GRC & Segregation of Duties (SOD)

GRC & Segregation of Duties (SOD)

The GRC and SOD Projects completed the first phase of implementing the SAP GRC tool, and cleaning up SOD violations for VPF and IS&T users, in June of 2013. As part of these two initiatives, new roles & responsibilities, processes, and reports were developed. Documentation and training materials on each of these can be found below.

On This Page

- 1.0 GRC Roles & Responsibilities
  - Risk Owners
  - Role Owners
  - Business Analysts (BAs)
  - Business Systems Analysts (BSAs)
  - All Users (During SOD Project)
- 2.0 SAP Security & Governance Processes
  - Process 1: New or Amended Roles
  - Process 2: Mitigation Analysis
  - Process 3: New Users and User Role Provisioning
  - Process 4: FireFighter Users and Roles
  - Process 5: Periodic Compliance
- 3.0 GRC Reporting
  - 3.1 Job Aids
  - 3.2 Reference Documents
- 4.0 Additional Documentation
  - 4.1 SOD Analysis Steps
  - 4.2 GRC Change Events
  - 4.3 Proposed GRC Forms
  - 4.4 GRC & SOD Terminology
- 5.0 Training Materials
  - 5.1 Training Presentations
  - 5.2 Training Packages

1.0 GRC Roles & Responsibilities

For those users with new responsibilities relating to GRC, below are quick reference guides for each role that provide an overview of processes in which they are now involved, and tasks for which they are now responsible. Also included, for future reference, is an overview of all responsibilities as they were defined during the project.

Risk Owners

- Roles and Responsibilities Risk Owner.docx

Role Owners

- Roles and Responsibilities Role Owner.docx

Business Analysts (BAs)

- Roles and Responsibilities BAs.docx

Business Systems Analysts (BSAs)

- Roles and Responsibilities BSAs.docx

All Users (During SOD Project)

- Roles and Responsibilities All.docx

2.0 SAP Security & Governance Processes

Detailed process documentation was created for five new GRC-related processes. This documentation includes both flowcharts and detailed descriptions of each step, including the person responsible and details of the task to be completed.

Process 1: New or Amended Roles

- Process 1 New or Amended Roles.pdf
- Process 1 New or Amended Roles.docx
- GRC Process 1 - New or Amended Roles.vsd

Process 2: Mitigation Analysis

- Process 2 Mitigation Analysis.pdf
- Process 2 Mitigation Analysis.docx
- GRC Process 2 - Mitigation Analysis.vsd

Process 3: New Users and User Role Provisioning

- Process 3 New Users and User Role Provisioning.pdf
- Process 3 New Users and User Role Provisioning.docx
- GRC Process 3 - New users and User Role Provisioning.vsd

Process 4: FireFighter Users and Roles

- Process 4 FireFighter Users and Roles.pdf
- Process 4 FireFighter Users and Roles.docx
- GRC Process 4 - FireFighter Users and Roles.vsd

Process 5: Periodic Compliance

- Process 5 Periodic Compliance Reviews.pdf
- Process 5 Periodic Compliance Reviews.docx
- GRC Process 5 - Periodic Compliance Reviews.vsd

3.0 GRC Reporting

A total of 15 new GRC reports, along with 2 SUIM (ECC) reports, were deployed to users in IS&T and VPF. Below are the detailed job aids created for each of these new reports, along with general reference documents for repeated actions related to GRC reporting. A quick reference guide for reporting is also available here: GRC Reports Quick Reference Guide.docx.

3.1 Job Aids

- 01 Risk Violations
- 02 User Analysis
- 03 Violations Comparisons
- 04 Access Rule Library
- 05 SUIM Roles by Role Name
- 06 User to Role Relationship
- 06 User to Role Relationship – Role Owners
- 07 Role Relationship with User - User Group
- 07 Role Relationship with User - User Group – Role Owners
- 08 SUIM Users by User ID
- 09 Count Authorizations for Users
- 10 Action Usage by User, Role and Profile
- 11 Mitigation Control Report
- 12 User Level
- 13 User Level Simulation
- 14 Role Level
- 15 Role Level Simulation
- 16 Profile Level
- 17 Profile Level Simulation

3.2 Reference Documents

- R1 Access GRC Reporting.docx
- R2 Add or Remove Search Lines to a Report.docx
- R3 Search for Input Values.docx
- R4 Save a Variant.docx
- R5 Execute a Background Job.docx
- R6 Filter a Report.docx
- R7 Change Your Report View.docx
- R8 Export Data from GRC.docx
- R9 Simple Sort.docx

4.0 Additional Documentation

4.1 SOD Analysis Steps

- GRC SOD Analysis Steps.docx

4.2 GRC Change Events

- GRC Change Events.docx

4.3 Proposed GRC Forms

- Ex Form A_GRC Mitigation Control Change Request.docx
- Ex Form B_GRC FireFighter Change Request.docx
- Ex Form C_SAP User or Role Change Checklist.docx

4.4 GRC & SOD Terminology

- GRC Terminology.docx

5.0 Training Materials

5.1 Training Presentations

- 05-23 GRC Training - Business Analysts.pptx
- 06-03 GRC Training - Risk Owners.pptx
- 06-04 GRC Training - Role Owners - Gerry.pptx
- 06-05 GRC Training - Role Owners - Basil.pptx
- 06-17 GRC Training - IST BSAs.pptx

5.2 Training Packages

- GRC Training - Business Analyst (BA)
- GRC Training - Business Systems Analyst (BSA)
- GRC Training - Risk Owner
- GRC Training - Role Owner

Please contact grc-sod-www@mit.edu with any questions.