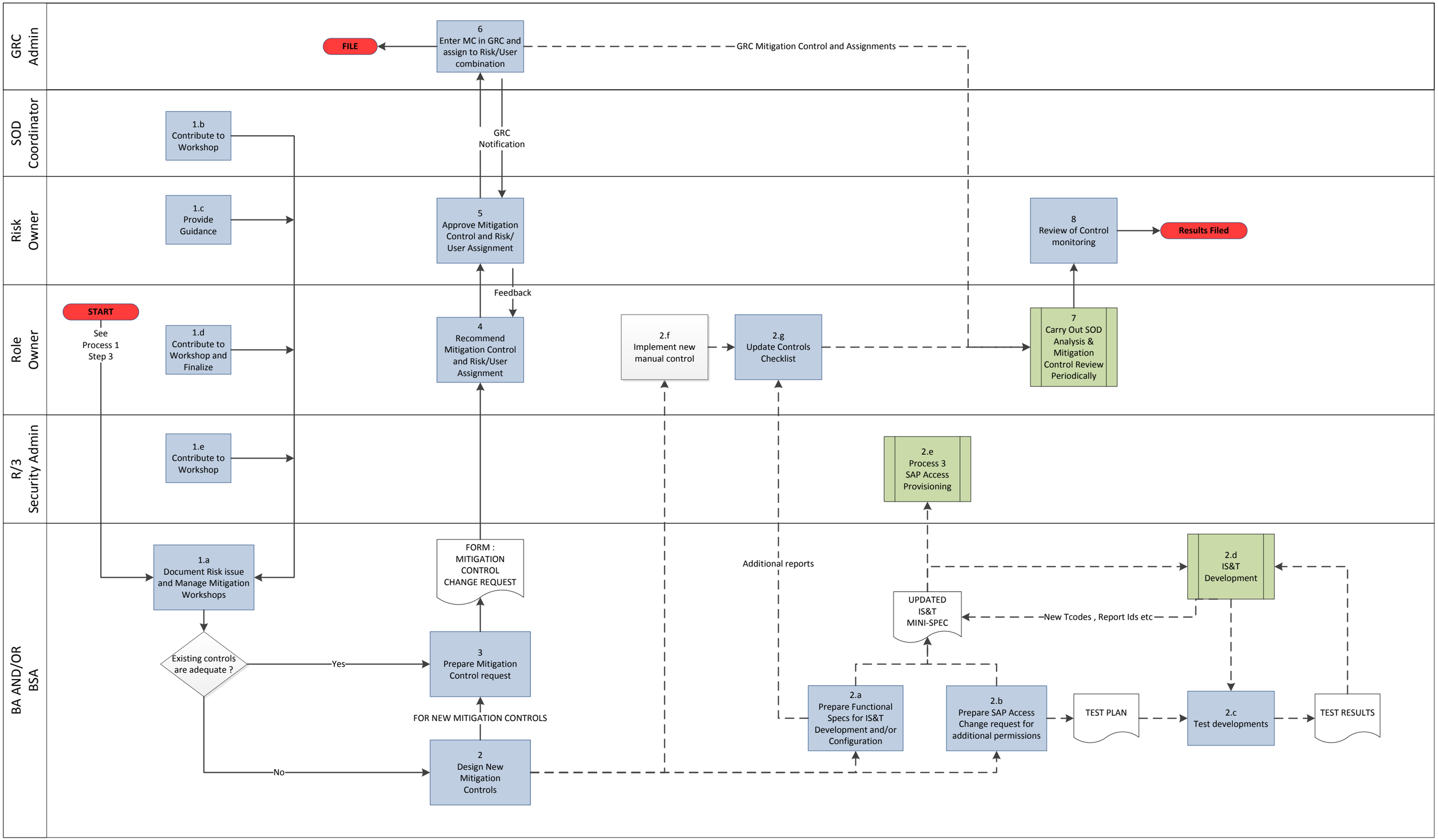
Massachusetts Institute of Technology

MIT SAP Security & GRC Process : 2. Mitigation Analysis



Process 2: Mitigation Analysis

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

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

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

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

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

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

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

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

Roles & Responsibilities for Process 2:

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

Reports available to support the Process 2:

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

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

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

Some important GRC concepts relevant to SOD Risk identification:

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

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

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

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

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

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

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

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

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

Process 2: Mitigation Analysis - Detailed Steps

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

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

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

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