GRC TRAINING:

RISK OWNERS

Massachusetts
Institute of
Technology

Table of Contents

GRC Roles & Responsibilities – Risk Owners

Risk Owners will carry out the following tasks as part of their GRC-related responsibilities:

- Provide guidance on:
  - acceptable level of risk related to SODs and critical access
  - adequacy of compensating (mitigating) controls
- Ensure control processes are in place:
  - Regular access review
  - Mitigation processes, including specific reports.
- Final approval on new/amended Mitigation Control definitions and assignment to Risk / User combinations.
- Approve recertification of mitigating controls – supported by Role Owner and Compliance Officer.
- Where designated as a FireFighter ID owner, will approve assignment of FireFighter ID to users.

Responsibilities Reference

TASKS	PROCESS & STEP
Maintain Risk Awareness : Role Owner emails Risk Owner of major role changes	1.14
Provide guidance on acceptable risk during the Mitigation Analysis process	2.1.c
Final approval of Mitigation Control definition– based on Role Owner's recommendations	2.5
Overall monitoring of control processes / reports	2.8, 5
Final approval of Mitigation Control assignment to users – based on Role Owner's recommendations	3.8 5.M.2, 5.Q.10
Approve assignment of FireFighter IDs to users	4.5
Final approval of periodic recertification of Mitigating Controls	5.A.3

REPORTS	PROCESS
01 Risk Violations	5
02 User Analysis	5
03 Violations Comparisons	5

FORMS	PROCESS & STEP
A: GRC Mitigation Control Change Request	2.5

WORKFLOW OR EMAIL-TRIGGERED ACTIONS	PROCESS & STEP
Email for Mitigation Changes – if designated as Monitor	2

SAP Security and Governance Procedures

PURPOSE OF THIS DOCUMENT

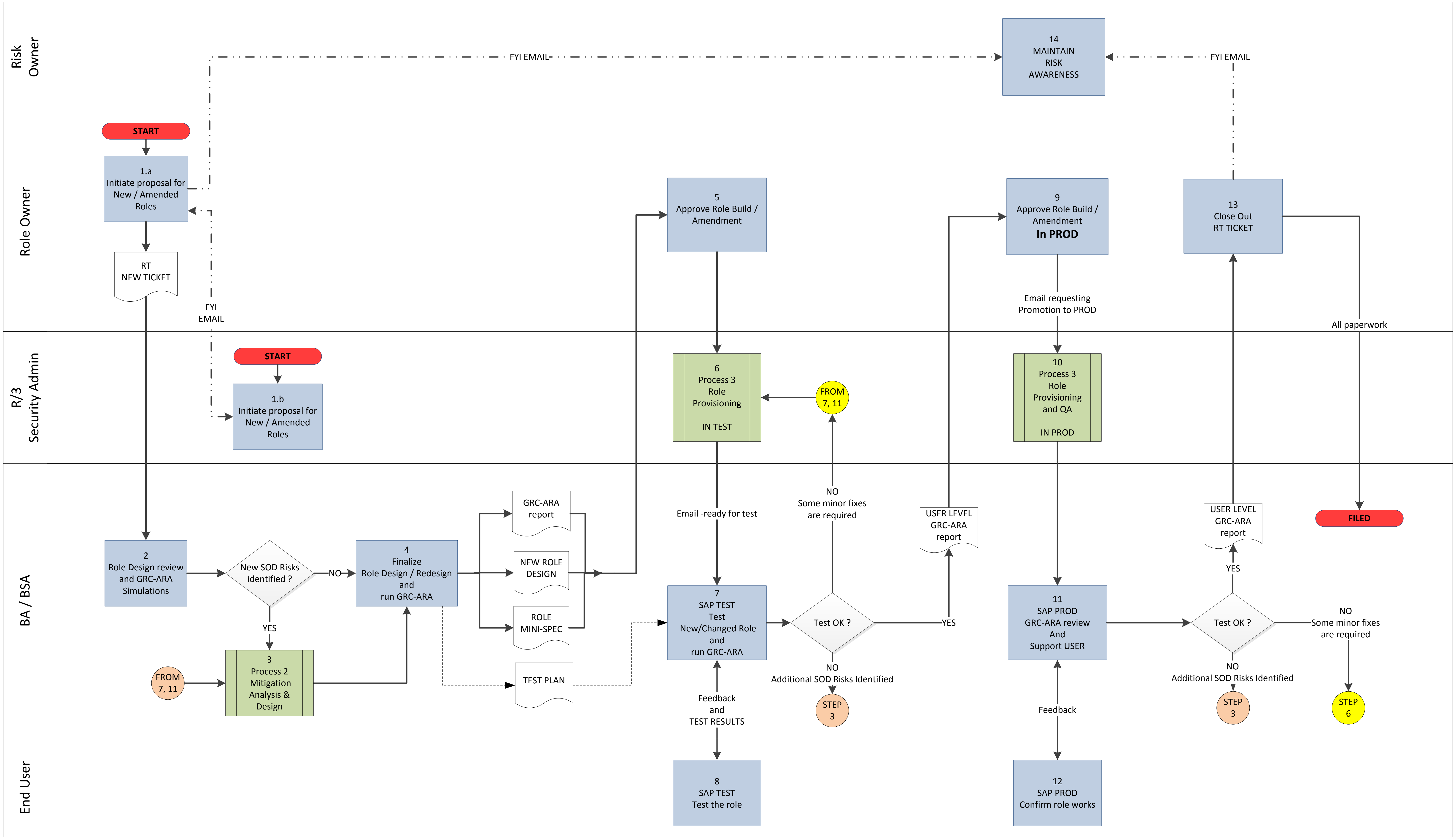
The SAP Security and Governance Procedures are documented in five flowcharts. The sections in this document describe the details of each step.

CONTENTS

Process 1: New or Amended Roles

Massachusetts Institute of Technology

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



Risk Owner

14 MAINTAIN RISK AWARENESS

FYI EMAIL

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

3 Process 2 Mitigation Analysis & Design

FROM 7, 11

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 Some minor fixes are required

STEP 6

NO Additional SOD Risks Identified

STEP 3

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.

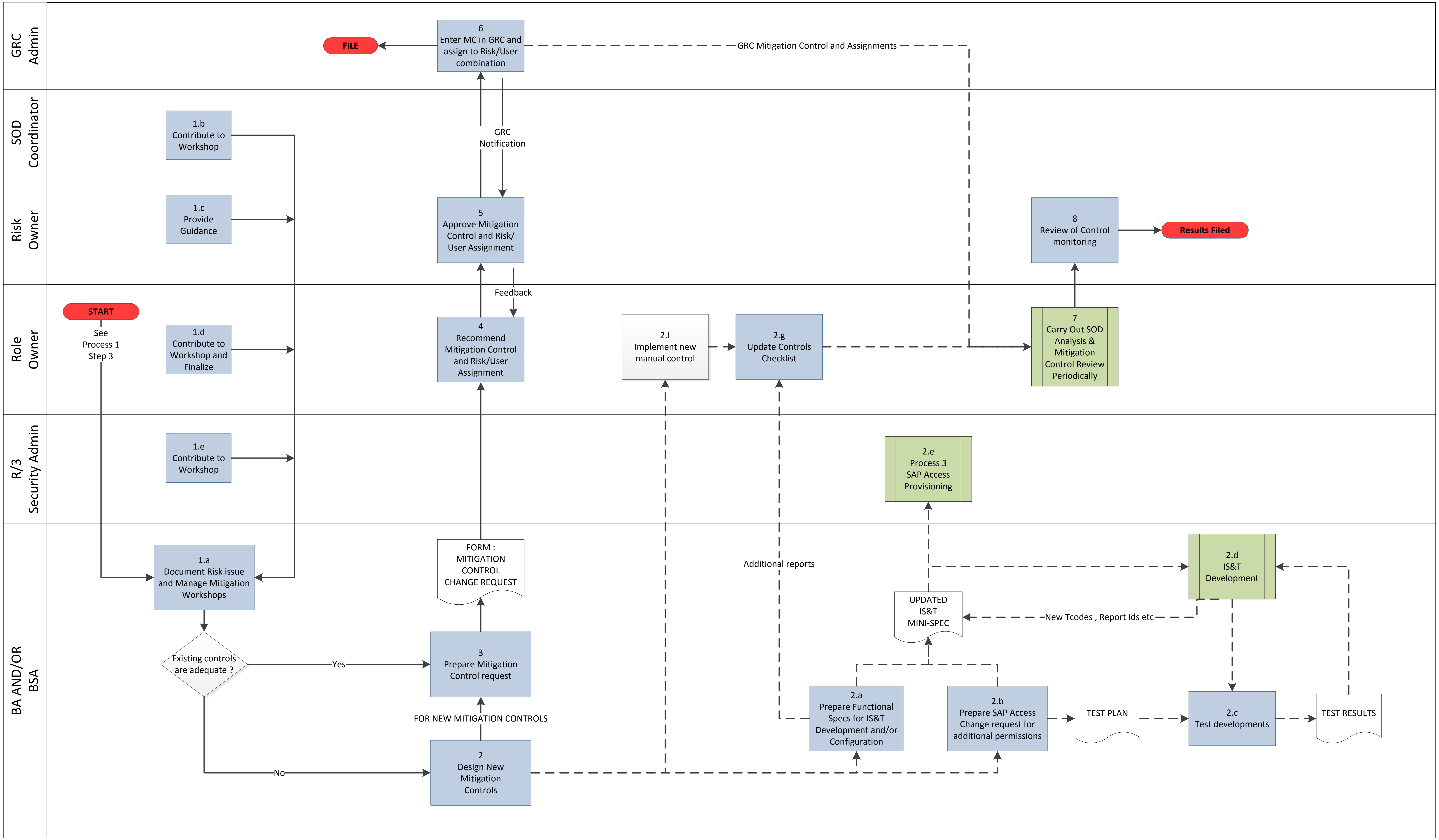
P.1 STEP	Business Role	Responsibility / Action	Output	Details
10	SAP Security Admin	Role provisioning and Transport QA review	• Email to BA/BSA and Role Owner when complete • Update RT Ticket	a. IS&T have a process for managing RT tickets, their prioritization and execution, including a QA review prior 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

Massachusetts Institute of Technology

MIT SAP Security & GRC Process : 2. Mitigation Analysis



GRC Admin

6 Enter MC in GRC and assign to Risk/User combination

FILE

GRC Mitigation Control and Assignments

SOD Coordinator

1.b Contribute to Workshop

GRC Notification

Risk Owner

1.c Provide Guidance

5 Approve Mitigation Control and Risk/ User Assignment

8 Review of Control monitoring

Results Filed

Feedback

Role Owner

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

R/3 Security Admin

1.e Contribute to Workshop

2.e Process 3 SAP Access Provisioning

BA AND/OR BSA

1.a Document Risk issue and Manage Mitigation Workshops

Existing controls are adequate ?

Yes

No

FORM : MITIGATION CONTROL CHANGE REQUEST

3 Prepare Mitigation Control request

FOR NEW MITIGATION CONTROLS

2 Design New Mitigation Controls

Additional reports

UPDATED IS&T MINI-SPEC

New Tcodes , Report Ids etc

2.d IS&T Development

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

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 combination 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.

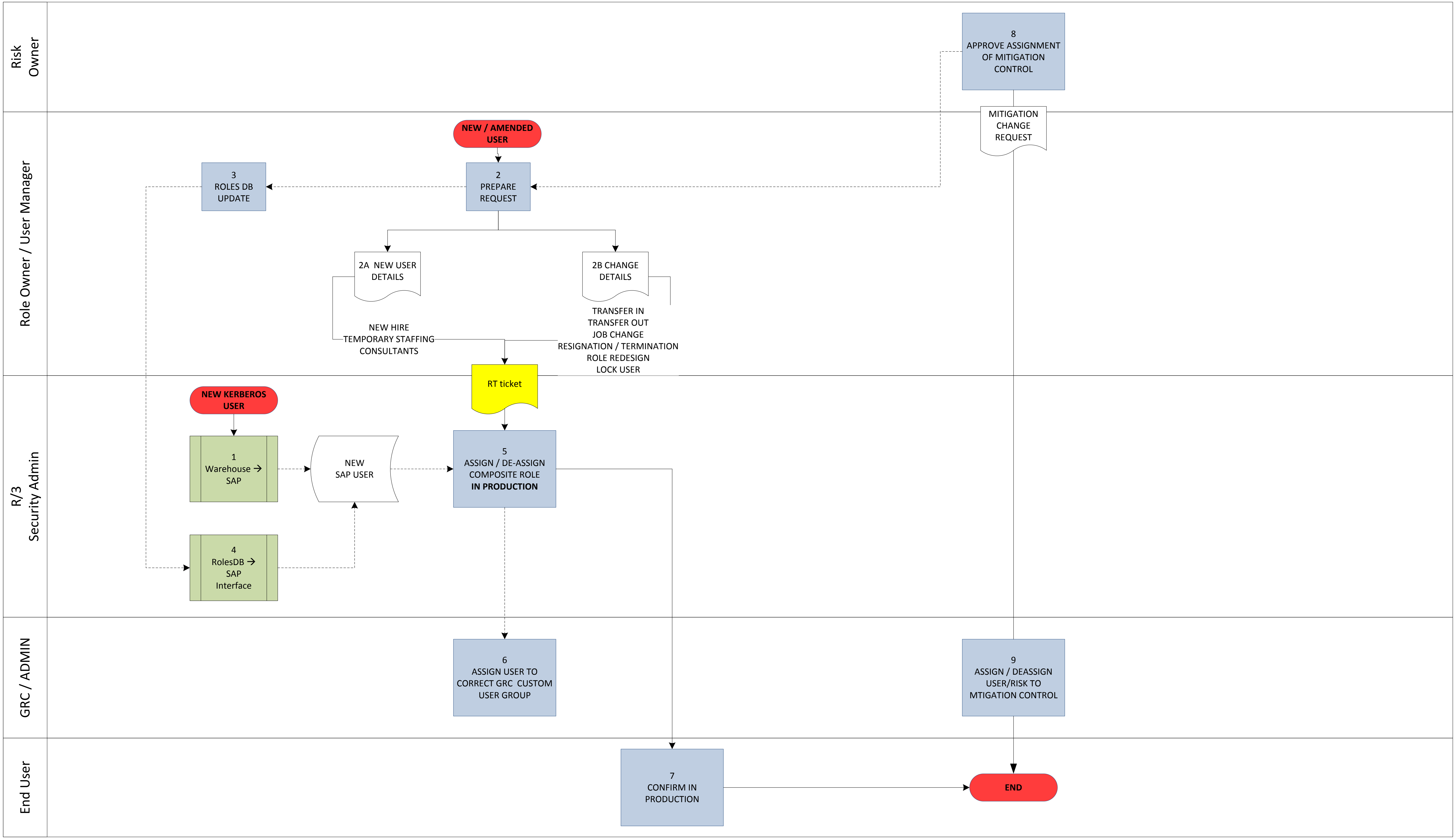
P.2 STEP	**Role**	**Responsibility / Action**	**Output**	**Responsibility / Action**
2	BA/BSA	Design new Mitigation Controls	• Detailed Workshop results with all proposed action items listed and reasons for rejecting alternatives.	**Design** the proposed Mitigation approach and detailed activities required 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



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

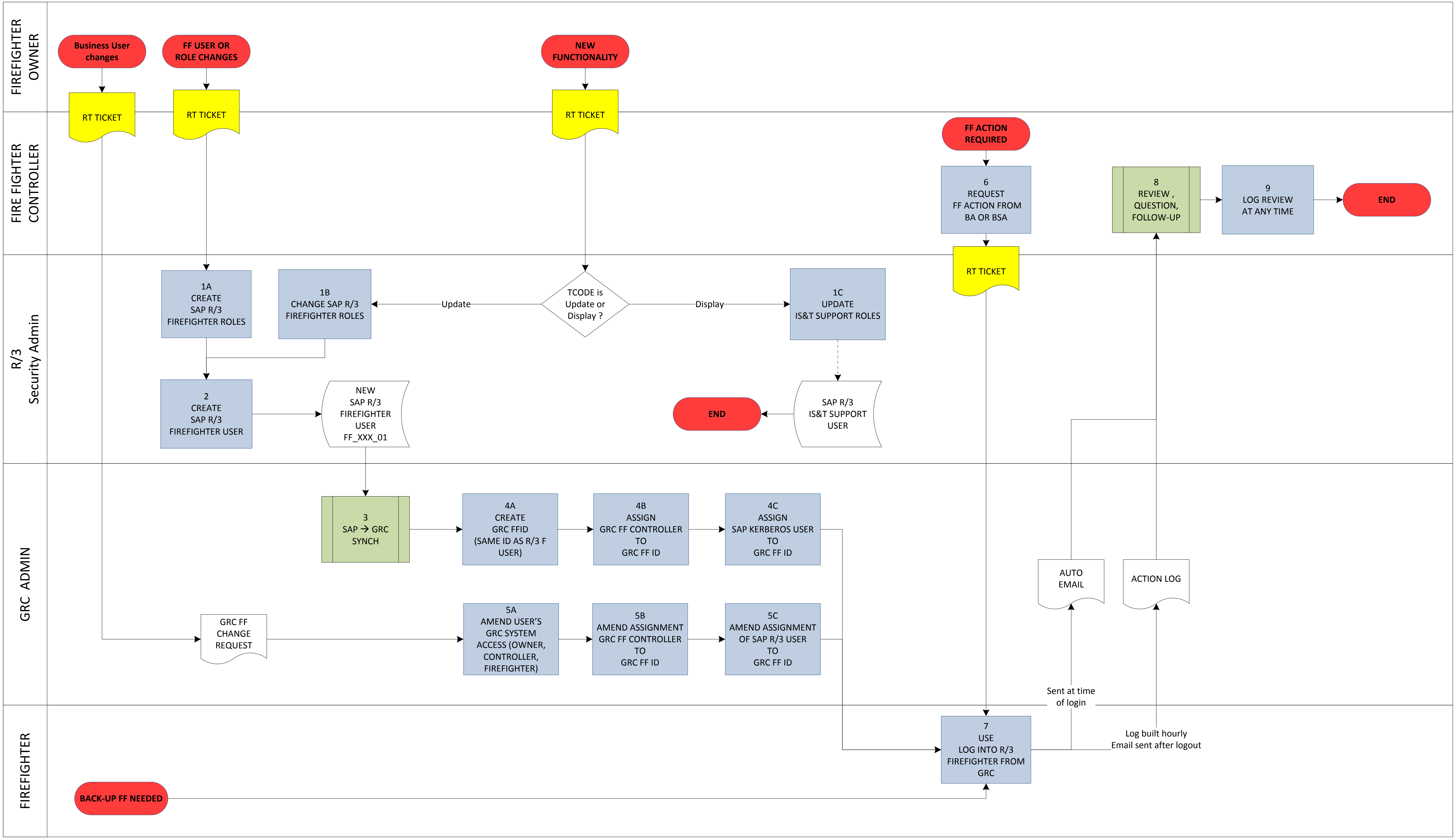
Process 3: New Users and User Role Provisioning - Detailed Steps

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

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

RT TICKET

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

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

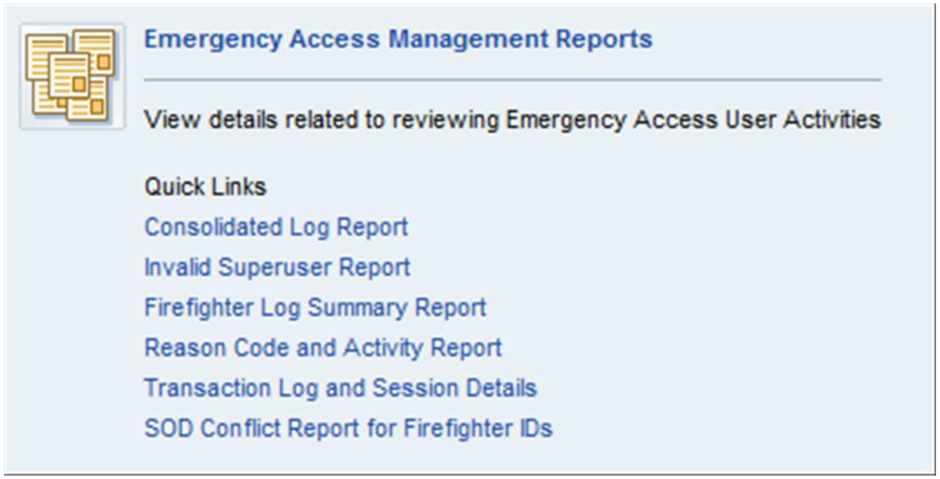
P.4 STEP	Business Role	Responsibility / Action	Output	Details
1a	R/3 Security Admin	Create FireFighter Roles	• Roles	There are several types of FF roles : • Business Analysts (BA) • IS&T Business System Analysts (BSA) • IS&T Basis Role • IS&T Developers • IS&T Managers • Business users – limited and 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.

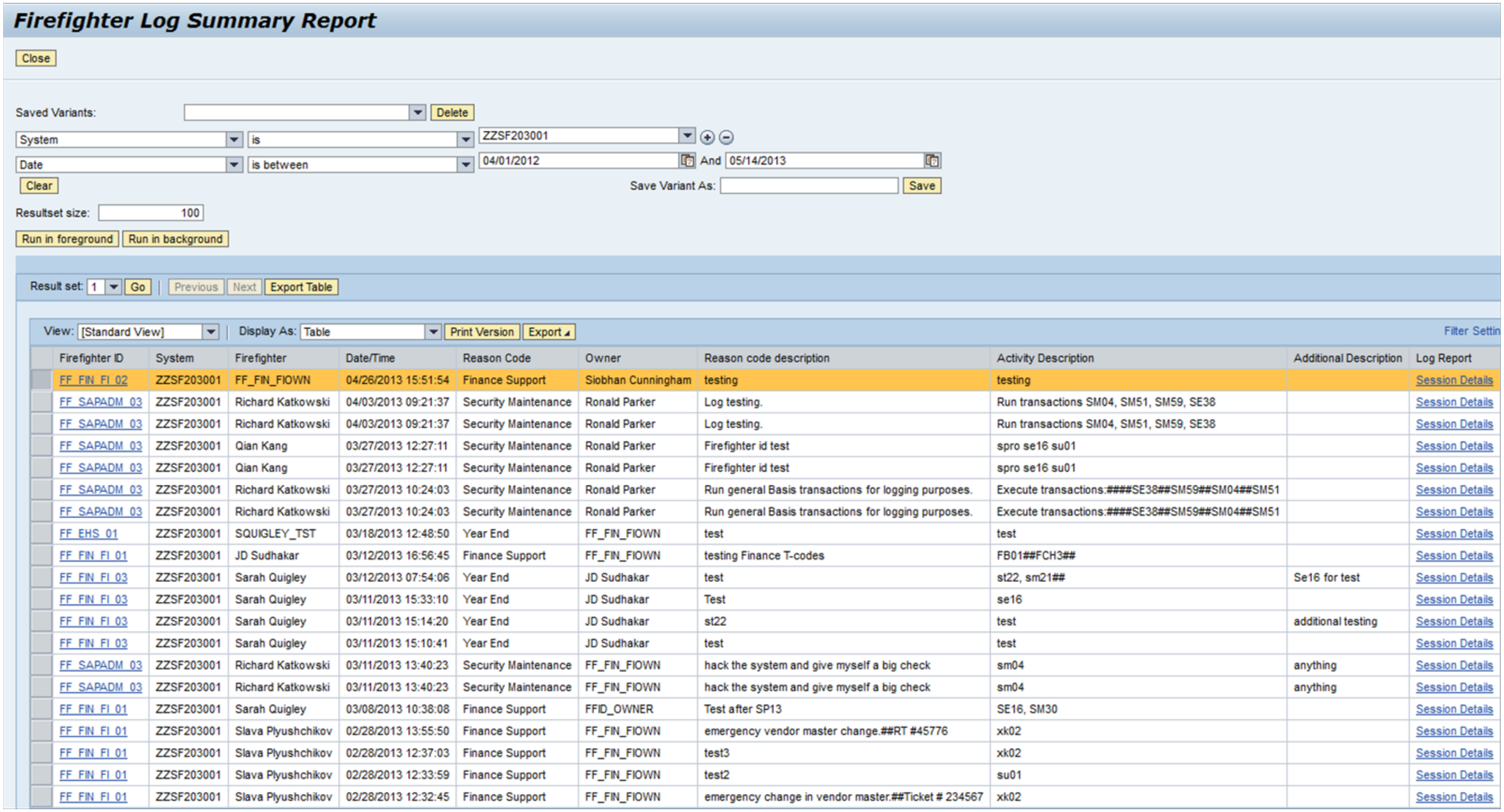
P.4 STEP	Business Role	Responsibility / Action	Output	Details
2A	R/3 Security Admin	Maintain FireFighter Users	• Users updated • Business Roles assigned • FireFighter role assigned	The R/3 FireFighter Users are generic in that they are assigned to anyone / more than one person via the GRC system. See 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:

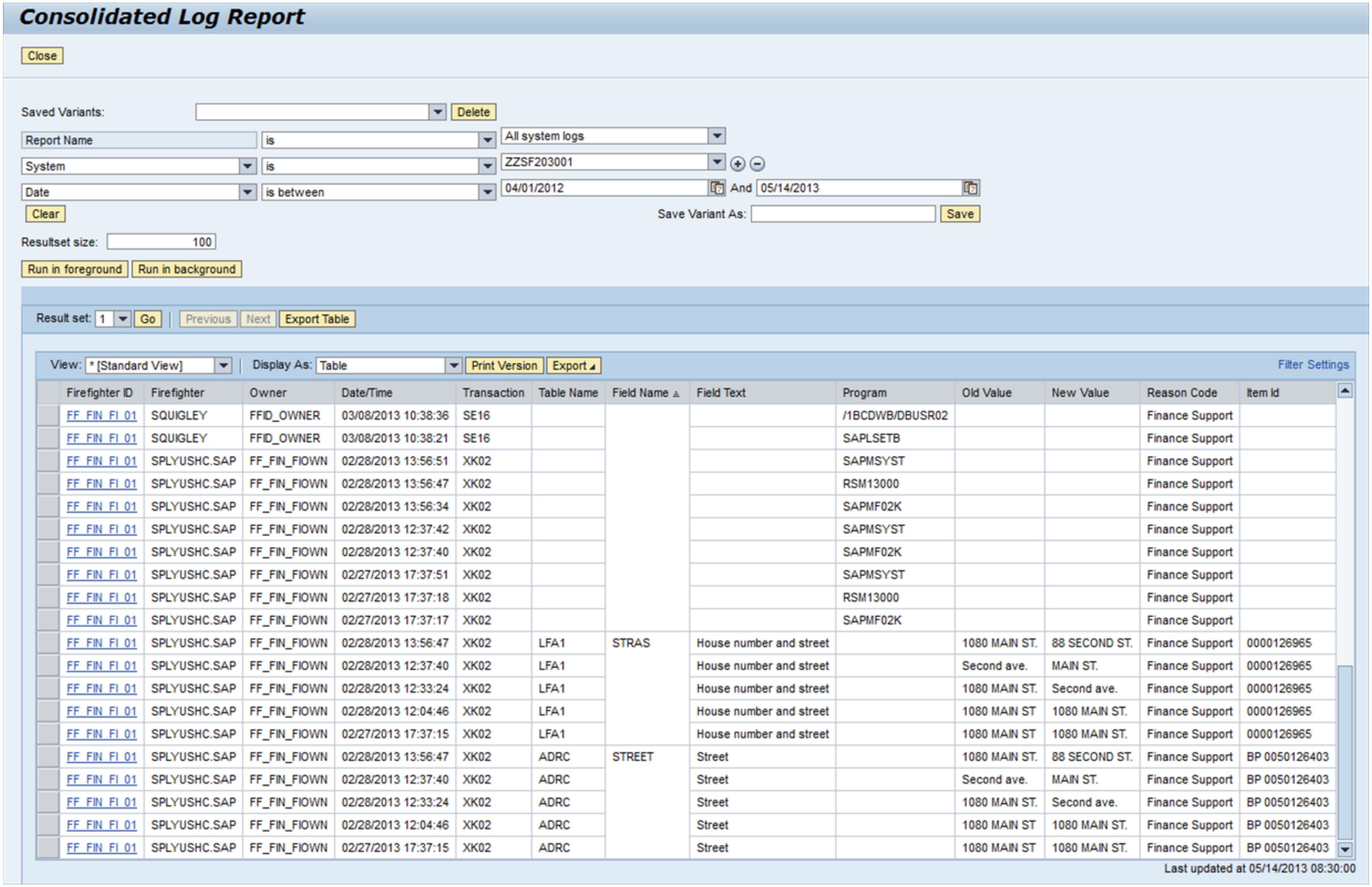
Resultset size: 100

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

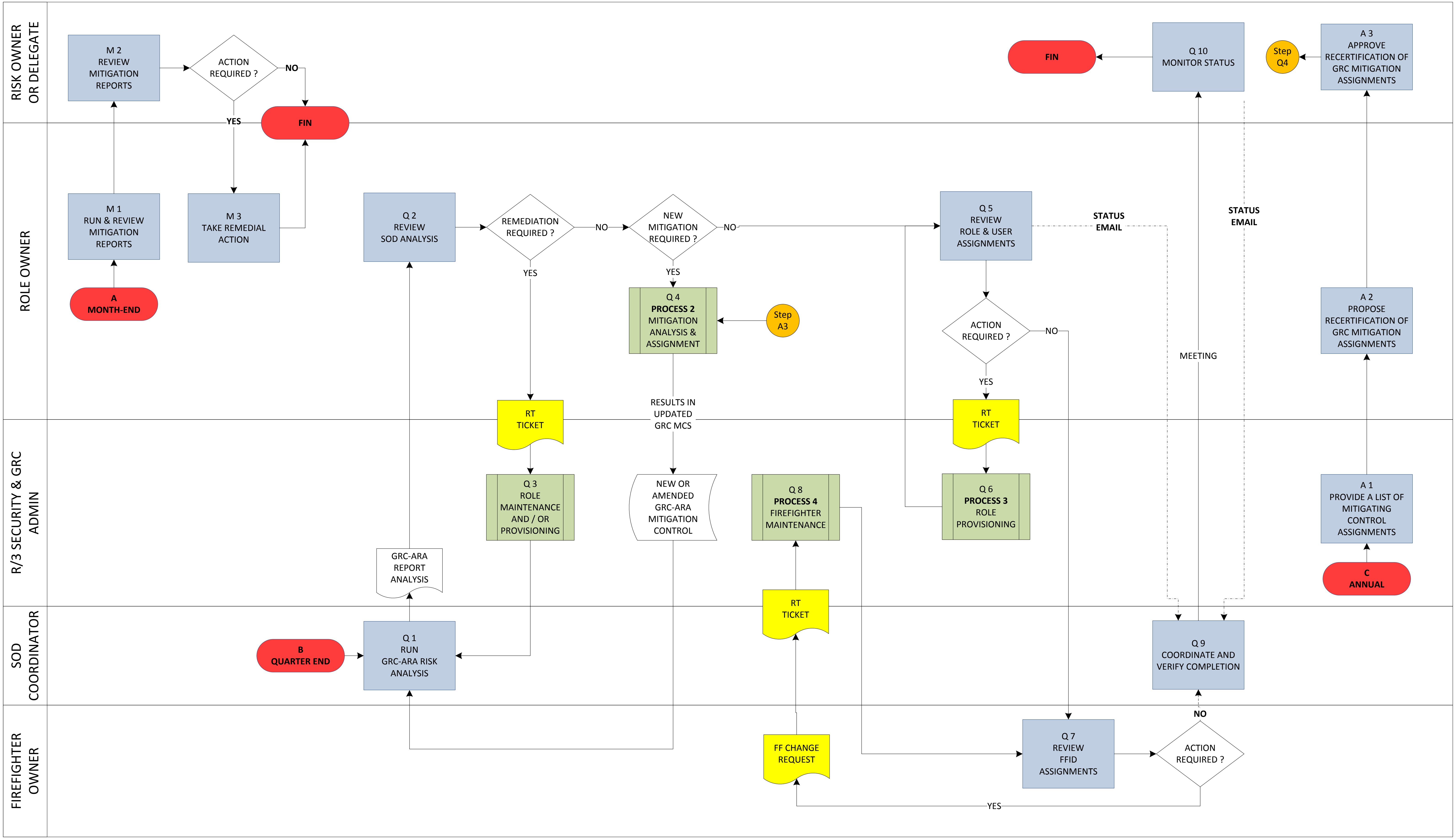
Firefighter ID	Firefighter	Owner	Date/Time	Transaction	Table Name	Field Name	Field Text	Program	Old Value	New Value	Reason Code	Item Id
FF_FIN_FI_01	SQUIGLEY	FFID_OWNER	03/08/2013 10:38:36	SE16				/1BCDWB/DBUSR02			Finance Support	
FF_FIN_FI_01	SQUIGLEY	FFID_OWNER	03/08/2013 10:38:21	SE16				SAPLSETB			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
ROLE OWNER
R/3 SECURITY & GRC ADMIN
SOD COORDINATOR
FIREFIGHTER OWNER
M 2 REVIEW MITIGATION REPORTS
ACTION REQUIRED ?
NO
YES
FIN
M 1 RUN & REVIEW MITIGATION REPORTS
M 3 TAKE REMEDIAL ACTION
A MONTH-END
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
RT TICKET
Q 3 ROLE MAINTENANCE AND / OR PROVISIONING
NEW OR AMENDED GRC-ARA MITIGATION CONTROL
GRC-ARA REPORT ANALYSIS
B QUARTER END
Q 1 RUN GRC-ARA RISK ANALYSIS
Q 8 PROCESS 4 FIREFIGHTER MAINTENANCE
RT TICKET
FF CHANGE REQUEST
Q 5 REVIEW ROLE & USER ASSIGNMENTS
STATUS EMAIL
ACTION REQUIRED ?
NO
YES
RT TICKET
Q 6 PROCESS 3 ROLE PROVISIONING
Q 7 REVIEW FFID ASSIGNMENTS
ACTION REQUIRED ?
NO
YES
FIN
Q 10 MONITOR STATUS
MEETING
STATUS EMAIL
Q 9 COORDINATE AND VERIFY COMPLETION
Step Q4
A 3 APPROVE RECERTIFICATION OF GRC MITIGATION ASSIGNMENTS
A 2 PROPOSE RECERTIFICATION OF GRC MITIGATION ASSIGNMENTS
A 1 PROVIDE A LIST OF MITIGATING CONTROL ASSIGNMENTS
C ANNUAL

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

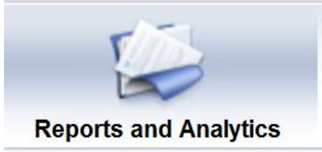
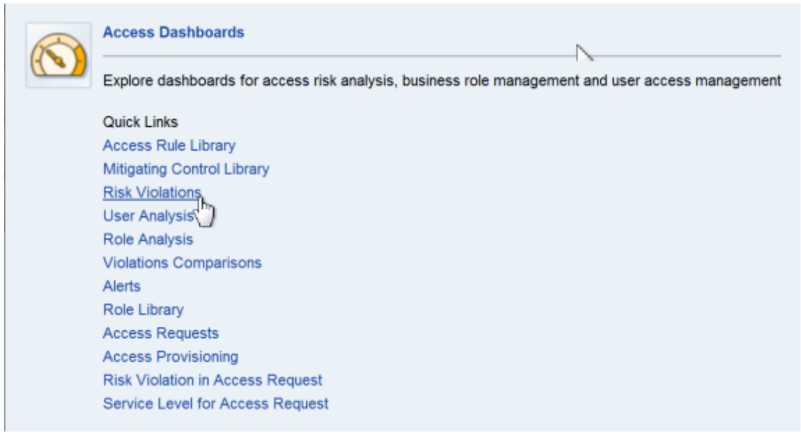
Risk count by risk level and process.

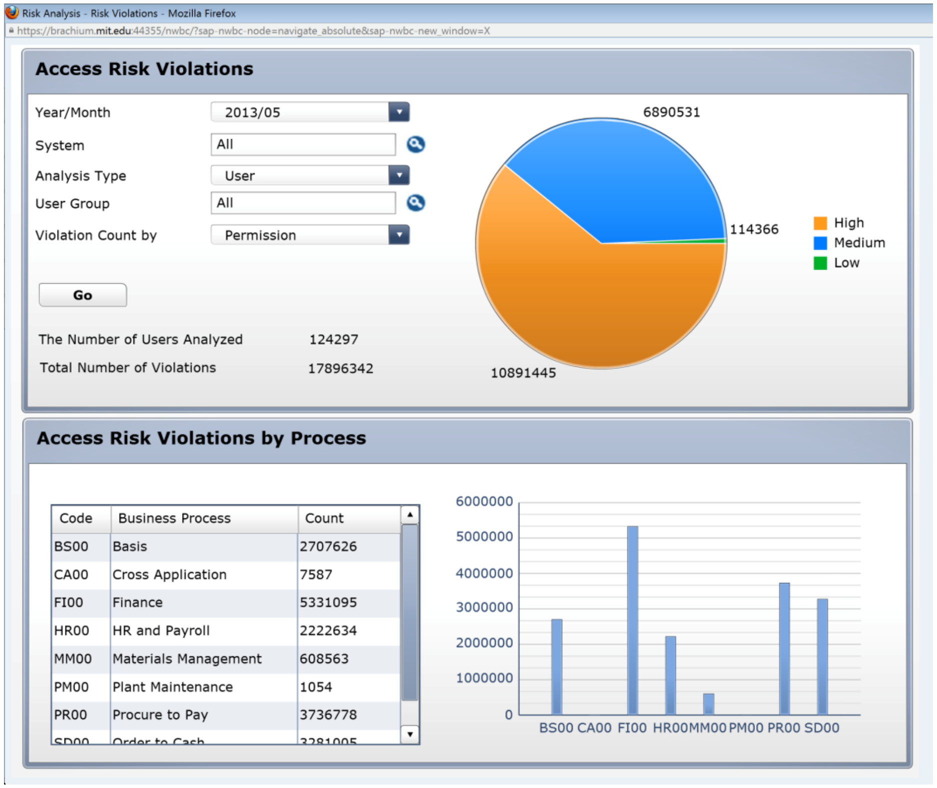
RELATED PROCESSES

- 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 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 Explore dashboards for access risk analysis, business role management and user access management

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

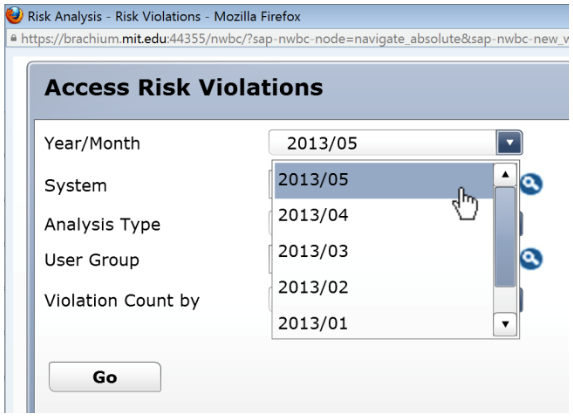
Go

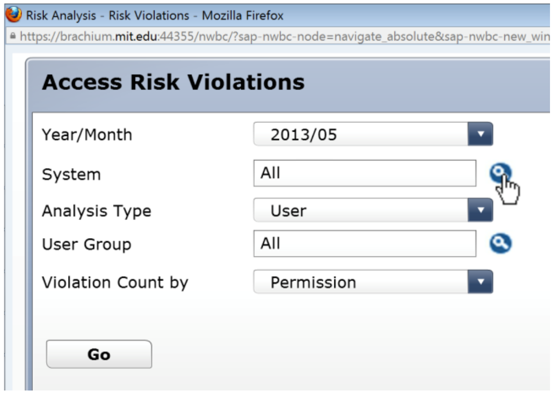
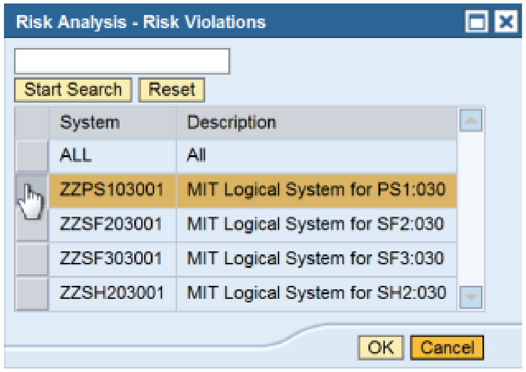
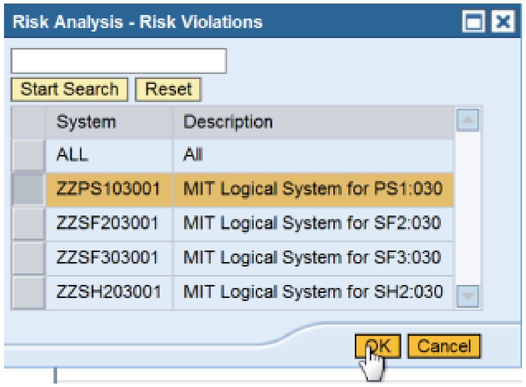
The Number of Users Analyzed: 124297

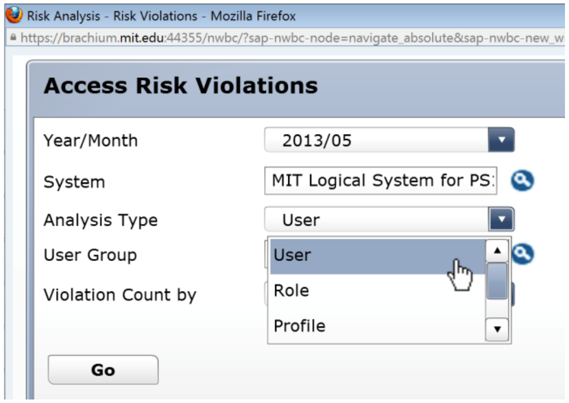
Total Number of Violations: 17896342

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 Go  Risk Analysis - Risk Violations 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 - Risk Violations 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

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

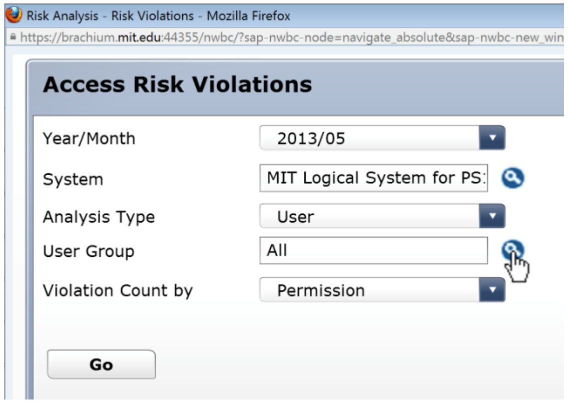
7

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'.

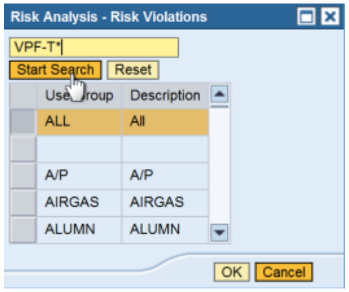


Risk Analysis - Risk Violations - Mozilla Firefox

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

Access Risk Violations

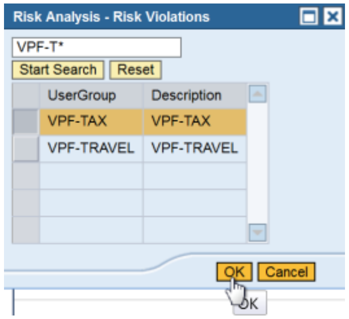
Year/Month	2013/05
System	MIT Logical System for PS:
Analysis Type	User
User Group	All
Violation Count by	Permission



Risk Analysis - Risk Violations

VPF-T*

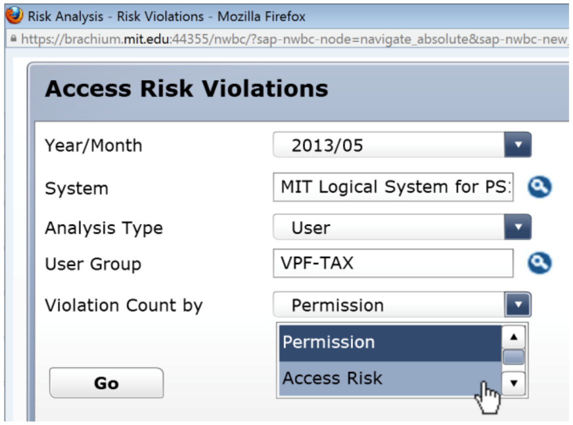
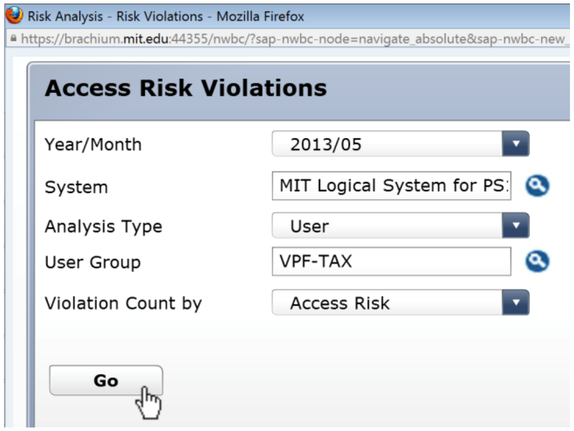
User Group	Description
ALL	All
A/P	A/P
AIRGAS	AIRGAS
ALUMN	ALUMN

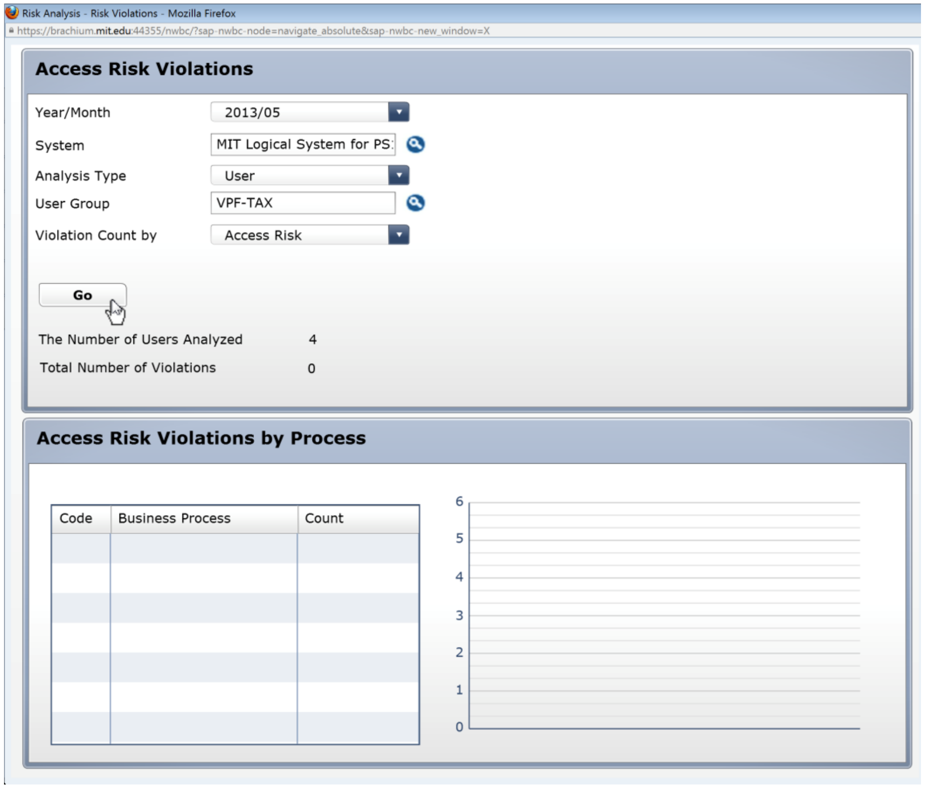


Risk Analysis - Risk Violations

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
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

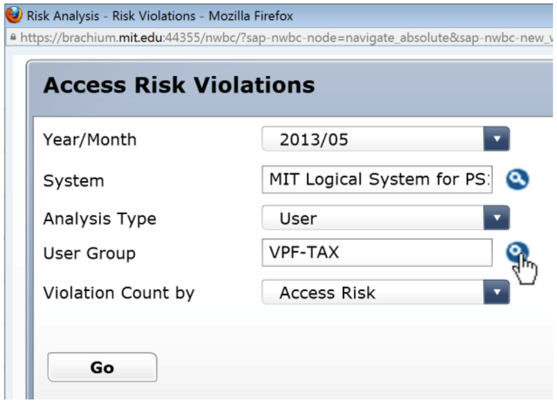
11

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’.

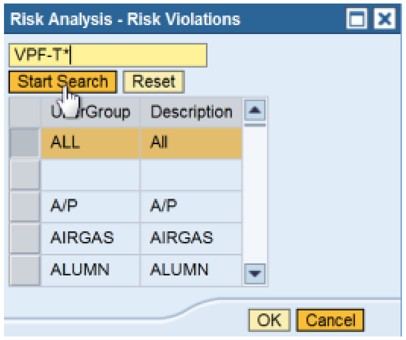


Risk Analysis - Risk Violations - Mozilla Firefox

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

Access Risk Violations

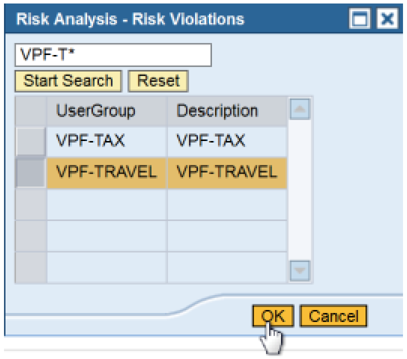
Year/Month	2013/05
System	MIT Logical System for PS:
Analysis Type	User
User Group	VPF-TAX
Violation Count by	Access Risk



Risk Analysis - Risk Violations

VPF-T*

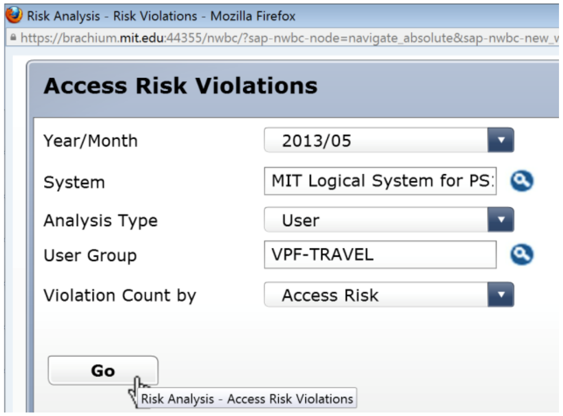
UserGroup	Description
ALL	All
A/P	A/P
AIRGAS	AIRGAS
ALUMN	ALUMN

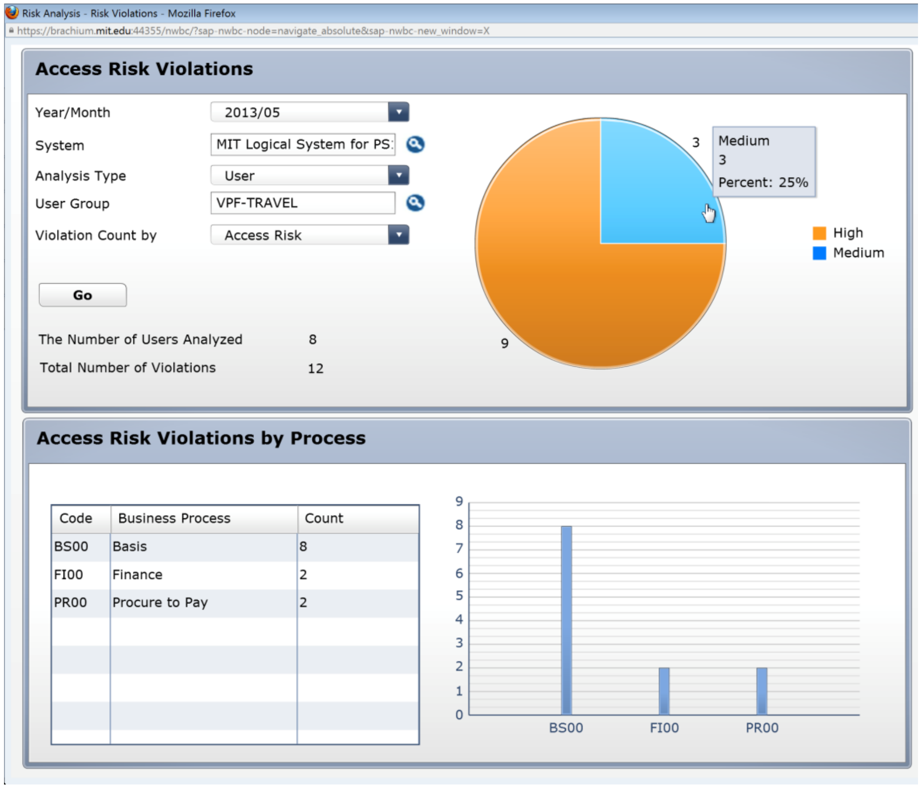


Risk Analysis - Risk Violations

VPF-T*

UserGroup	Description
VPF-TAX	VPF-TAX
VPF-TRAVEL	VPF-TRAVEL

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_w 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 Go Risk Analysis - Access Risk Violations

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

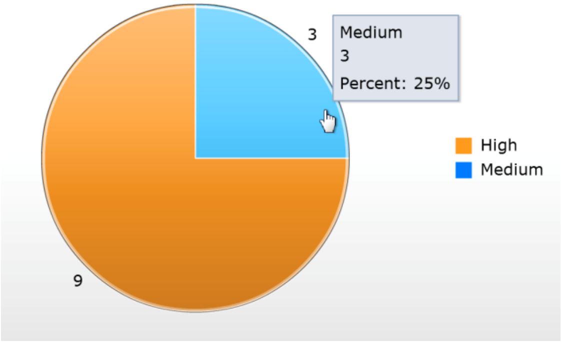
Year/Month	2013/05
System	MIT Logical System for PS
Analysis Type	User
User Group	VPF-TRAVEL
Violation Count by	Access Risk

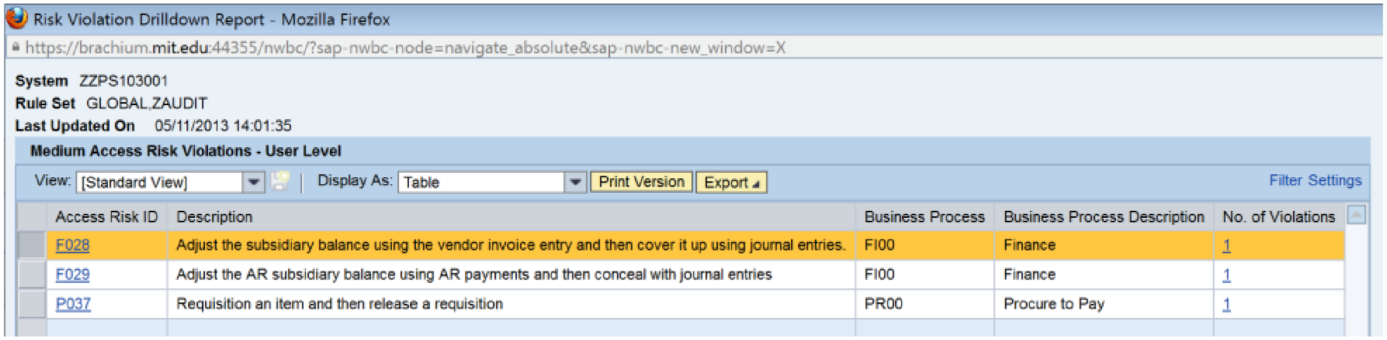
Go

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	

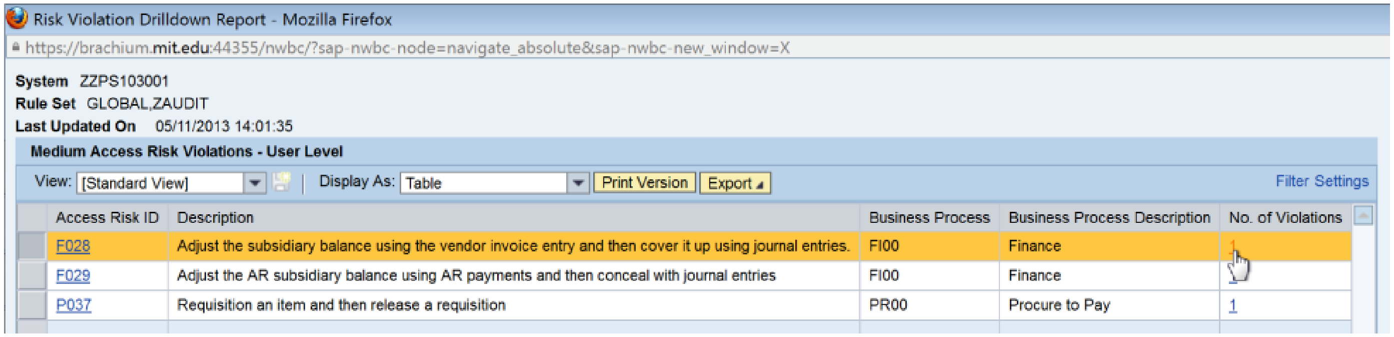
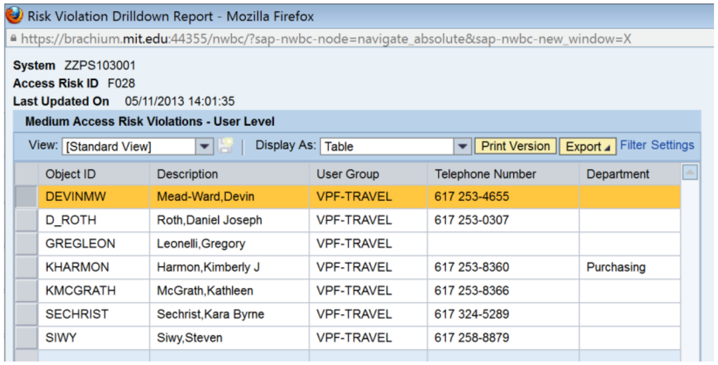
Risk Violation Drilldown Report - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

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

Medium Access Risk Violations - User Level

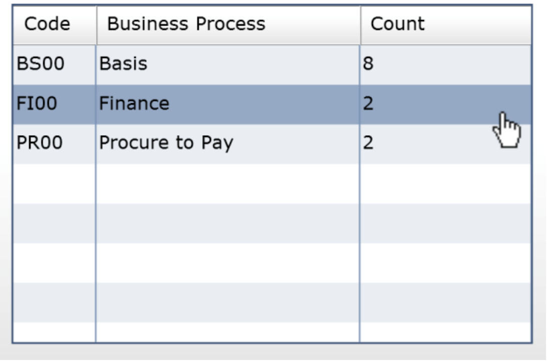
View: [Standard View] | Display As: Table | Print Version | Export | Filter Settings

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

<table>
<tr>
<td>14A-3</td>
<td>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.</td>
<td>

Risk Violation Drilldown Report - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
<b>System</b> ZZPS103001
<b>Rule Set</b> GLOBAL,ZAUDIT
<b>Last Updated On</b> 05/11/2013 14:01:35
<b>Medium Access Risk Violations - User Level</b>
View: [Standard View] Display As: Table Print Version Export Filter Settings
<table>
<tr><th>Access Risk ID</th><th>Description</th><th>Business Process</th><th>Business Process Description</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>FI00</td><td>Finance</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>FI00</td><td>Finance</td><td>1</td></tr>
<tr><td>P037</td><td>Requisition an item and then release a requisition</td><td>PR00</td><td>Procure to Pay</td><td>1</td></tr>
</table>

Risk Violation Drilldown Report - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X
<b>System</b> ZZPS103001
<b>Access Risk ID</b> F028
<b>Last Updated On</b> 05/11/2013 14:01:35
<b>Medium Access Risk Violations - User Level</b>
View: [Standard View] Display As: Table Print Version Export Filter Settings
<table>
<tr><th>Object ID</th><th>Description</th><th>User Group</th><th>Telephone Number</th><th>Department</th></tr>
<tr><td>DEVINMW</td><td>Mead-Ward,Devin</td><td>VPF-TRAVEL</td><td>617 253-4655</td><td></td></tr>
<tr><td>D_ROTH</td><td>Roth,Daniel Joseph</td><td>VPF-TRAVEL</td><td>617 253-0307</td><td></td></tr>
<tr><td>GREGLEON</td><td>Leonelli,Gregory</td><td>VPF-TRAVEL</td><td></td><td></td></tr>
<tr><td>KHARMON</td><td>Harmon,Kimberly J</td><td>VPF-TRAVEL</td><td>617 253-8360</td><td>Purchasing</td></tr>
<tr><td>KMCGRATH</td><td>McGrath,Kathleen</td><td>VPF-TRAVEL</td><td>617 253-8366</td><td></td></tr>
<tr><td>SECHRIST</td><td>Sechrist,Kara Byrne</td><td>VPF-TRAVEL</td><td>617 324-5289</td><td></td></tr>
<tr><td>SIWY</td><td>Siwy,Steven</td><td>VPF-TRAVEL</td><td>617 258-8879</td><td></td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td>14B-1</td>
<td>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.

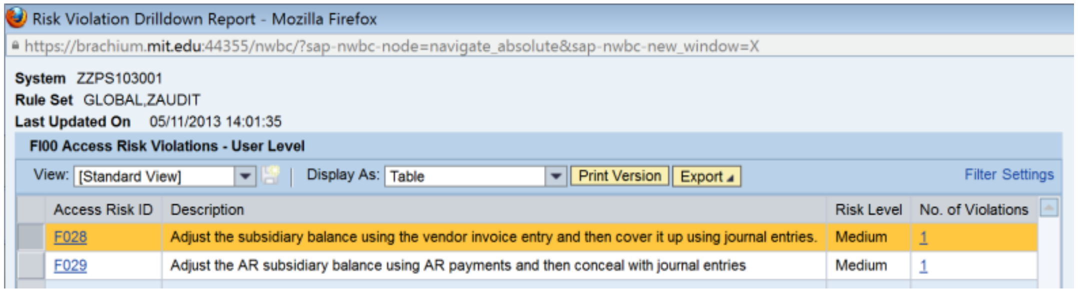
Click on the ‘Finance’ risk level row of the Table for more information about Finance Risks.</td>
<td>
<table>
<tr><th>Code</th><th>Business Process</th><th>Count</th></tr>
<tr><td>BS00</td><td>Basis</td><td>8</td></tr>
<tr><td>FI00</td><td>Finance</td><td>2</td></tr>
<tr><td>PR00</td><td>Procure to Pay</td><td>2</td></tr>
</table>
</td>
</tr>
</table>

<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

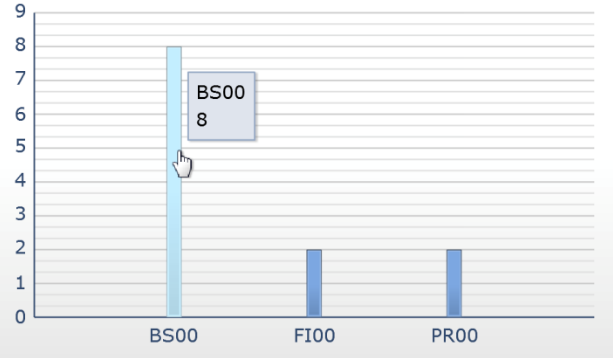
Description: Business description of the Access Risk

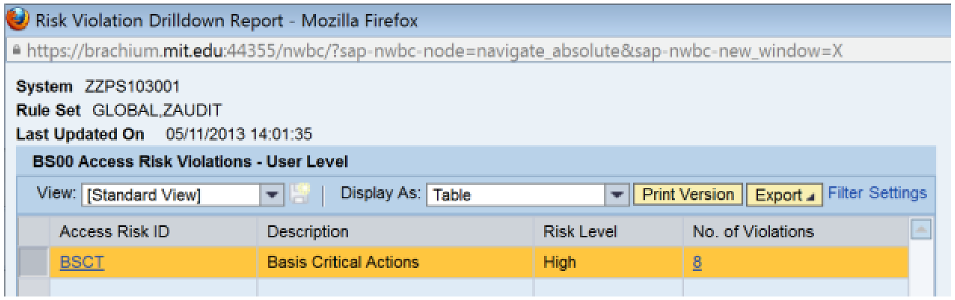
Risk Level: The risk level defined for each Access Risk in the standard rule set

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
<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 Print Version Export Filter Settings

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

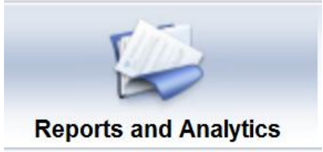
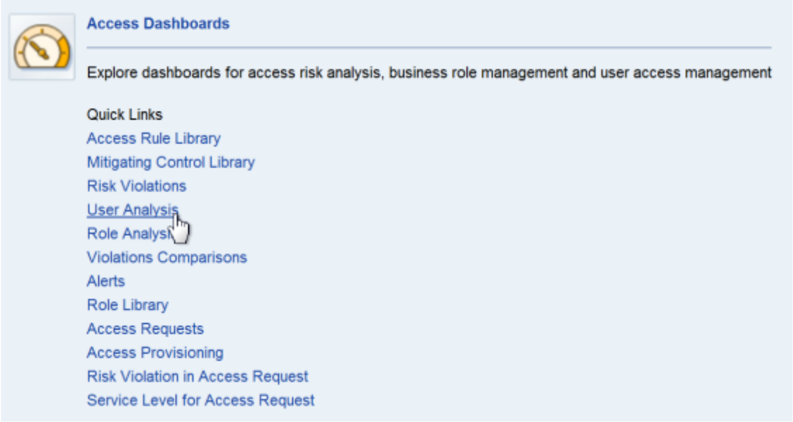
Risk count by risk type and user.

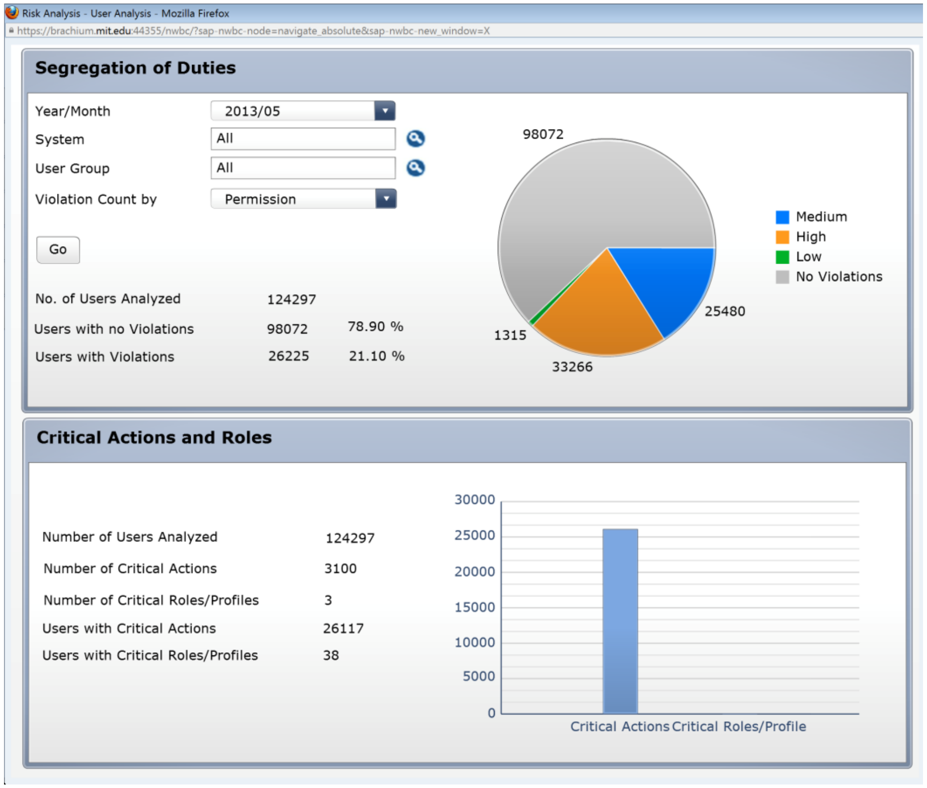
RELATED PROCESSES

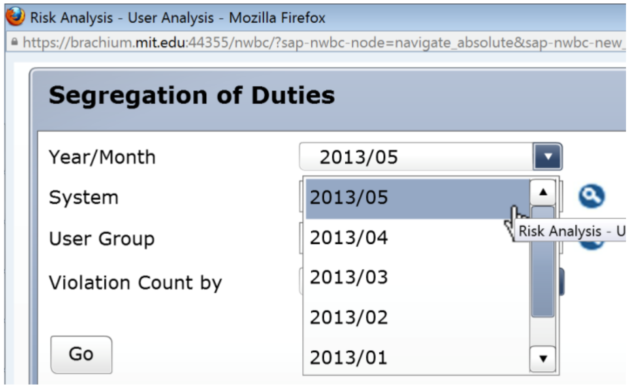
- Process 5: Periodic Compliance Reviews

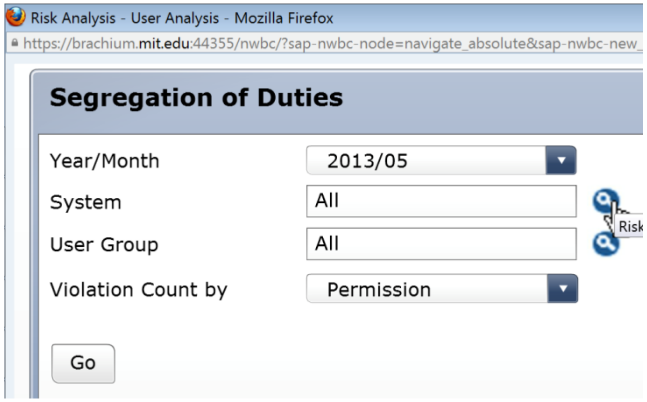
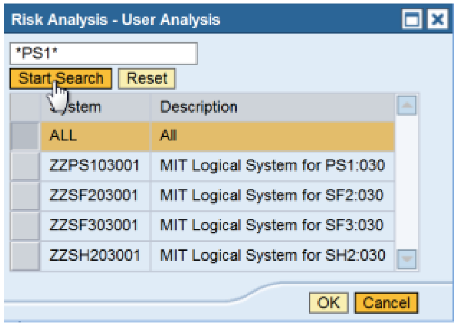
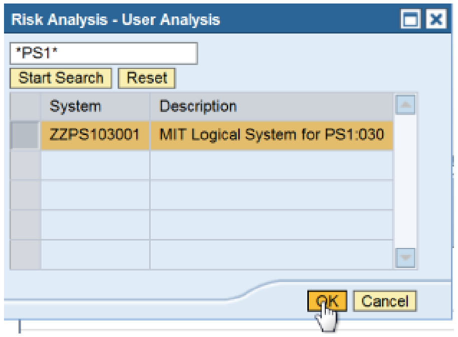
SPECIFIC SCENARIOS

- 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.	 Reports and Analytics
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 % 98072 25480 33266 1315 Medium High Low No Violations **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 30000 25000 20000 15000 10000 5000 0 Critical Actions Critical Roles/Profile

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

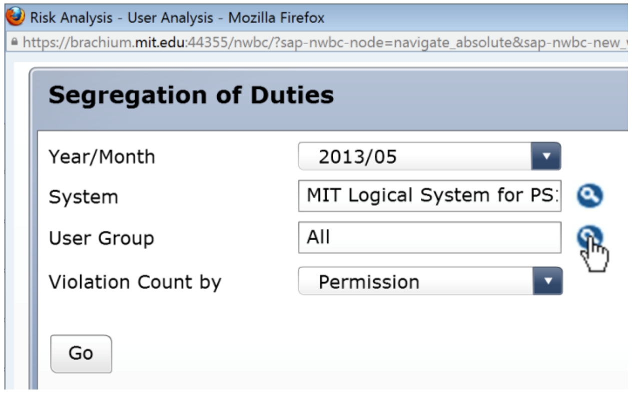
6

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'.



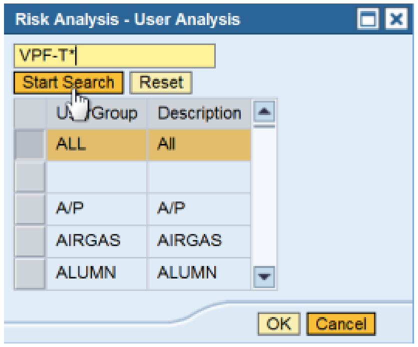
Risk Analysis - User Analysis - Mozilla Firefox

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



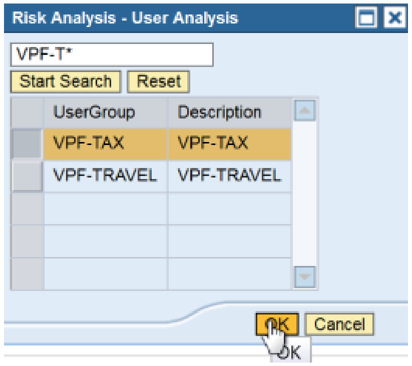
Risk Analysis - User Analysis

VPF-T*

Start Search | Reset

UserGroup	Description
ALL	All
A/P	A/P
AIRGAS	AIRGAS
ALUMN	ALUMN

OK | Cancel



Risk Analysis - User Analysis

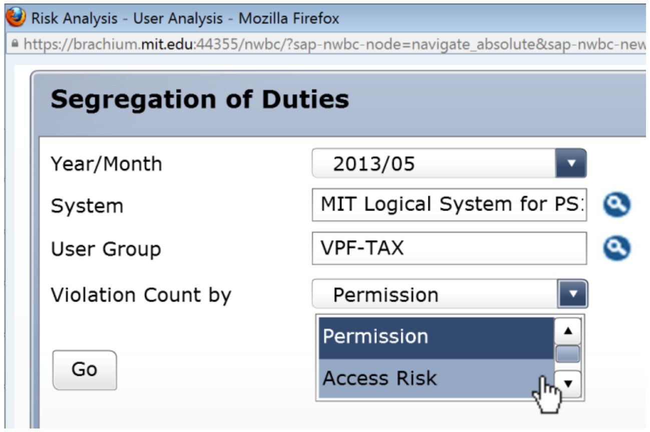
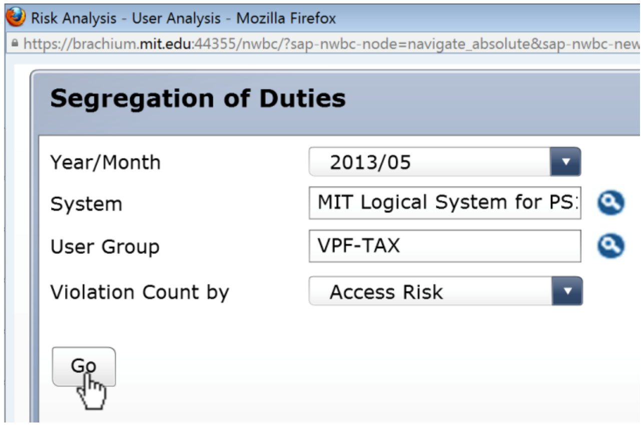
VPF-T*

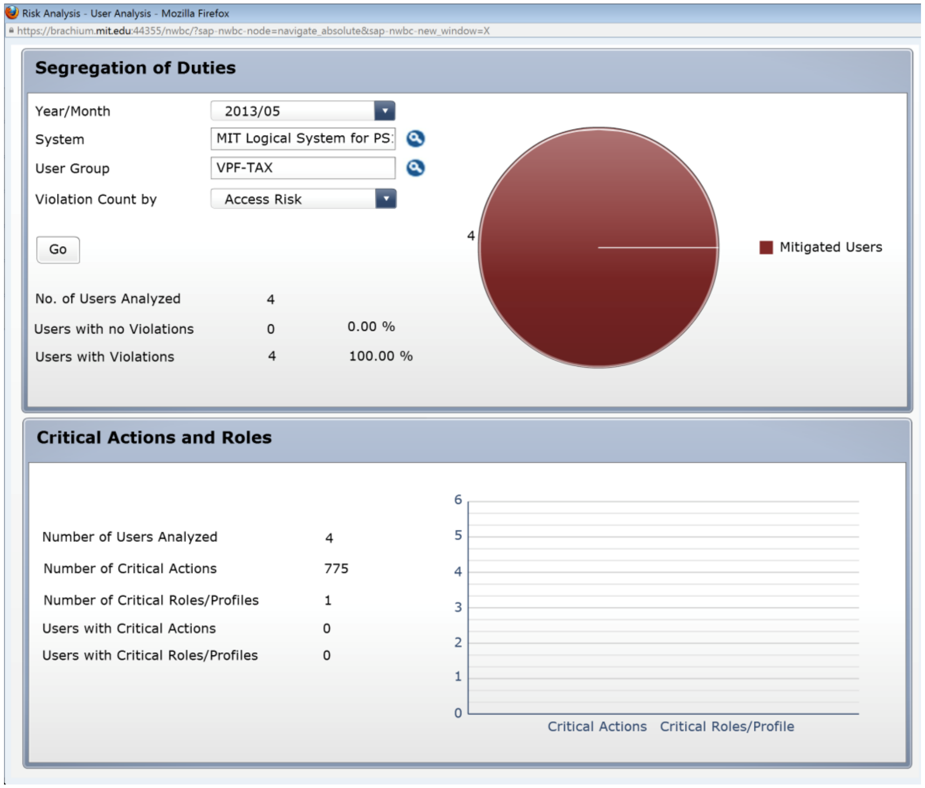
Start Search | Reset

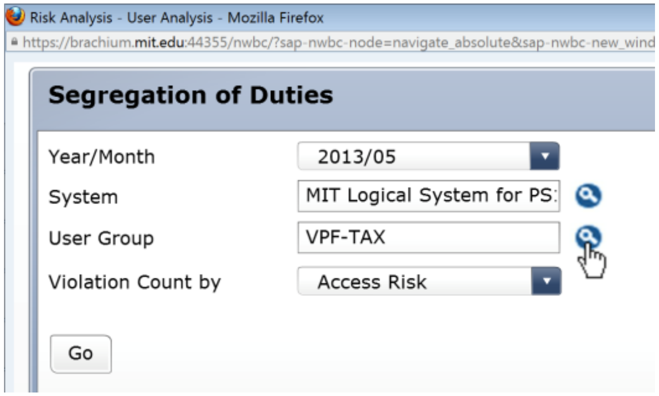
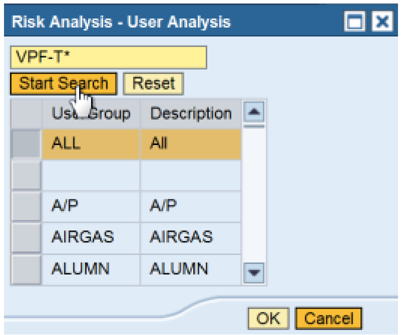
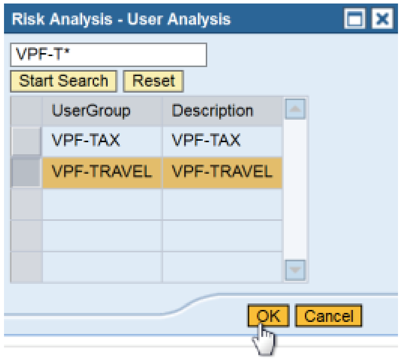
UserGroup	Description
VPF-TAX	VPF-TAX
VPF-TRAVEL	VPF-TRAVEL

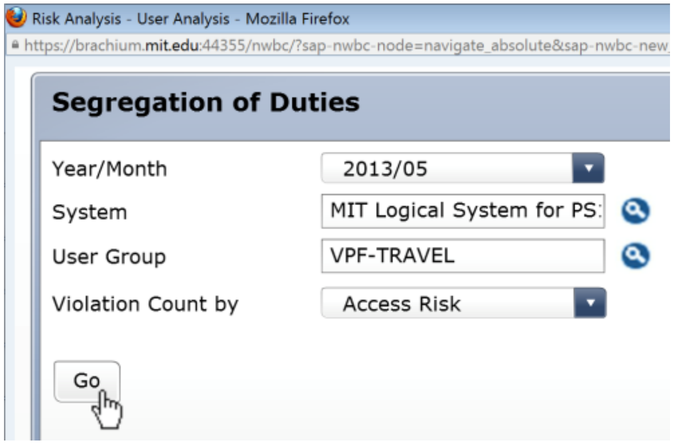
OK | Cancel

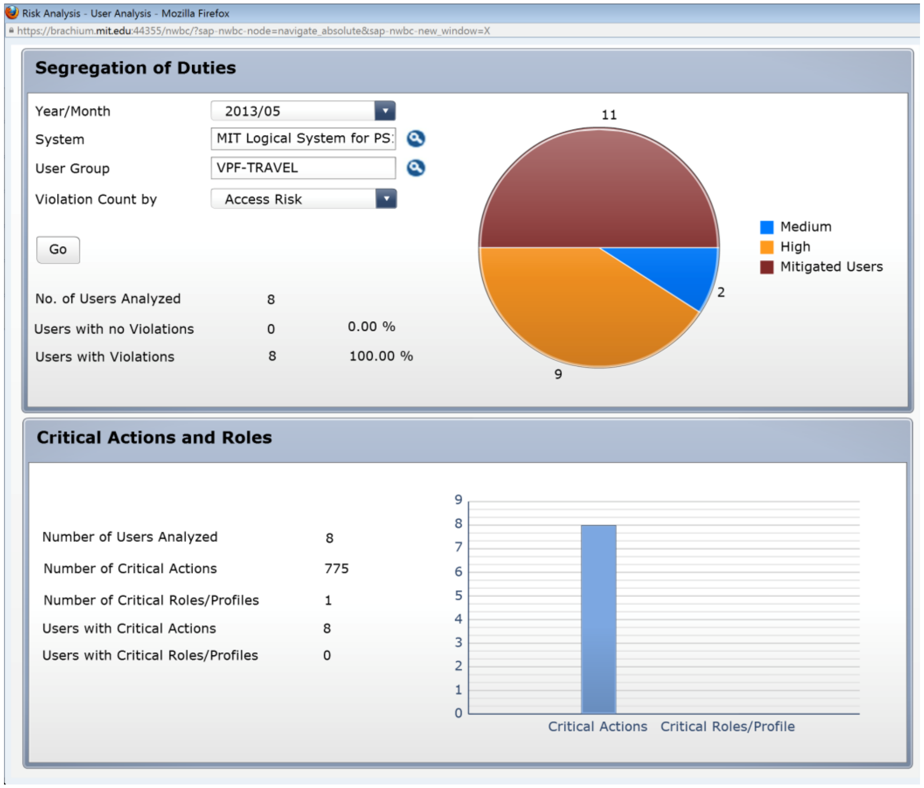
OK

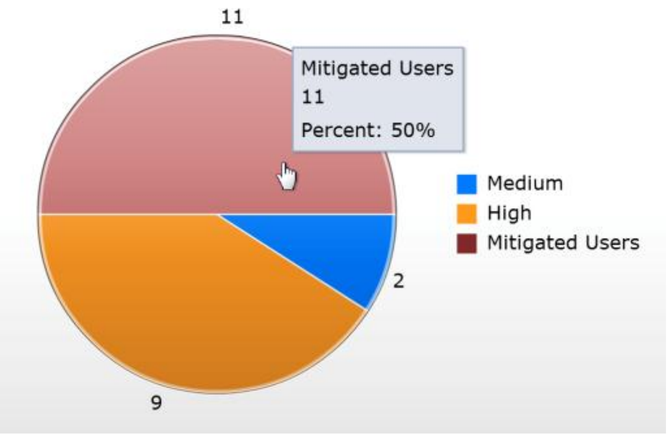
7	In the report filters section, click on the drop down for ‘Violation Count by’ to select the count methodology required for the report. In this case, ‘Access Risk’ is selected to count unique violations per User.	 Risk Analysis - User Analysis - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new 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

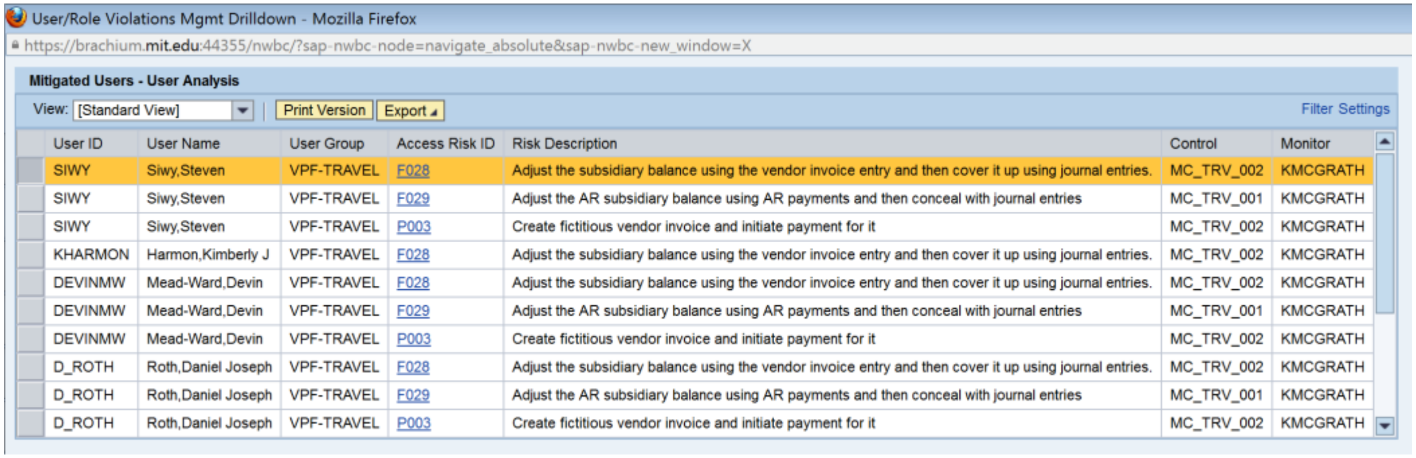
9	The report shows that there are a total of 4 Users in the 'VPF-TAX' user group. The report also shows that these 4 Users all have mitigated violations. In the 'Critical Actions and Roles' section, the report shows: • 4 Users were analyzed • The users were evaluated for violations against 775 Critical 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 6 5 4 3 2 1 0 Critical Actions Critical Roles/Profile

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

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	

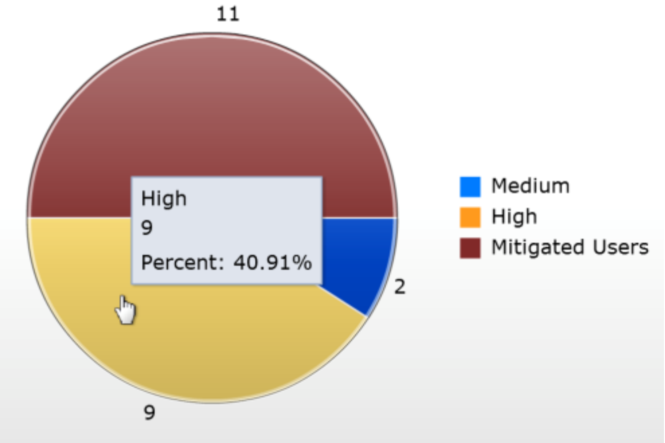
User/Role Violations Mgmt Drilldown - Mozilla Firefox

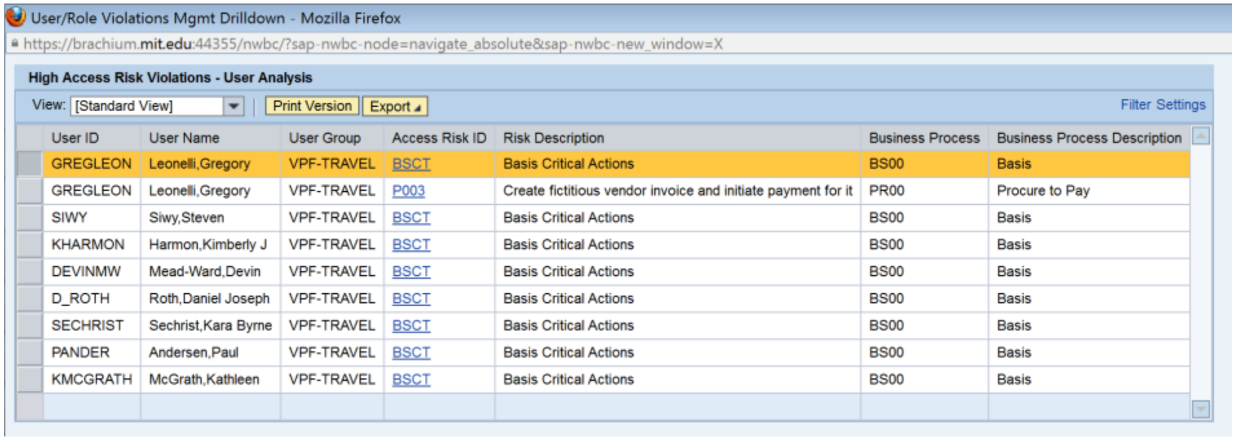
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Mitigated Users - User Analysis

View: [Standard View]

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	

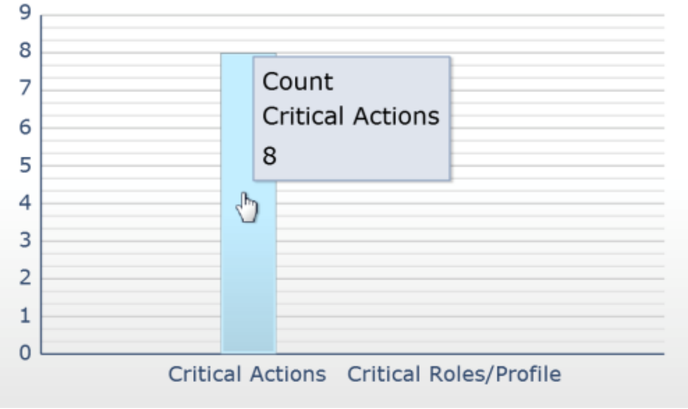
User/Role Violations Mgmt Drilldown - Mozilla Firefox

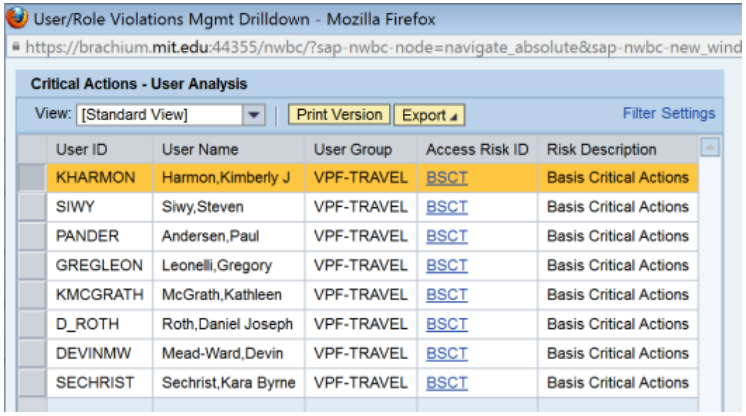
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

High Access Risk Violations - User Analysis

View: [Standard View]

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.	 9 8 7 6 5 4 3 2 1 0 Count Critical Actions 8 Critical Actions Critical Roles/Profile

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

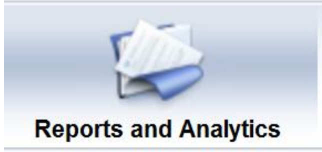
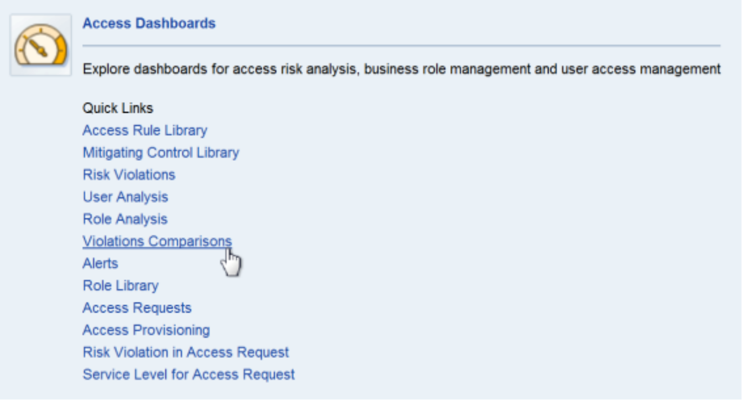
Violation count and comparison over time.

RELATED PROCESSES

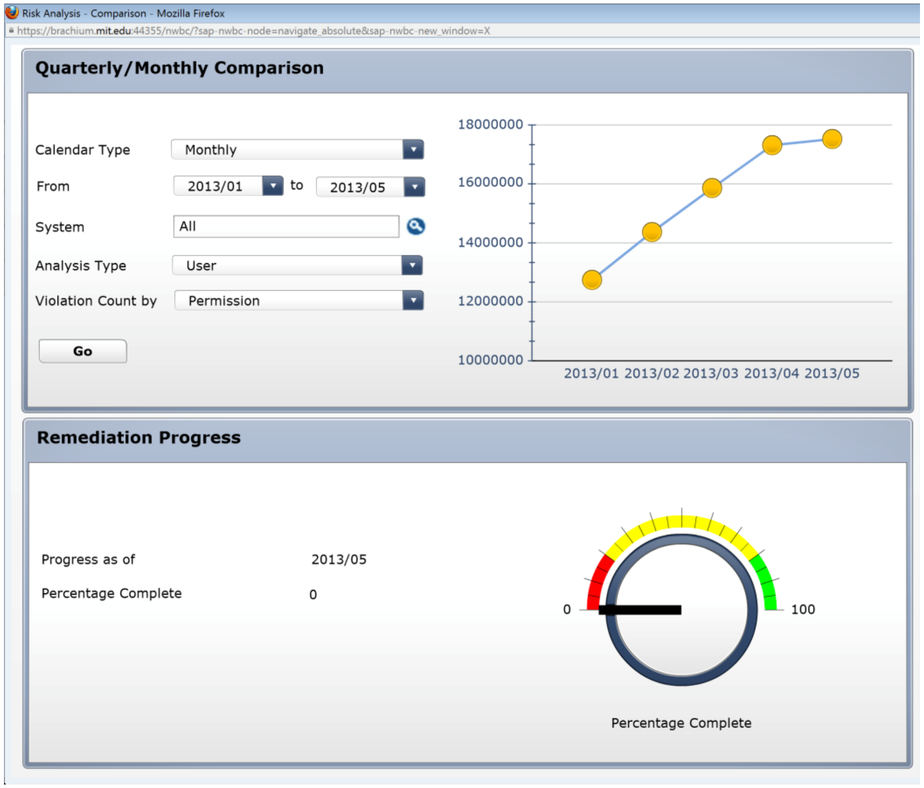
- Process 5: Periodic Compliance Reviews

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

<table>
<tr>
<td>3</td>
<td>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).

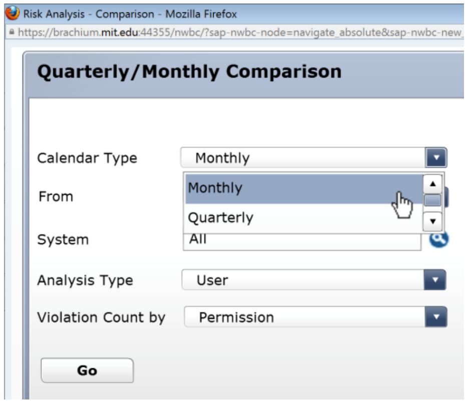
The report data must be appropriately filtered to provide information that can be of use to MIT.</td>
<td>
Risk Analysis - Comparison - Mozilla Firefox
https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

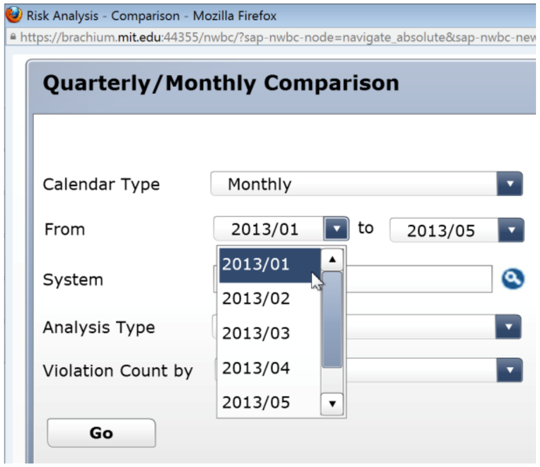
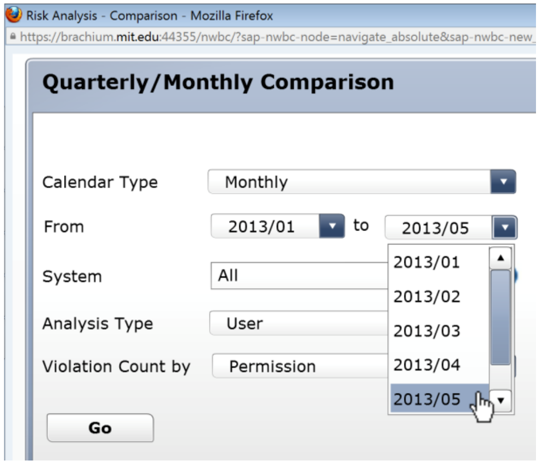
Quarterly/Monthly Comparison
Calendar Type: Monthly
From: 2013/01 to 2013/05
System: All
Analysis Type: User
Violation Count by: Permission
Go

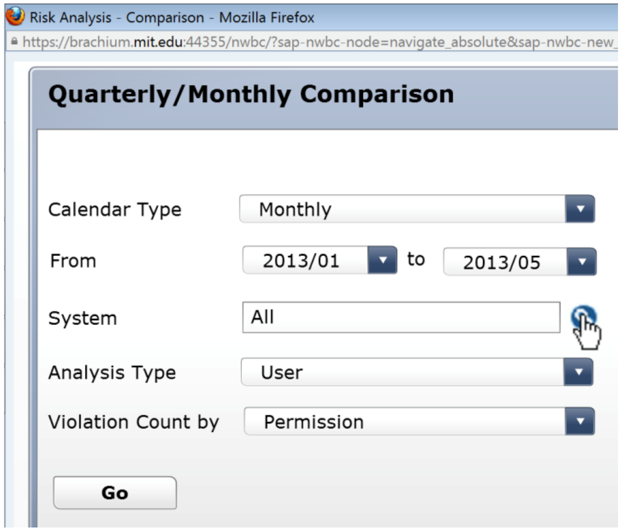
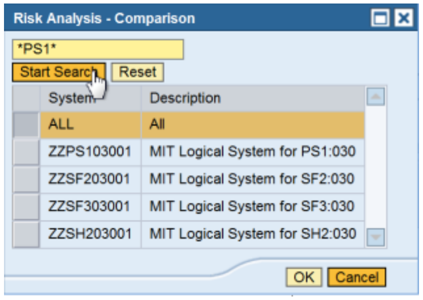
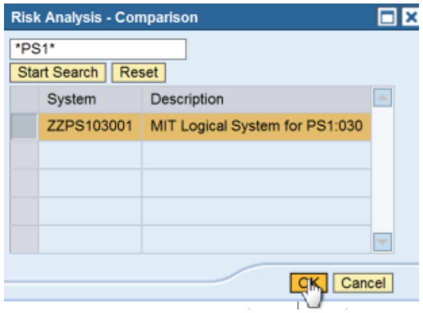
Remediation Progress
Progress as of: 2013/05
Percentage Complete: 0

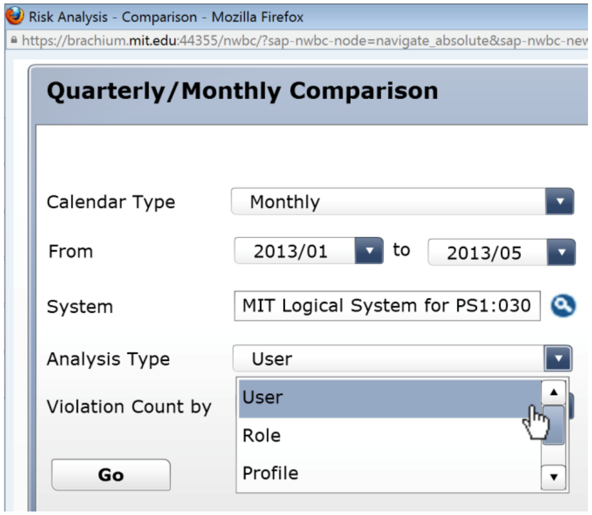
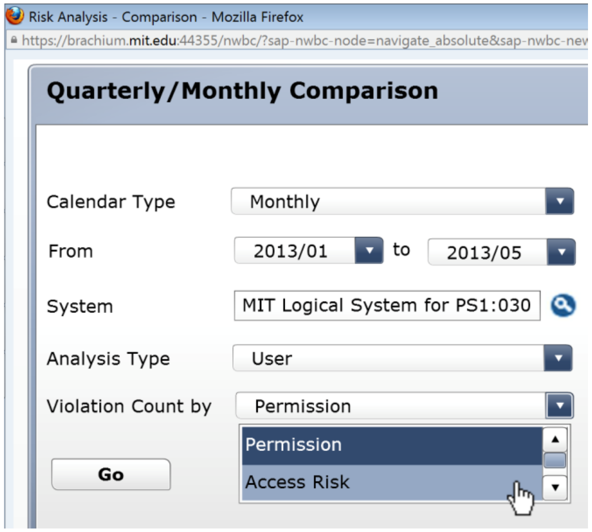
18000000
16000000
14000000
12000000
10000000
2013/01 2013/02 2013/03 2013/04 2013/05
0
100
Percentage Complete

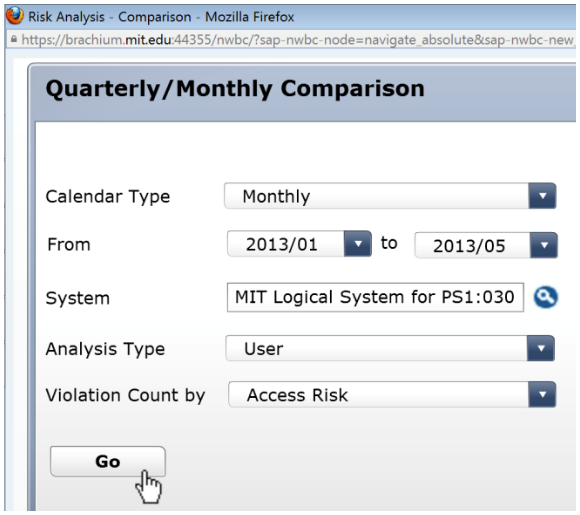
</td>
</tr>
</table>

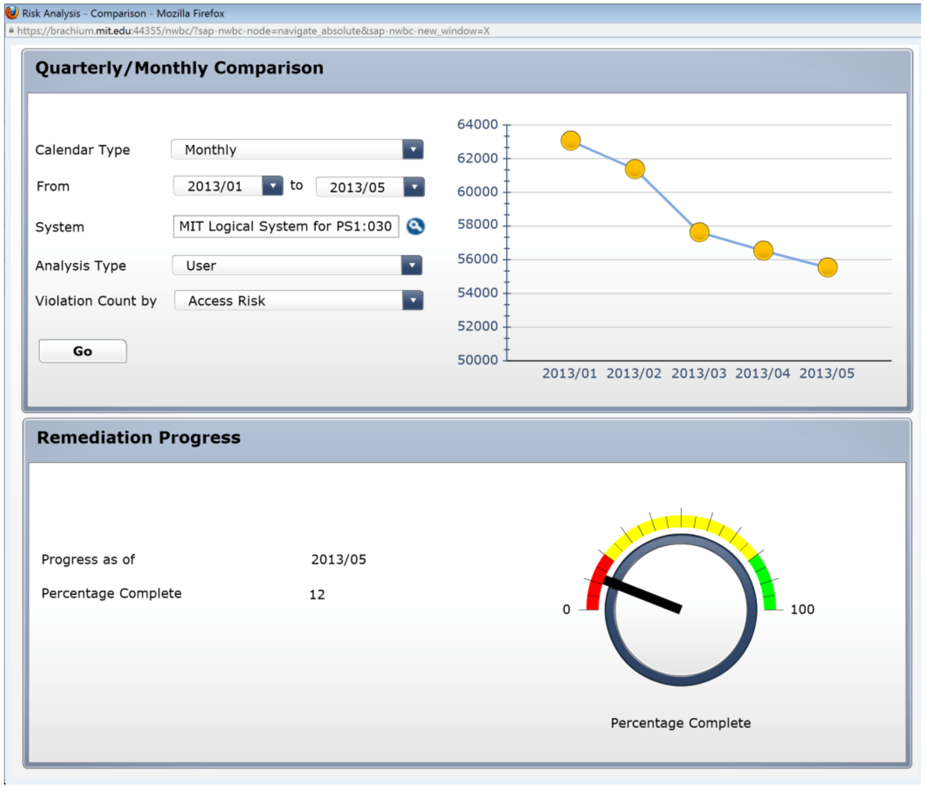
4	In the report filters section, click on the drop down for ‘Calendar Type’ to select the reporting periods by which data will be reported. In this case, ‘Monthly’ is selected.	 Risk Analysis - Comparison - Mozilla Firefox https://brachium.mit.edu:44355/nwbc/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_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

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  Risk Analysis - Comparison *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  Risk Analysis - Comparison *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

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 **Remediation Progress** Progress as of: 2013/05 Percentage Complete: 12

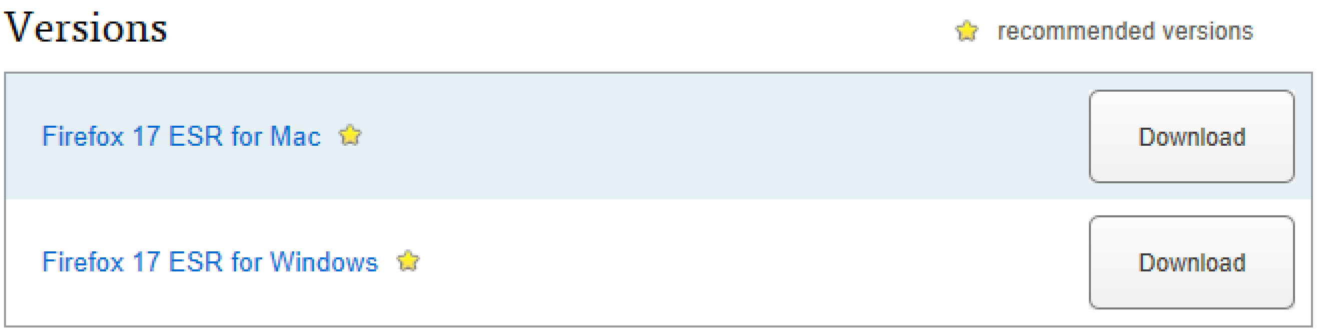
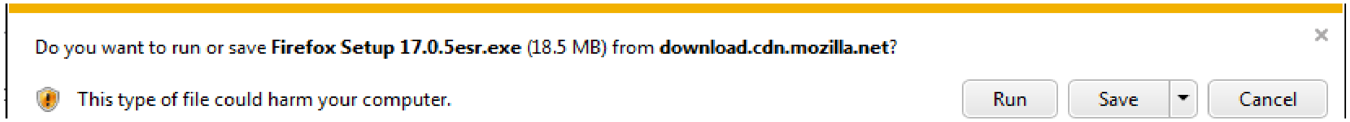
Reference Aids

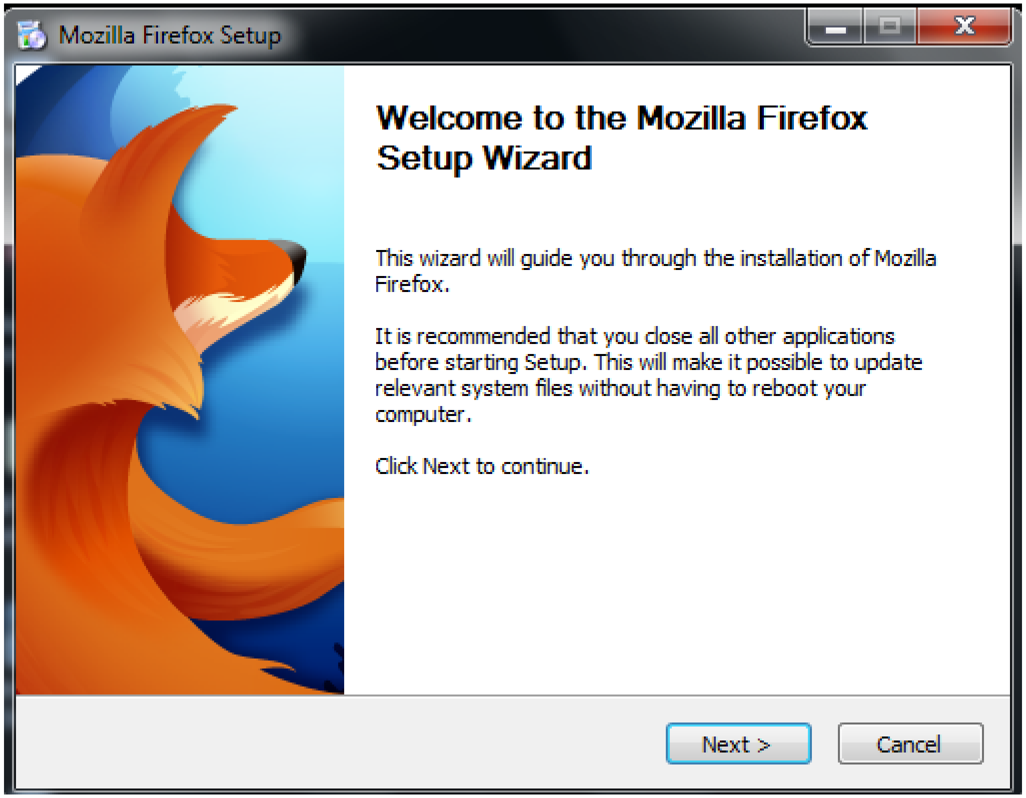
PURPOSE OF THIS DOCUMENT

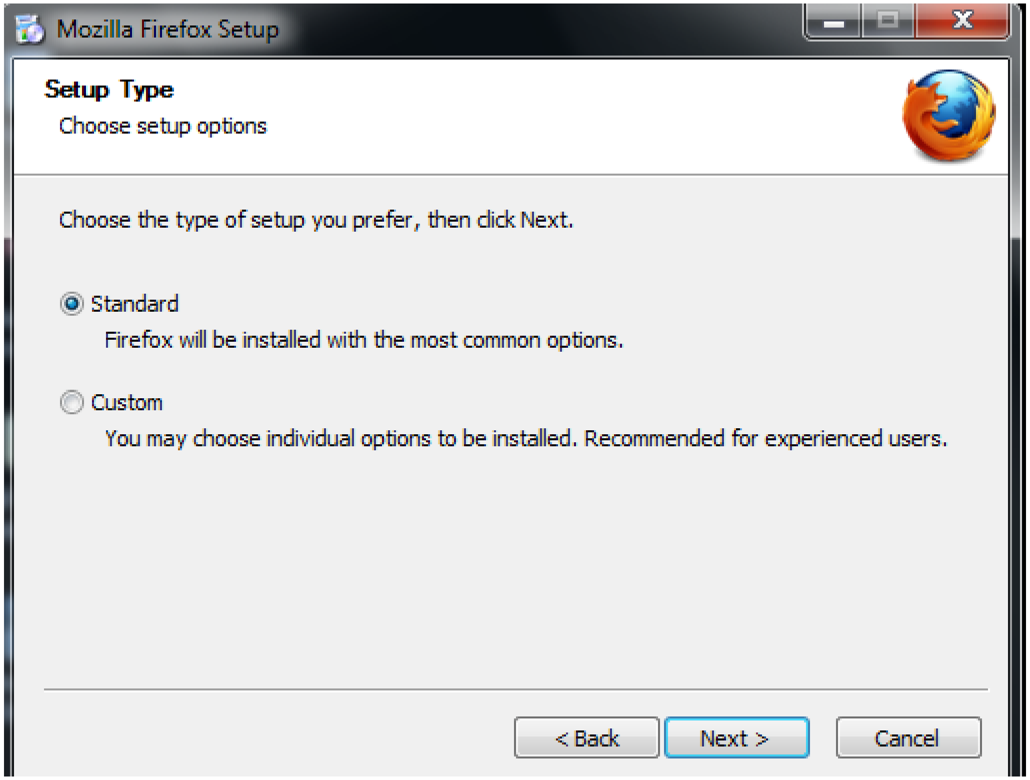
Procedures on repetitive tasks and actions related to GRC Reports are documented in reporting Reference Aids. Each Reference Aid provides details on execution for a particular repeated action.

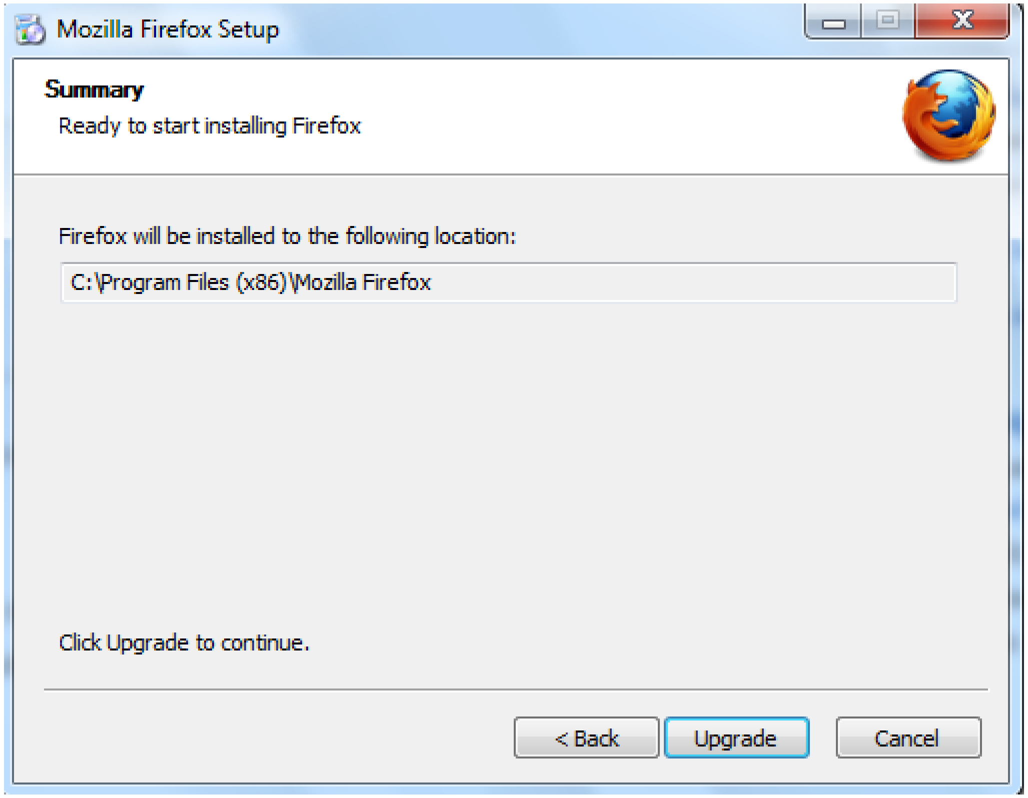
CONTENTS

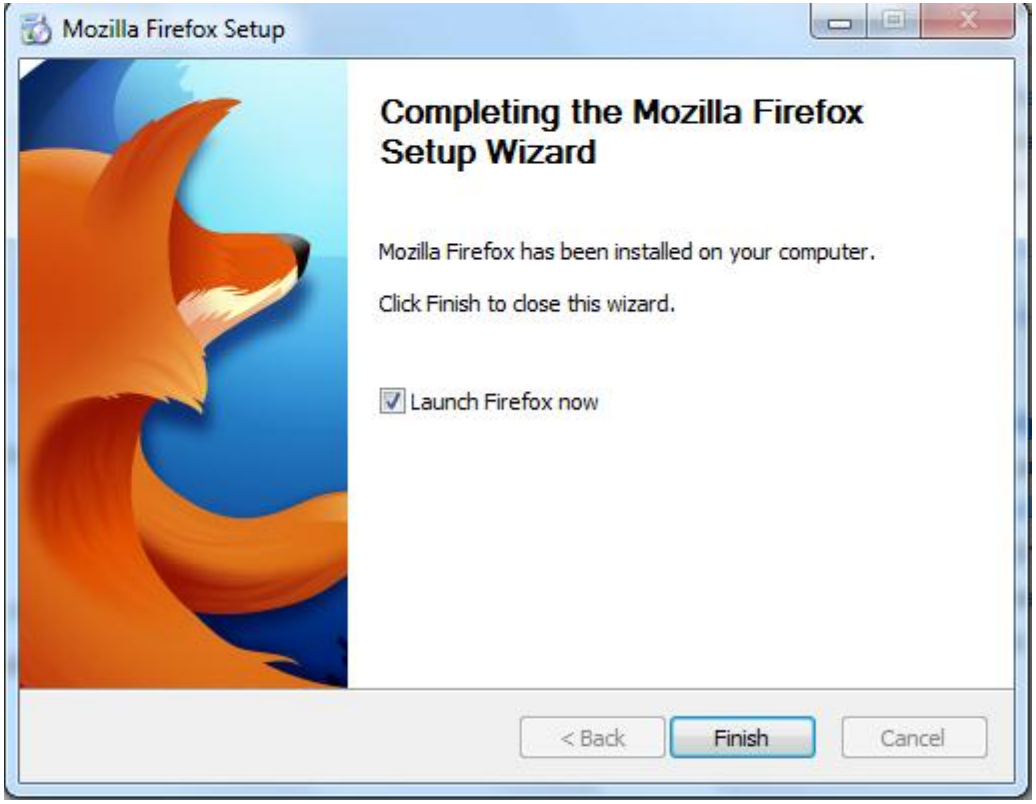
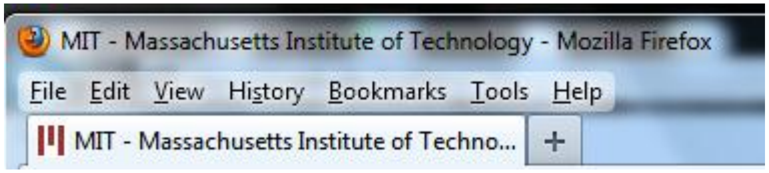
Reference R1 Access GRC Reporting

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.

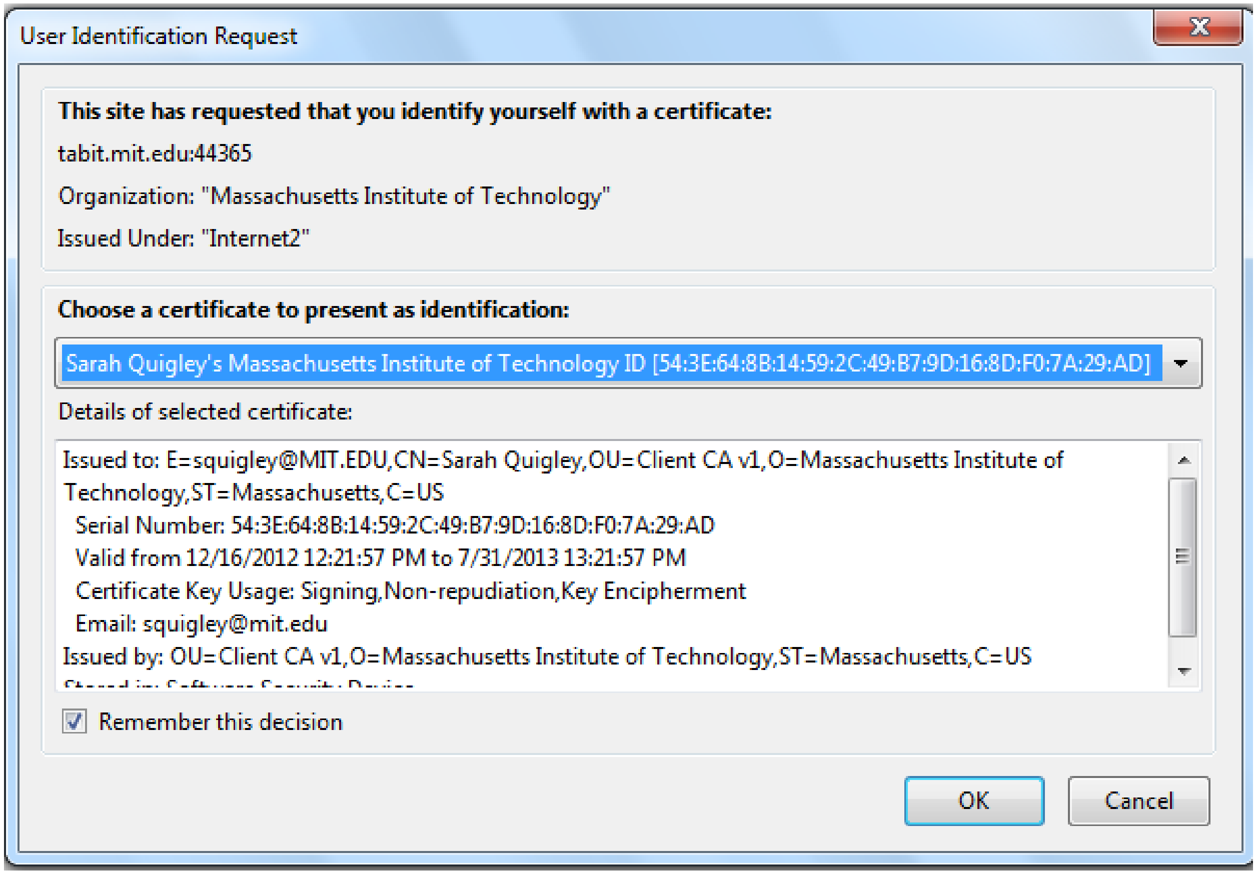
4	A *'Running Security Scan'* message will appear at the bottom of the screen. Then the Mozilla Firefox Setup Window will appear. Click *Next.*	 Welcome to the Mozilla Firefox Setup Wizard This wizard will guide you through the installation of Mozilla Firefox. It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer. Click Next to continue.

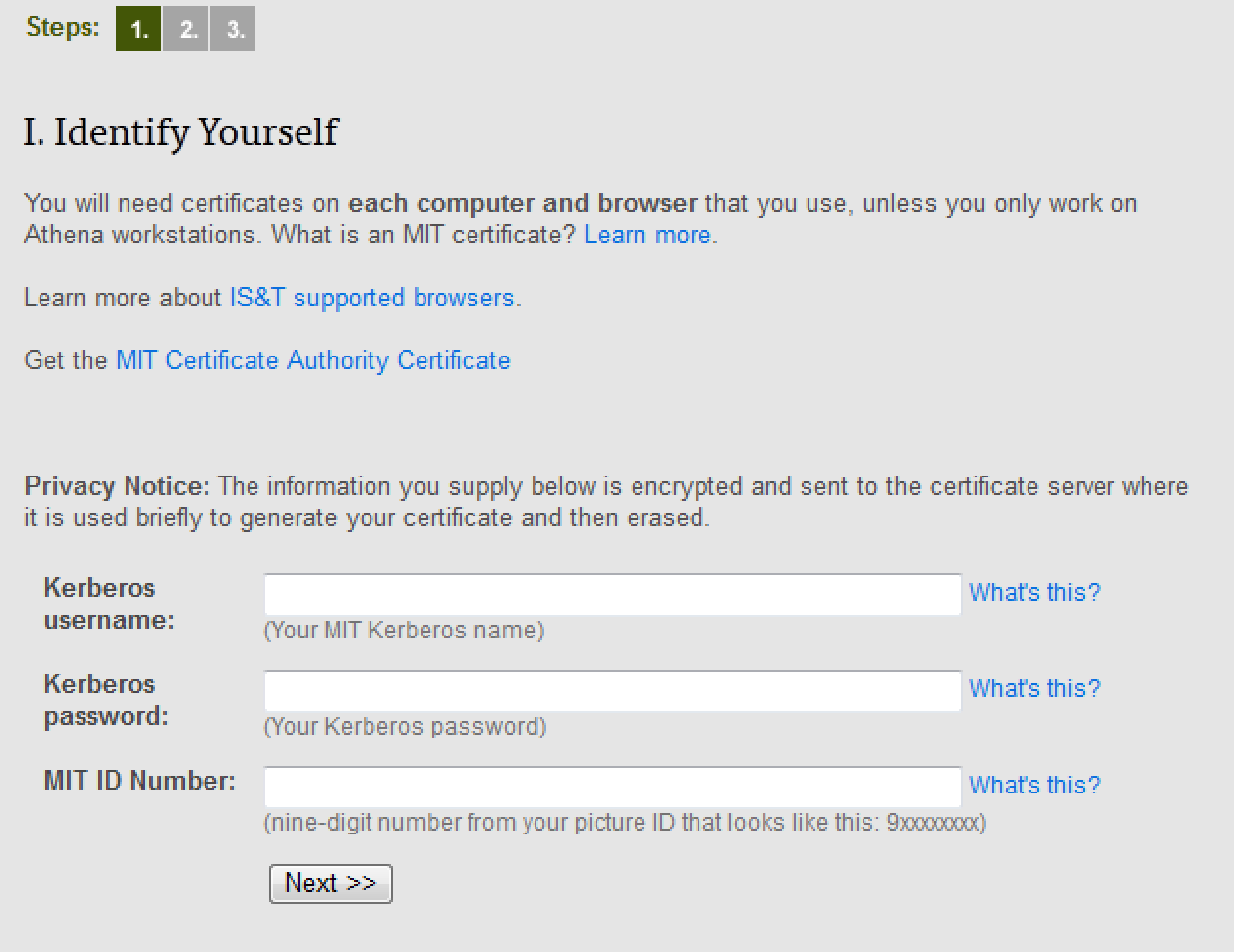
5	Leave the Setup Type option as *Standard*, which is the default. Click *Next.*	 Mozilla Firefox Setup **Setup Type** Choose setup options Choose the type of setup you prefer, then click Next. ● Standard Firefox will be installed with the most common options. ○ Custom You may choose individual options to be installed. Recommended for experienced users.

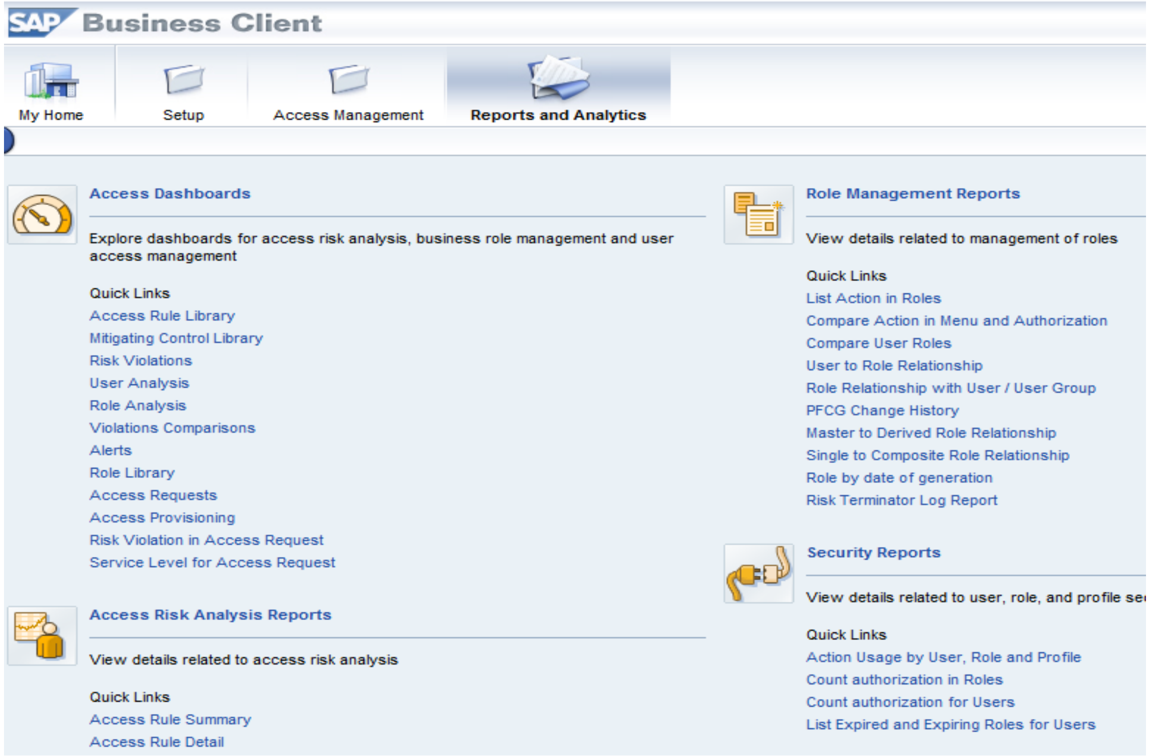
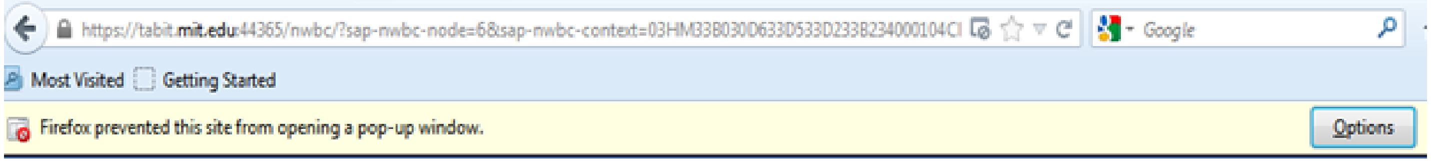
6	A screen with the installation location on the C drive will appear. Click the *Upgrade* or *Install* button.	 **Summary** Ready to start installing Firefox Firefox will be installed to the following location: C:\Program Files (x86)\Mozilla Firefox Click Upgrade to continue.

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.

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, **plus** 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, **plus** : ○ 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

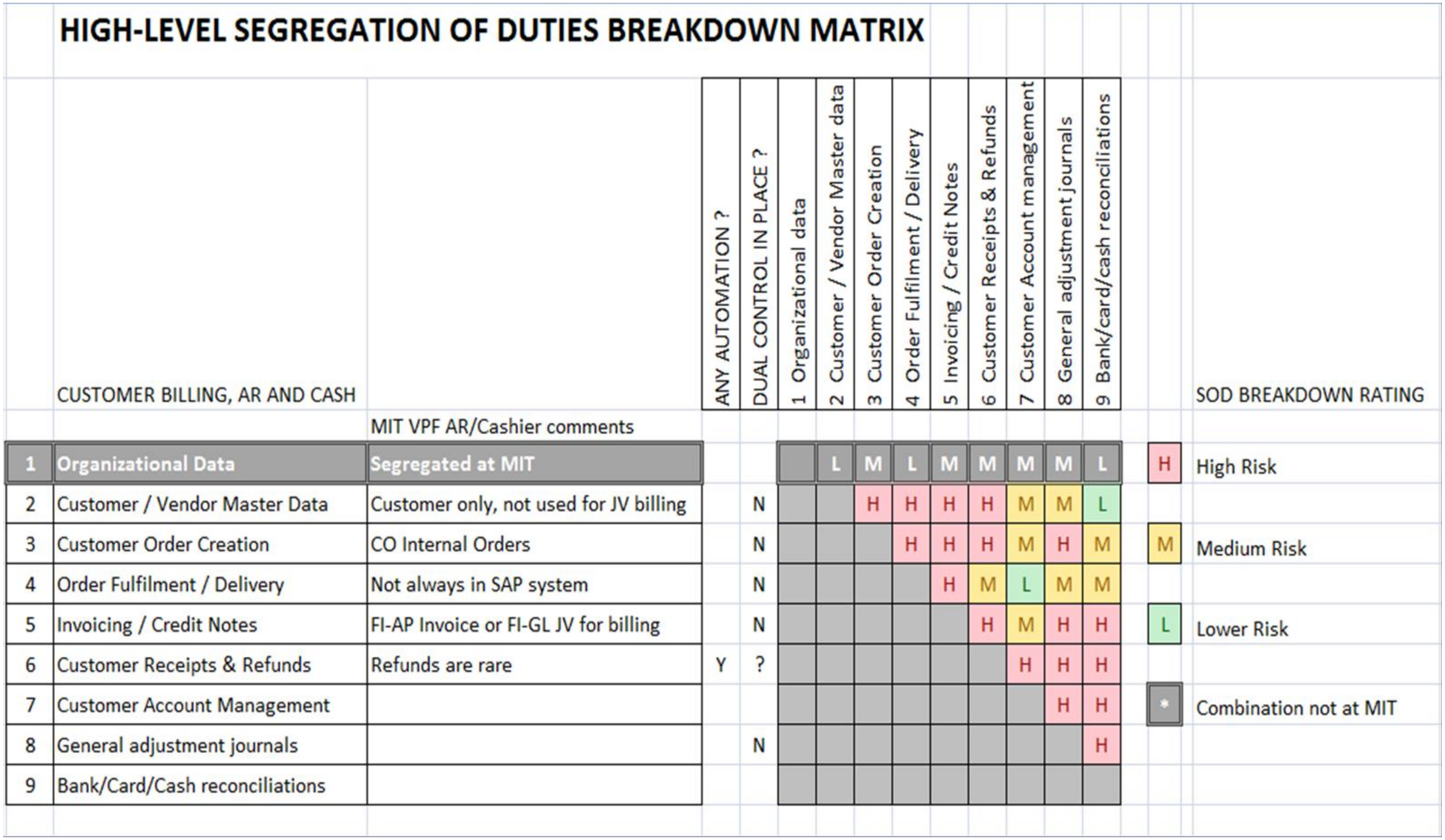
INFORMATION INPUT	ROLE DESIGN / REDESIGN STEPS
	in any other way. d. List of roles / composite roles assigned to the users e. Additional Authorizations used to restrict access by organizational, functional, or business classification. • This may include authorizations provisioned through the MIT custom 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– <u>Role Build and SOD Analysis (8)</u>**
	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	MIT VPF AR/Cashier comments	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
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 :* ➢

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 ?			
□	Coordinate with other SAP R/3 Production transports ? Date Required in Production > *MM / DD / YY*					**PROD** *DD/MM/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

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	➢

COMPOSITE ROLE CHANGES

COMPOSITE ROLE	NEW ROLE	ADD SINGLE	REMOVE SINGLE	SINGLE ROLE	GRC ARA ROLE	GRC ARA USERS
	□	□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			
		□	□			

SAP PS1 SECURITY CHANGE CHECKLIST

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**

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

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