back into SAP.	• Role analysis • User Analysis • Mitigation reassignments / deassignments with validity dates • Possibly need New / Changed Mitigation Control • Possibly need reassignment of FireFighter IDs	Potentially changed	1. Roles Maintenance 2. Mitigation 3. Role Provisioning 4. FireFighter
Existing job position • New hire • Employee Transfer in (new manager's actions)	Replacement or additional staff – no other changes	• User added to SAP with same roles as an existing user • For Transfer In, amend User Group.	• User added to RDB or amended in to have the same attributes as existing users	• Add UserId to mitigation assignment	No change – but include user Id in selection for Mitigation reports.	1. Roles Maintenance 3. Role Provisioning
New or changed job duties • New hire • Existing employee	New job, new duties	• New role / composite role • New role combination for the user • Probably an existing User Group, but may be a new one.	• User added to RDB with appropriate attributes.	• Role analysis • User Analysis • Mitigation reassignments / deassignments and Validity Date changes	Potentially changed	1. Roles Maintenance 2. Mitigation 3. Role Provisioning 4. FireFighter
Temporary staffing	Several types : • Existing job • Combination of jobs • Special project/access	• User added to SAP with same roles for sub-set of roles as an existing user • User added to SAP with new combination or roles	• Some additional provisioning may be needed	• Simulations of any new role combinations • Mitigation reassignments / deassignments after periodic GRC reporting – using Validity Dates. • May need FireFighter access		1. Roles Maintenance 2. Mitigation 3. Role Provisioning 4. FireFighter
Employee Transfer Out (prior manager's actions)	Employee remains at MIT, but moves to a different DLC	• User's job-related access to be removed • Variation : user performs old duties and new duties for a while !	• User's old permissions removed by prior manager – at some point. • User's new permissions added by new manager before job assignment commences	• Amend "Valid To" date for mitigation assignment. • User Analysis – where user is to retain old access overlapping with new access. • FireFighter de-assignments	Potentially changed	2. Mitigation 3. Role Provisioning 4. FireFighter
Employee resigns, is terminated or has taken long-term/permanent leave.	Employee no longer needs access to SAP. Note : procedure is different for terminations.	• Roles can be removed from User • ESS access remains ?? • User is deactivated (but not removed) • IS&T employee - deactivated in all SAP systems	• User's permissions removed , by ????	• Mitigation/User assignment remains for historical reporting. Amend "Valid To" date. • FireFighter de-assignments	User Id remains in selection variant for historical reporting.	2. Mitigation 3. Role Provisioning 4. FireFighter
Non-employee leaves MIT	Student, associate, consultant no longer needs access	• User is deactivated (but not removed) • Consultants – deactivated in all SAP systems	?	• No changes – and Mitigation/User assignment remains for historical reporting.	User Id remains in selection variant for historical reporting.	3. Role Provisioning
New SAP application functionality added	Standard SAP or "Z" tcodes to be added	• Standard SAP tcodes – add to roles – Business Users and related FireFighters (for business, BA and BSA) • May require separate single role, to be included in composite roles.	• May be no change. If RDB already controls similar auth/qualifier, then maybe new object is added to RDB.	• Custom "Z" tcodes – identify SAP equivalent and add to Ruleset (Functions) wherever SAP equivalent is. • Role analysis • User Analysis	Potentially changed	1. Roles Maintenance 2. Mitigation

MIT BUSINESS EVENTS TRIGGERING SAP/RDB AUTH CHANGES AND THE IMPACT ON GRC

Event triggering change	**Type of change**	**SAP UserId and Auth changes**	**MIT Roles Database (RDB) changes**	**GRC changes, SOD Risk Analysis impact, FireFighter**	**Mitigation Signoff**	**Process Flowchart**
Functionality removed	No replacement, just removal. *Change of tcode usage - e.g.* • *FV50 replaces F-65* • *FBCJ replaces ZCxx*	• Typically tcodes are removed from a role. • *Rare – a role could be deactivated* • *See “New Functionality Added” for action on any replacement tcodes. Cannot assume replacements have the same SODs as those replaced.*	• May be no change. If RDB controls a related auth/qualifier, then it can be removed from / disabled in RDB.	• Determine if a Risk was removed, and so the user can be deassigned from a mitigation control. • Role analysis • User Analysis may be needed	Potentially changed	1. Roles Maintenance 2. Mitigation
Missing authorization	New SAP Authorizations, role maintenance errors, Roles DB errors	• Affected role is updated – all role users are fixed	• If missing authorization is provided from RDB, missing due to technical or provisioning error, fix in RDB.	• Unlikely to be affected , unless new authorization is already added to GRC and causes an SOD • User analysis – just to be sure	Potentially changed	1. Roles Maintenance
Firefighter assignment changes	Request for User → Firefighter assignment	N/A	N/A	• Assign SAP R/3 User to Firefighter ?	Should not be affected	4. FireFighter
SAP Auth Role redesign	Technical – behind the scenes – should not affect the business	• Role / composite role changes	• Some may be removed, if SAP Auth roles becomes the controller	• Role analysis • User Analysis • Unlikely to be removing risks, but it is possible where unnecessary access was removed – so potentially may be able to deassign mitigations.	Should not be affected	1. Roles Maintenance
Business or Audit controls review	• Additional mitigation controls to be added and assigned. • “Remove access” request from Audit	• May have new reports – may need new tcode and role to be assigned to users to run mitigation reports • Role removed from user(s) • Possible role redesign	Possible change.	• New Mitigation Control created • Change assignment of Risk / Mitigation / User.	New control added to Signoff documentation.	2. Mitigation 3. Role Provisioning
Mitigation Control – periodic expiry of User assignment and subsequent recertification	Expiry dates for Mitigation Control / User Assignment need to be extended	N/A	N/A	• May identify some assignments that can be removed • Extend all valid assignments = “recertify”	Unchanged	2. Mitigation
Ruleset changes – MIT or PWC	Different ratings (H/M/L) on risks, added/removed critical transactions, tcodes removed from Function, etc	N/A	N/A	• Role analysis • User Analysis	Should not be affected	N/A - GRC MAINTENANCE
SAP annual system and content changes	Additional Tcodes, Functions and Rules added to ruleset	N/A	N/A	Additional Tcodes, Functions and Rules added to SAP delivered ruleset. Note : if any new functionality is actually used, the new tcodes would have been added to user roles – see “New Functionality Added” above.	Should not be affected	N/A - GRC MAINTENANCE
User locked, name changes, etc	• User locks / unlocks • Password Resets • User information/name • Other ?	• User Master updated	N/A	N/A	Not affected	3. Role Provisioning

Massachusetts Institute of Technology

MIT BUSINESS EVENTS TRIGGERING SAP/RDB AUTH CHANGES AND THE IMPACT ON GRC

Event triggering change	Type of change	SAP UserId and Auth changes	MIT Roles Database (RDB) changes	GRC changes, SOD Risk Analysis impact, FireFighter	Mitigation Signoff	Process Flowchart
MONITORING AND REPORTING						
Ongoing Risk Analysis Review	Identifies a changed user – with unmitigated SOD Access Risk or critical transaction	• Correct provisioning error – remove role from user • ?	Possible change – most likely, a converted user is still getting old common roles or was incorrectly provisioned.	• May need to assign user to Risk/Mitigation	Potentially changed	2. Mitigation 3. Role Provisioning
Monthly Compliance review	Execution of mitigation processes and their review and sign-off by the risk owner	• May trigger a role change or a role assignment change	N/A	•		1. Roles Maintenance 3. Role Provisioning 5. Compliance review
Ongoing User Access reviews	Review of user access and critical access	• May trigger a role change or a role assignment change	N/A	•		1. Roles Maintenance 3. Role Provisioning 5. Compliance review
Firefighter usage		• Review of security logs ?	N/A	• Review of Firefighter usage logs ?		4. FireFighter
Ad Hoc reviews	N/A	Maybe some limited use of SUIM reports	N/A	• Various informational reports – who has what role, what roles does a user have, what is in a role, what are the differences between roles or users, etc • ARA Simulations, in preparation for change requests (User/Role reassignment or Role design).		2. Mitigation 5. Compliance review