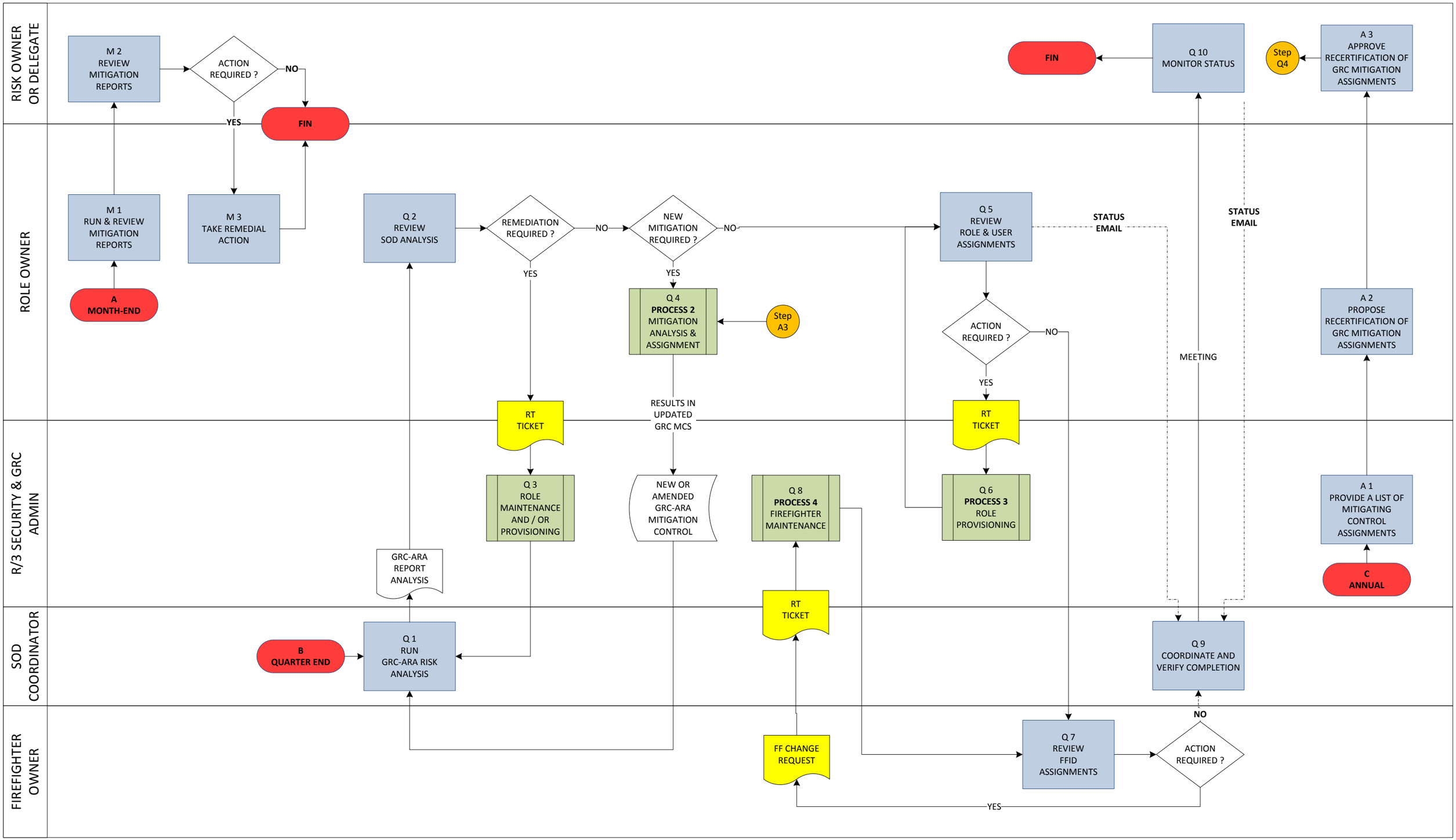
MIT SAP Security & GRC Process : 5. Periodic Compliance Reviews

Massachusetts Institute of Technology



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 o unusual but not an issue o a mistake which may or may not need correcting / reversing / reposting o 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