

PREPARED BY  
ADITYA JOSYULA

**The Naming Differences between VIRSA and GRC5.3 and GRC10.0:**

<b>VIRSA</b>	<b>GRC5.3</b>	<b>GRC10.0</b>
Compliance Calibrator	Risk Analysis and Remediation (RAR)	Access Risk Analysis(ARA)
Access Enforcer	Compliant User Provisioning (CUP)	Access Request Management (ARM)
Role Architect/ Role Expert	Enterprise Role Management (ERM)	Business Role Management (BRM)
Fire Fighter	Superuser Privilege Management (SPM)	Emergency Access Management (EAM)



Version IT

UNDER THE GUIDANCE OF  
RASHEED AHMED

## **VIRSA(COMPLIANCE CALIBRATOR)**

### **Overview:**

Virsa Compliance Calibrator provides real-time compliance monitoring and controls, integrated within your SAP deployment. Compliance Calibrator uses its built-in analysis engine to identify risks associated with Segregation of Duty (SoD), critical actions, and critical permissions. Once identified, you use Compliance Calibrator controls to mitigate or eliminate compliance risks.

Virsa Access Enforcer provides tools for assigning, enforcing, and logging (cross-system) network resource access permissions, based on job-related database objects, such as users, groups, roles, and profiles. You can also create and use workflows that model your business approval process for access requests. If you use Compliance Calibrator, you can configure Access Enforcer to provide risk analysis and mitigation controls, to identify and resolve access control risks and violations in your workflows.

Virsa Role Expert provides tools to create, manage, and define access permissions, either individual access controls, or groups of access controls—based on job functions (roles). Creating role-based access controls enables you to assign a group of access permissions to user(s) who perform a specific job function, eliminating the need to manually reassign these permissions following a change of the user(s) who perform that job function. If you use Compliance Calibrator, you can configure Role Expert to use the Compliance Calibrator risk analysis engine when creating roles and assigning mitigation controls. If you use Access Enforcer, you can configure Role Expert to require approval for new and changed roles using Access Enforcer workflows.

Virsa Firefighter provides flexible controls that allow you to assign special permissions for emergency access to network resources that would otherwise be restricted from the user or users performing the emergency tasks. In addition to network emergencies, you can use Firefighter to provide temporary and/or time and date-restricted access permissions, for tasks that require those permissions only during certain times, such as auditing services. Firefighter allows you to designate these permissions and who must approve the assignment of these permissions. Once the access has been approved, Firefighter provides an audit trail log of every action performed using these enhanced access privileges. If you use Compliance Calibrator, you can configure Firefighter to use the risk analysis engine to identify and resolve Firefighter risks and violations.

PREPARED BY  
ADITYA JOSYULA

The Components of Virsa are:

1. Compliance Calibrator
2. Access Enforcer
3. Fire Fighter
4. Role Architect

**How to find the Risk with the User or Role Using VIRSA:**

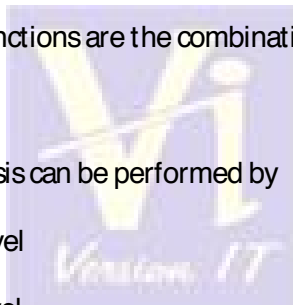
Risk can be due to

- i. whenever two different Tcodes come together that will be one risk or
- ii. Two similar kind of functions come together that might be a risk.

Here, Functions are the combination of multiple Actions(nothing but Tcodes) or Authorizations.

Risk Analysis can be performed by

1. User Level
2. Role Level



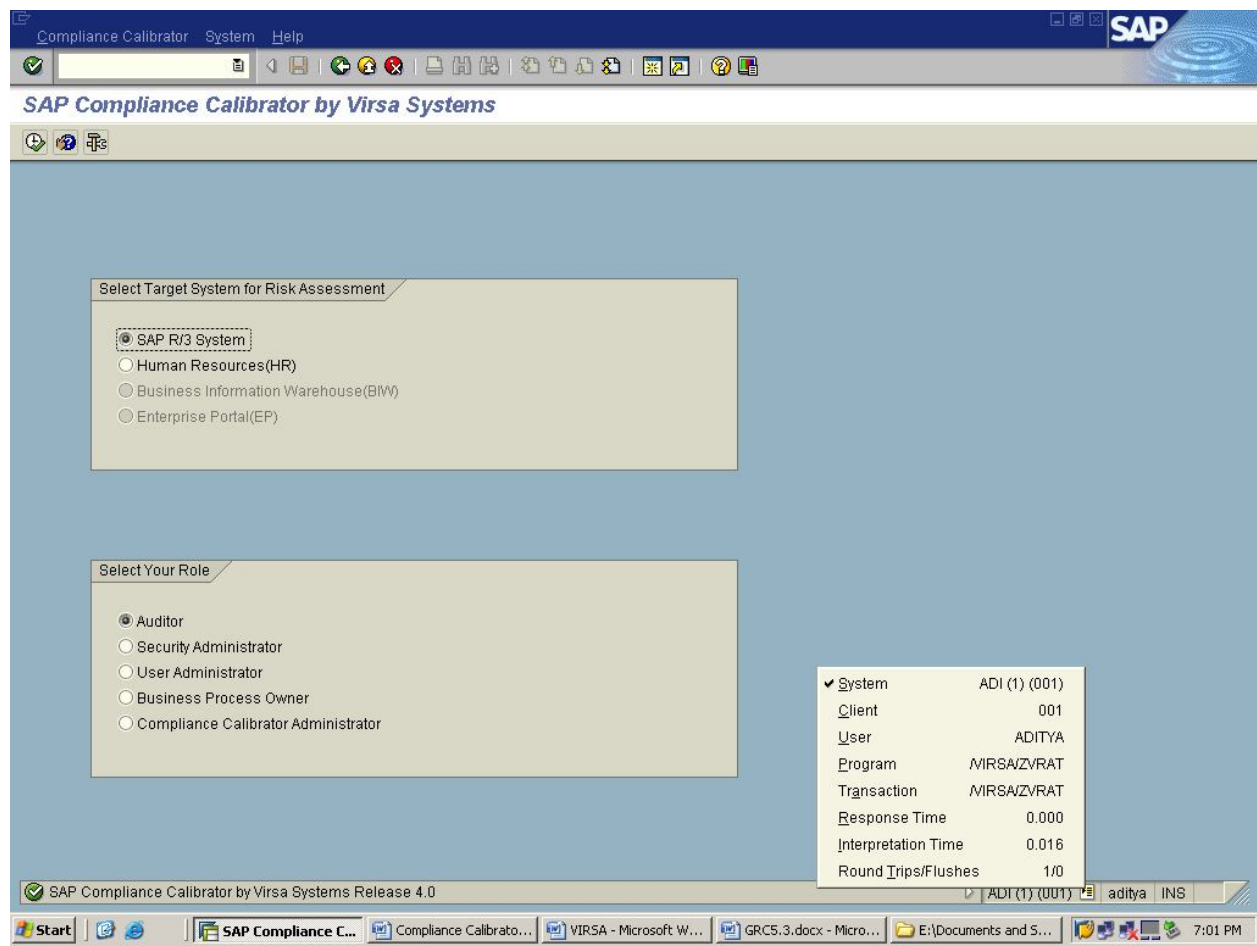
Version IT

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

## Risk Analysis – User Level

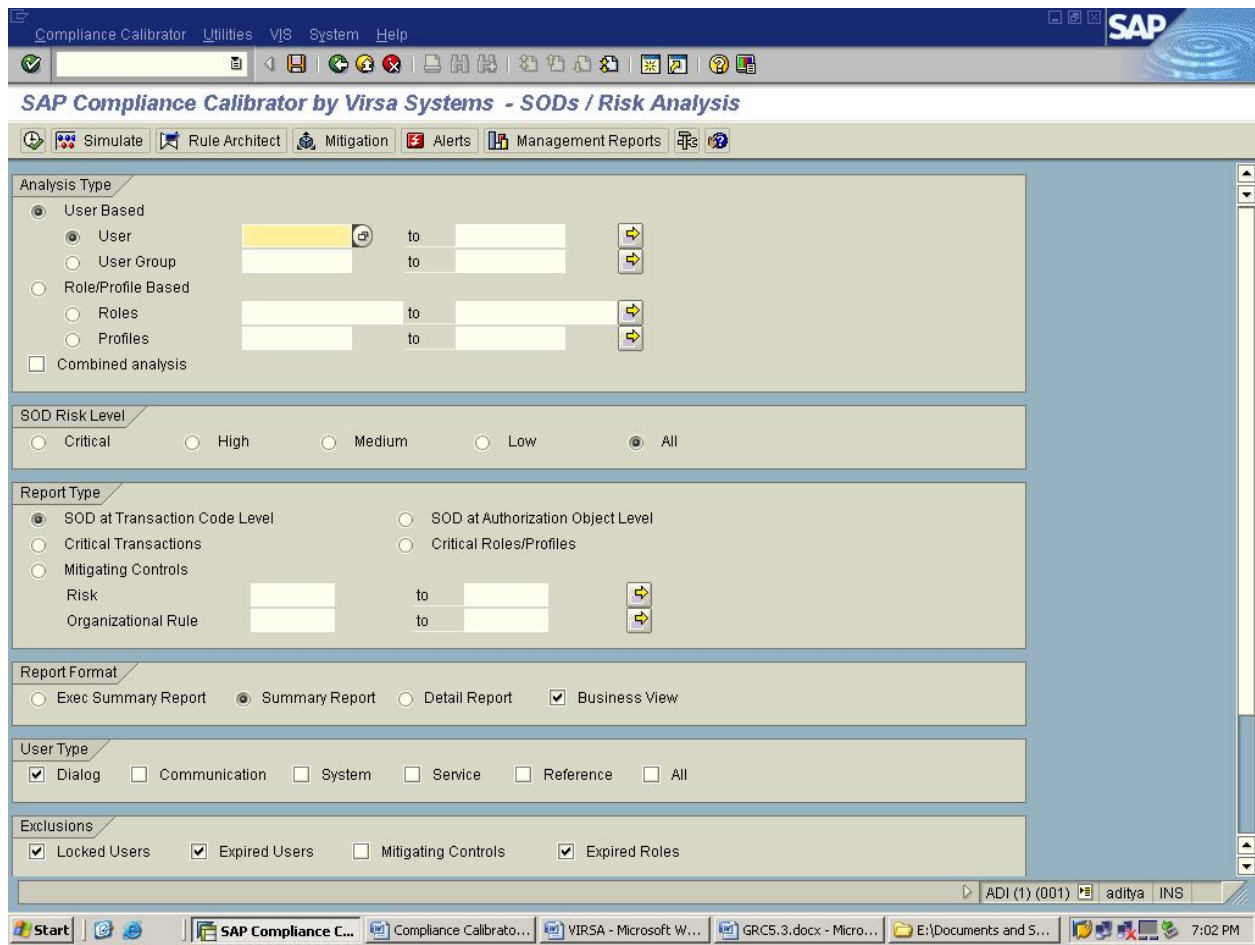
To Logon to VIRSA Compliance Calibrator, the Tcode is /n/virsa/zvrat



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Select the Target System & Role then Click on Execute.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

→In Analysis Type, Under User Based Select the User and Mention the user name

→In SOD Risk Level, select the option level ALL

→ Select the Report Type which you want to perform, Here we are using SOD at Transaction Code Level

→Select the Report Format

→Select the User Type .

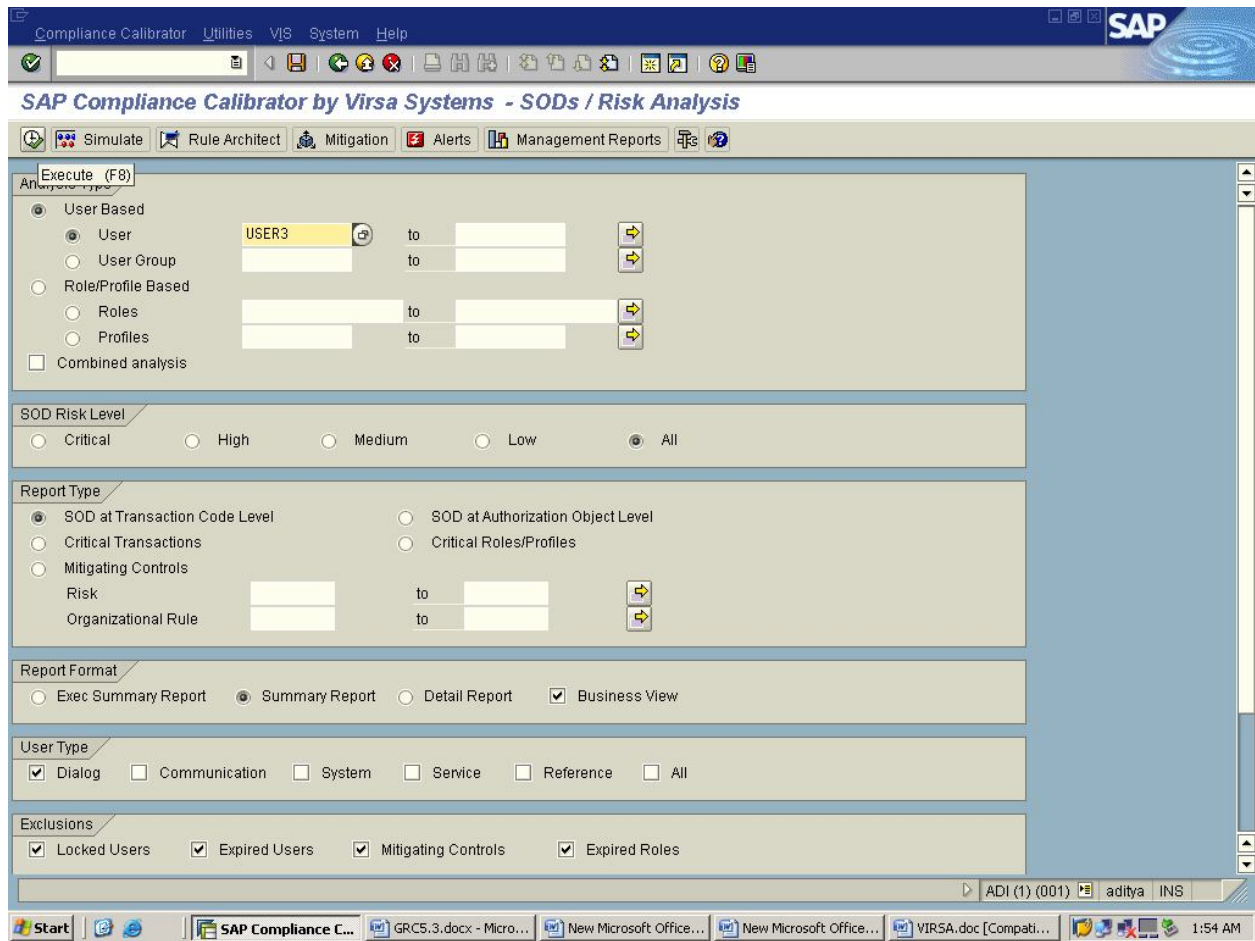
Check the below Screen Shot



Version IT

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



Click on Execute.

After executing you will get all the levels of Risks i.e., High, Medium, Low and critical.

Check the below screen

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

System Help SAP

Compliance Calibrator - Segregation Of Duties at TCode Level

Detail Report Exec Summary Report Technical View

Detail Report (Shift+F9)

User Id : USER3 (USER3) User Group : Basis

Conflicting Transactions	Risk Description	Level	Business Process
Client Administration ( SCC4 ) and User Maintenance ( SU01 )	B011016: Security Administration & Client Administration	High	Basis
Delete Client ( SCC5 ) and User Maintenance ( SU01 )	B011017: Security Administration & Client Administration	High	Basis

ADI (1) (001) aditya INS

Start Compliance Calibr... GRC5.3.docx - Micro... New Microsoft Office... New Microsoft Office... VIRSA.doc [Compati... 1:56 AM

By seeing the level of the risk we need to remove the risk or we need to mitigate the risk.

Click on Detail Report and Copy the Role Name.

UNDER THE GUIDANCE OF  
RASHEED AHMED



PREPARED BY  
ADITYA JOSYULA

The screenshot shows the SAP Compliance Calibrator interface. The title bar reads "Compliance Calibrator - Segregation Of Duties at TCode Level". Below the title bar, there are three tabs: "Summary Report", "Exec Summary Report", and "Technical View". The "Summary Report" tab is active. The main content area displays a table for User Id: USER3 (USER3) and User Group: . The table has four columns: Risk Description, Level, Transaction, and Role Description. The data rows are as follows:

Risk Description	Level	Transaction	Role Description
B011016: Security Administration & Client Administration	High	Client Administration (SCC4)	Z:ADITYA_BC_CLIENT_ADMIN: BC CLIENT ADMINISTRATION
B011016: Security Administration & Client Administration	High	User Maintenance (SU01)	Z:ADITYA_BC_CLIENT_ADMIN: BC CLIENT ADMINISTRATION
B011017: Security Administration & Client Administration	High	Delete Client (SCC5)	Z:ADITYA_BC_CLIENT_ADMIN: BC CLIENT ADMINISTRATION
B011017: Security Administration & Client Administration	High	User Maintenance (SU01)	Z:ADITYA_BC_CLIENT_ADMIN: BC CLIENT ADMINISTRATION

The taskbar at the bottom shows the Start button, several open applications including "Compliance Calibr...", "GRC5.3.docx - Micro...", "New Microsoft Office...", "New Microsoft Office...", "VIRSA.doc [Compati...", and the system clock showing 1:59 AM.

To see the conflicts you need to click Technical View tab.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

System Help SAP

Compliance Calibrator - Segregation Of Duties at TCode Level

Detail Report Exec Summary Report Technical View

Technical View (Shift+F7)

User Id : USER3 (USER3) User Group :

Conflicting Transactions	Risk Description	Level	Business Process
Client Administration ( SCC4 ) and User Maintenance ( SU01 )	B011016: Security Administration & Client Administration	High	Basis
Delete Client ( SCC5 ) and User Maintenance ( SU01 )	B011017: Security Administration & Client Administration	High	Basis

ADI (1) (001) aditya INS

Start Compliance Calibr... GRC5.3.docx - Micro... New Microsoft Office... New Microsoft Office... VIRSA.doc [Compati... 2:02 AM

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

The screenshot shows the SAP Compliance Calibrator interface. The title bar reads "SAP Compliance Calibrator - Segregation Of Duties at TCode Level". Below the title bar, there are tabs for "Detail Report", "Exec Summary Report", and "Business View". The main area displays a table with the following data:

User	Full Name	User Group	Transactions	Risk Id	Risk Description	Risk Level	Control Id
USER3	USER3		SU01,SCC4	B011016	Security Administration & Client Administration	High	
USER3	USER3		SU01,SCC5	B011017	Security Administration & Client Administration	High	

The taskbar at the bottom shows the Start button, several open applications including "Compliance Calibr...", "GRC5.3.docx - Micro...", and "New Microsoft Office...", and the system clock showing "2:00 AM".

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

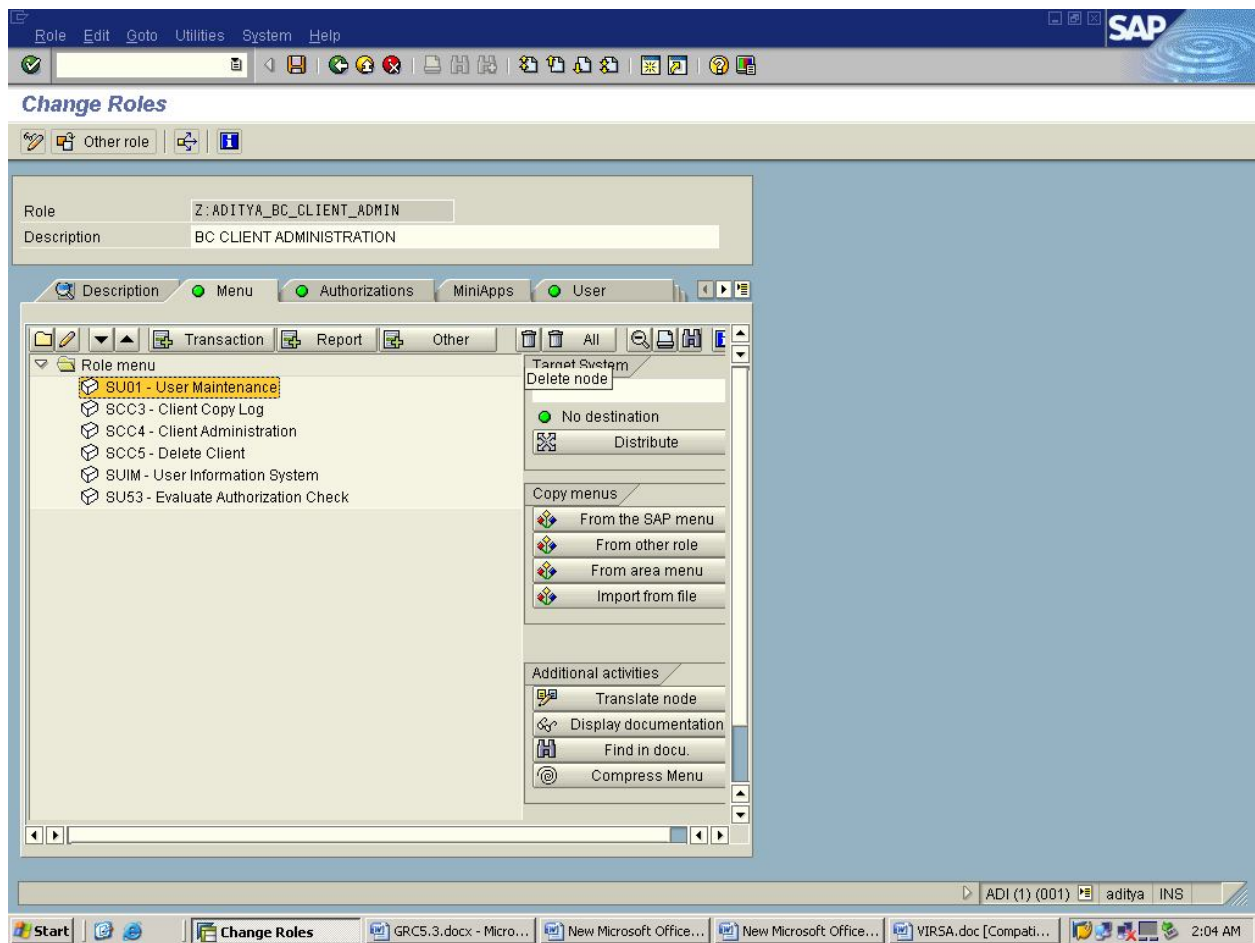
To remove the risk, Copy the Role Name after that go to the backend system and remove the risk from the role.

After going to the backend system remove one confliction actions (Tcodes) from the role.

Here confliction actions are SCC4 and SU01 & SCC5 and SU01.

Then Goto PFCG and mention the role name and remove the Tcodes from the role .

Check the below screens for removing the Tcodes from the role .

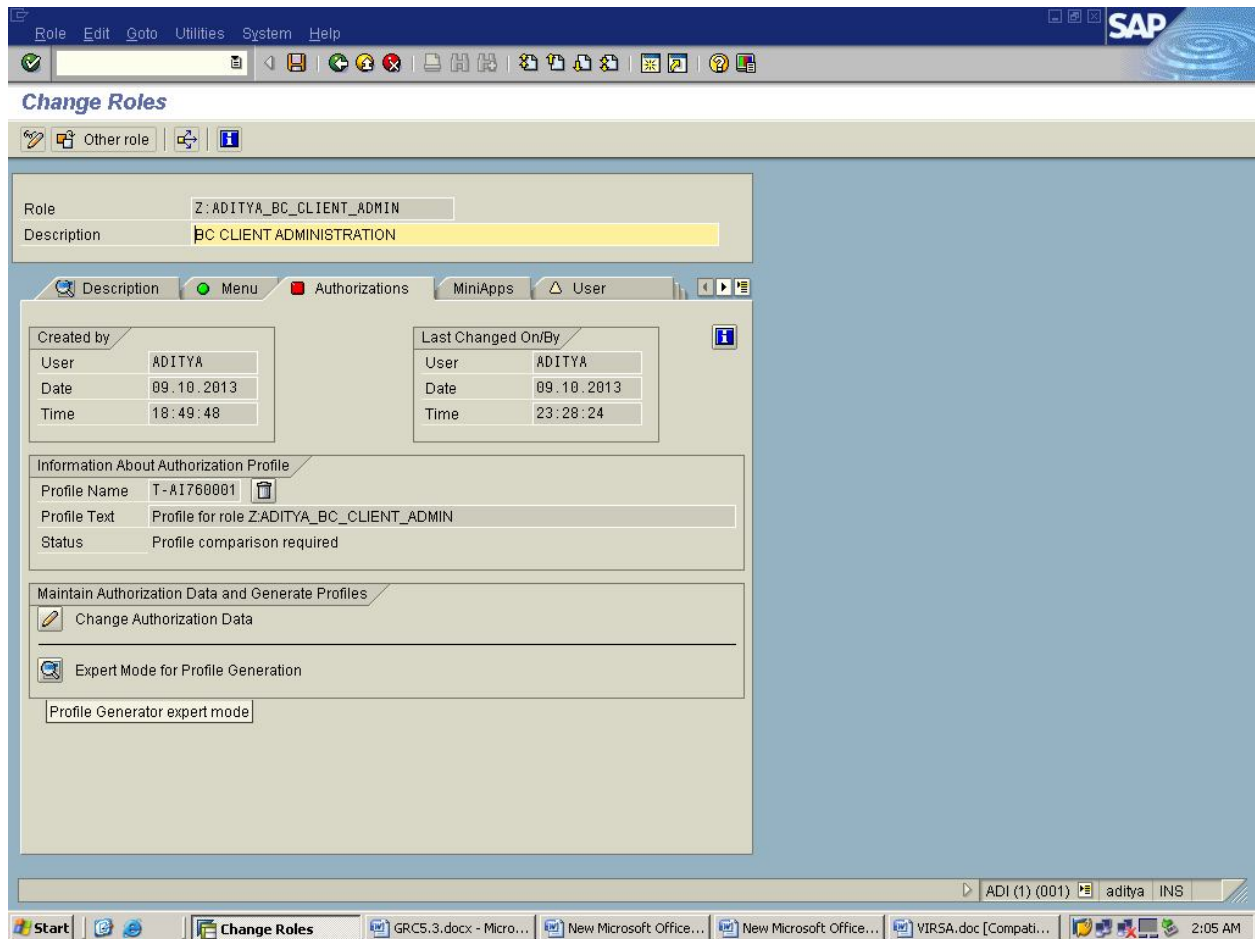


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

After removing the Tcode from the role goto Authorization tab and go for Expert Mode for Profile Generation.

Check the below screen shot .

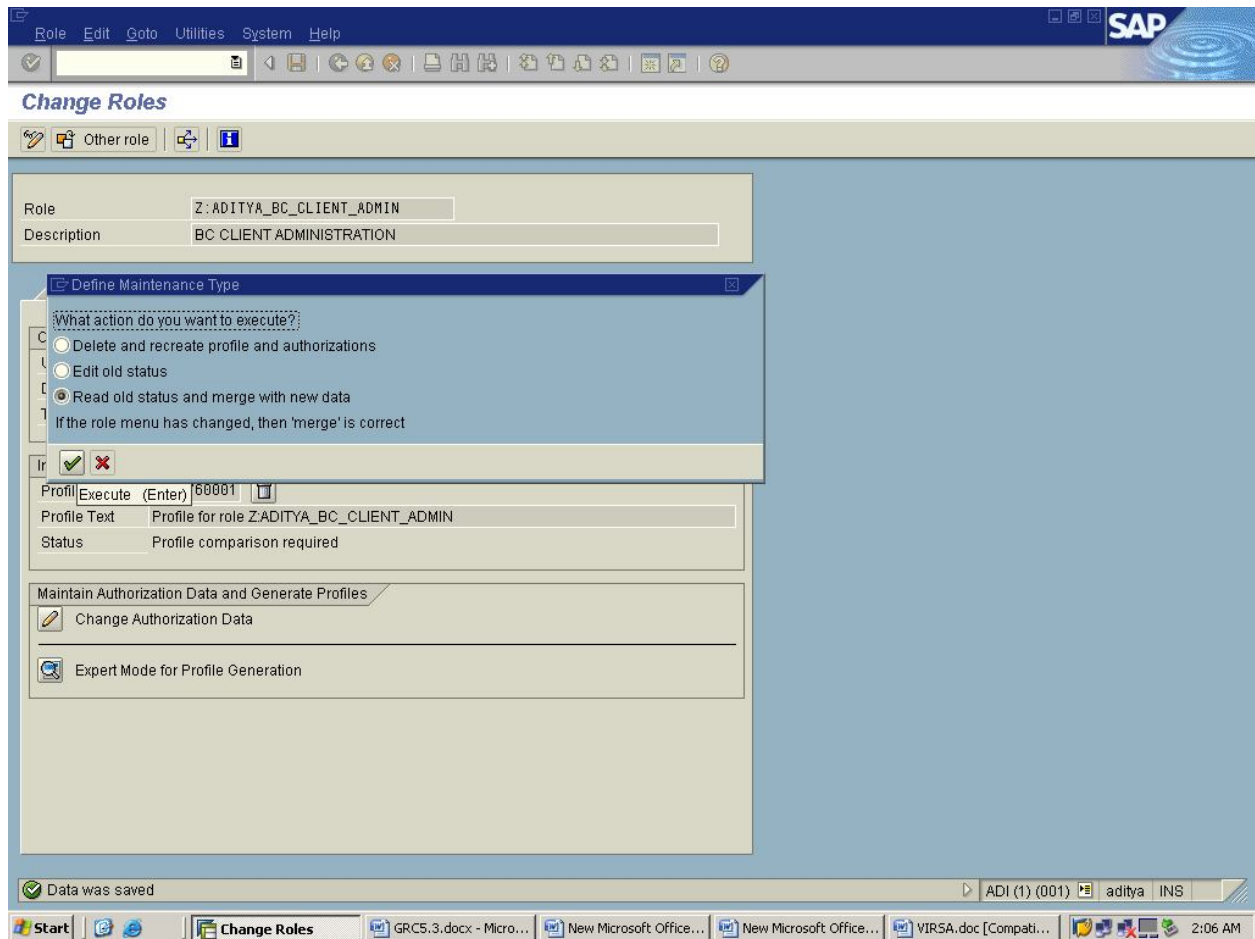


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Then go with Read Old Status and Merge with New Data option and click Nike.

Check the below screen

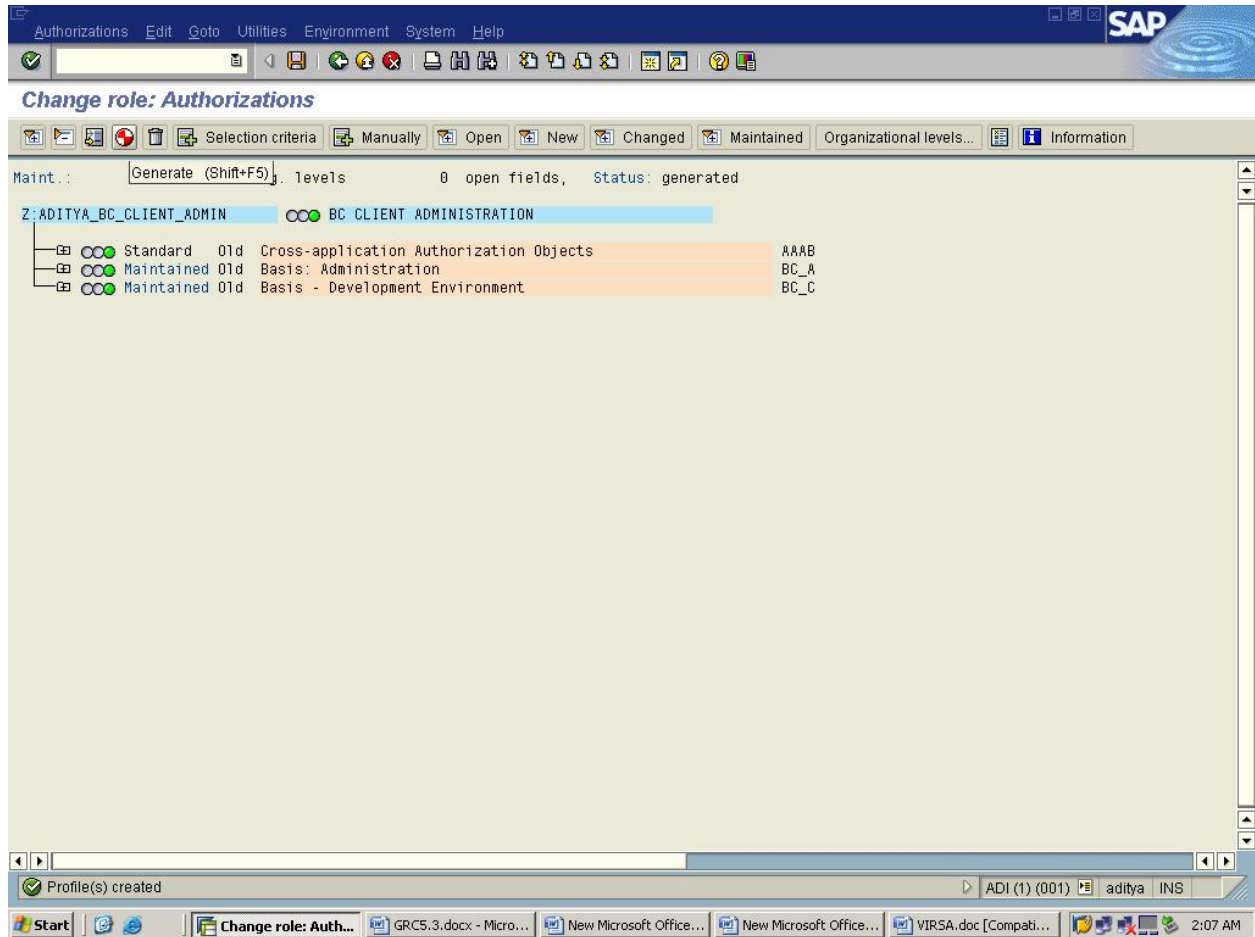


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

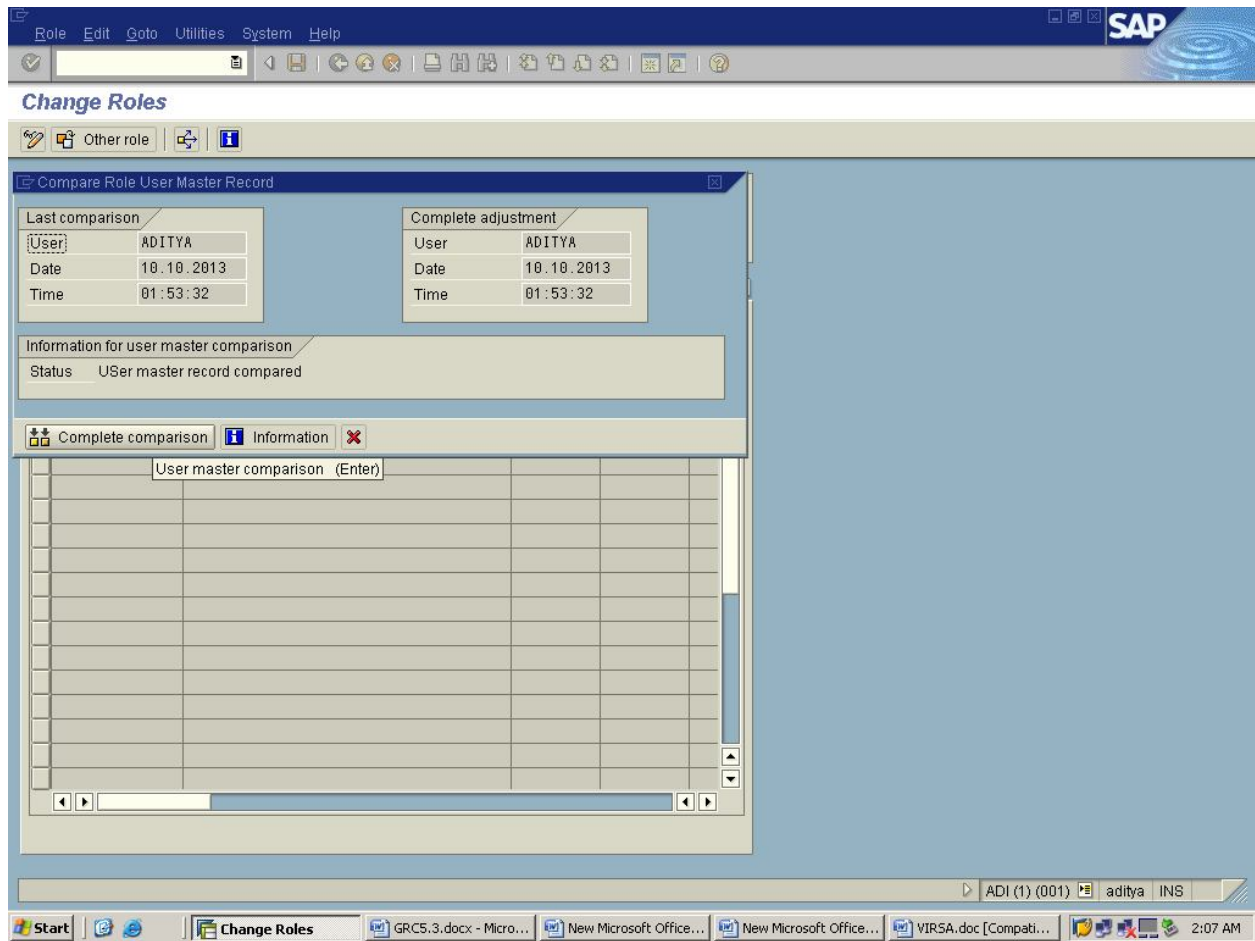
Then generate the role and do the User Comparison.

Check the below screens.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



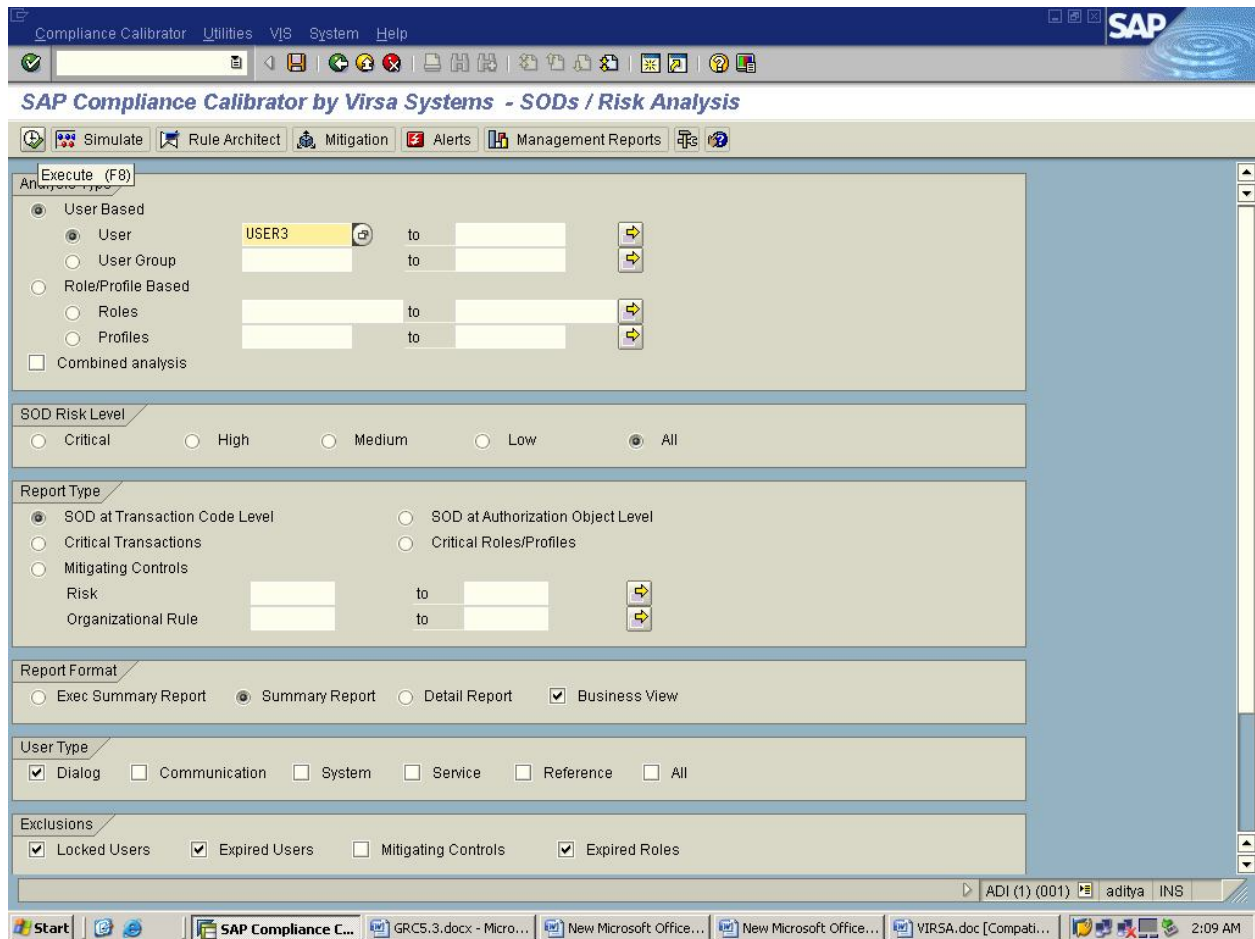
UNDER THE GUIDANCE OF  
RASHEED AHMED



PREPARED BY  
ADITYA JOSYULA

Now go back to the Analysis Type, Under User Based Select the User and Mention the user name.

Check the below screen



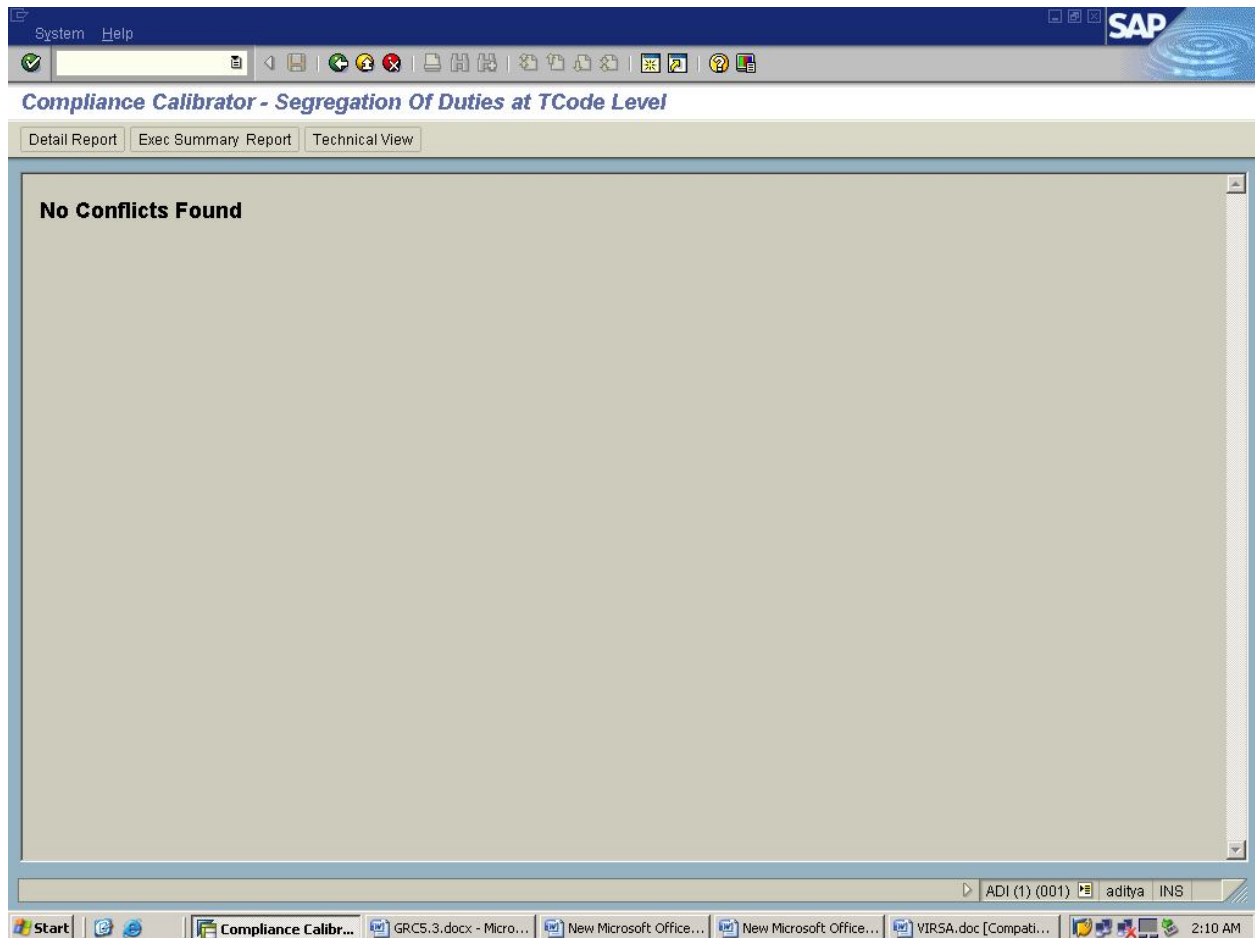
UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on execute.

Now you will get a screen with No violations found .

Check the below screen

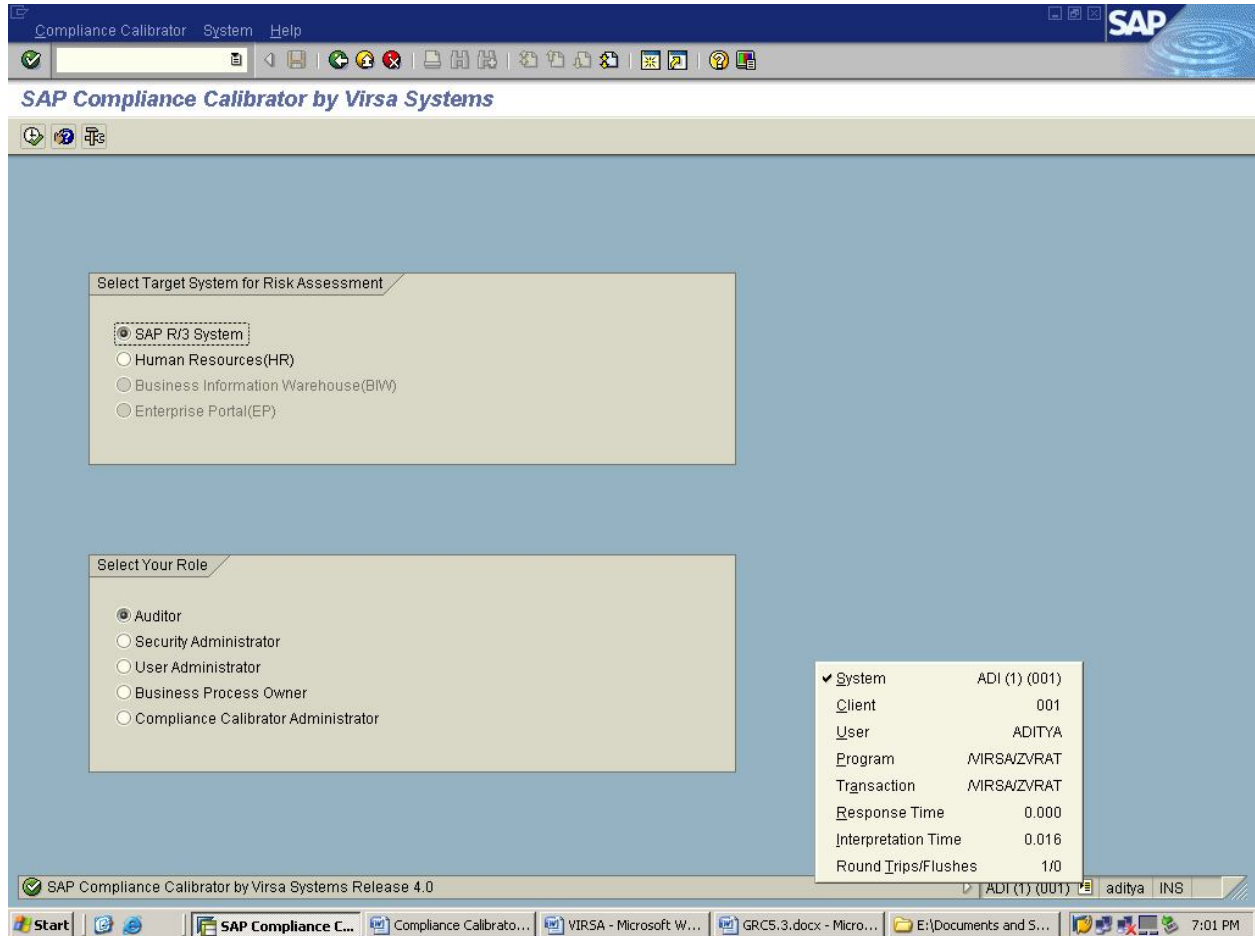


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

## Risk Analysis – ROLE Level

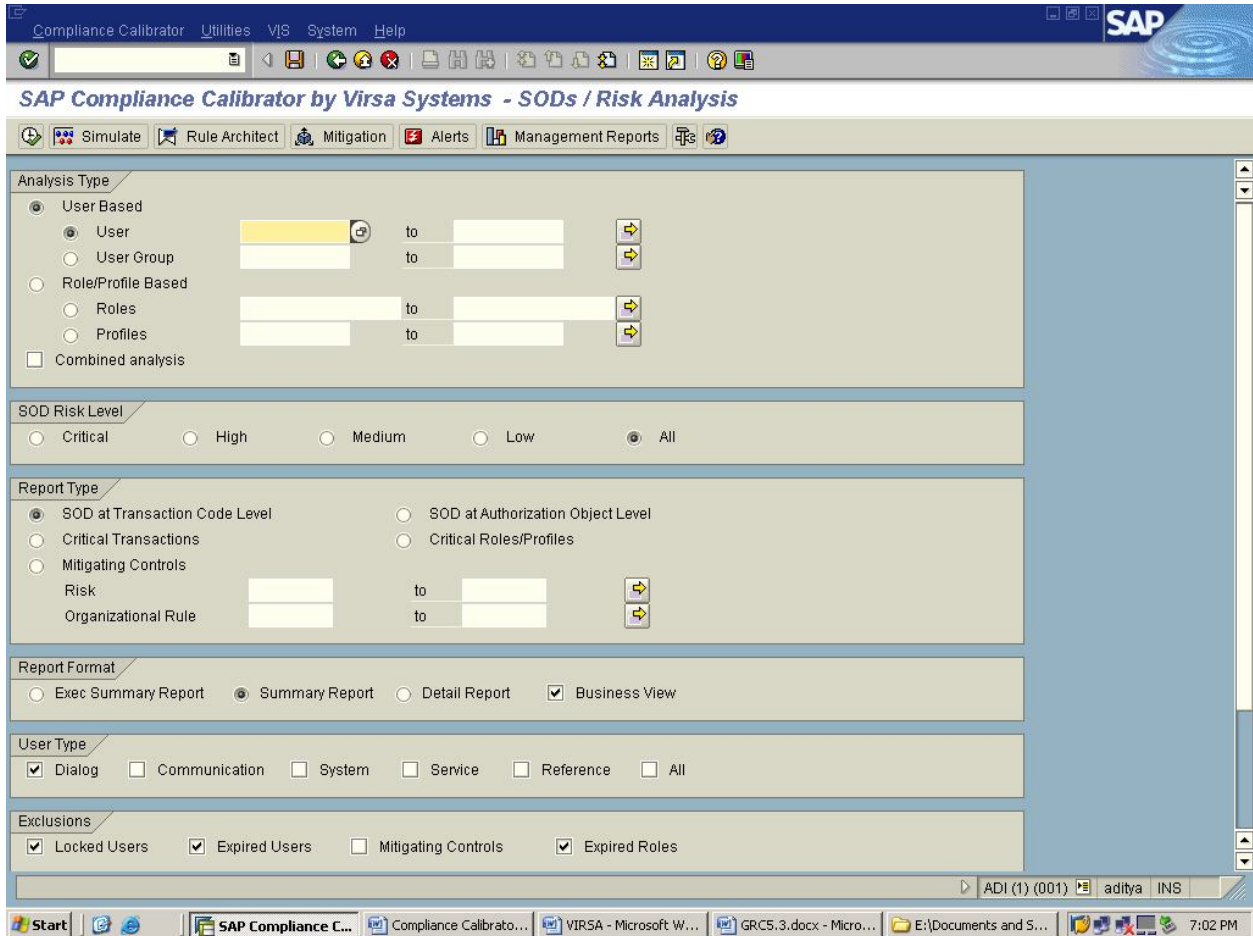
To Logon to VIRSA Compliance Calibrator, the Tcode is /n/virsa/zvrat



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Select the Target System & Role then Click on Execute.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

→In Analysis Type, Under Role/Profile Based Select the Roles and Mention the Role name

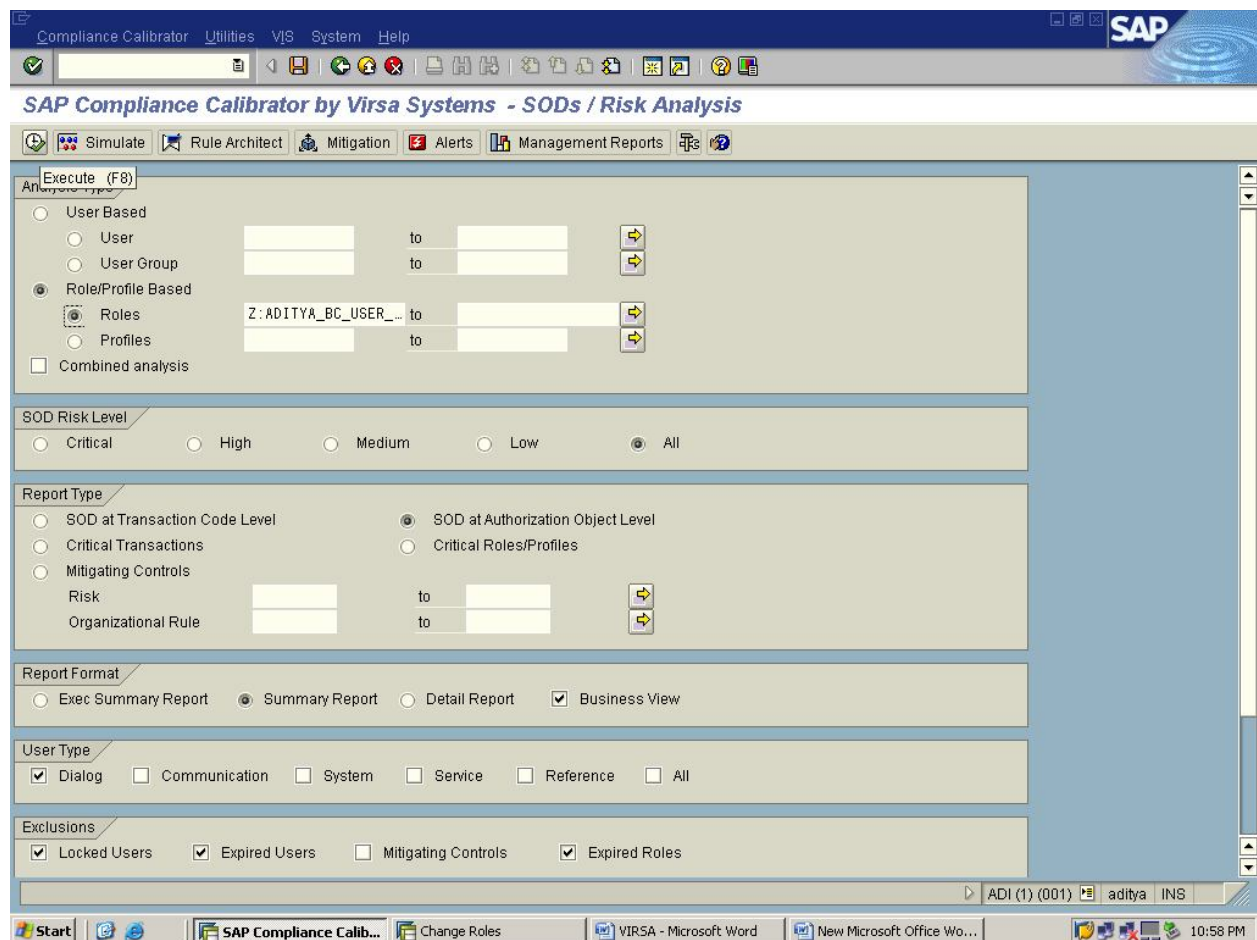
→In SOD Risk Level, select the option level ALL

→Select the Report Type which you want to perform, Here we are using SOD at Authorization Object Level

→Select the Report Format

→Select the User Type .

Check the below Screen Shot



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on Execute.

After executing you will get all the levels of Risks i.e., High, Medium, Low and critical.

Click on Technical View.

Check the below screen

System Help SAP

Compliance Calibrator-Segregation Of Duties at Object Level

Detail Report Technical View

Technical View (Shift+F6)

Role : Z:ADITYA\_BC\_USER\_ADMIN -BC USER ADMINISTRATION

Conflicting Transactions	Risk Description	Level	Business Process	Mitigating Control	Monitor
Delete Client ( SCC5 ) and User Maintenance ( SU01 )	B01101701: Security Administration & Client Administration	High	Basis		
Delete Client ( SCC5 ) and User Mass Maintenance ( SU10 )	B01104501: Security Administration & Client Administration	High	Basis		

ADI (1) (001) aditya INS

Start Compliance Calibrato... Change Roles VIRSA - Microsoft Word New Microsoft Office Wo... 11:01 PM

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

By seeing the level of the risk we need to remove the risk or we need to mitigate the risk.

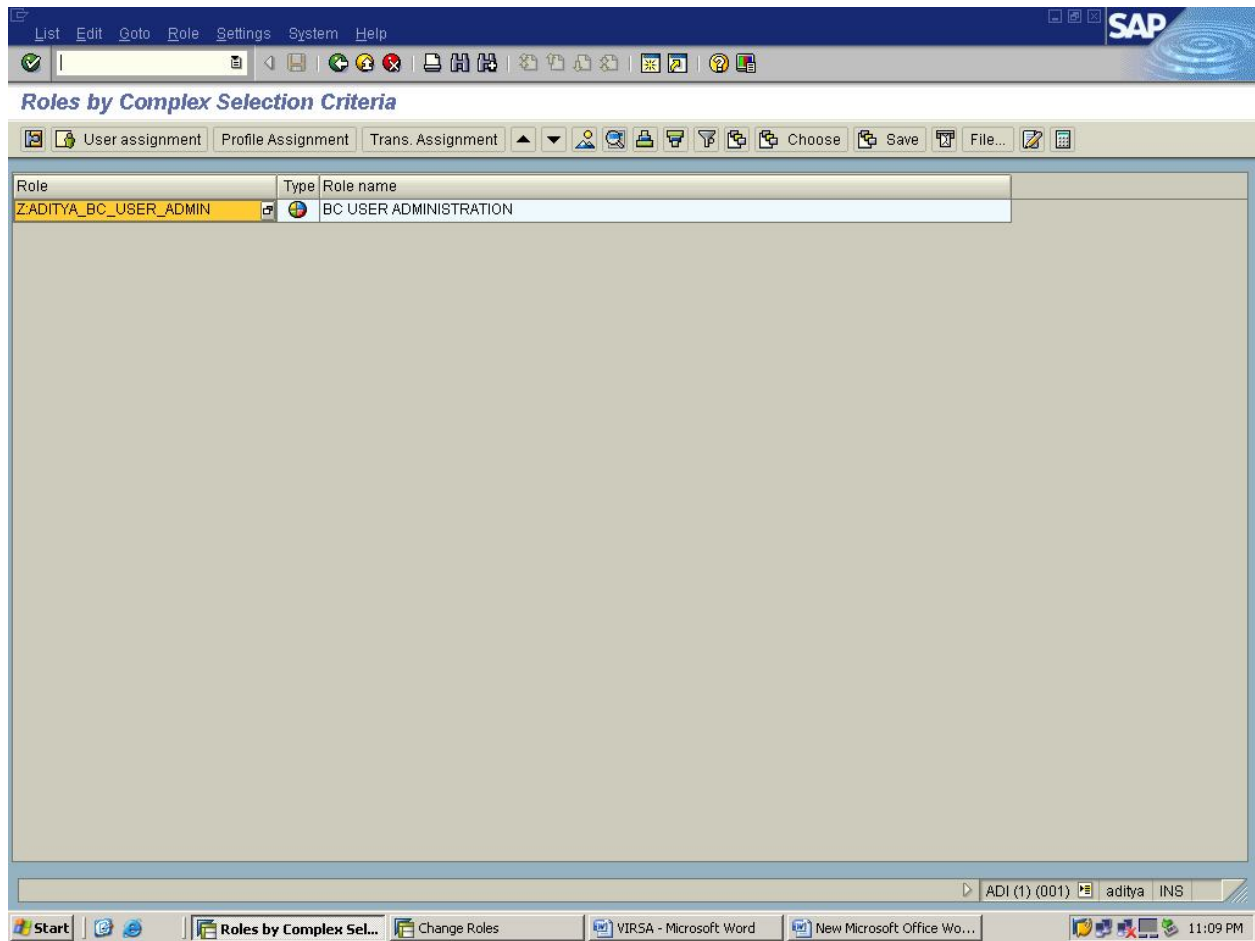
Then Click on the Role Name.

Check the below Screen shot.

Role	Risk Id	Transactions	Risk Description	Risk Level	Control Id
ZADITYA_BC_USER_ADMIN	B01101701	SCC5,SU01	Security Administration & Client Administration	High	
ZADITYA_BC_USER_ADMIN	B01104501	SCC5,SU10	Security Administration & Client Administration	High	

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED

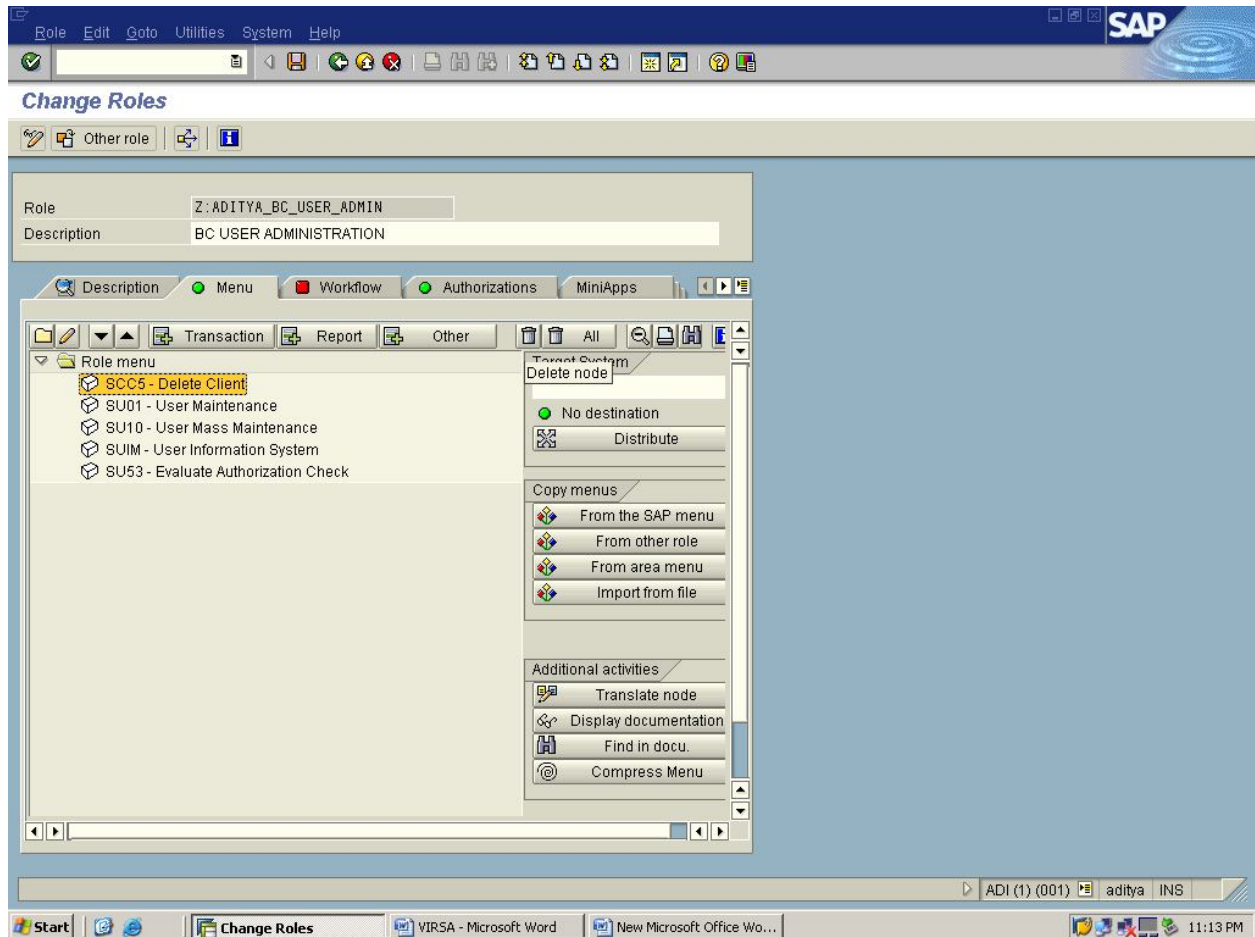


PREPARED BY  
ADITYA JOSYULA

Again Double click on the Role name.

By Double clicking the role name you will get PFCG Screen directly where you can remove the conflicts.

Check the below screens for removing the Tcodes from the role .

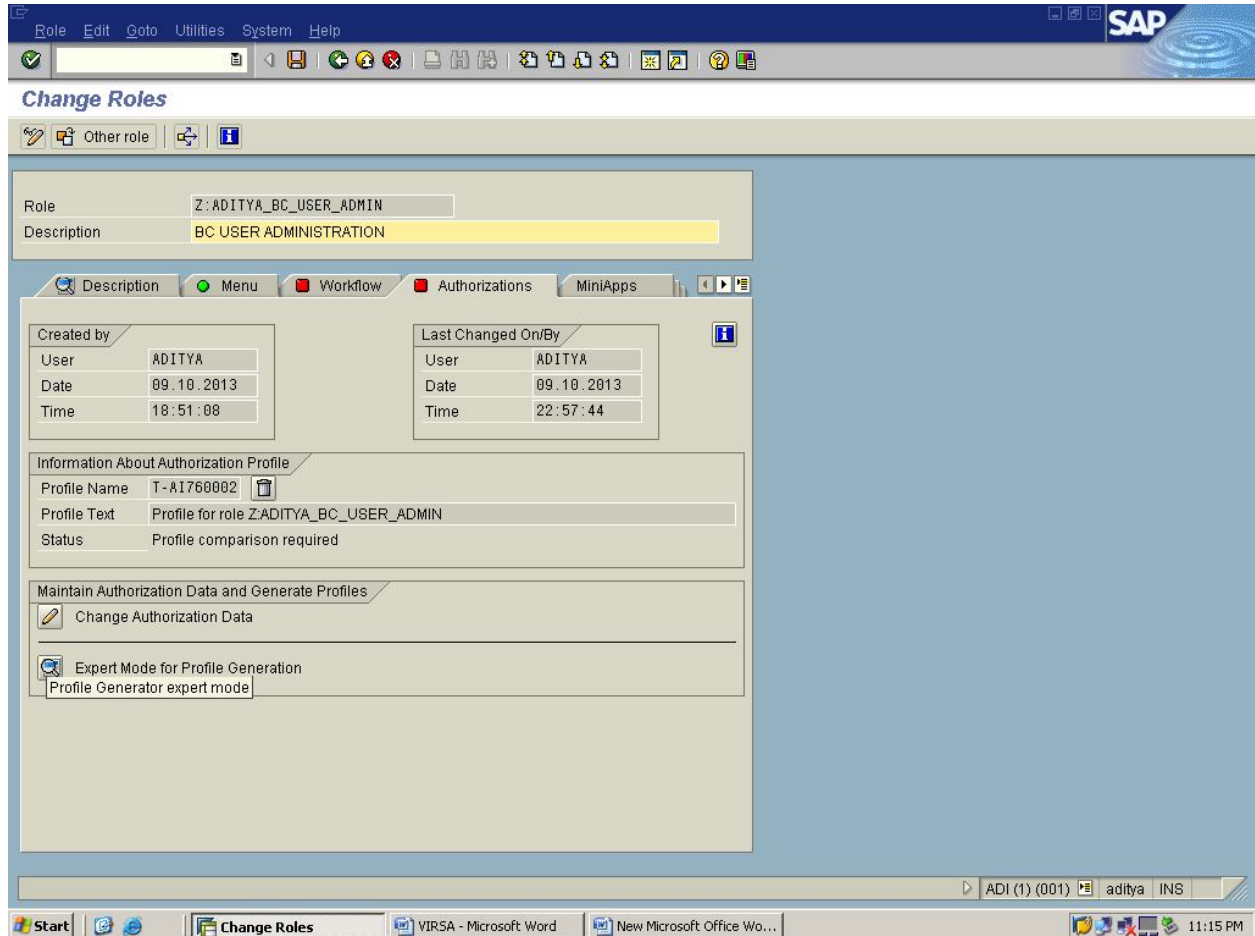


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

After removing the Tcode from the role goto Authorization tab and go for Expert Mode for Profile Generation.

Check the below screen shot .

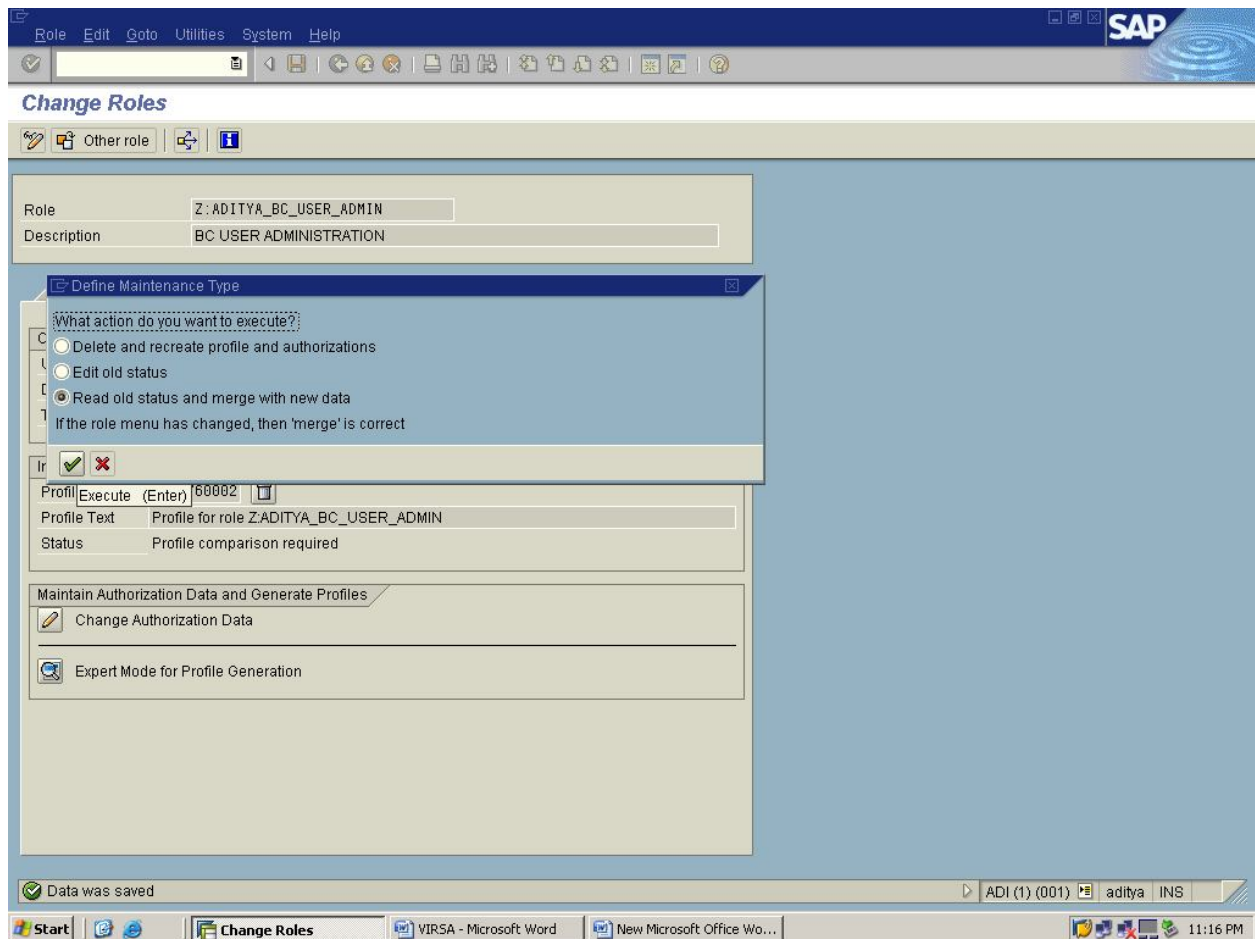


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Then go with Read Old Status and Merge with New Data option and click Nike.

Check the below screen

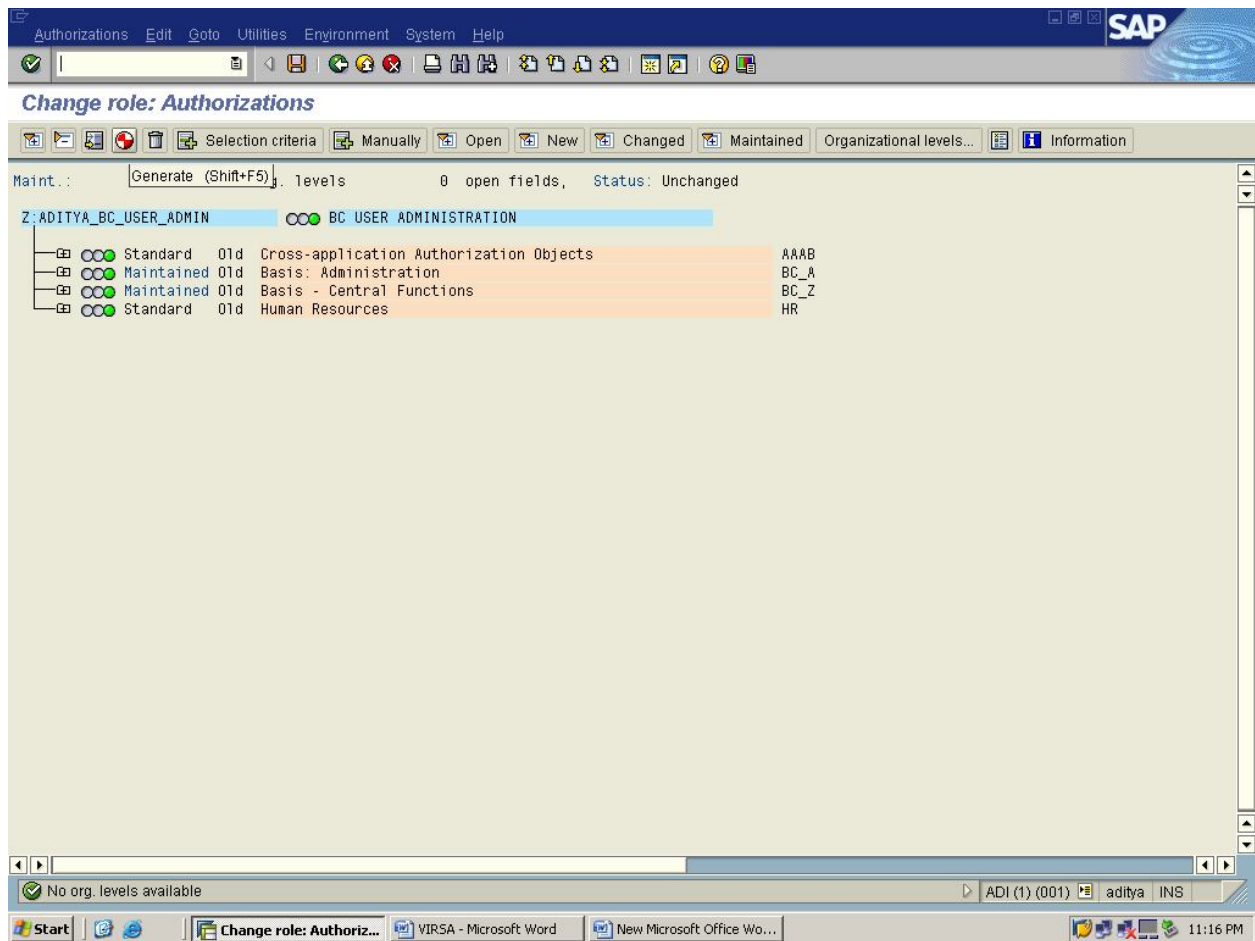


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

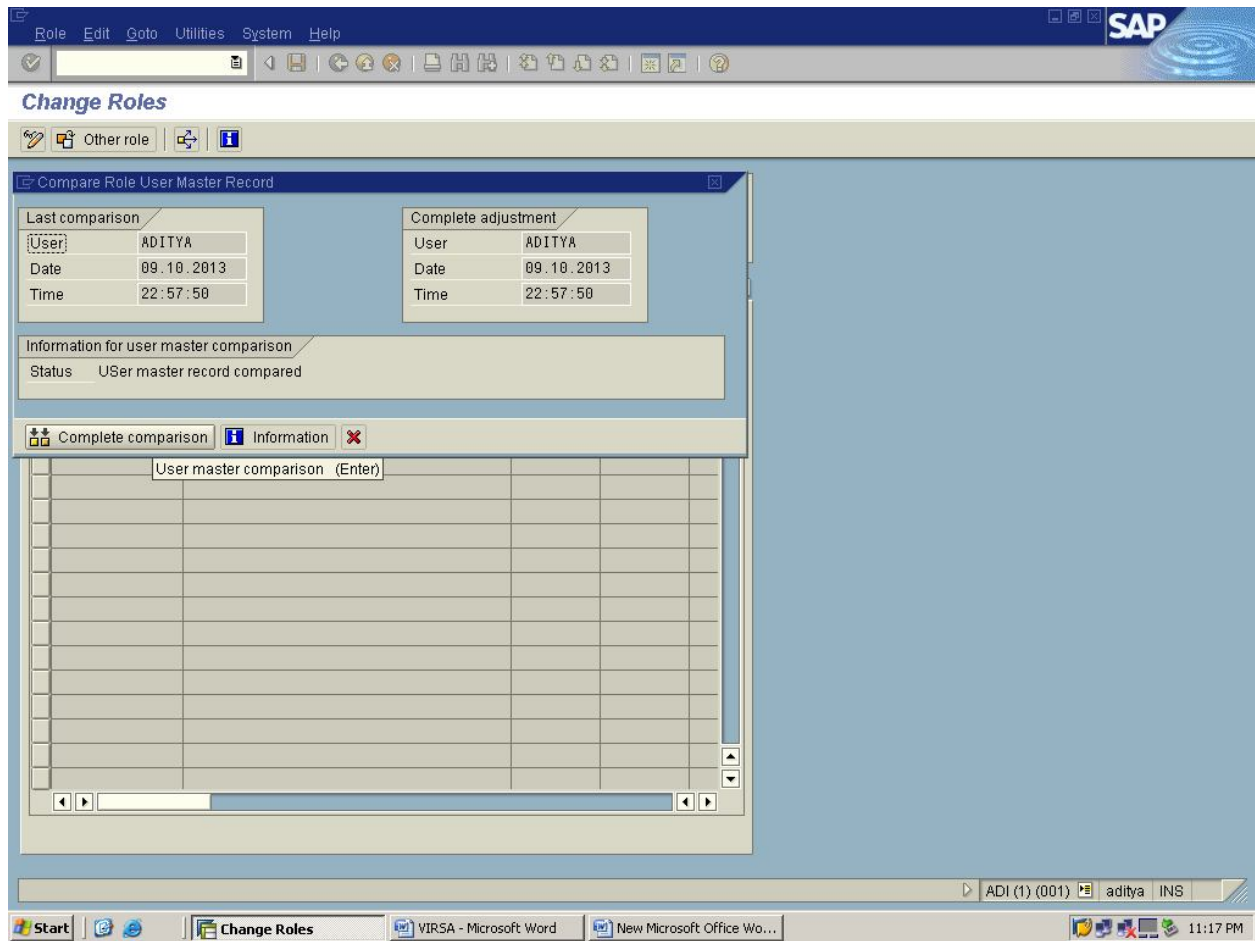
Then generate the role and do the User Comparison .

Check the below screens



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

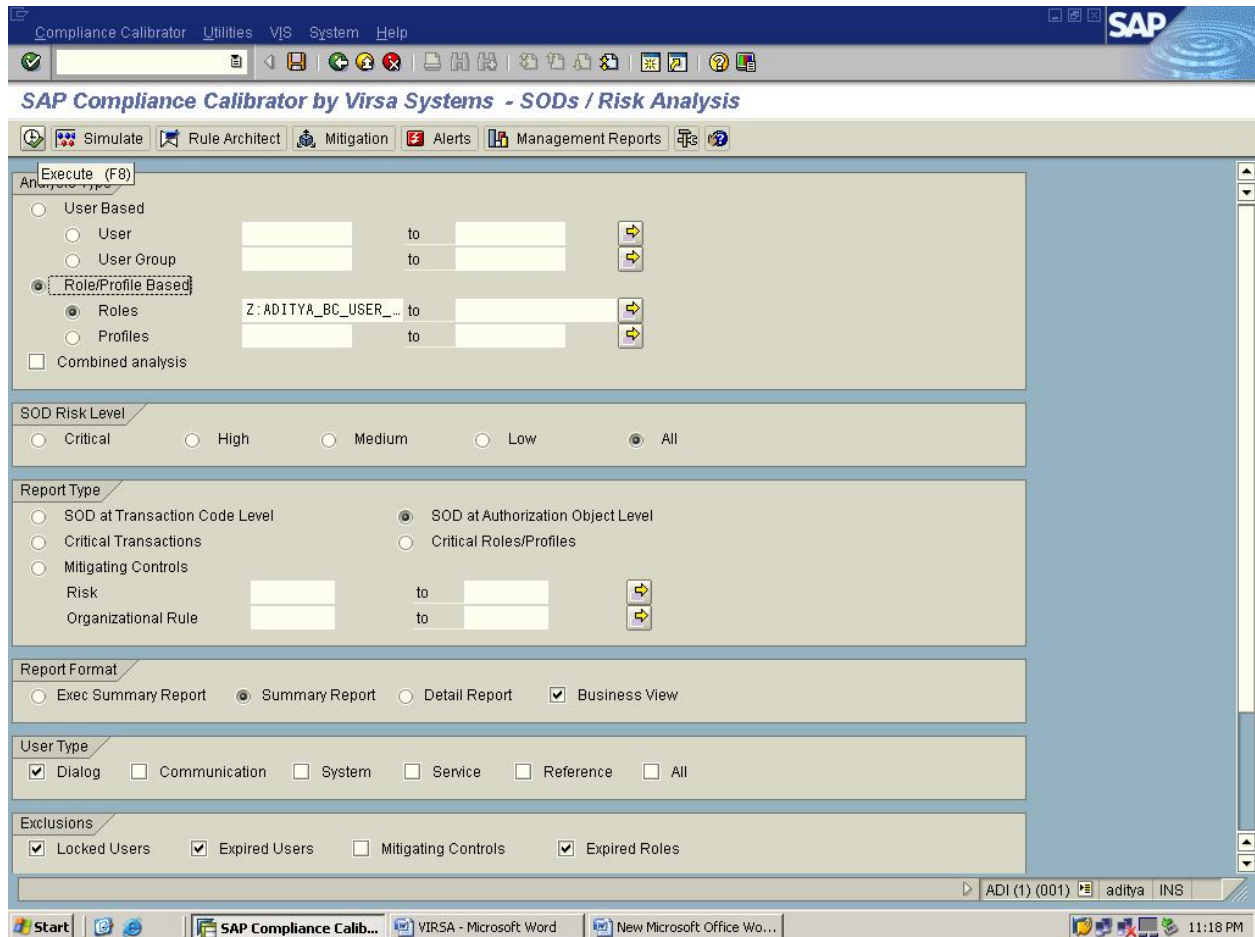


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Now go back to the Analysis Type, Under Role/ Profile Based Select the Role and Mention the Role name.

Check the below screen



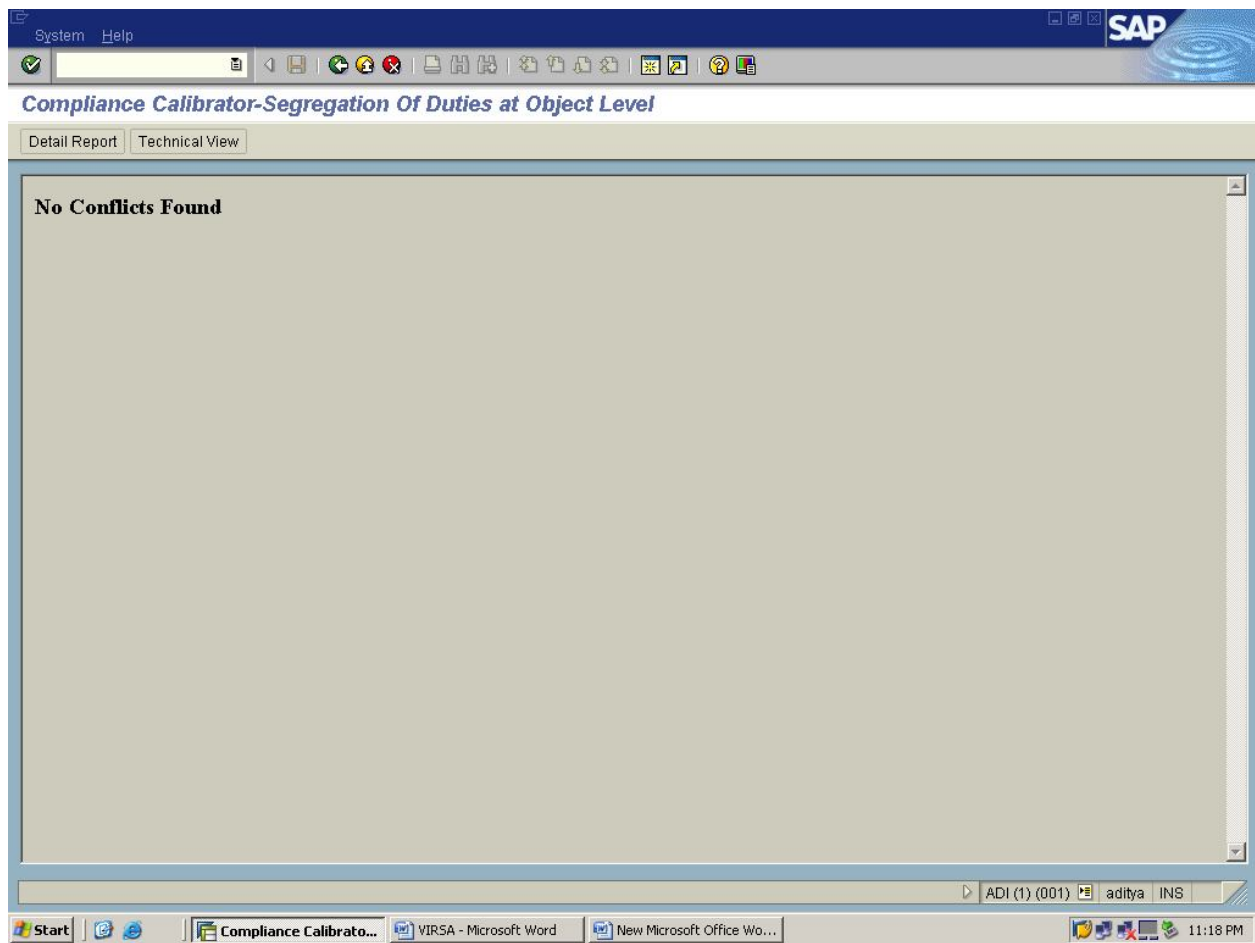
UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on execute.

Now you will get a screen with No violations found .

Check the below screen



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

### **Simulation:**

By using this option we can able to identify the risk information before adding the Tcode to Role or User.

EX: If Business is asking you to add 1 particular Tcode to the existing Role then we can get the risk information by putting the Role name & Tcode information under Simulate option and click on Simulate Button, then system will show the Risk Analysis information without adding a Tcode to Role.

### **Steps for Simulation at User Level**

To Logon to VIRSA Compliance Calibrator, the Tcode is /n/virsa/zvrat

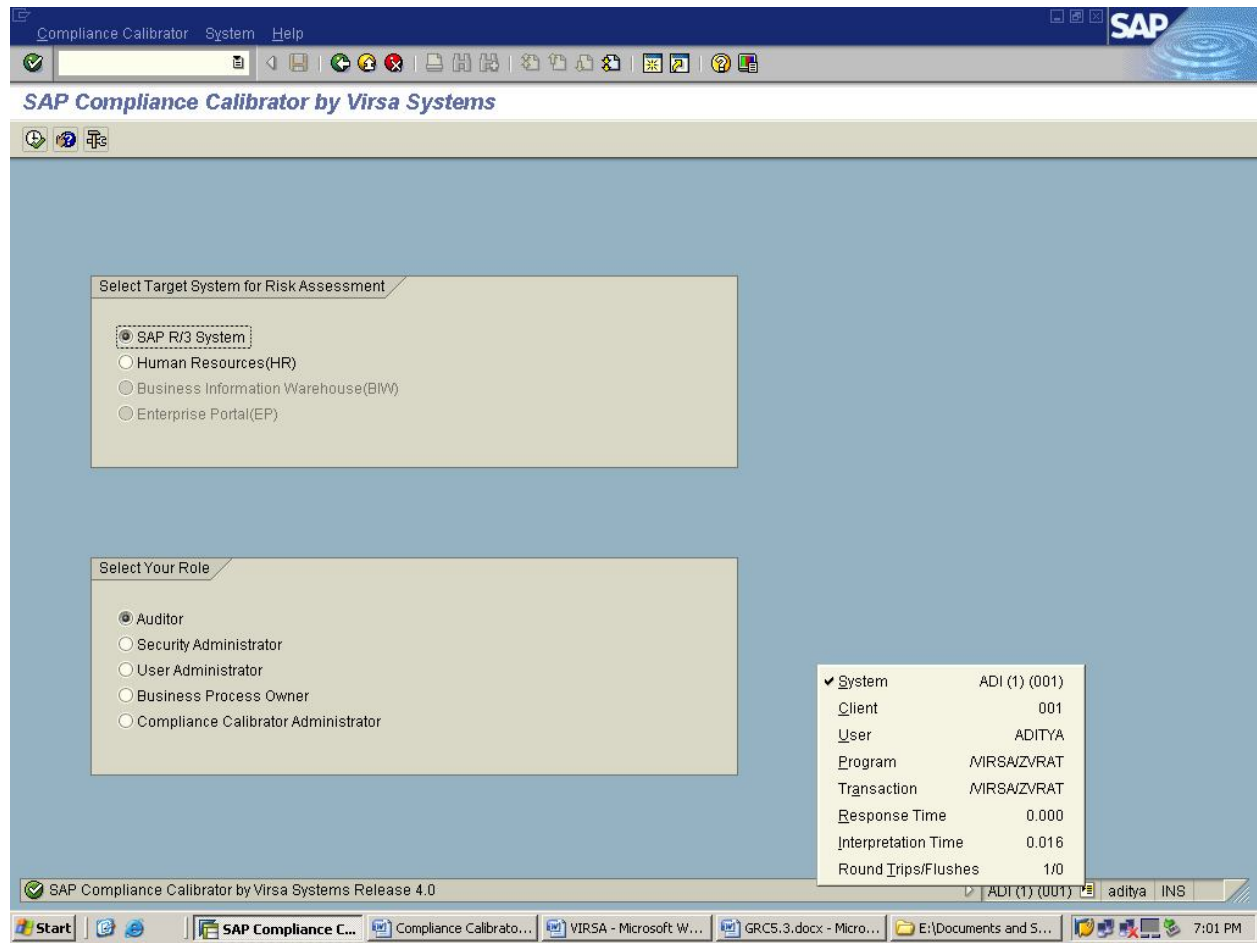


Version IT

UNDER THE GUIDANCE OF  
RASHEED AHMED



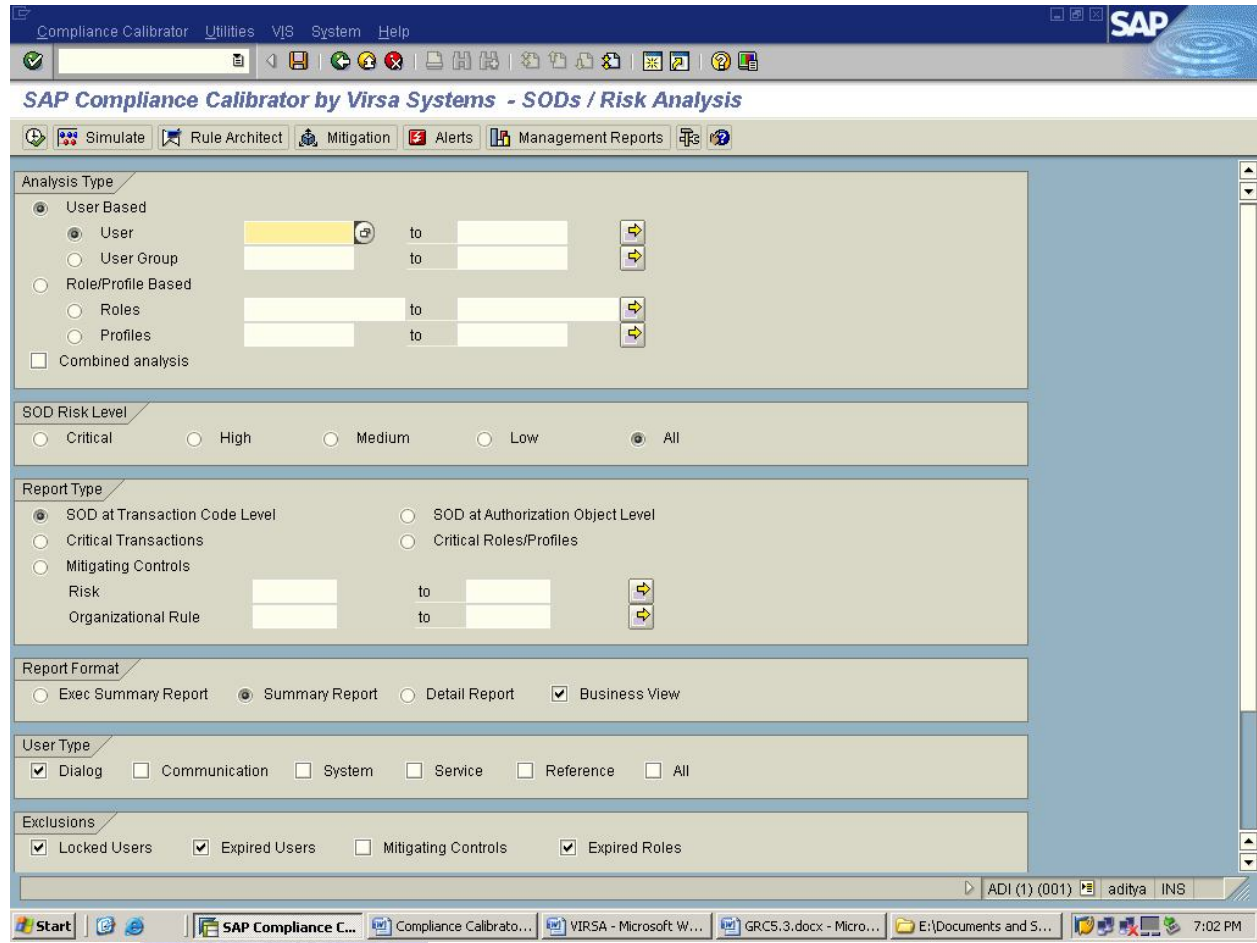
PREPARED BY  
ADITYA JOSYULA



Select the Target System & Role then Click on Execute.

UNDER THE GUIDANCE OF  
RASHEED AHMED

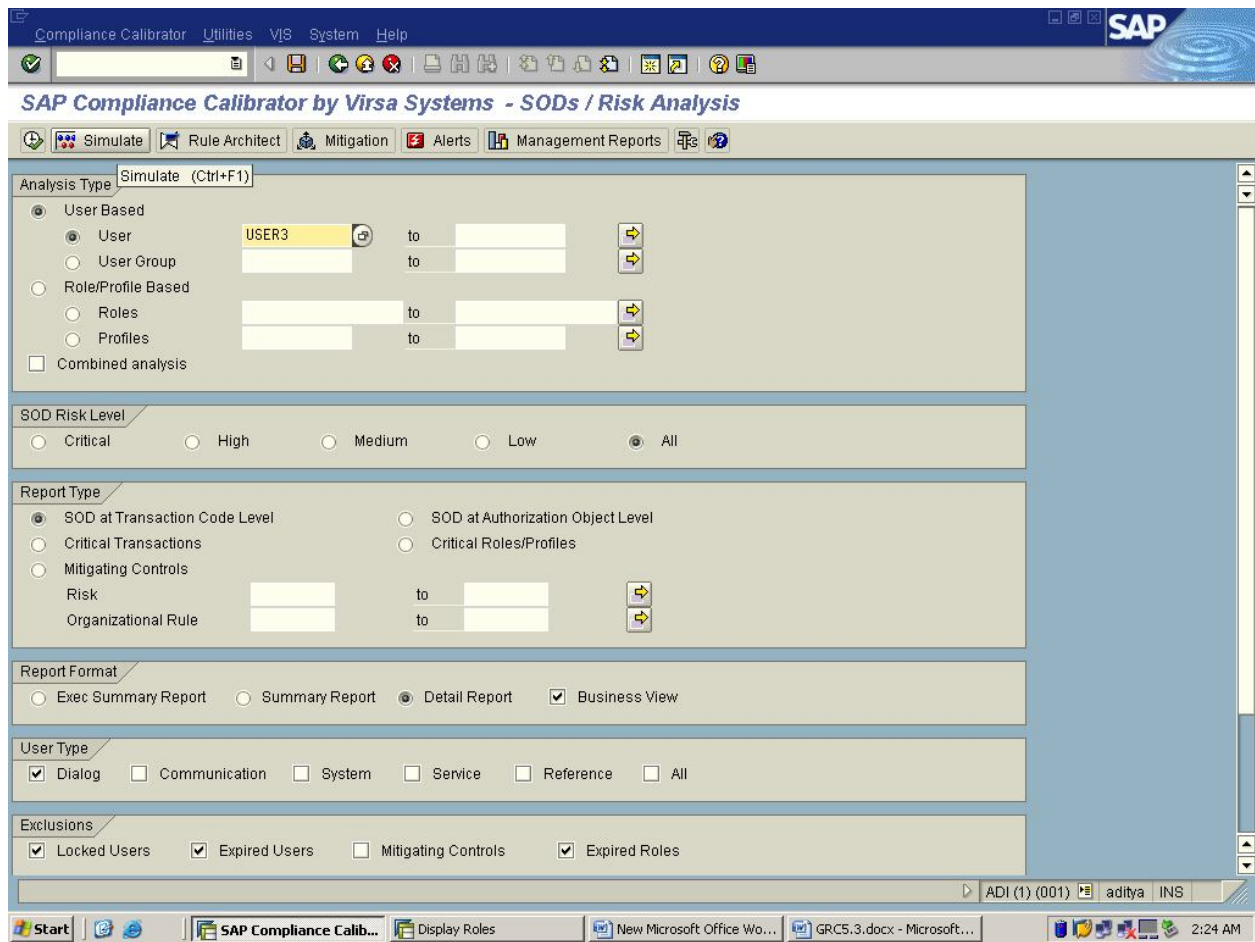
PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Now give the User name and Click on Simulate Tab.



UNDER THE GUIDANCE OF  
RASHEED AHMED

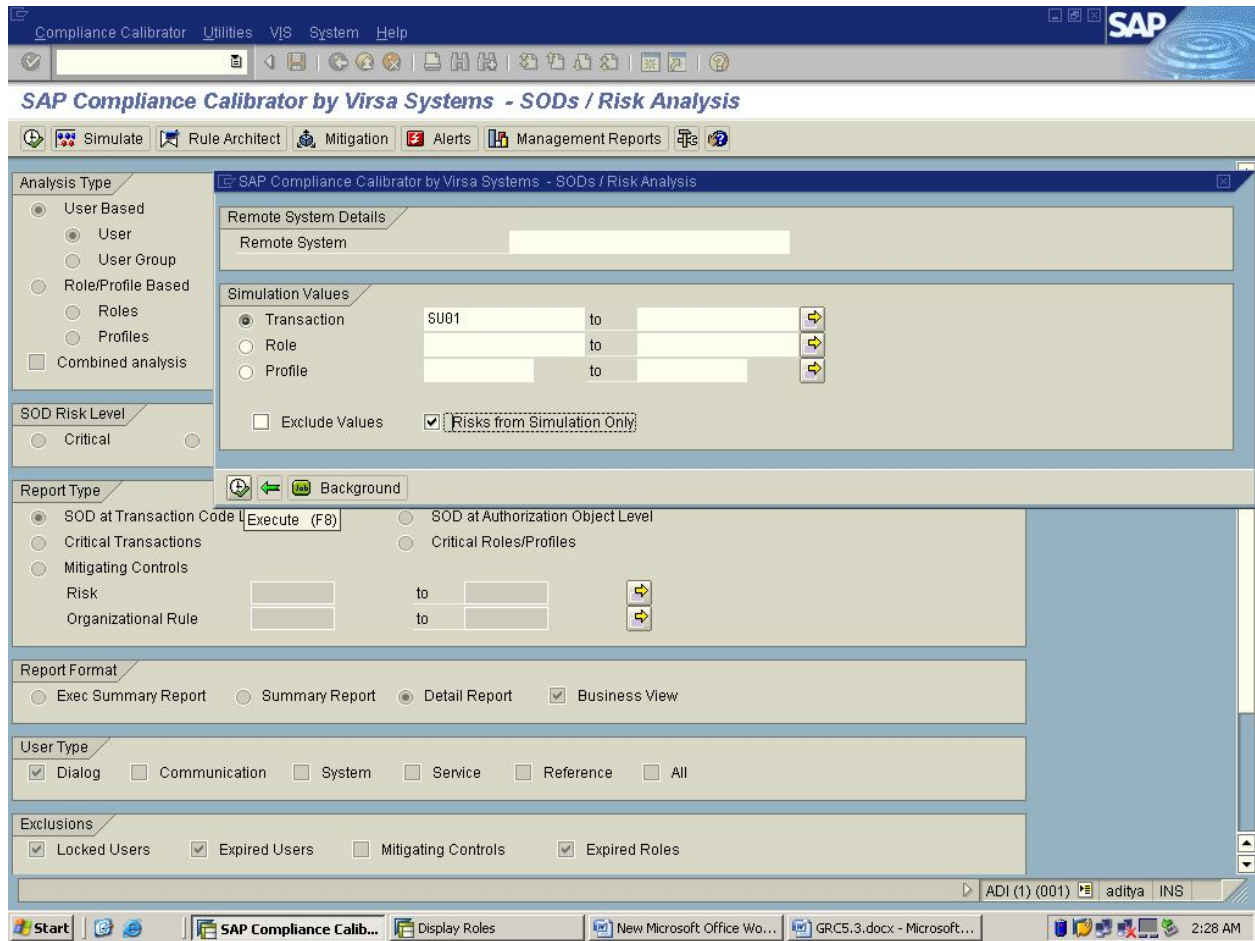
PREPARED BY  
ADITYA JOSYULA

Here Under the Simulation Values give the Transaction which you want to add.

Note: Leave the Remote System Details as blank.

And check Risks from Simulation Only.

Then click on Execute.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

The screenshot displays the SAP Compliance Calibrator interface. The title bar reads "Compliance Calibrator - Segregation Of Duties at TCode Level". Below the title bar, there are tabs for "Summary Report", "Exec Summary Report", and "Technical View". The main content area shows a report for "User Id : USER3 (USER3)". The report is a table with the following columns: Risk Description, Level, Transaction, Role Description, Mitigating Control, Monitor, and System Id. The data rows are as follows:

Risk Description	Level	Transaction	Role Description	Mitigating Control	Monitor	System Id
B011016: Security Administration & Client Administration	High	Client Administration (SCC4)	Z:ADITYA_BC_CLIENT_ADMIN: BC CLIENT ADMINISTRATION			
B011016: Security Administration & Client Administration	High	User Maintenance (SU01)	Simulation:			
B011017: Security Administration & Client Administration	High	Delete Client (SCC5)	Z:ADITYA_BC_CLIENT_ADMIN: BC CLIENT ADMINISTRATION			
B011017: Security Administration & Client Administration	High	User Maintenance (SU01)	Simulation:			

Here the value which we have used is SU01 to the user and its showing the risk in High Level.

So this clarifies the value which we have used shouldn't be assigned to the user.

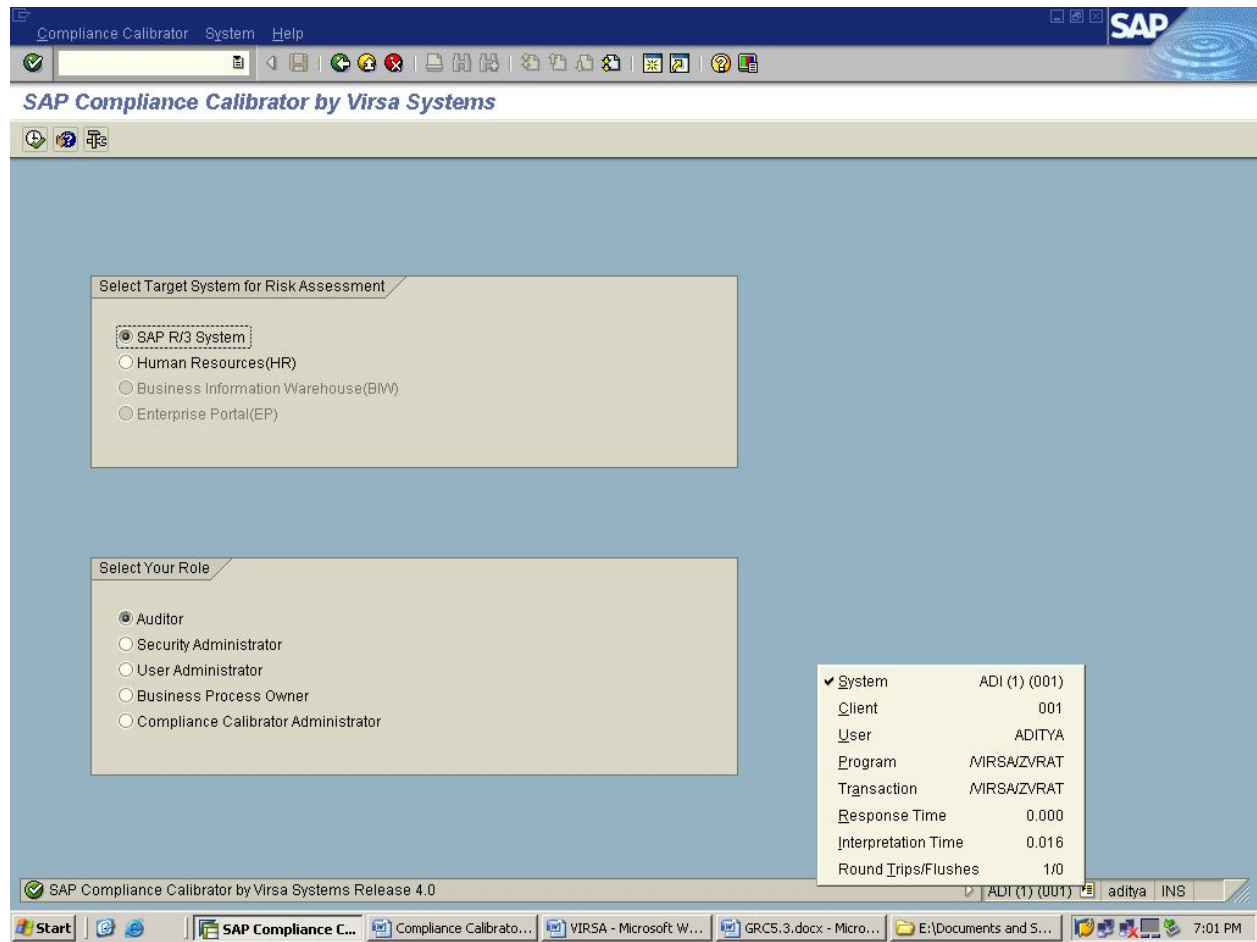
But if the business wants to allow this risk to the user we can do it by using Mitigation Control Option.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

## Steps for Simulation at Role Level

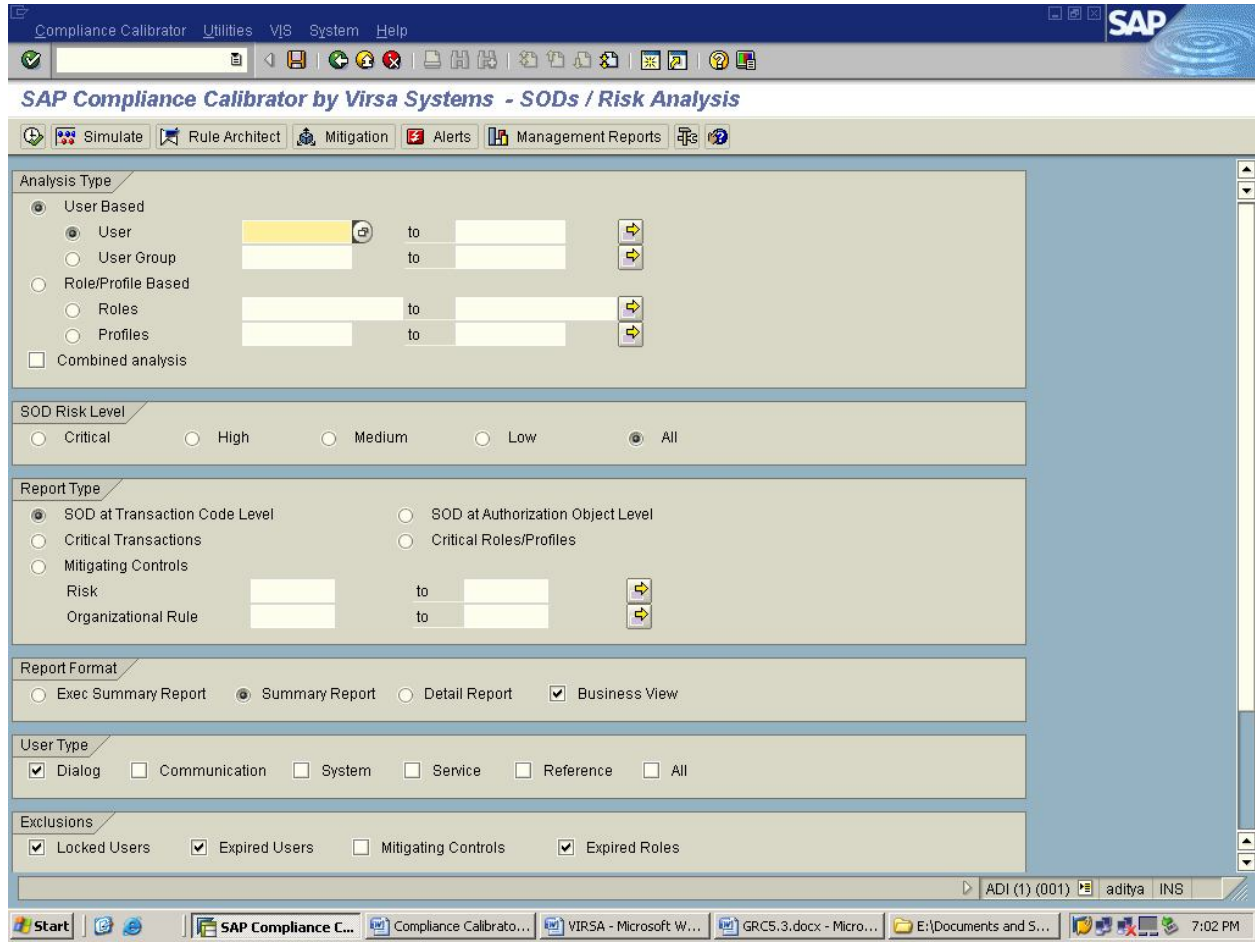
To Logon to VIRSA Compliance Calibrator, the Tcode is /n/virsa/zvrat



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

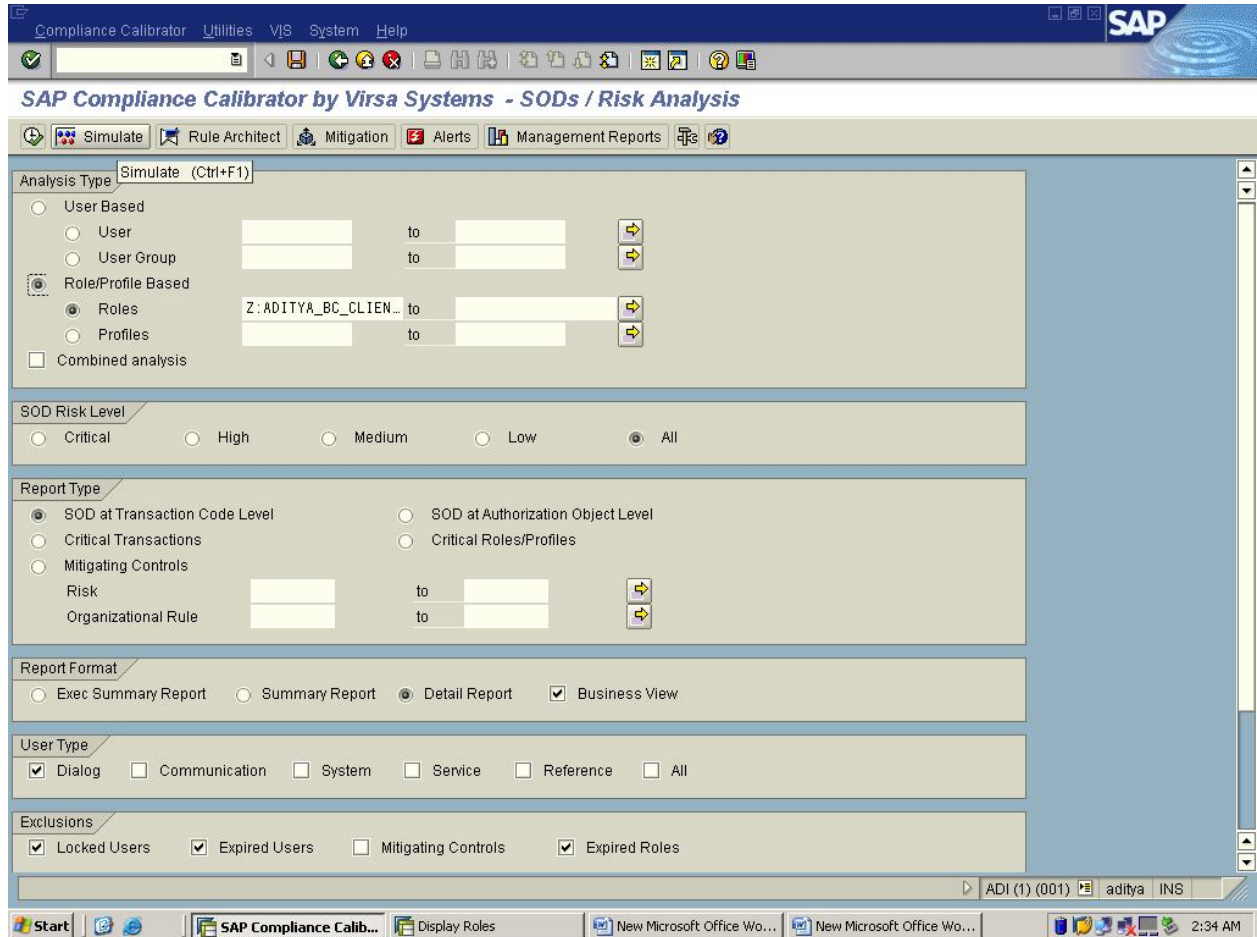
Select the Target System & Role then Click on Execute.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Now give the Role name and Click on Simulate Tab.



UNDER THE GUIDANCE OF  
RASHEED AHMED



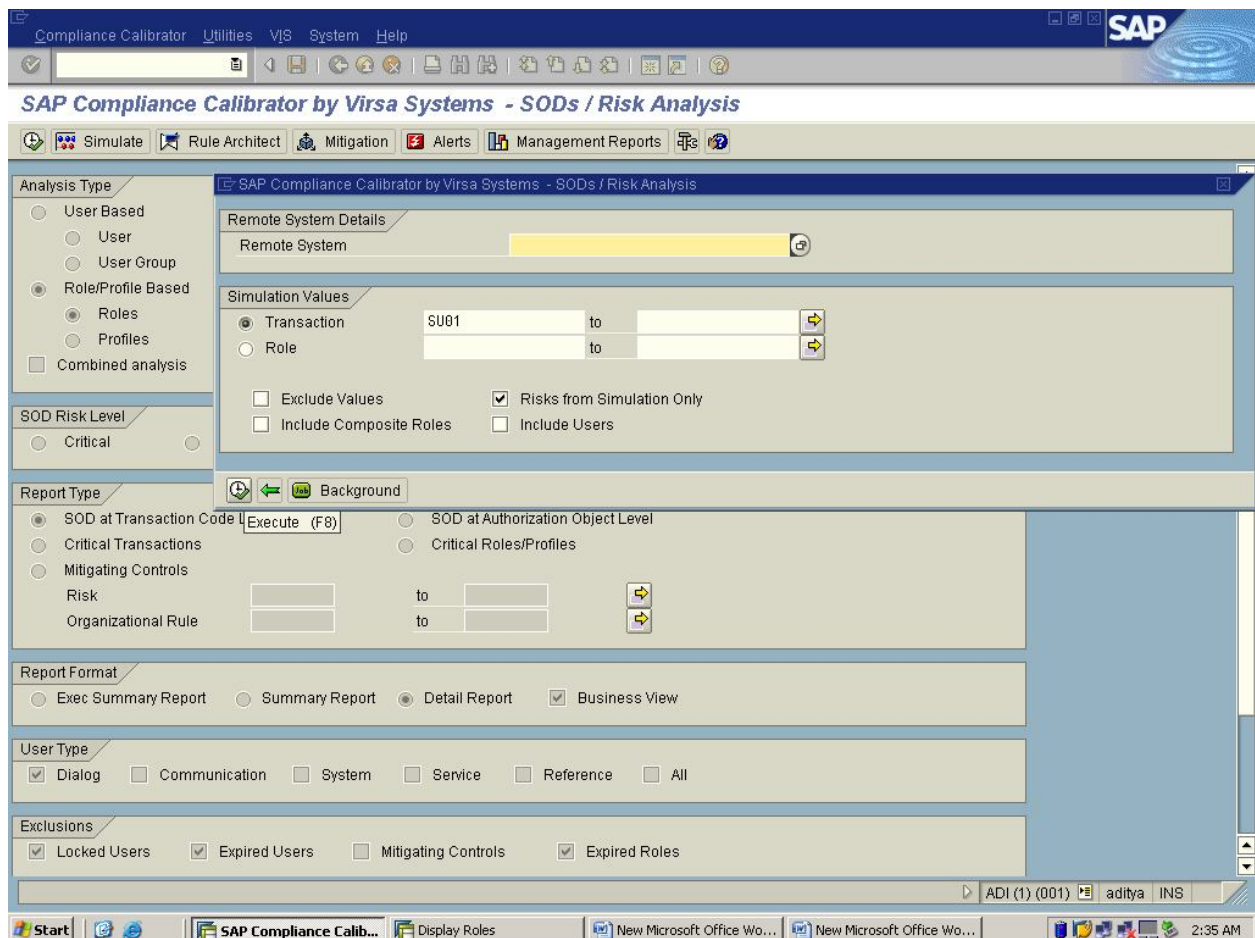
PREPARED BY  
ADITYA JOSYULA

Here Under the Simulation Values give the Transaction which you want to add.

Note: Leave the Remote System Details as blank.

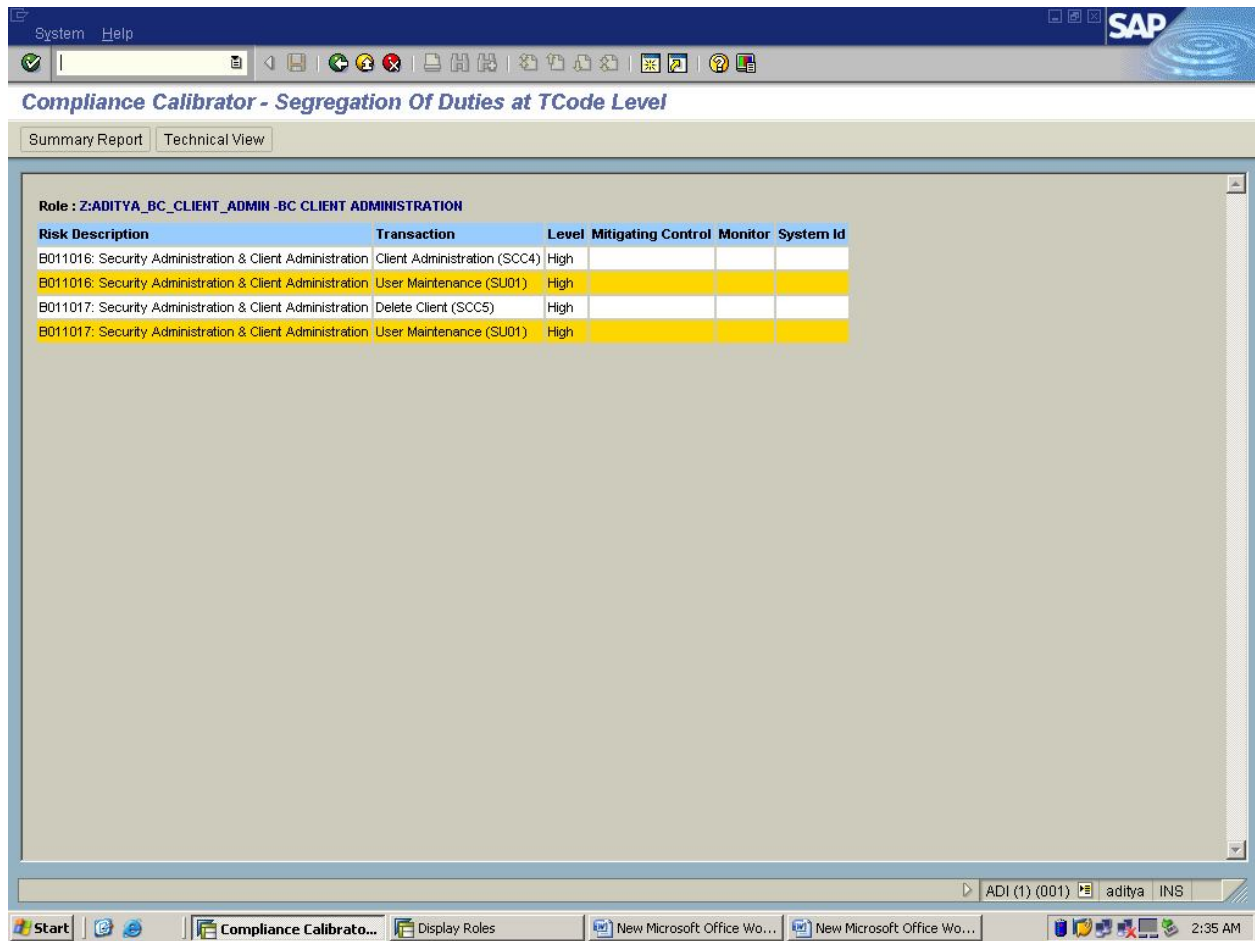
And check Risks from Simulation Only.

Then click on Execute.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



The screenshot displays the SAP Compliance Calibrator interface. The title bar reads "Compliance Calibrator - Segregation Of Duties at TCode Level". Below the title bar, there are tabs for "Summary Report" and "Technical View". The main content area shows a table for the role "Z:ADITYA\_BC\_CLIENT\_ADMIN -BC CLIENT ADMINISTRATION". The table has six columns: Risk Description, Transaction, Level, Mitigating Control, Monitor, and System Id. The data rows are as follows:

Risk Description	Transaction	Level	Mitigating Control	Monitor	System Id
B011016: Security Administration & Client Administration	Client Administration (SCC4)	High			
B011016: Security Administration & Client Administration	User Maintenance (SU01)	High			
B011017: Security Administration & Client Administration	Delete Client (SCC5)	High			
B011017: Security Administration & Client Administration	User Maintenance (SU01)	High			

Here the value which we have used is SU01 to the Role and its showing the risk in High Level.

So this clarifies the value which we have used shouldn't be assigned to the Role.

But if the business wants to allow this risk to the Role we can do it by using Mitigation Control Option.

UNDER THE GUIDANCE OF  
RASHEED AHMED

### Mitigation:

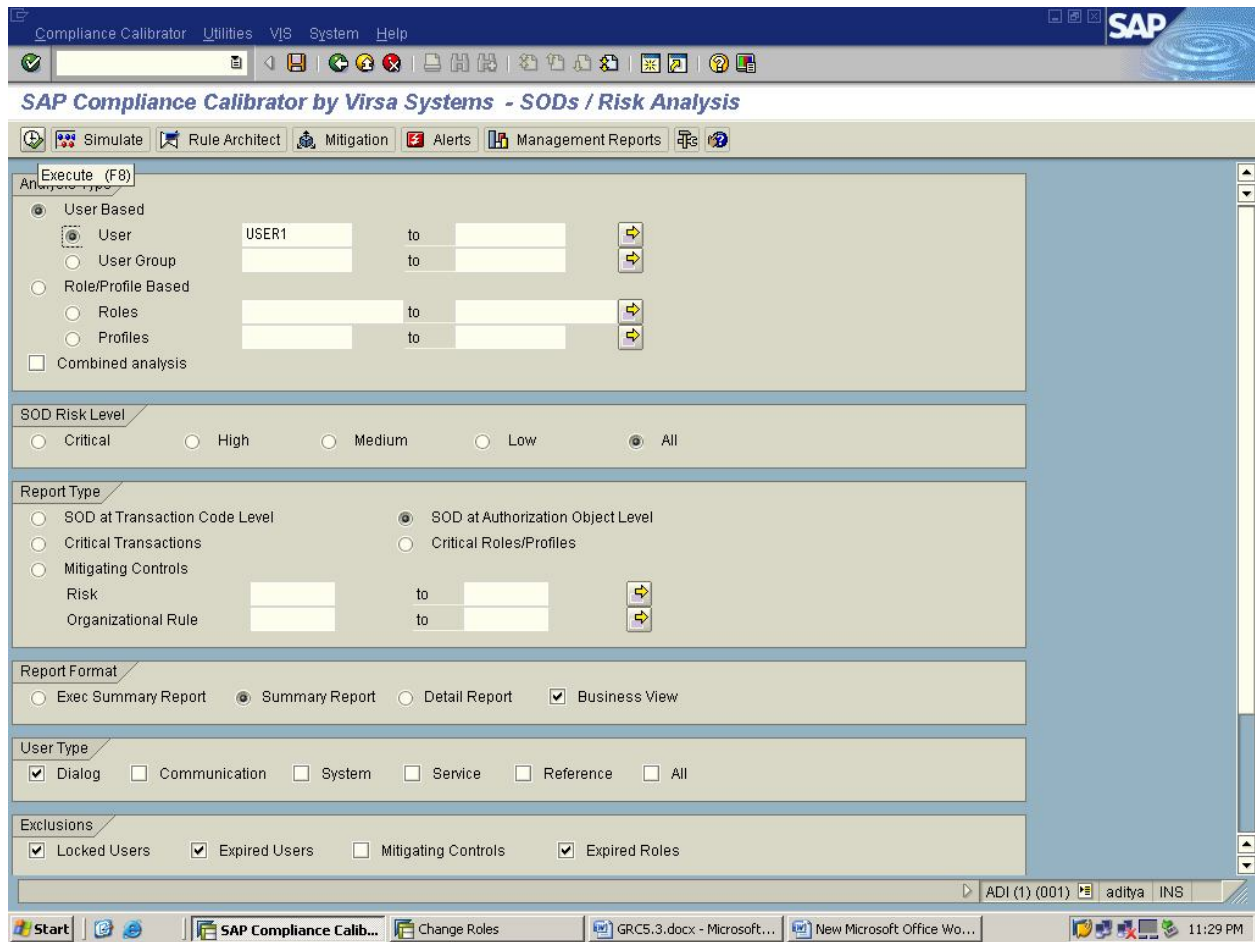
Allowing the risk by using or creating the Mitigation Control ID's as per the Business.

You can use Mitigation Controls to associate controls with the Risk, and assign them to Users, Roles, Profiles, or HR Objects.

Make individuals as Control Monitors or Approvers and then assign them to Controls.

### Steps for Creating Mitigation

Here we are creating a Mitigation Control for the below Screen Shot.



PREPARED BY  
ADITYA JOSYULA

The screenshot displays the SAP Compliance Calibrator interface for 'Segregation Of Duties at Object Level'. The user is identified as 'USER1 (USER1)'. The interface shows a table of conflicting transactions with the following data:

Conflicting Transactions	Risk Description	Level	Business Process	Mitigating Control	Monitor
Client Administration (SCC4) and User Maintenance ( SU01 )	B01101601: Security Administration & Client Administration	High	Basis		
Delete Client (SCC5) and User Maintenance ( SU01 )	B01101701: Security Administration & Client Administration	High	Basis		

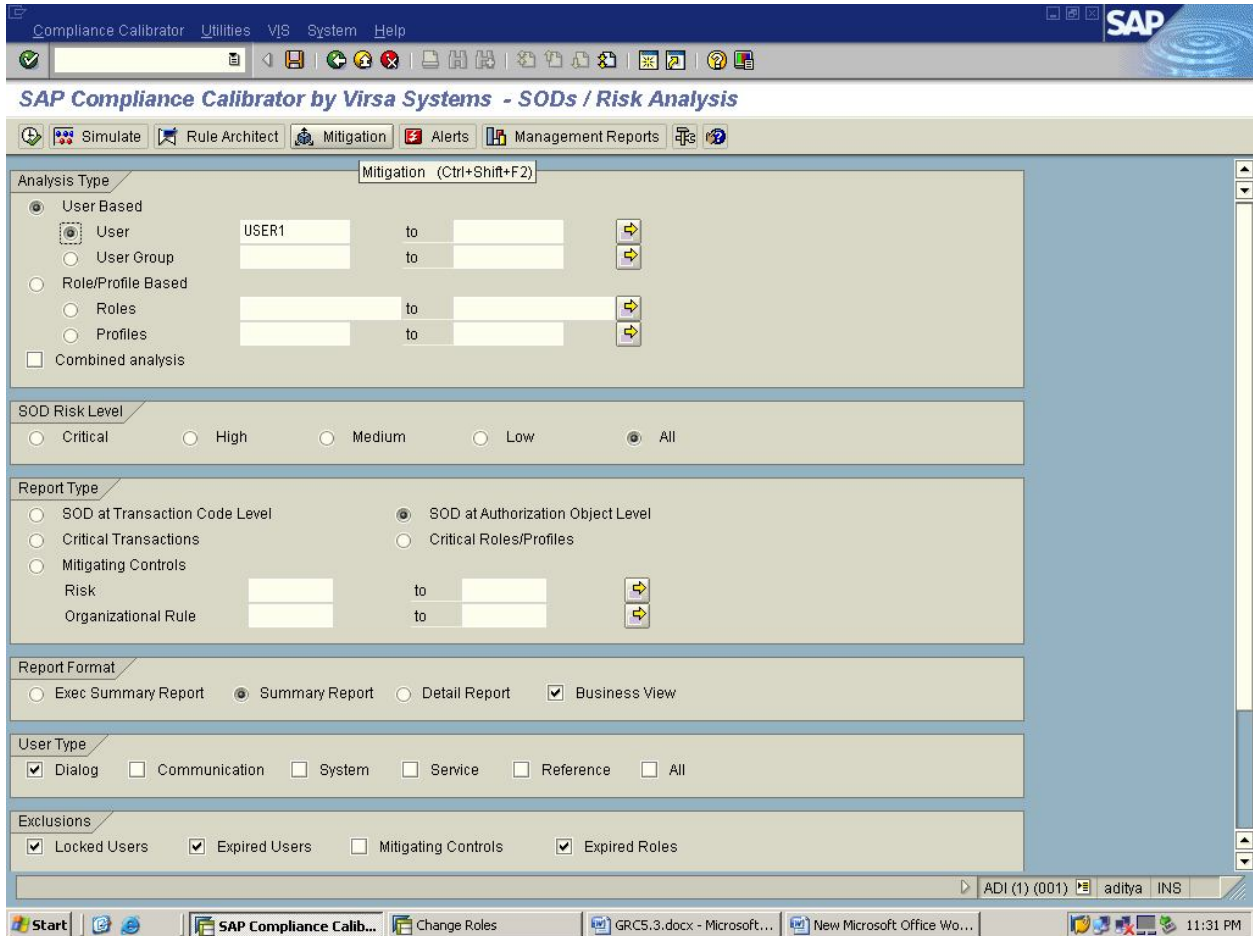
The taskbar at the bottom shows the Start button, several open applications including 'Compliance Calibrato...', 'Change Roles', 'GRC5.3.docx - Microsoft...', and 'New Microsoft Office Wo...', and the system clock showing 11:29 PM.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Now come back to Virsa screen & Click on Mitigation tab.

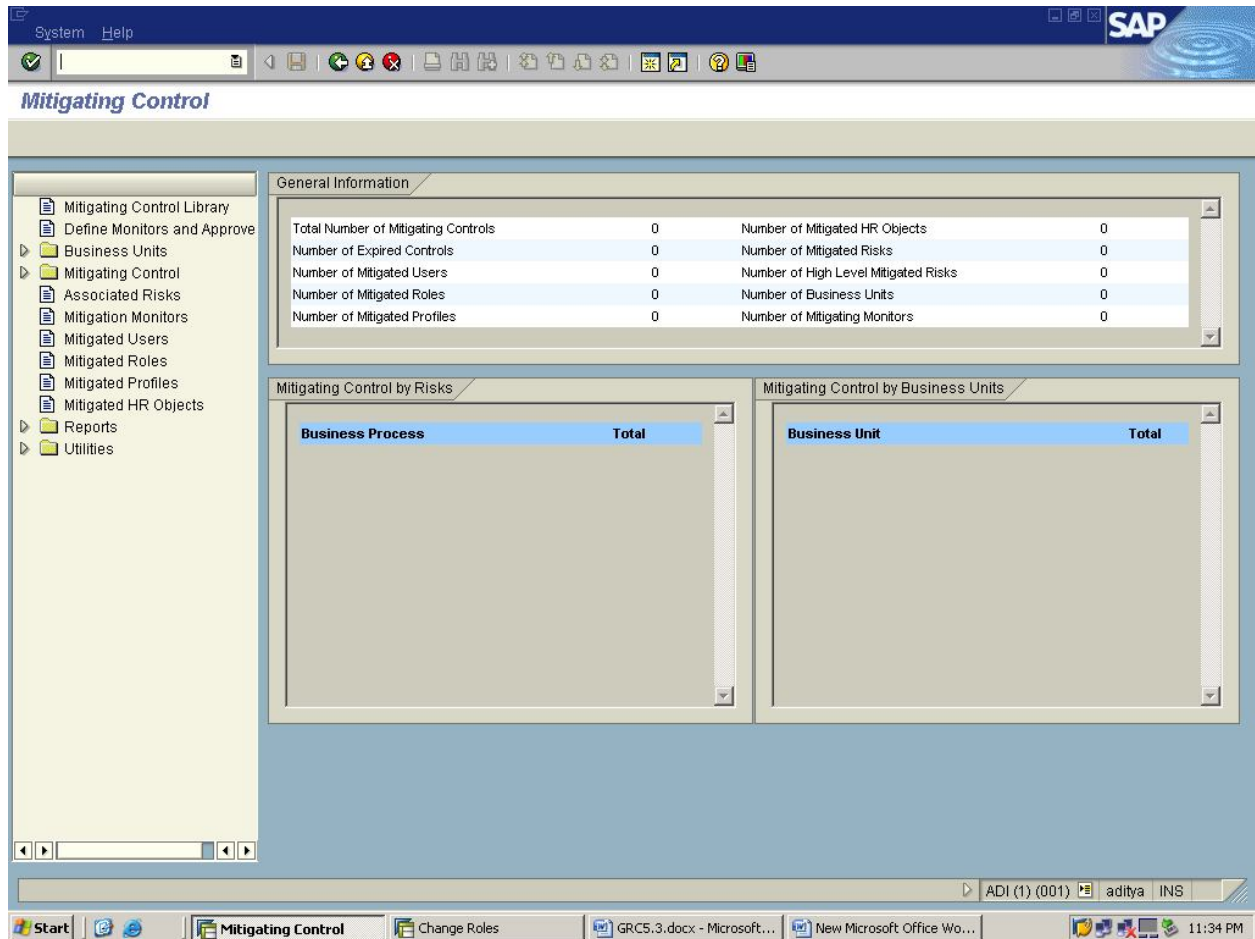
Check the below screen shot.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

After clicking the Mitigation tab you will get the below screen.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Here we have to create the Approvers, Monitors, Business Unit, Mitigating Control ID, Mitigated Users.

Check the below screen shot for the process.

STEP1:

In this Mitigation Screen we are going to create Approvers, Monitors.

Click on Define Monitors and Approvers

Check the below screen shots.



Version IT

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

The screenshot displays the SAP Mitigating Control interface. On the left is a navigation tree with the following items: Mitigating Control Library, Define Monitors and Approvers (highlighted), Business Units, Mitigating Control, Associated Risks, Mitigation Monitors, Mitigated Users, Mitigated Roles, Mitigated Profiles, Mitigated HR Objects, Reports, and Utilities. The main content area is divided into three sections:

- General Information:** A table showing summary statistics for various categories.
- Mitigating Control by Risks:** A table with columns for Business Process and Total.
- Mitigating Control by Business Units:** A table with columns for Business Unit and Total.

General Information			
Total Number of Mitigating Controls	0	Number of Mitigated HR Objects	0
Number of Expired Controls	0	Number of Mitigated Risks	0
Number of Mitigated Users	0	Number of High Level Mitigated Risks	0
Number of Mitigated Roles	0	Number of Business Units	0
Number of Mitigated Profiles	0	Number of Mitigating Monitors	0

Mitigating Control by Risks	
Business Process	Total

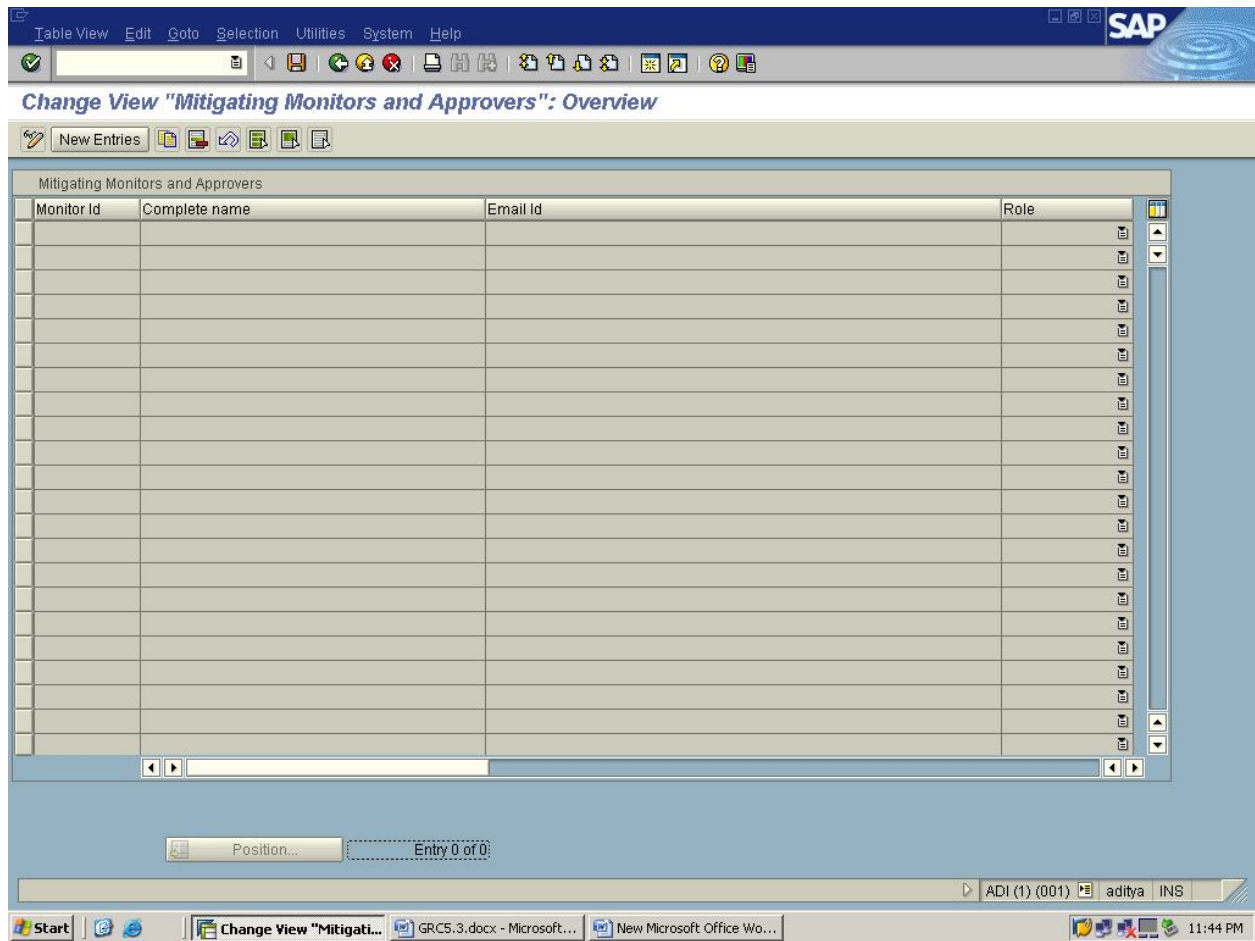
Mitigating Control by Business Units	
Business Unit	Total

The bottom of the screenshot shows the Windows taskbar with the Start button, several open applications (Mitigating Control, User Maintenance: Initial..., GRC5.3.docx - Microsoft..., New Microsoft Office Wo...), and the system tray displaying the user 'aditya' and the time '11:43 PM'.

UNDER THE GUIDANCE OF  
RASHEED AHMED



PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on New Entries and mention the Monitor ID, Company Name, Email, Role.

Here in Role option we need to select either Approver or Monitor.

Here we are creating Approver & Monitor at a time.

After that click on Save.

Check the below Screen Shot.

The screenshot displays the SAP Change View for 'Mitigating Monitors and Approvers'. The window title is 'Change View "Mitigating Monitors and Approvers": Overview'. The main area contains a table with the following data:

Monitor Id	Complete name	Email Id	Role
ADDY	Addy	addy@gmail.com	Monitor
ADITYA	Aditya	aditya@gmail.com	Approver

The interface also shows a 'New Entries' button, a 'Position...' button, and a status bar indicating 'Data already saved' and 'Entry 1 of 2'. The taskbar at the bottom shows the Start button and several open applications, including 'Change View "Mitigati...', 'GRC5.3.docx - Microsoft...', and 'New Microsoft Office Wo...'. The system clock shows 11:49 PM.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

**STEP2:**

Business Unit is based upon Business Processes for Functions Identification. Here Business Unit ID is a unique ID which was picked by our own.

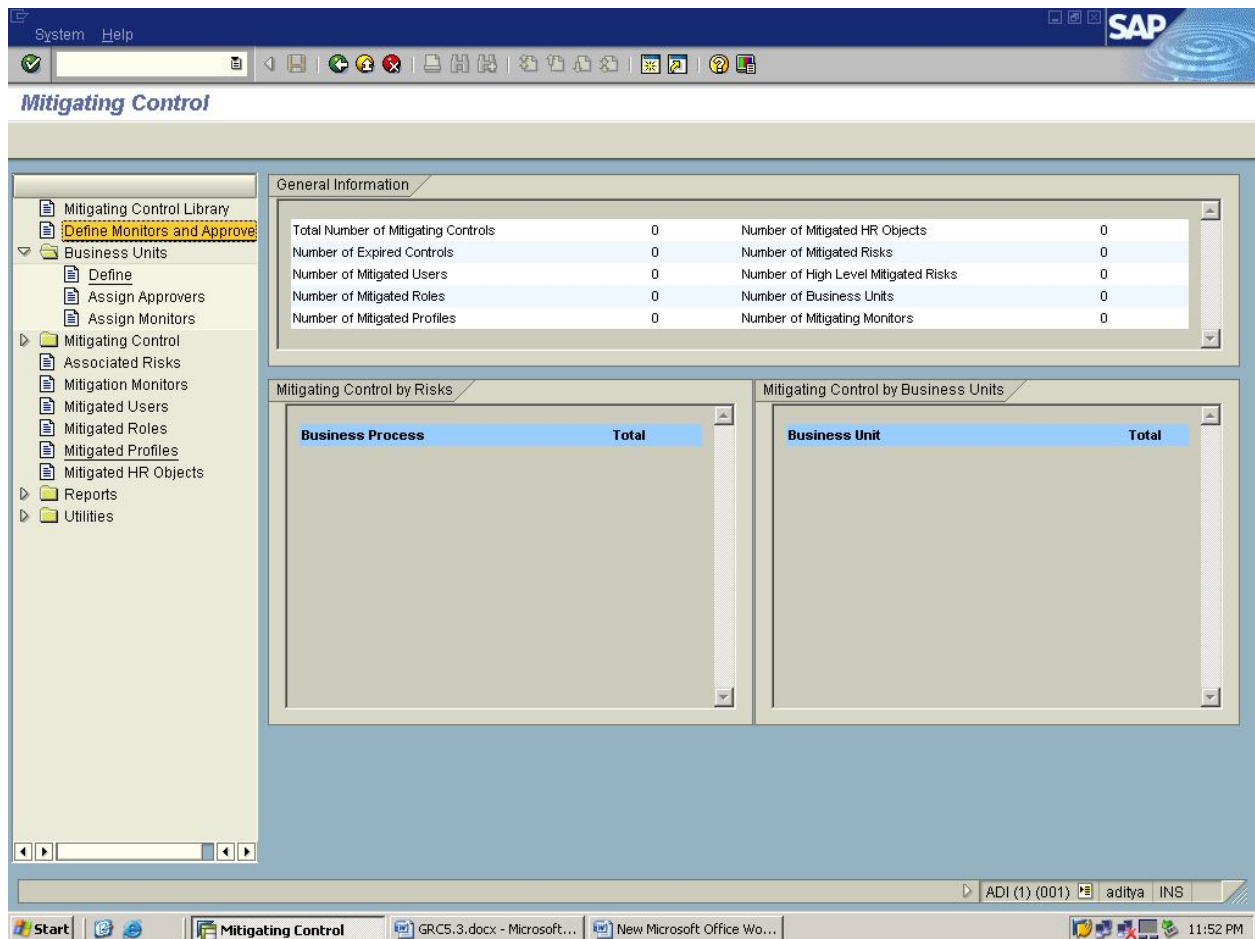
EX:B100

Goto Business Units → Click on Define → Click on New Entries.

→ Give the Business ID, Description.

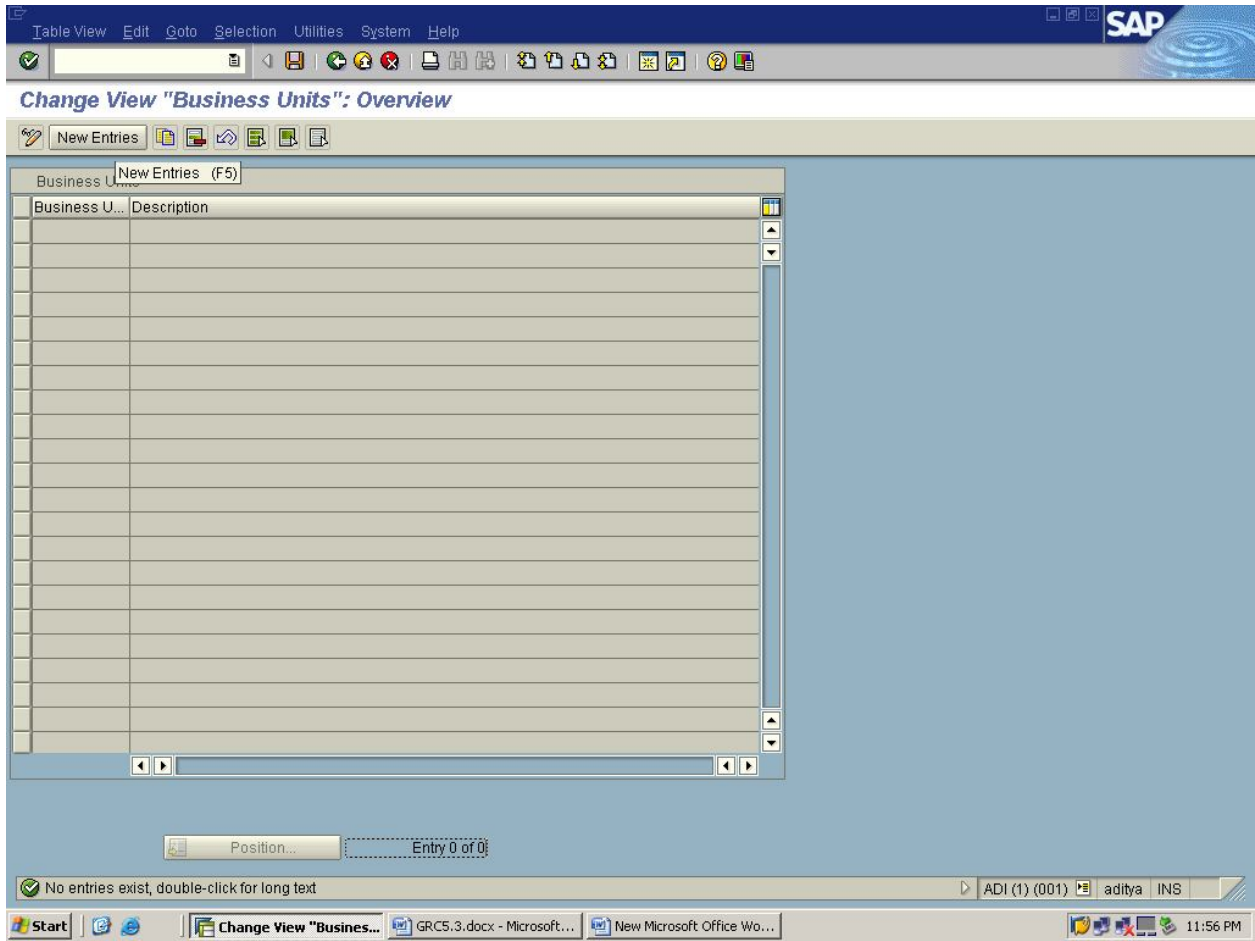
→ Click on Save.

Check the below screen shots



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED



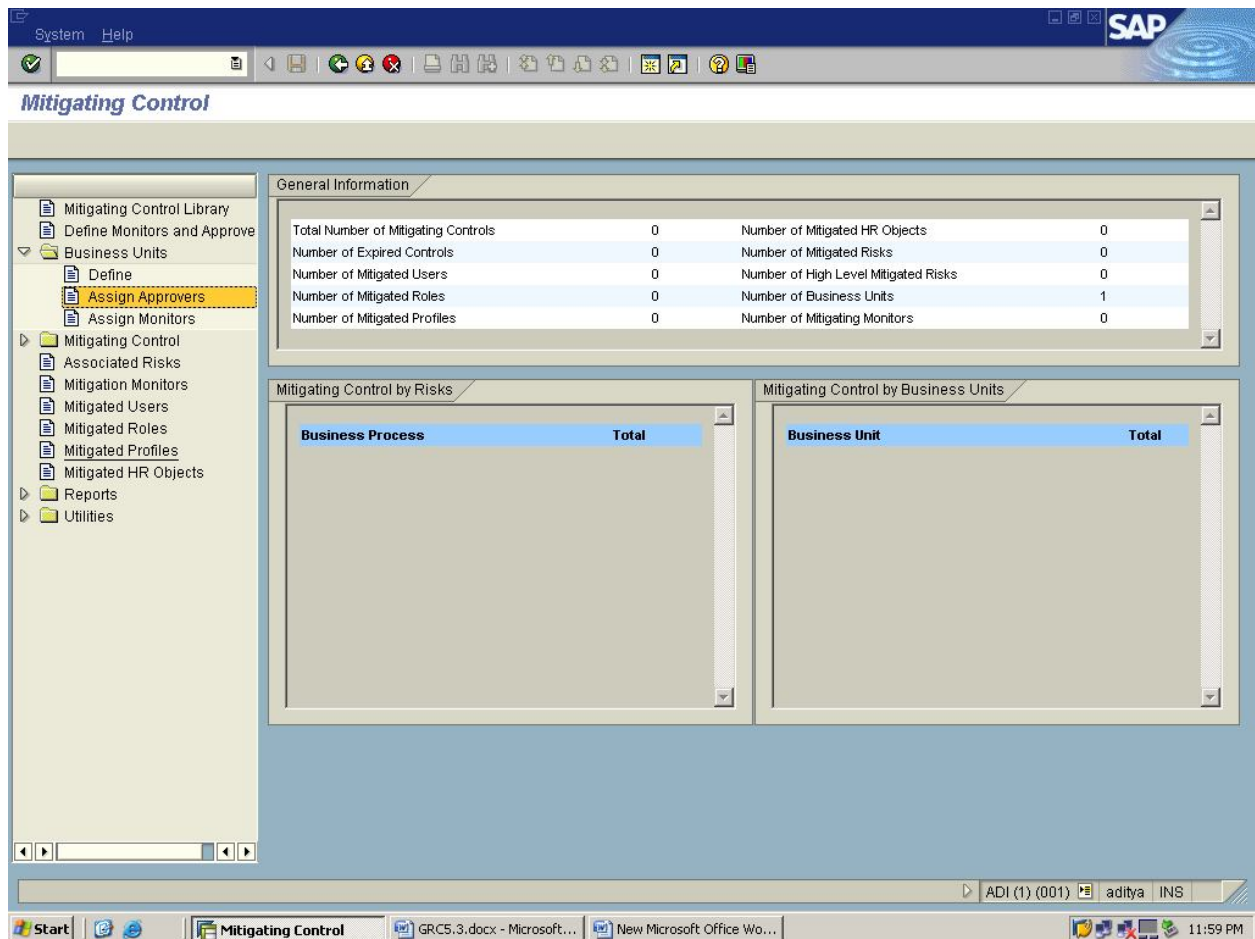
PREPARED BY  
ADITYA JOSYULA

Again Goto Business Units → Click on Assign Approvers → Click on New Entries.

→ Give the Business Unit ID and mention the Approver ID.

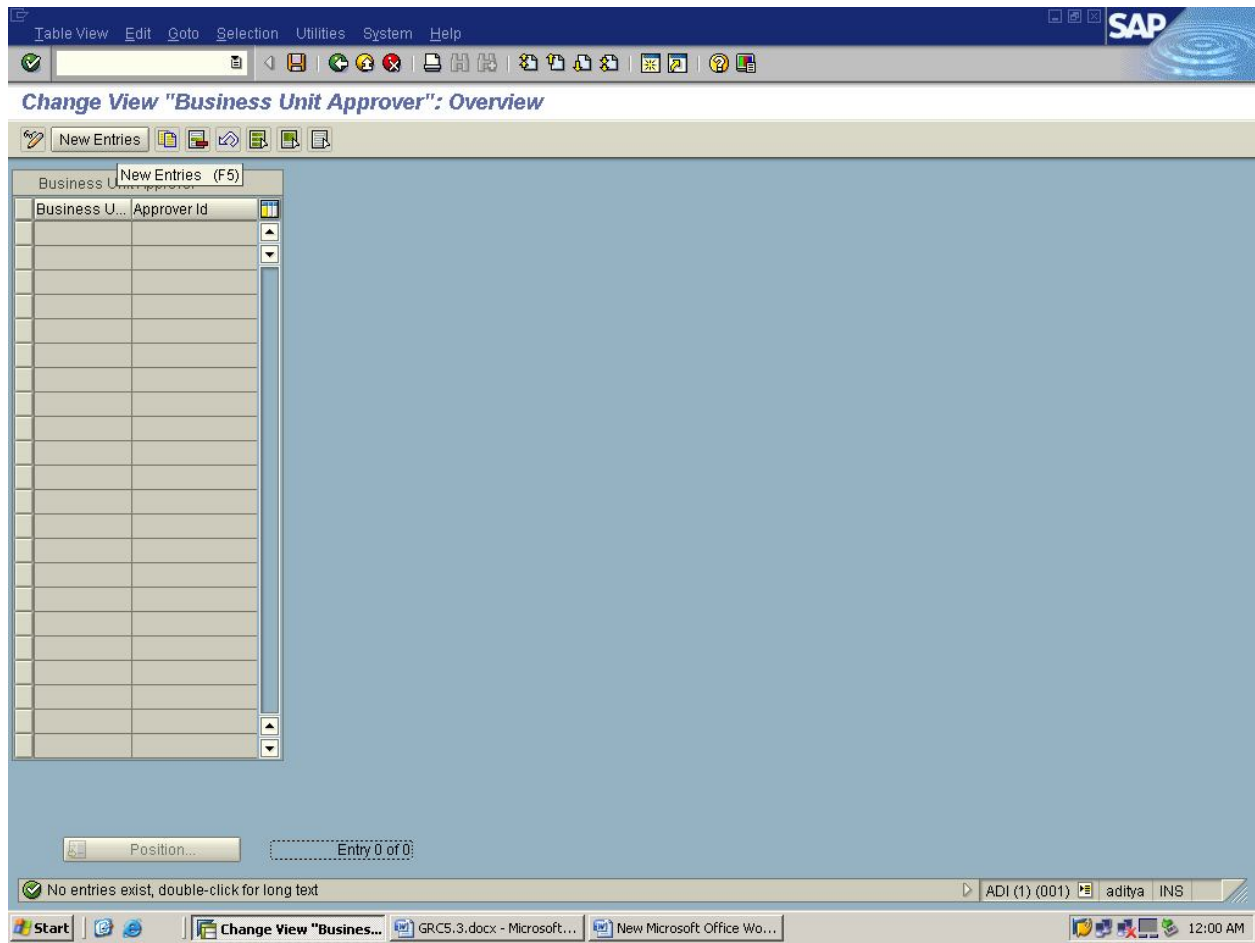
→ Click on Save.

Check the below screen shots



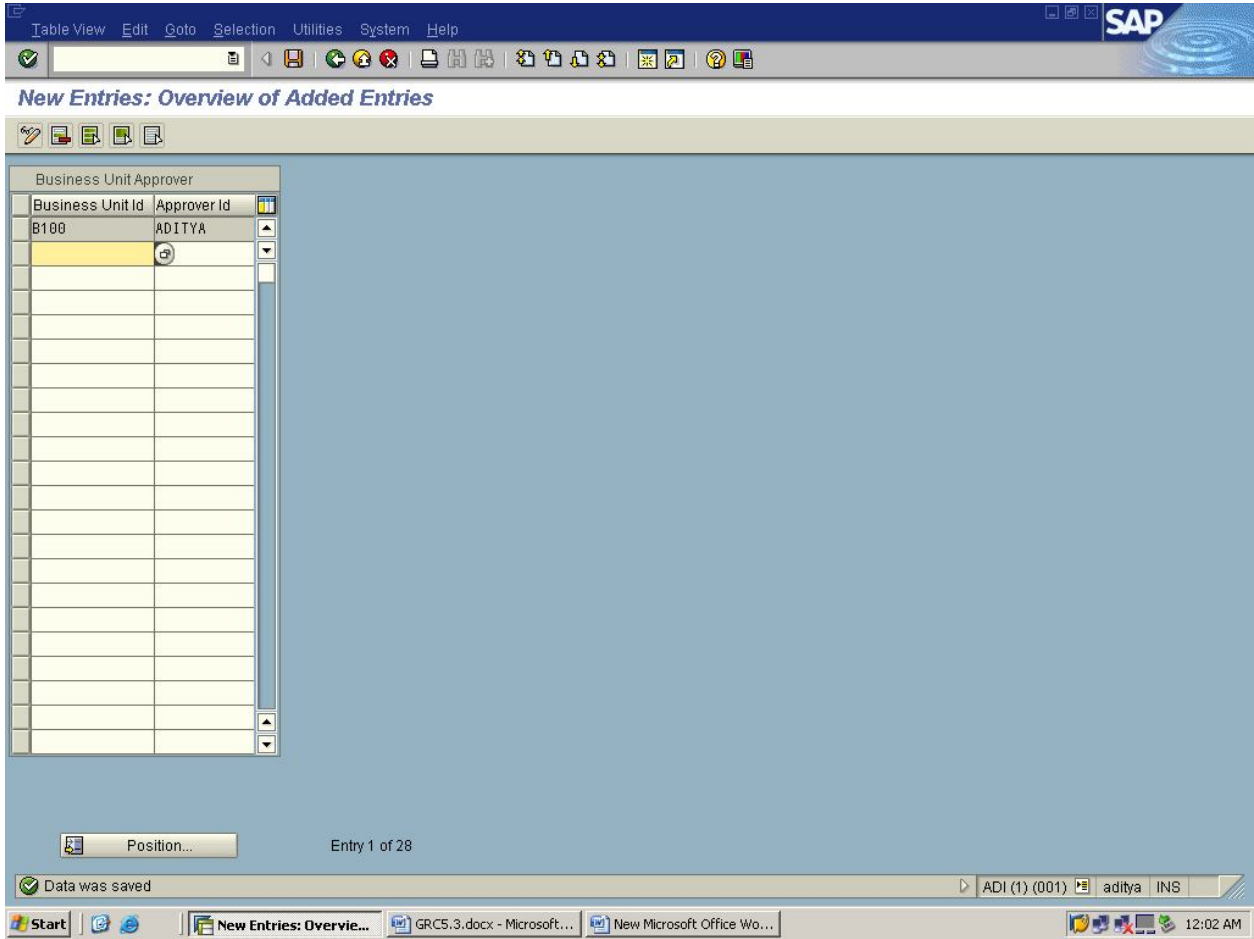
UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED



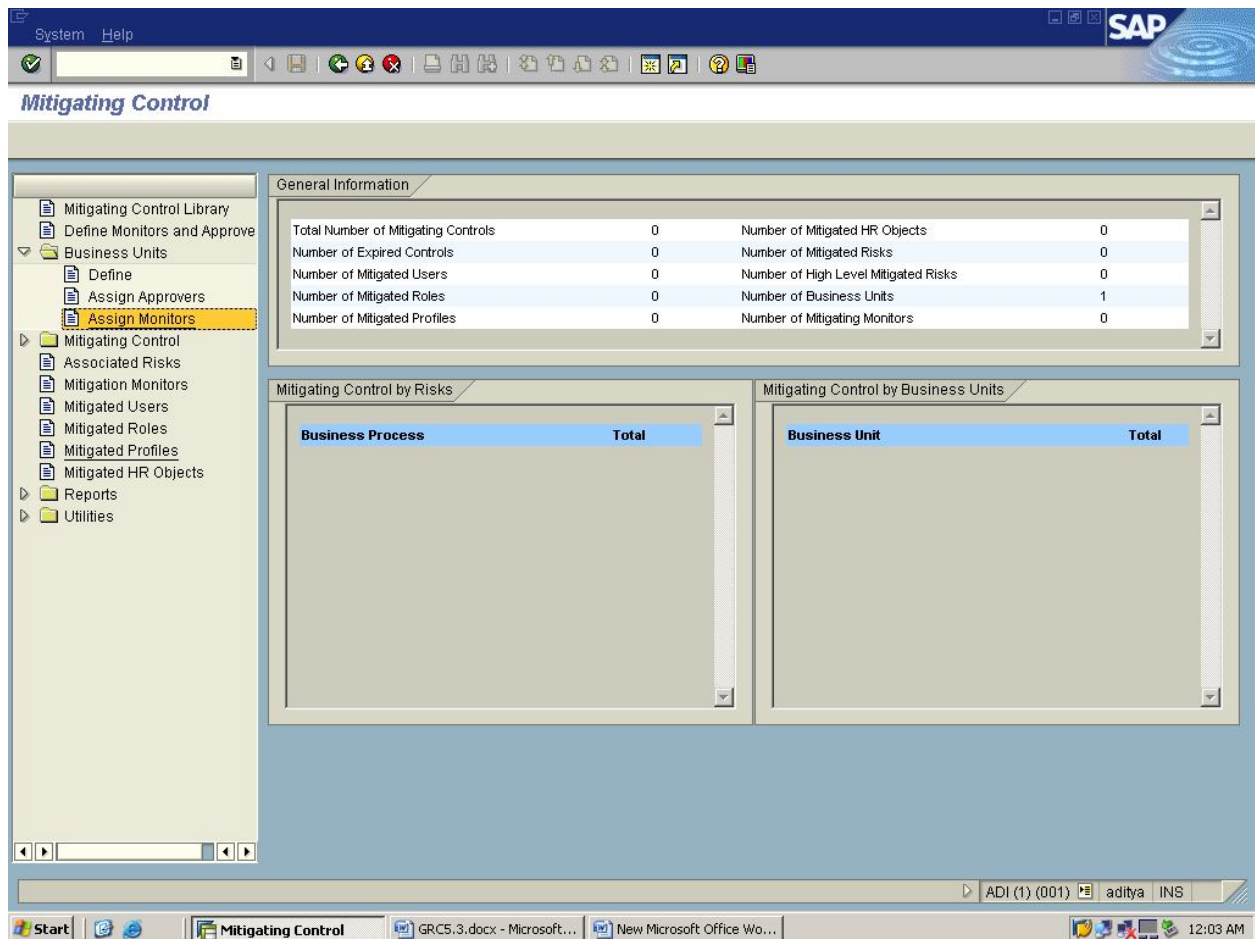
PREPARED BY  
ADITYA JOSYULA

Again Goto Business Units → Click on Assign Monitors → Click on New Entries.

→ Give the Business Unit ID and mention the Monitor ID.

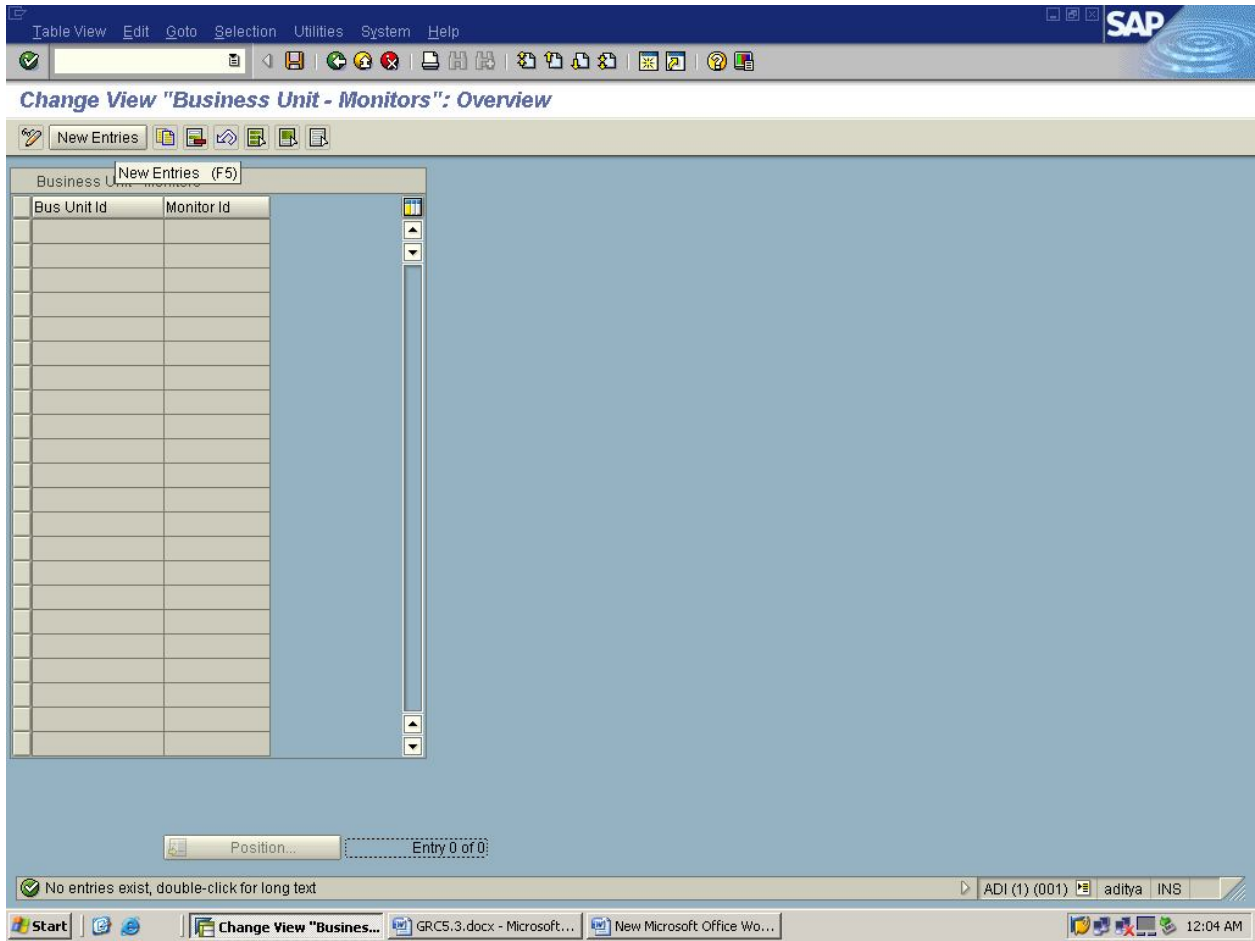
→ Click on Save.

Check the below screen shots



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED



PREPARED BY  
ADITYA JOSYULA

STEP3:

Mitigating Controls is based upon Risk IDs for Identification. Here Mitigating Control ID is a unique ID which was picked by our own.

EX:B200

Goto Mitigating Controls → Click on Create → then fill the required details.

→ Give the Mitigating Control ID, Description, Business Unit, Management Approver.

→ **Add the Associated Risk ID & Monitor.**

→ **Click on Save.**

Check the below screen shots.



Version IT

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

The screenshot displays the SAP Mitigating Control interface. On the left is a navigation tree with the following items: Mitigating Control Library, Define Monitors and Approve, Business Units, Mitigating Control (expanded to show Create and Display/Change), Associated Risks, Mitigation Monitors, Mitigated Users, Mitigated Roles, Mitigated Profiles, Mitigated HR Objects, Reports, and Utilities. The main area is divided into three sections:

- General Information:** A table with two columns of metrics and their values.
- Mitigating Control by Risks:** A table with columns for Business Process and Total.
- Mitigating Control by Business Units:** A table with columns for Business Unit and Total.

The bottom of the window shows the SAP taskbar with the user 'aditya' in role 'INS' and the system ID 'ADI (1) (001)'. The Windows taskbar at the very bottom shows the Start button, the Mitigating Control application icon, and other open applications like 'GRC5.3.docx - Microsoft...' and 'New Microsoft Office Wo...'. The system clock shows 12:07 AM.

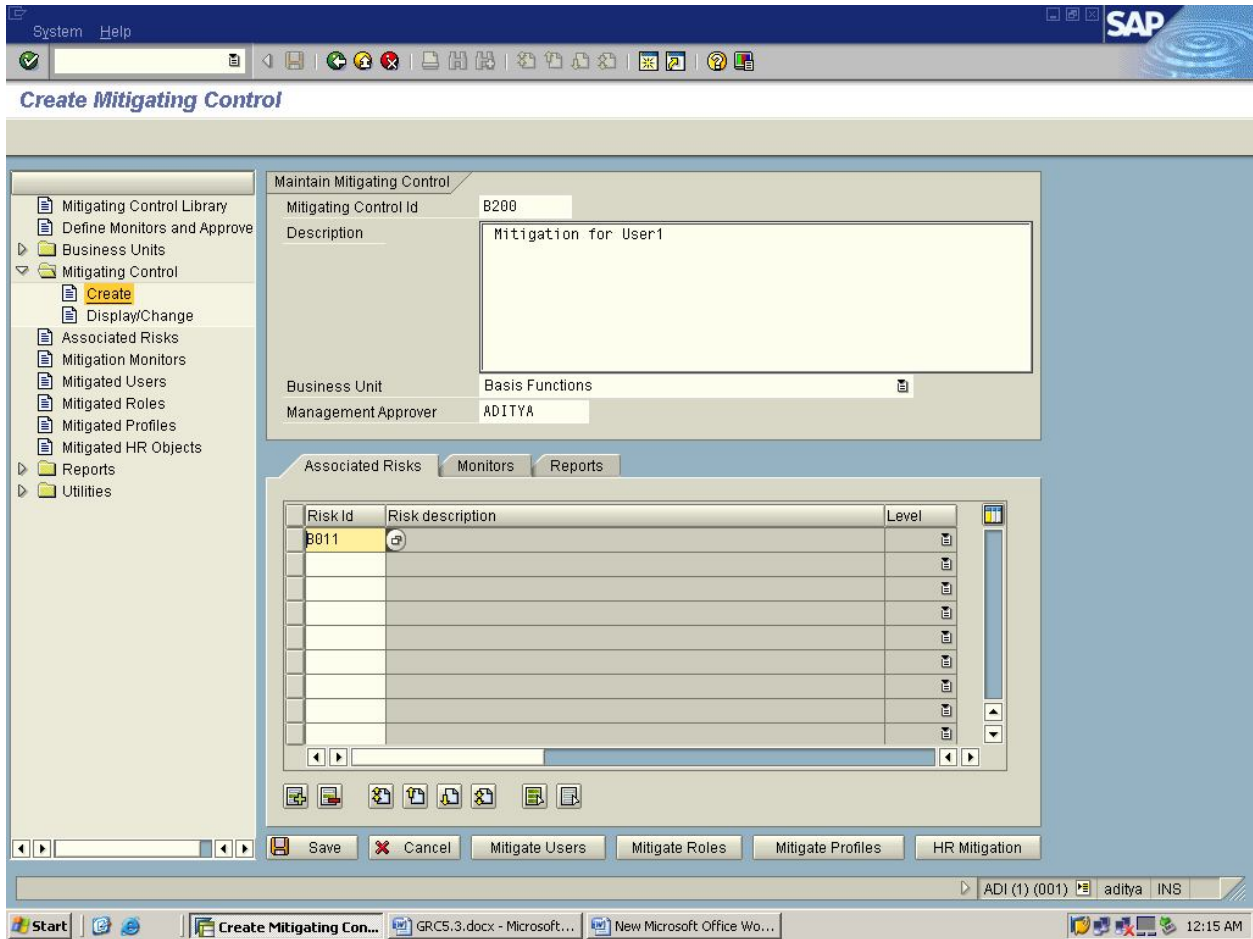
Metric	Value	Metric	Value
Total Number of Mitigating Controls	0	Number of Mitigated HR Objects	0
Number of Expired Controls	0	Number of Mitigated Risks	0
Number of Mitigated Users	0	Number of High Level Mitigated Risks	0
Number of Mitigated Roles	0	Number of Business Units	1
Number of Mitigated Profiles	0	Number of Mitigating Monitors	0

Business Process	Total
------------------	-------

Business Unit	Total
---------------	-------

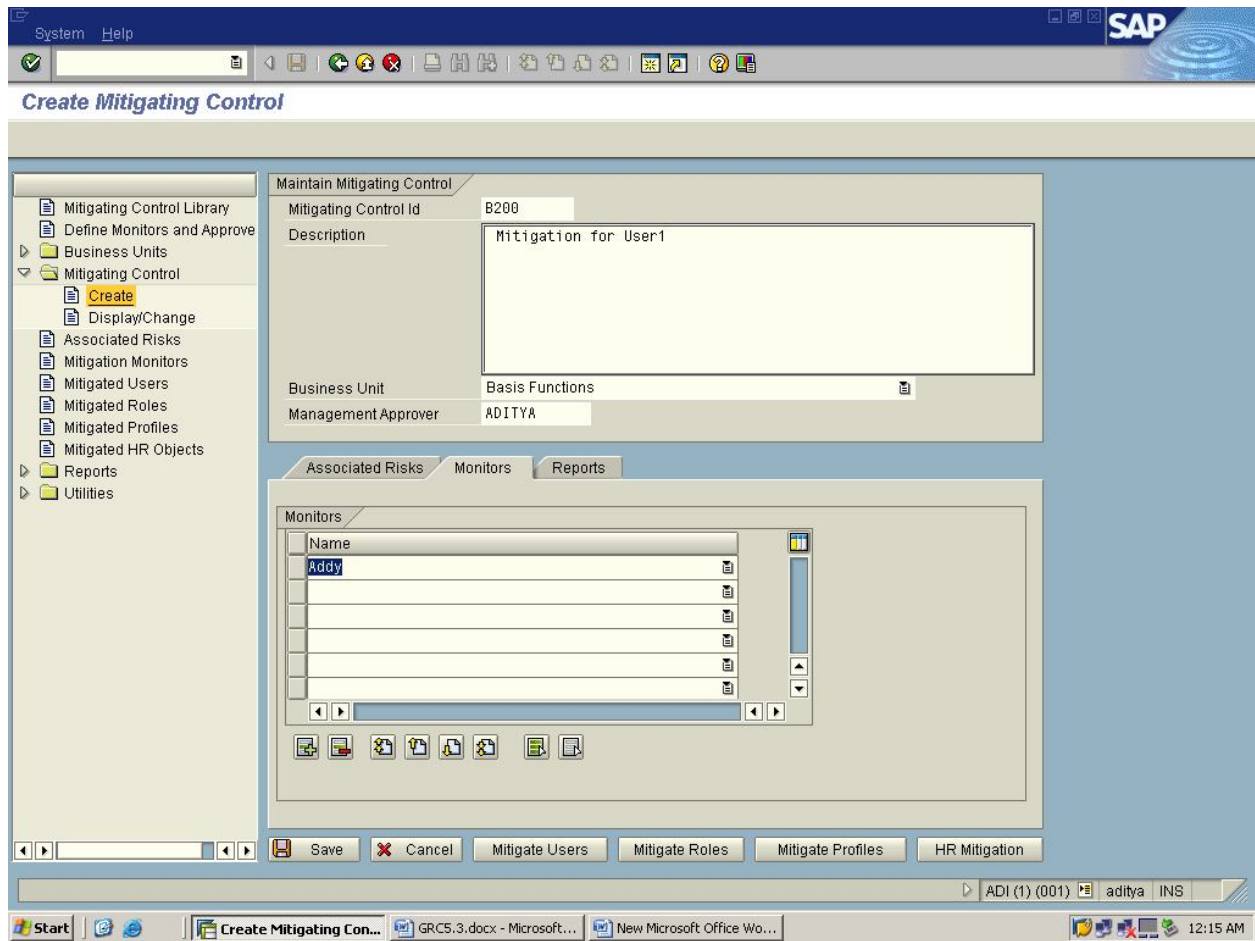
UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED

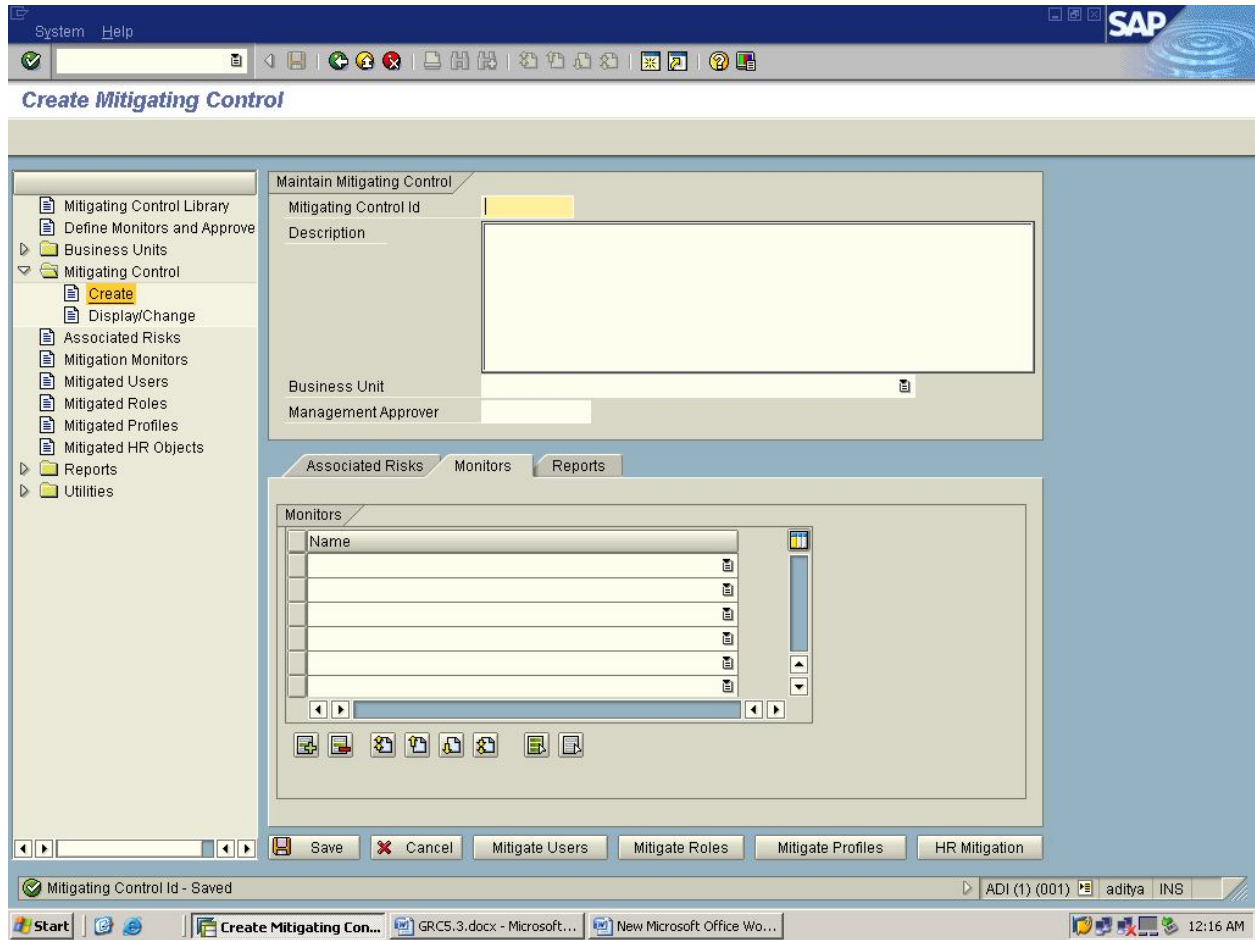
PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Then click on Save.



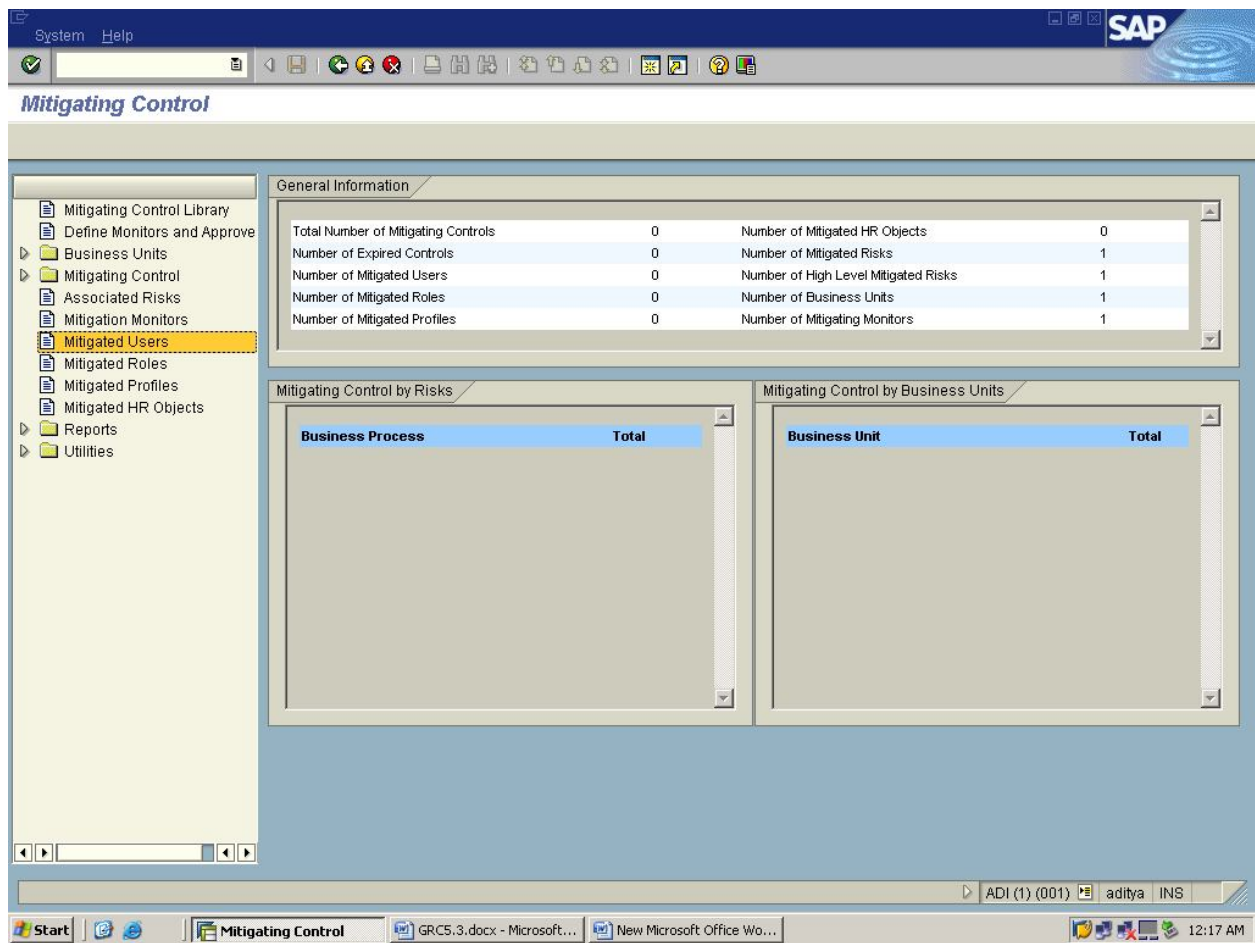
UNDER THE GUIDANCE OF  
RASHEED AHMED



STEP4:

Mitigated Users is used for assigning the Mitigating Control ID's to the User to allow the Risk.

Goto Mitigated Users



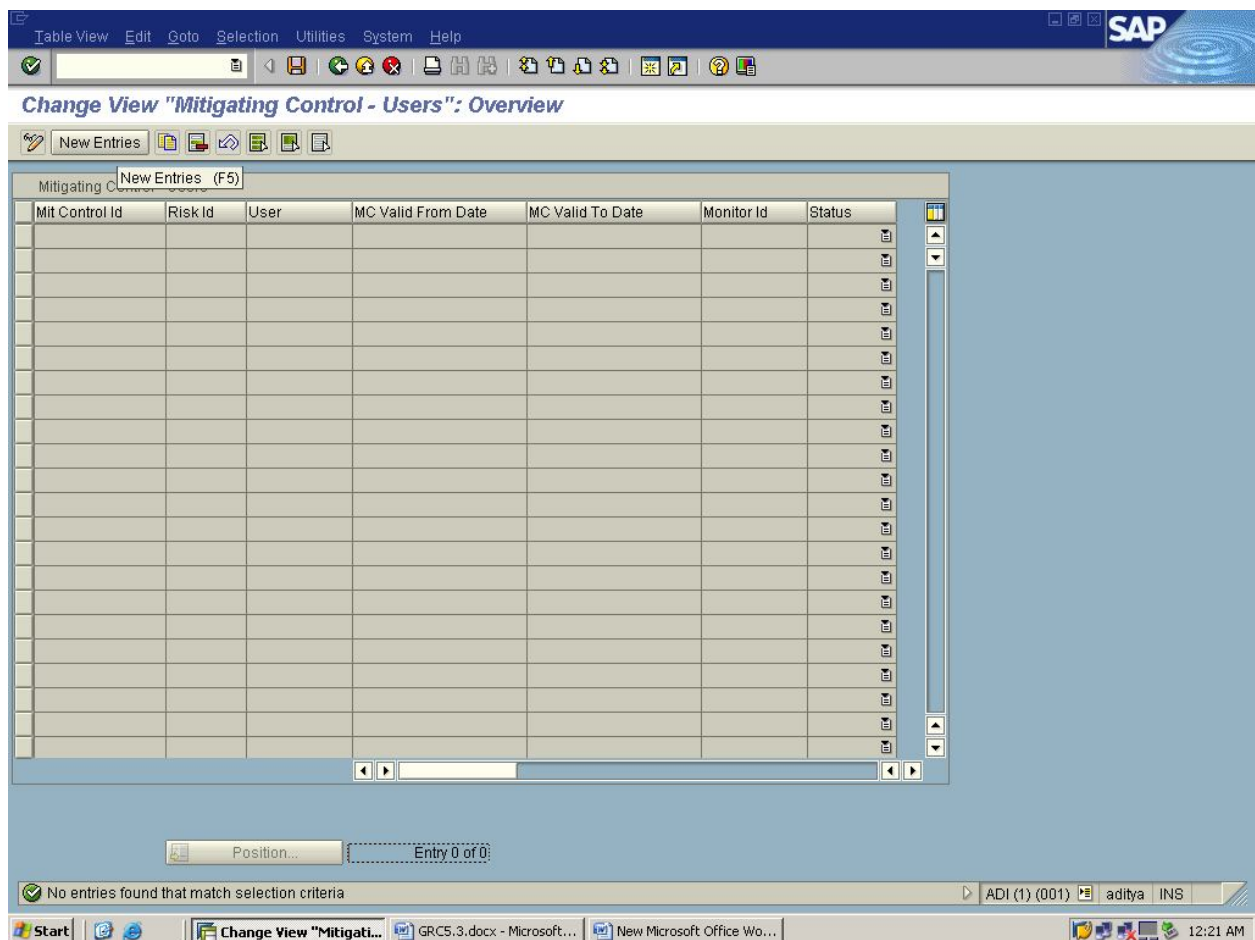
PREPARED BY  
ADITYA JOSYULA

Click on New Entries. Then give the Mitigating Control ID, User, Risk ID, Mitigation Validity & Monitor ID.

Here we need to give the Risk ID-B011 Manually because the Risk ID for the both violations is the same.

Click on Save.

Check the below screen shots.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

The screenshot displays the SAP Change View interface for 'Mitigating Control - Users'. The window title is 'Change View "Mitigating Control - Users": Overview'. The main area contains a table with the following data:

Mit Control Id	Risk Id	User	MC Valid From Date	MC Valid To Date	Monitor Id	Status
B200	B011	USER1	09.10.2013	29.11.2013	ADDY	Enable

Below the table, there is a 'Position...' button and the text 'Entry 1 of 1'. The status bar at the bottom indicates 'Data already saved' and shows the user 'aditya' in the 'INS' role. The taskbar at the very bottom shows the Start button and several open applications, including 'GRC5.3.docx - Microsoft...', 'New Microsoft Office Wo...', and 'Change View "Mitigati...'.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Now come back to Virsa screen and find out the Risk to that User ID:USER1

In Analysis Type, Under User Based Select the User and Mention the User name

→In SOD Risk Level, select the option level ALL

→Select the Report Type which you want to perform, Here we are using SOD at Transaction Code Level

→Select the Report Format

→Select the User Type .

→In Exclusions Tab, Check the Locked Users, Expired Users, Mitigating Controls, Expired Roles.

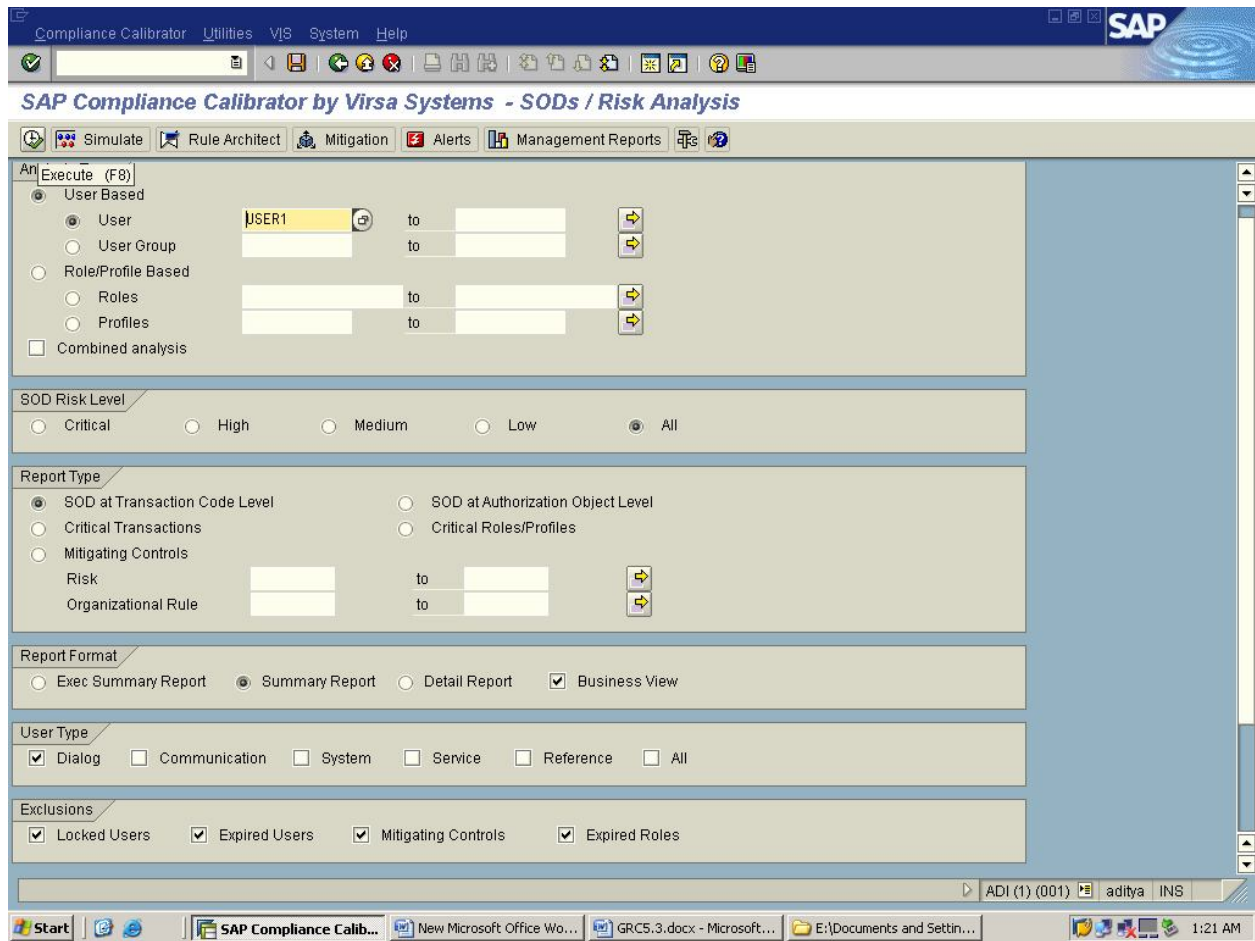
Check the below Screen Shot



Version IT

UNDER THE GUIDANCE OF  
RASHEED AHMED

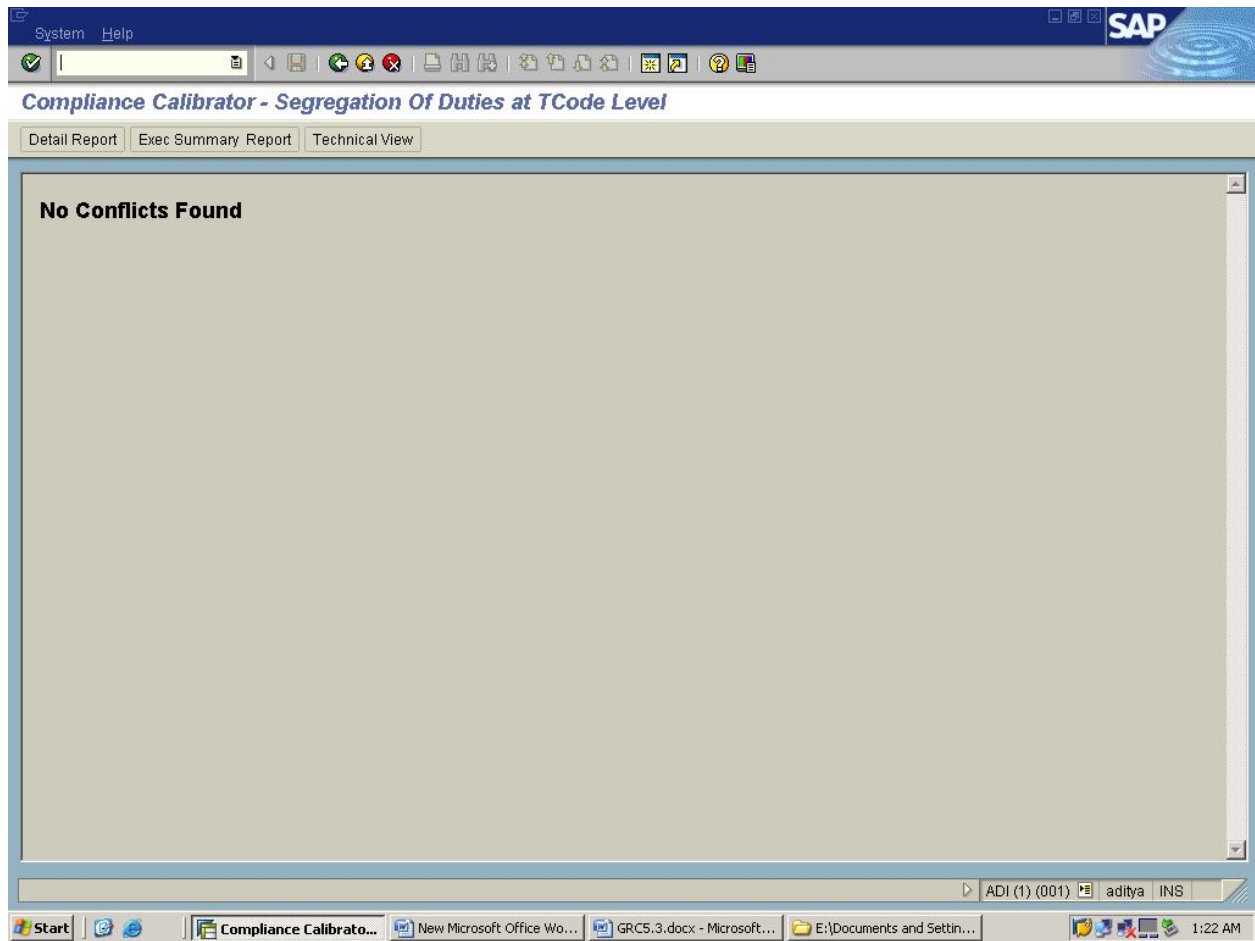
PREPARED BY  
ADITYA JOSYULA



Click on Execute

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



Now you won't find any Violations.

UNDER THE GUIDANCE OF  
RASHEED AHMED

## GRC5.3 (Governance Risk Compliance)

### **Overview:**

Being closely related concerns, governance, risk and compliance activities are increasingly being integrated and aligned to some extent in order to avoid conflicts, wasteful overlaps and gaps. While interpreted differently in various organizations, GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.

Governance, risk, and compliance or GRC are increasingly recognized terms that reflect a new way in which organizations are adopting an integrated approach to these aspects of their business.

The following are the major advantages of GRC:

1. To increase Risk awareness and resulting in better decision making.
2. Improved visibility of risk, exposure across the organization.
3. Reduced risk of reaching segregation of duties violations.
4. Simplified Compliance, minimise Audit time & Cost.

The Components of GRC5.3 are:

1. Access Control (AC)
2. Process Control (PC)
3. Global Trade System (GTS)
4. Environmental Health & Safety (EHS)
5. Risk Management (RM)

### **Access Control:**

With a built-in list of critical transactions and a matrix of segregation of duties conflicts, SAP GRC Access Control lets you check if user or role maintenance introduces risks to your business. It also lets you record the steps you take to mitigate those risks.

SAP GRC Access Control consists of the following modules:

- Risk Analysis and Remediation (RAR)
- Compliant User Provisioning (CUP)
- Superuser Privilege Management (SPM)
- Enterprise Role Management (ERM)

#### **Risk Analysis and Remediation (RAR)**

Previously known as Compliance Calibrator, RAR is the repository for definitions of segregation of duties rules and critical transactions. As well as using the rules to check if user and role administration activities could introduce risks to your business, RAR reports on the risks within the system – presenting them in a graphical format within a web browser.

#### **Compliant User Provisioning (CUP)**

CUP provides the workflow engine to drive compliant user and role maintenance processes within the SAP environment. These processes are auditable and verifiable, with clear, configurable processes for approval, SoD checking and provisioning.

#### **Enterprise Role Management (ERM)**

ERM rigorously applies naming conventions and validations to role creation, reducing management effort and the risk of segregation of duties violations. To use ERM you have to define structured working methods.



PREPARED BY  
ADITYA JOSYULA

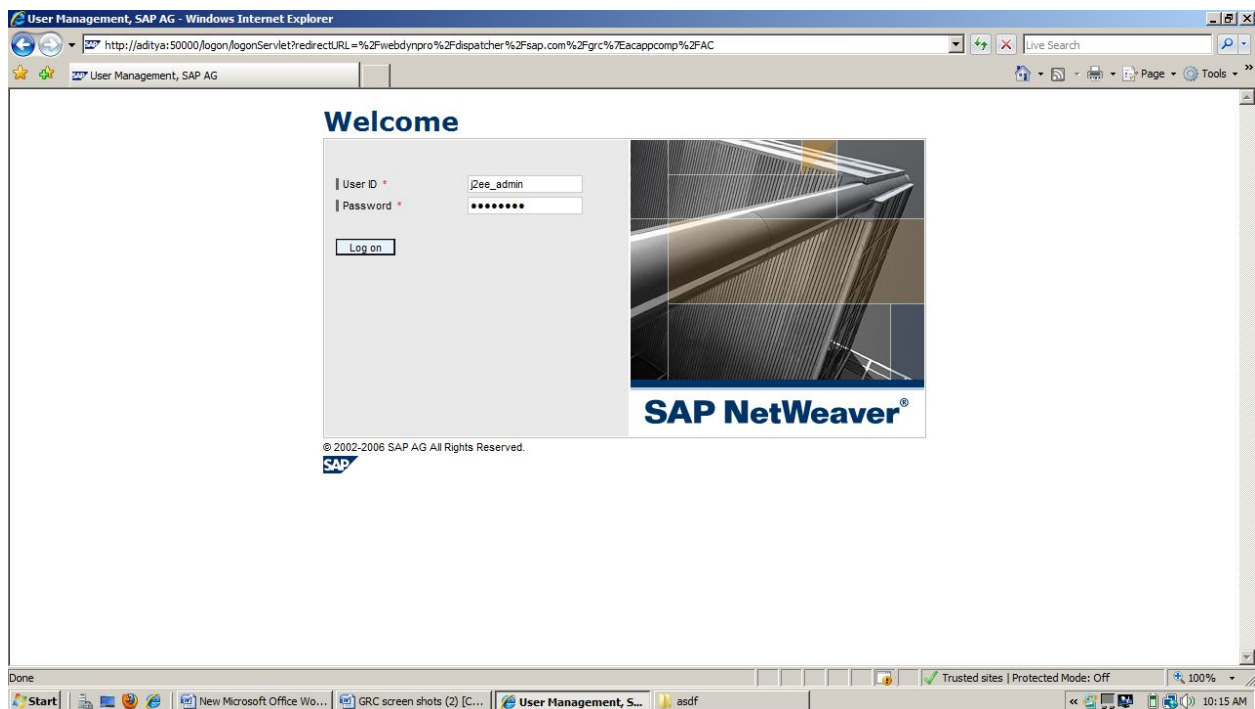
## Superuser Privilege Management (SPM)

Previously known as Firefighter, SPM lets you assign 'emergency user' status to normal support users, giving them extended access for exceptional circumstances. A notification is linked to the use of this extended access. And all activities are logged during its use to reduce the risk of unauthorised activities taking place. SPM is one of the simplest Access Control components to deploy.

To Logon to GRC5.3 Access Control, below is the link.

<http://aditya:50000/webdynpro/dispatcher/sap.com/grc-acappcomp/AC>

↓  
HostName



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

**How to find the Risk with the User or Role using Risk Analysis and Remediation:**

Risk can be due to

- i. whenever two different Tcodes come together that will be one risk or
- ii. Two similar kind of functions come together that might be a risk.

Here, Functions are the combination of multiple Actions(nothing but Tcodes) or Permissions(nothing but Authorizations).

Click on Risk Analysis & Remediation

UNDER THE GUIDANCE OF  
RASHEED AHMED

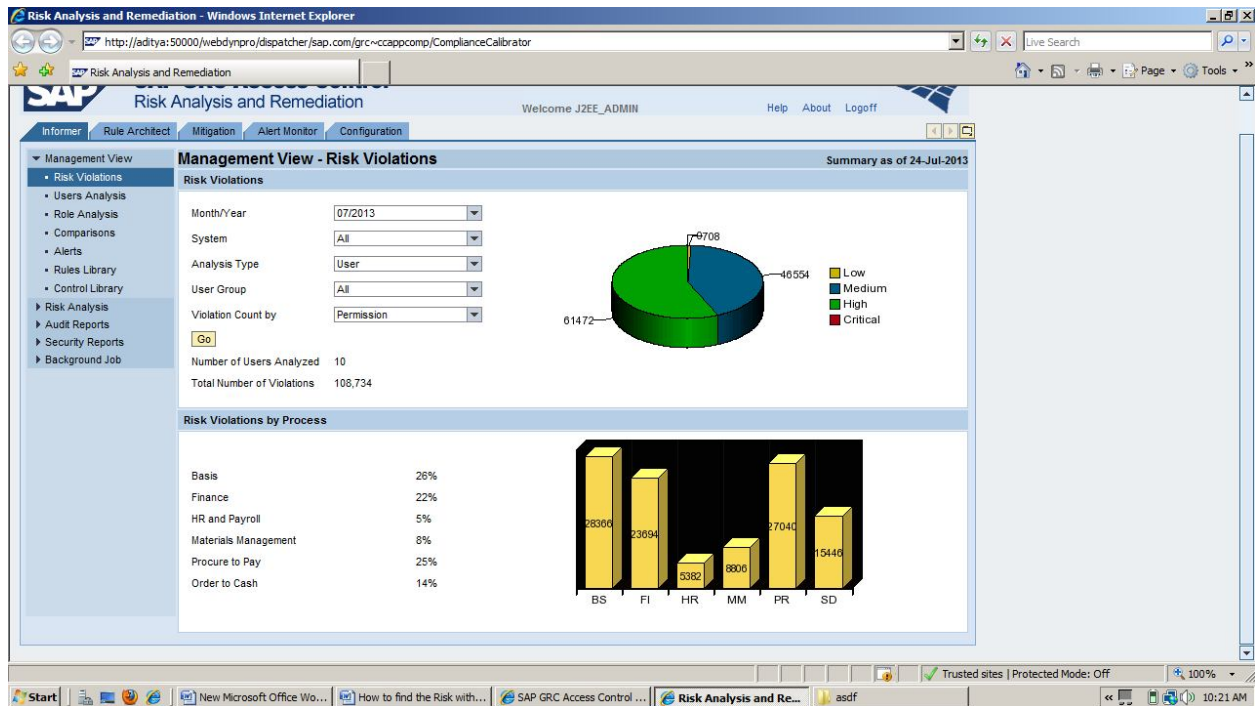
PREPARED BY  
ADITYA JOSYULA



In a New window the below screen will be appeared.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



Risk Analysis can be performed by

1. User Level
2. Role Level

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

## Risk Analysis- Role Level

Click on the Informer tab, under Informer tab

⇒ Go to Risk Analysis Option

⇒ Click on User/ Role Level and specify the required details as below screen.

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The browser window title is "Risk Analysis and Remediation - Windows Internet Explorer". The URL is "http://aditya:50000/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCallibrator". The page header includes the SAP logo, "SAP GRC Access Control Risk Analysis and Remediation", and "Welcome J2EE\_ADMIN". The navigation tabs are "Informer", "Rule Architect", "Mitigation", "Alert Monitor", and "Configuration". The left sidebar shows a tree view with "Risk Analysis" expanded to "Role Level". The main content area is titled "Risk Analysis - Role Level" and contains the following fields:

System *	ADITYA		
Role:	Z.ADITYA_CLIENT_ADMIN	to:	
Profile:		to:	
Risks by Process: *	All		
Risk ID:		to:	
Risk Level:	All		
Rule Set:	GLOBAL		
Report Type:	Permission Level		
Report Format:	Summary		<a href="#">More Options</a>

At the bottom of the form, there are buttons: Execute, Simulate, Background, Reset, Search Variant, and Save Variant.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

and click on execute.

After executing you will get all the levels of Risks i.e., High, Medium, Low and critical.

Check the below screen

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The main window shows a 'Role Analysis at Permission Level - Summary Report' for the role 'Z:ADITYA\_CLIENT\_ADMIN'. The report includes a table of conflicting actions with their risk levels and business processes.

Conflicting Actions	Risk Description	Level	Business Process
Client Administration (SCC4) and User Maintenance (SU01)	B0111BD01: Security Administration & Client Administration	High	Basis
Local Client Copy (SCCL) and User Maintenance (SU01)	B0111BI01: Security Administration & Client Administration	High	Basis

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

By seeing the level of the risk we need to remove the risk or we need to mitigate the risk.

→To remove the risk click on the risk description then you will know the role name after that go to the back end system and remove the risk from the role, below is the screen of the role name

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The main content area shows a 'Role Analysis at Permission Level - Summary Report' for the role 'CLIENT\_ADMIN (Z:ADITYA\_CLIENT\_ADMIN)'. The report includes selection criteria and a table of conflicting actions.

**Selection Criteria**

- System: PRD
- Role: Z:ADITYA\_CLIENT\_ADMIN
- Risks by Process: All
- Risk Level: All
- Risk ID:
- Rule Set: GLOBAL
- Report Type: Permission Level
- Ignored Users: Locked and Expired
- Exclude Mitigated Risk: Yes

Offline Analysis: No  
Run Date/Time: 2013-10-07 12:15:41

Role: CLIENT\_ADMIN (Z:ADITYA\_CLIENT\_ADMIN)      System: ADITYA

Conflicting Actions	Risk Description	Level	Business Process
Client Administration (SCC4) and User Maintenance (SU01)	B0111BD01: Security Administration & Client Administration	High	Basis
Local Client Copy (SCCL) and User Maintenance (SU01)	B0111BI01: Security Administration & Client Administration	High	Basis

UNDER THE GUIDANCE OF  
RASHEED AHMED



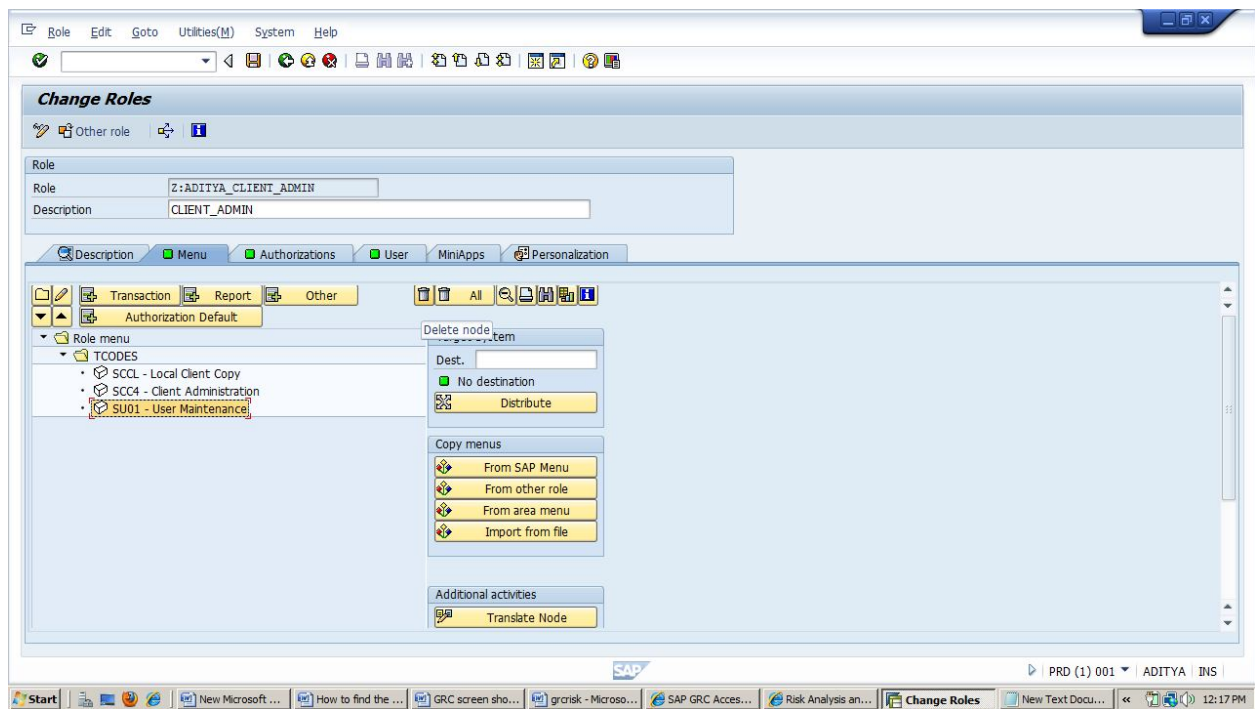
PREPARED BY  
ADITYA JOSYULA

After going to the backend system remove one conflict actions (Tcodes) from the role.

Here conflict actions are SCC4 and SU01 & SCCL and SU01.

Then Goto PFOG and mention the role name and remove the Tcodes from the role .

Check the below screens for removing the Tcodes from the role.

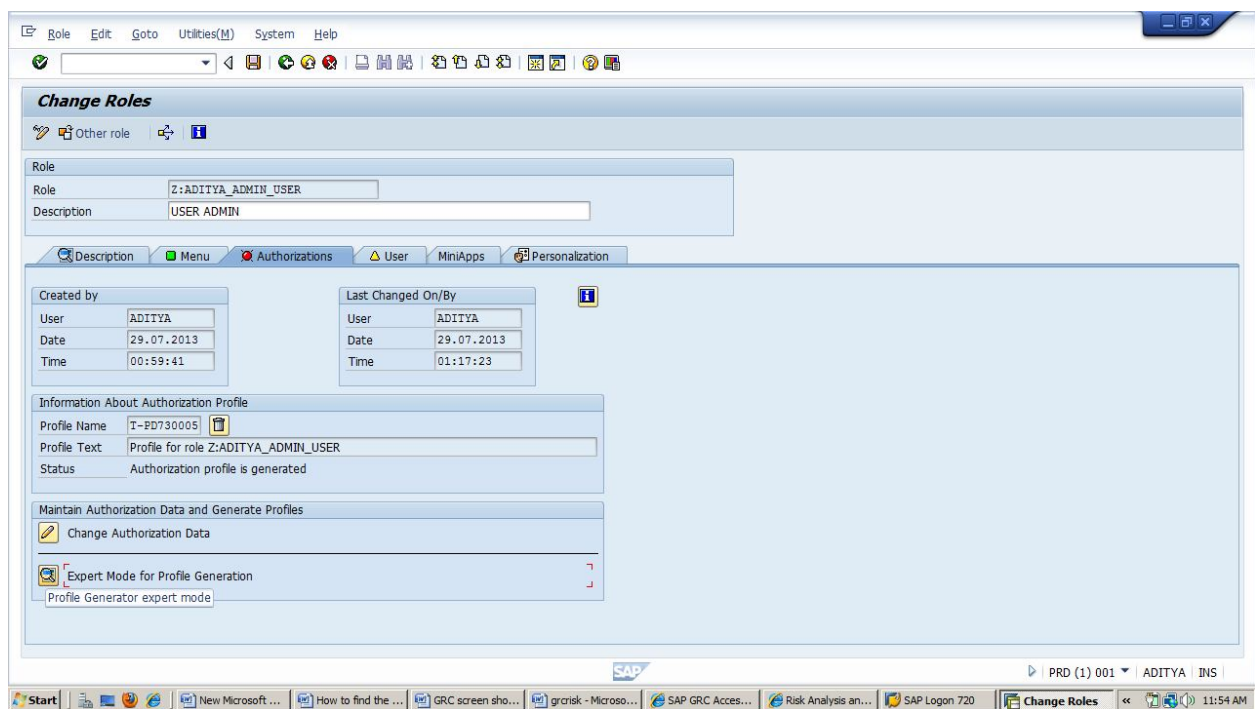


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

After removing the Tcode from the role goto Authorization tab and go for Expert Mode for Profile Generation.

Check the below screen shot

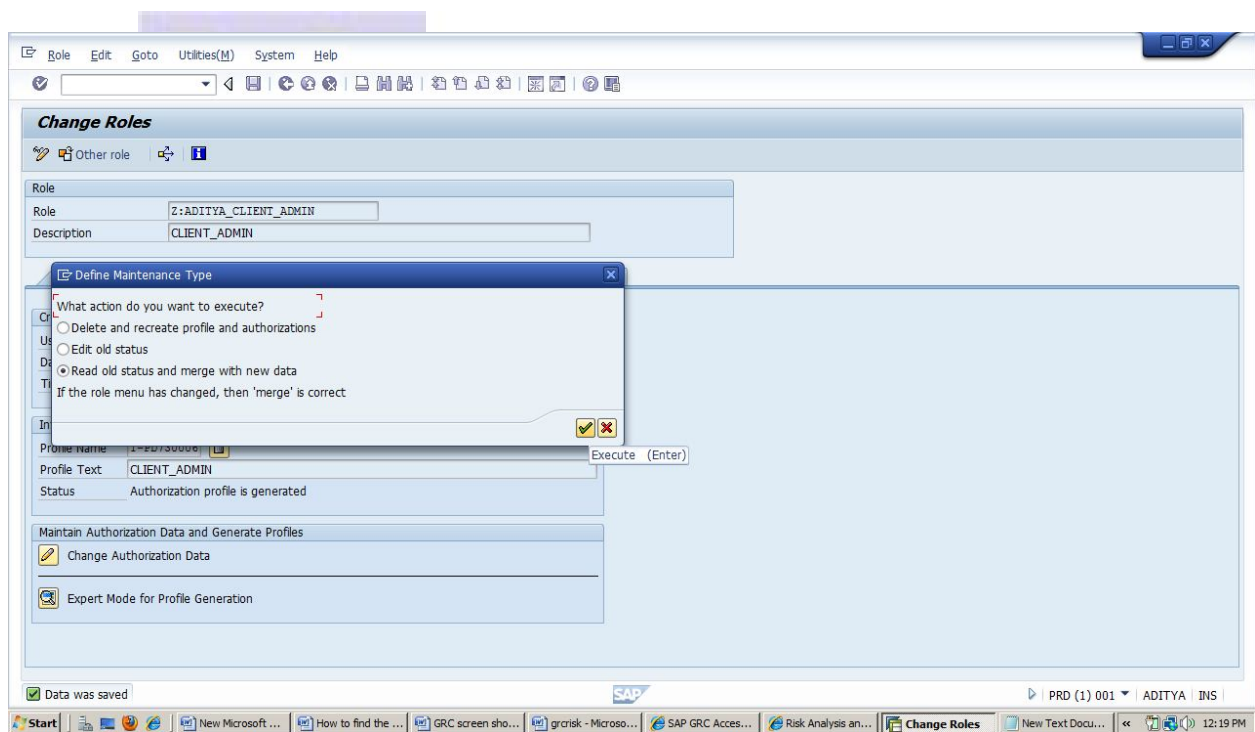


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Then go with Read Old Status and Merge with New Data option and click Nike.

Check the below screen

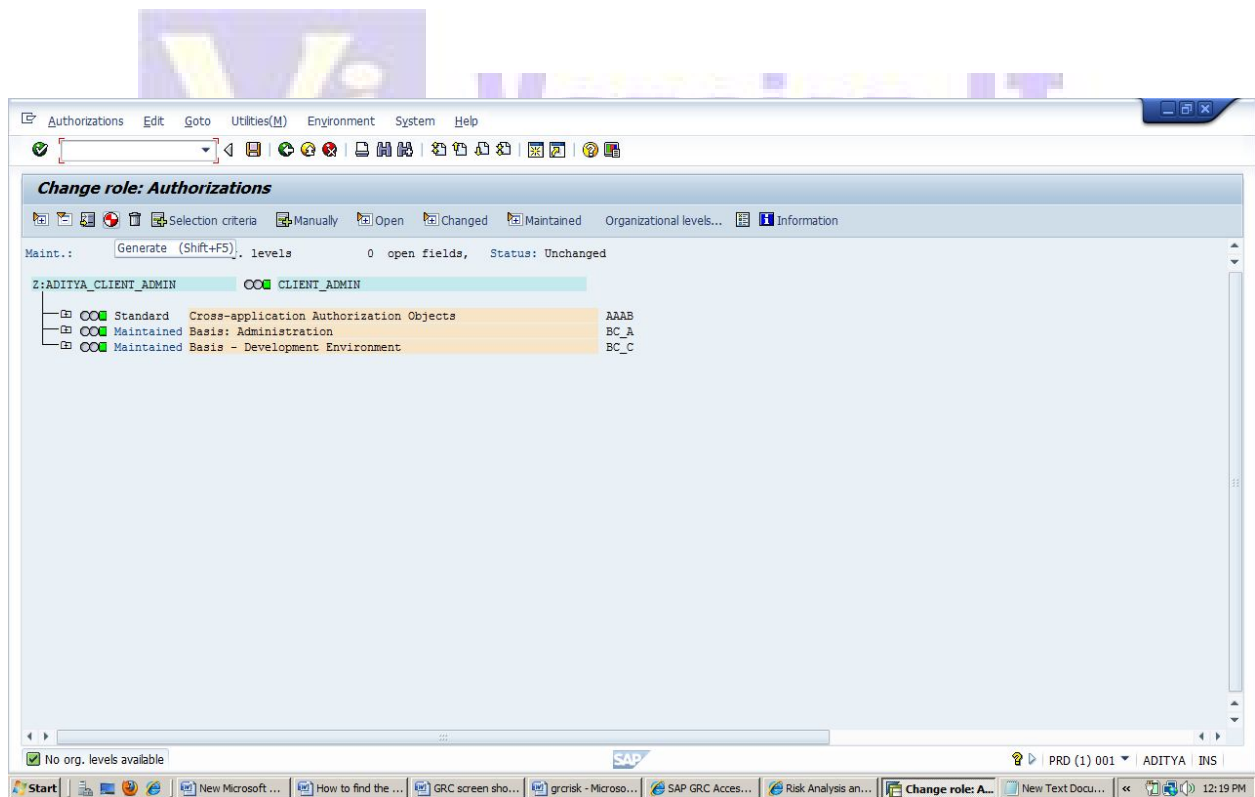


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

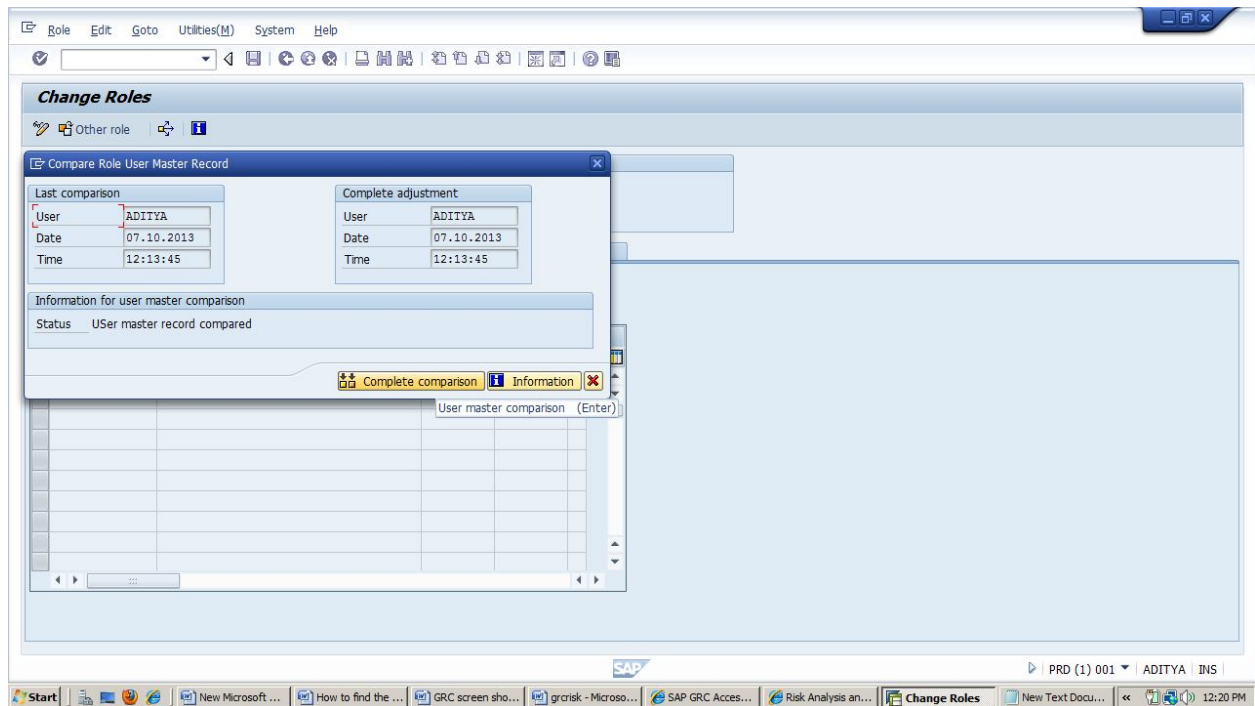
Then generate the role and do the User Comparison .

Check the below screens



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

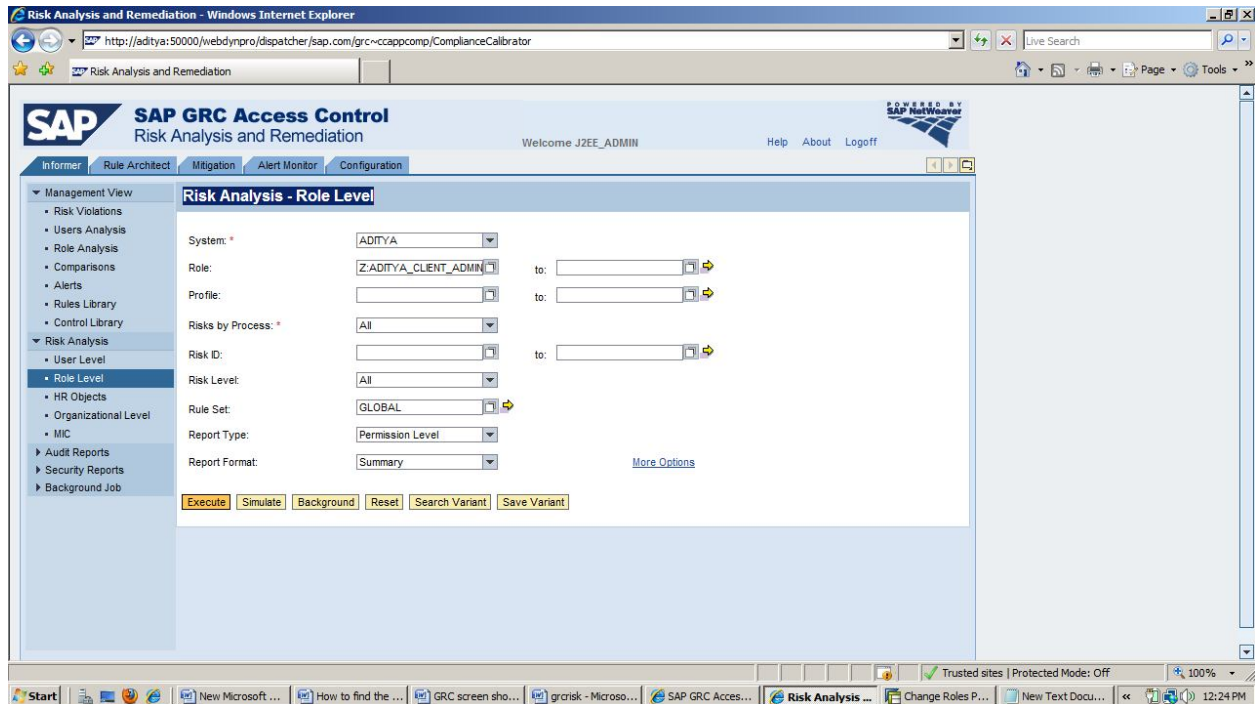


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Now go back to the Risk Analysis - Role Level and mention the role name which was removed in back end system .

Check the below screen



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on execute.

Now you will get a screen with No violations found .

Check the below screen

**SAP GRC Access Control**  
Risk Analysis and Remediation

Welcome J2EE\_ADMIN Help About Logoff

Informers Rule Architect Mitigation Alert Monitor Configuration

Management View  
• Risk Violations  
• Users Analysis  
• Role Analysis  
• Comparisons  
• Alerts  
• Rules Library  
• Control Library  
▼ Risk Analysis  
• User Level  
• Role Level  
• HR Objects  
• Organizational Level  
• MIC  
▶ Audit Reports  
▶ Security Reports  
▶ Background Job

**Role Analysis at Permission Level - Summary Report**

Selection Criteria [- Hide](#) Run Date/Time: 2013-10-07 12:25:28

System: PRD  
Role: Z:ADITYA\_CLIENT\_ADMIN  
Risks by Process: All  
Risk Level: All  
Risk ID:  
Rule Set: GLOBAL  
Report Type: Permission Level  
Ignored Users: Locked and Expired  
Exclude Mitigated Risk: Yes

Offline Analysis: No

Role: CLIENT\_ADMIN (Z:ADITYA\_CLIENT\_ADMIN) System: ADITYA

Conflicting Actions	Risk Description	Level	Business Process
No Violations Found			

Start | New Microsoft ... | How to find the ... | GRC screen sho... | grcrisk - Microso... | SAP GRC Acces... | Risk Analysis ... | Change Roles P... | New Text Docu... | 12:28 PM

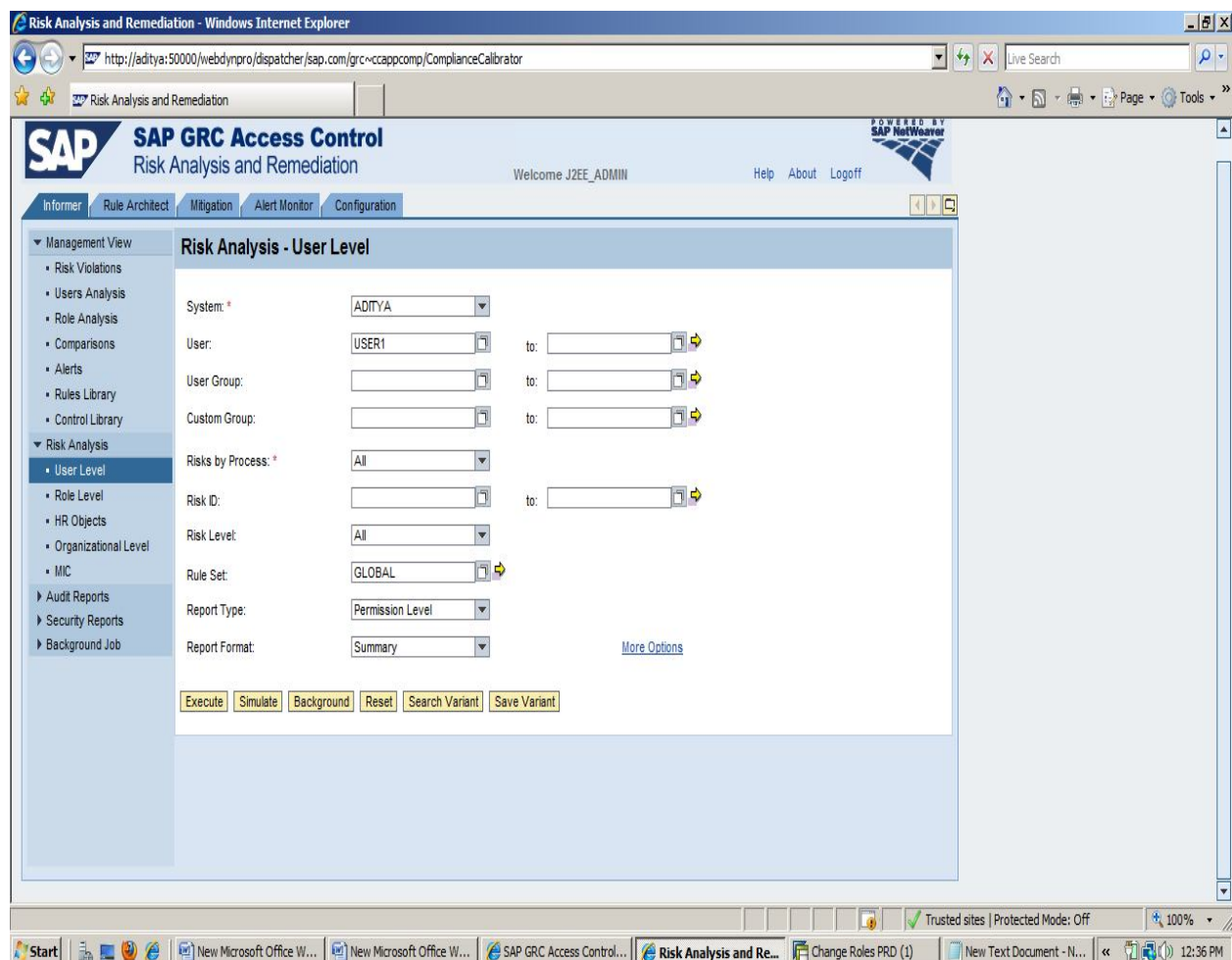
UNDER THE GUIDANCE OF  
RASHEED AHMED

## Risk Analysis - User Level

Click on the Informer tab, under Informer tab

⇒ Goto Risk Analysis Option

⇒ Click on User Level as below screen.





PREPARED BY  
ADITYA JOSYULA

Click on execute.

After executing you will get all the levels of Risks i.e., High, Medium, Low and critical.

Check the below screen

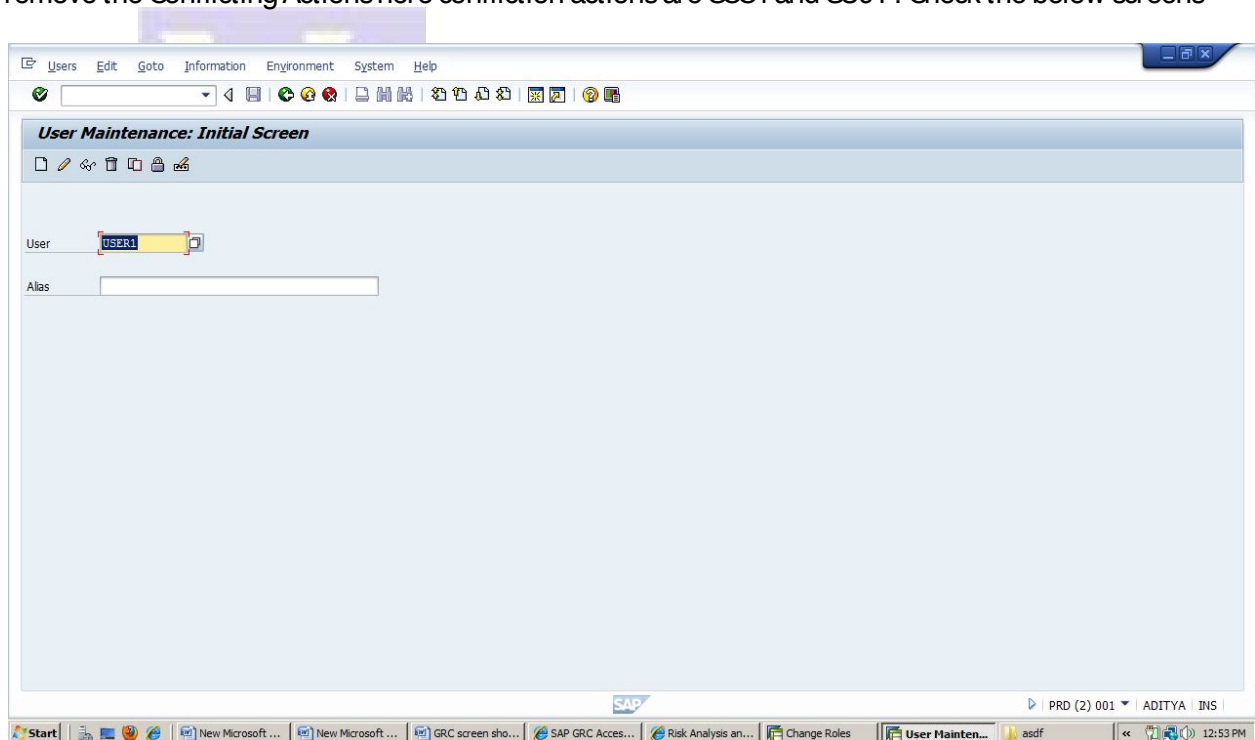
The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The main content area shows a 'User Analysis at Permission Level - Summary Report'. The report includes selection criteria such as System (PRD), User (USER1), and Report Type (Permission Level). Below the criteria, there is a table with columns for Conflicting Actions, Risk Description, Level, and Business Process. The table lists two high-risk items related to Client Administration and User Maintenance.

Conflicting Actions	Risk Description	Level	Business Process
Client Administration (SCC4) and User Maintenance (SU01)	B0111BD01: Security Administration & Client Administration	High	Basis
Local Client Copy (SCCL) and User Maintenance (SU01)	B0111BI01: Security Administration & Client Administration	High	Basis

UNDER THE GUIDANCE OF  
RASHEED AHMED

By seeing the level of the risk we need to remove the risk or we need to mitigate the risk.

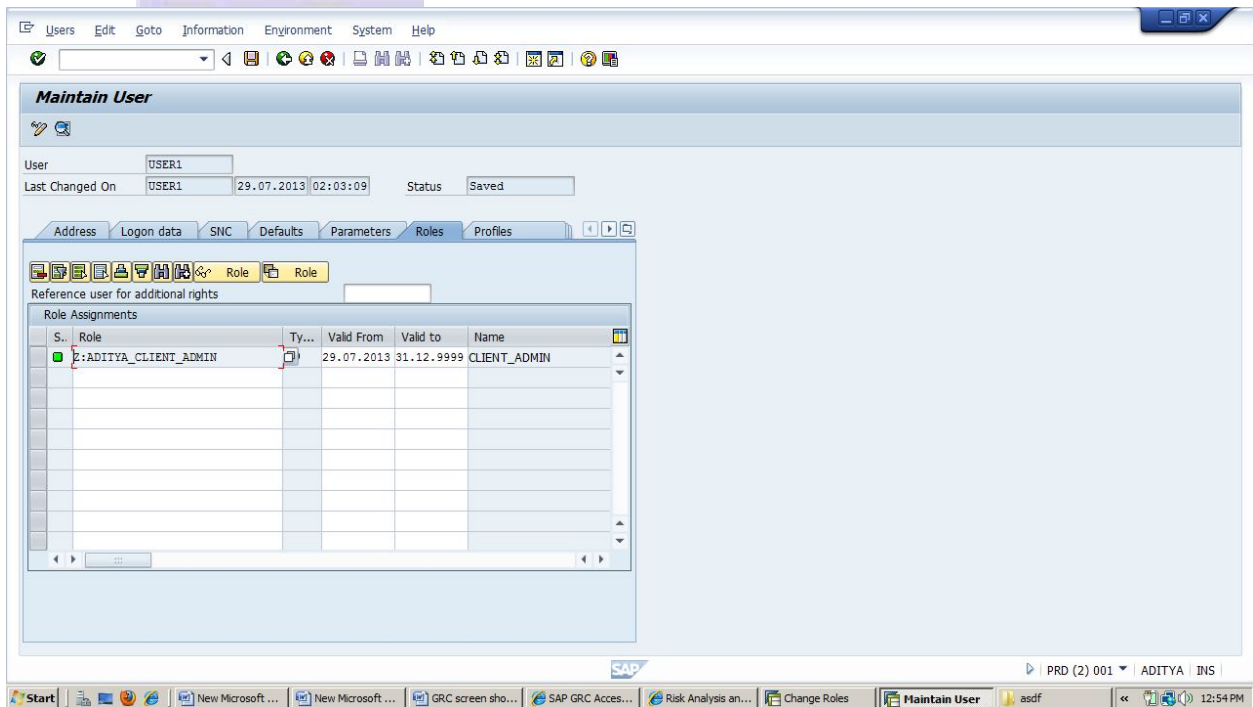
→To remove the risk Go to backend system and Goto SU01 and mention the user name and select the role tab and check the role and copy the role names and goto PFCG and mention the role name and remove the Conflicting Actions here confliction actions are SOC4 and SU01 . Check the below screens



PREPARED BY  
ADITYA JOSYULA

Click on change and copy the role name

Check the below screen



The screenshot displays the SAP 'Maintain User' dialog box. The 'Roles' tab is active, showing a table of role assignments for user 'USER1'. The table has columns for 'S...', 'Role', 'Ty...', 'Valid From', 'Valid to', and 'Name'. One role is assigned: 'Z:ADITYA\_CLIENT\_ADMIN' with type 'A' and validity from '29.07.2013' to '31.12.9999'. The role name is 'CLIENT\_ADMIN'. The status is 'Saved'.

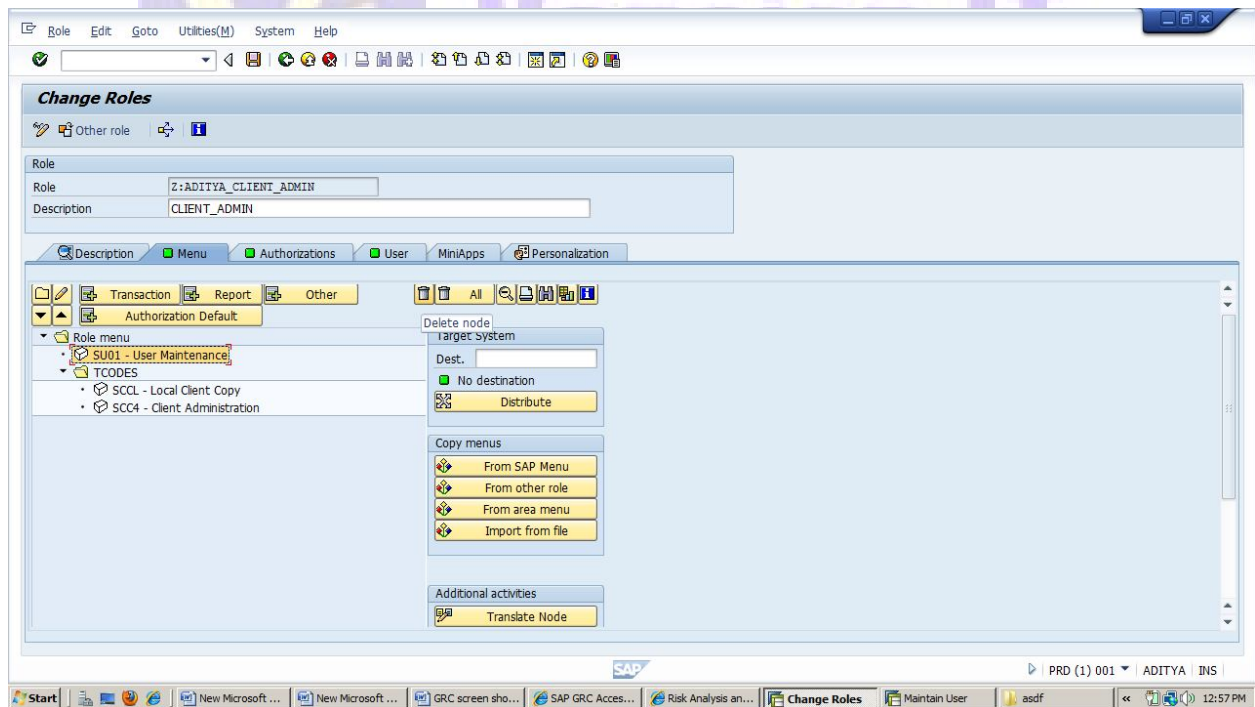
S...	Role	Ty...	Valid From	Valid to	Name
✓	Z:ADITYA_CLIENT_ADMIN	A	29.07.2013	31.12.9999	CLIENT_ADMIN

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Then Goto PFCG and mention the role name and remove the Tcodes from the role .

Check the below screens

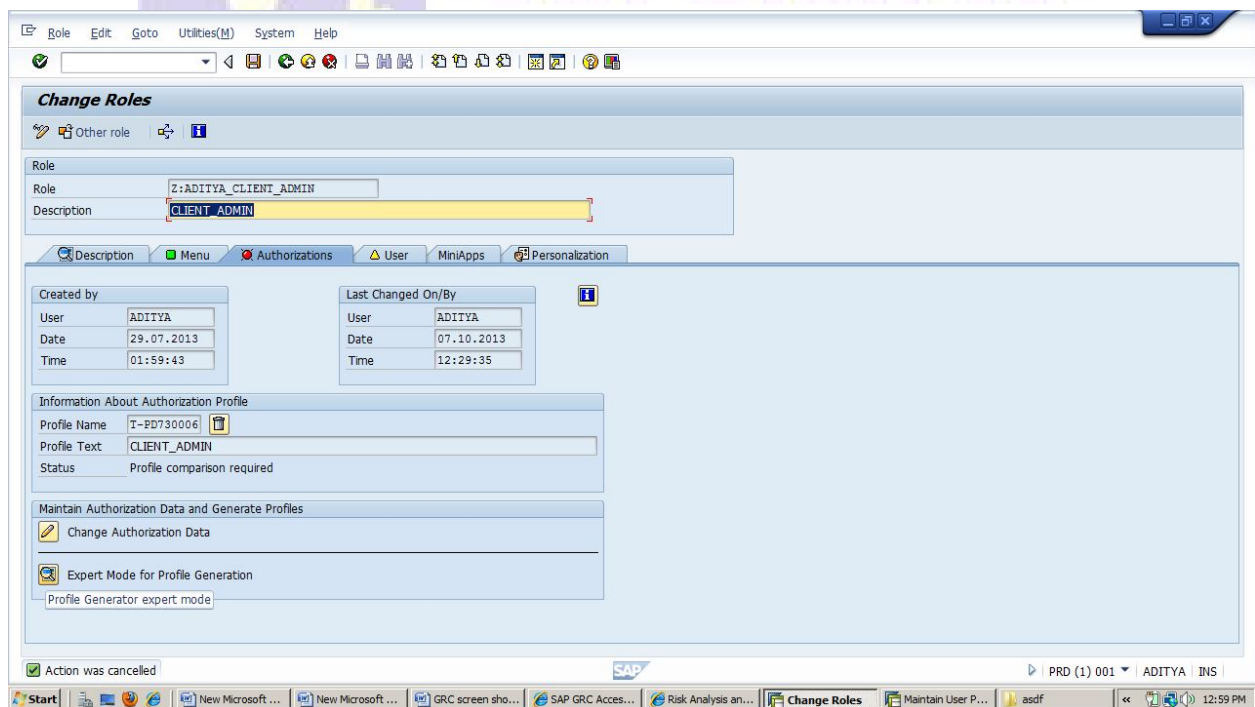


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

After removing the Tcode from the role goto Authorization tab and go for Expert Mode for Profile Generation.

Check the below screen shot



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

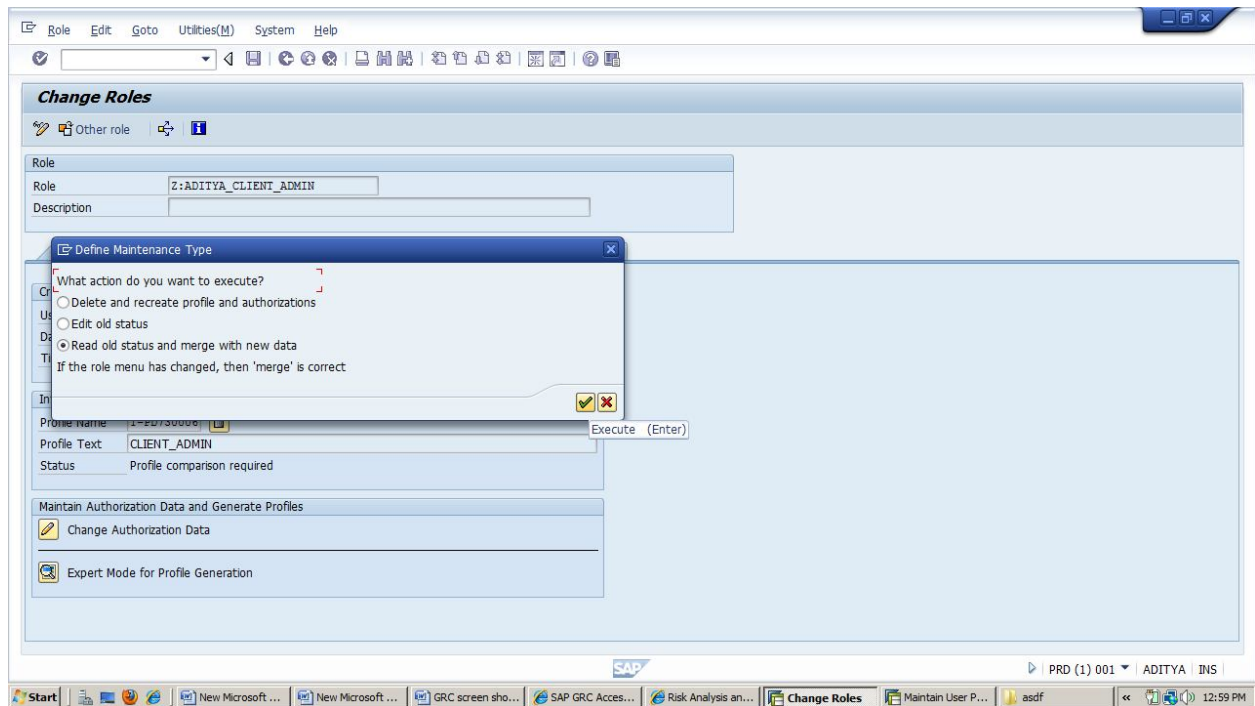


Then go with Read Old Status and Merge with New Data option and click Nike.

Check the below screen

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

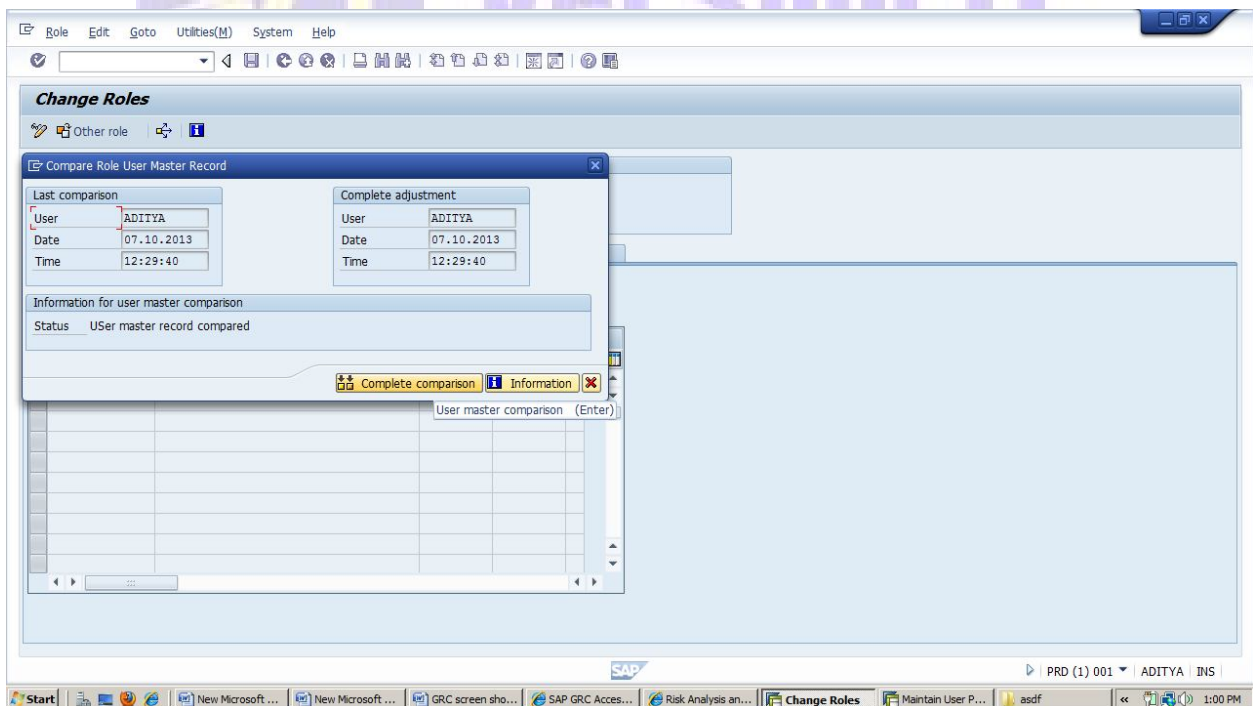
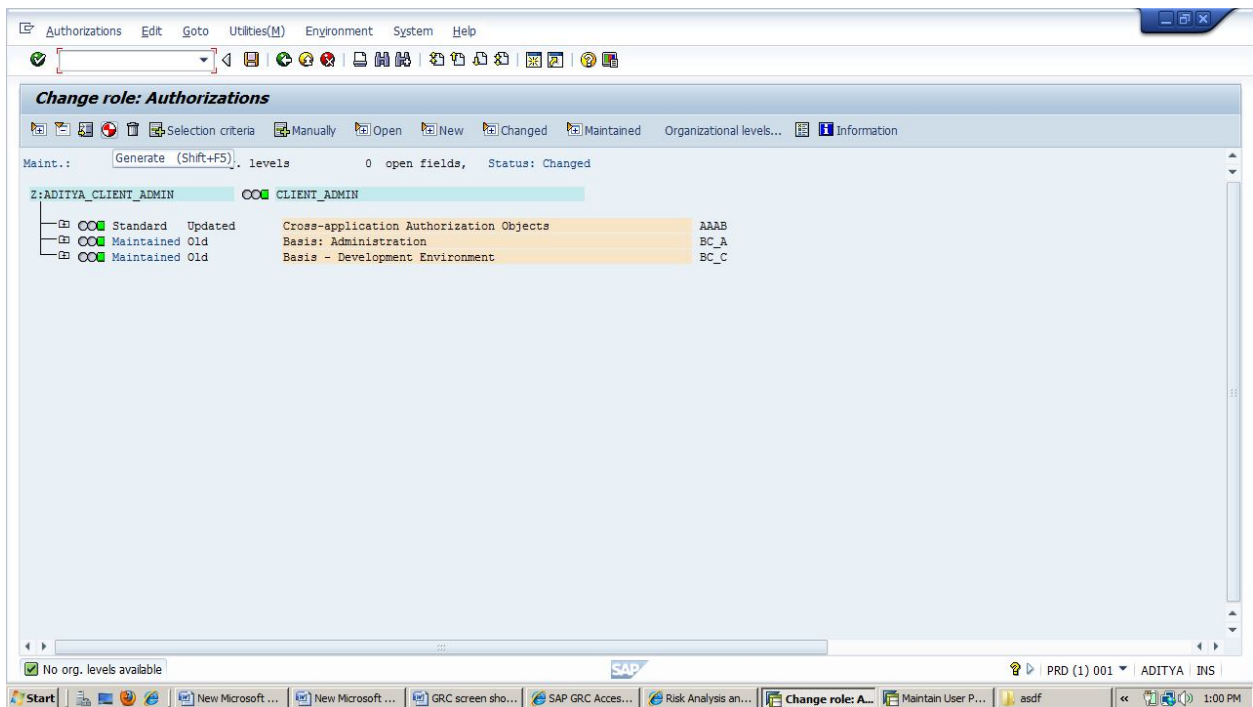


Then generate the role and do the User Comparison.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Check the below screens



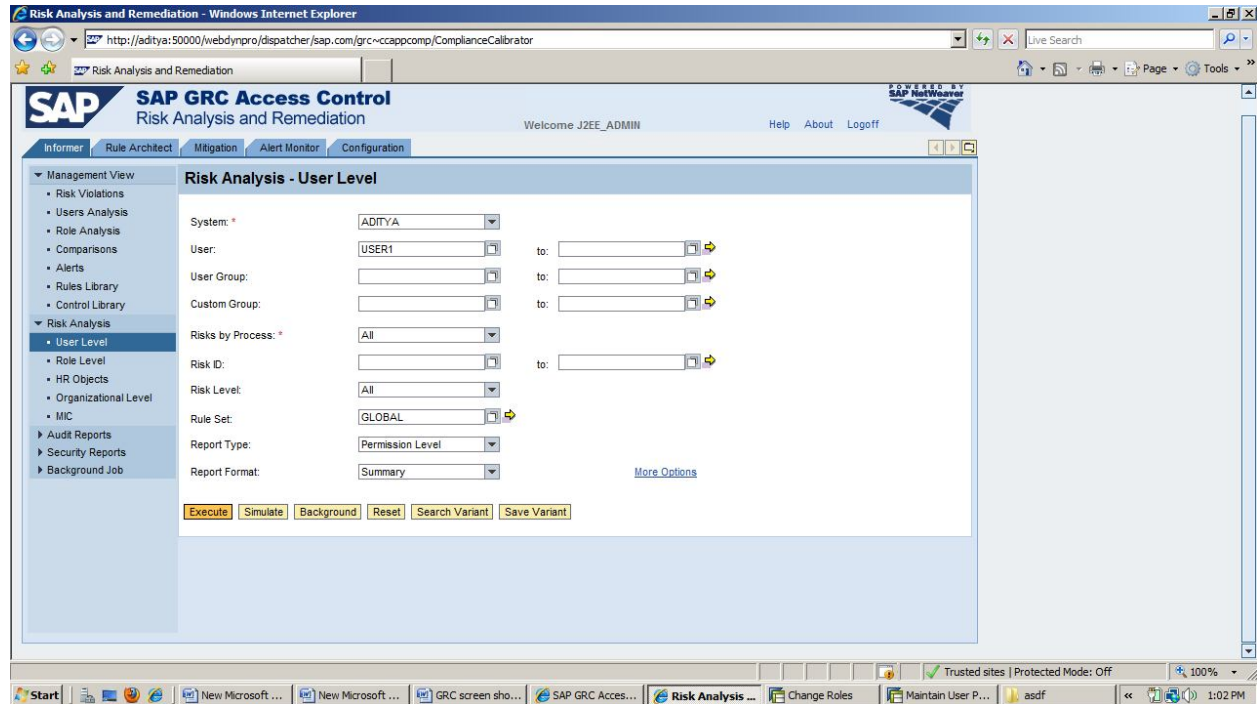
UNDER THE GUIDANCE OF  
RASHEED AHMED



PREPARED BY  
ADITYA JOSYULA

Now go back to the Risk Analysis - User Level and mention the user name.

Check the below screen



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on execute.

Now you will get a screen with No violations found .

Check the below screen

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The main content area shows a 'User Analysis at Permission Level - Summary Report' for user 'USER1' in system 'ADITYA'. The report indicates 'No Violations Found'.

**Selection Criteria**

- System: PRD
- User: USER1
- User Group: USER1
- Custom Group:
- Risks by Process: All
- Risk Level: All
- Risk ID:
- Rule Set: GLOBAL
- Report Type: Permission Level
- User Type: Dialog
- Ignored Users: Locked and Expired
- Exclude Mitigated Risk: Yes
- Offline Analysis: No

**User: USER1 (USER1)      User Group:      System: ADITYA**

Conflicting Actions	Risk Description	Level	Business Process
No Violations Found			

Run Date/Time: 2013-10-07 13:02:56

UNDER THE GUIDANCE OF  
RASHEED AHMED

## Simulation:

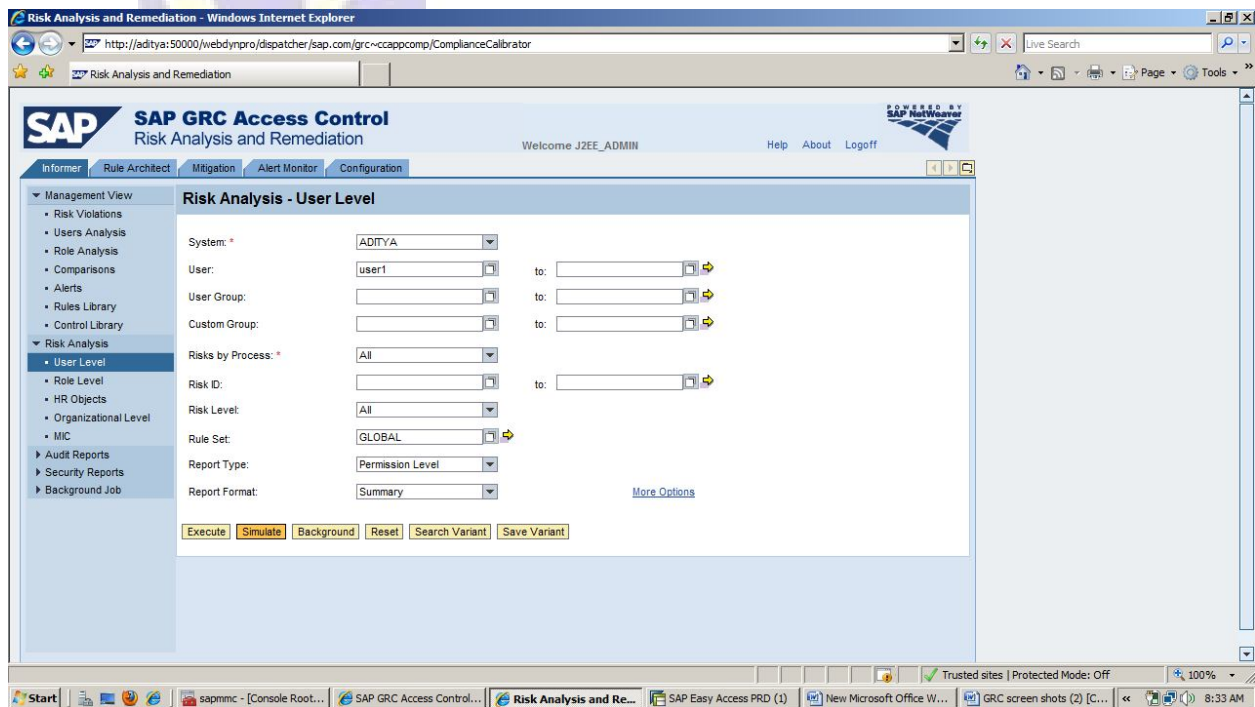
By using this option we can able to identify the risk information before adding the Tcode to Role or User.

EX: If Business is asking you to add 1 particular Tcode to the existing Role then we can get the risk information by putting the Role name & Tcode information under Simulate option and click on Simulate Button, then system will show the Risk Analysis information without adding a Tcode to Role.

## Steps for Simulation at User Level

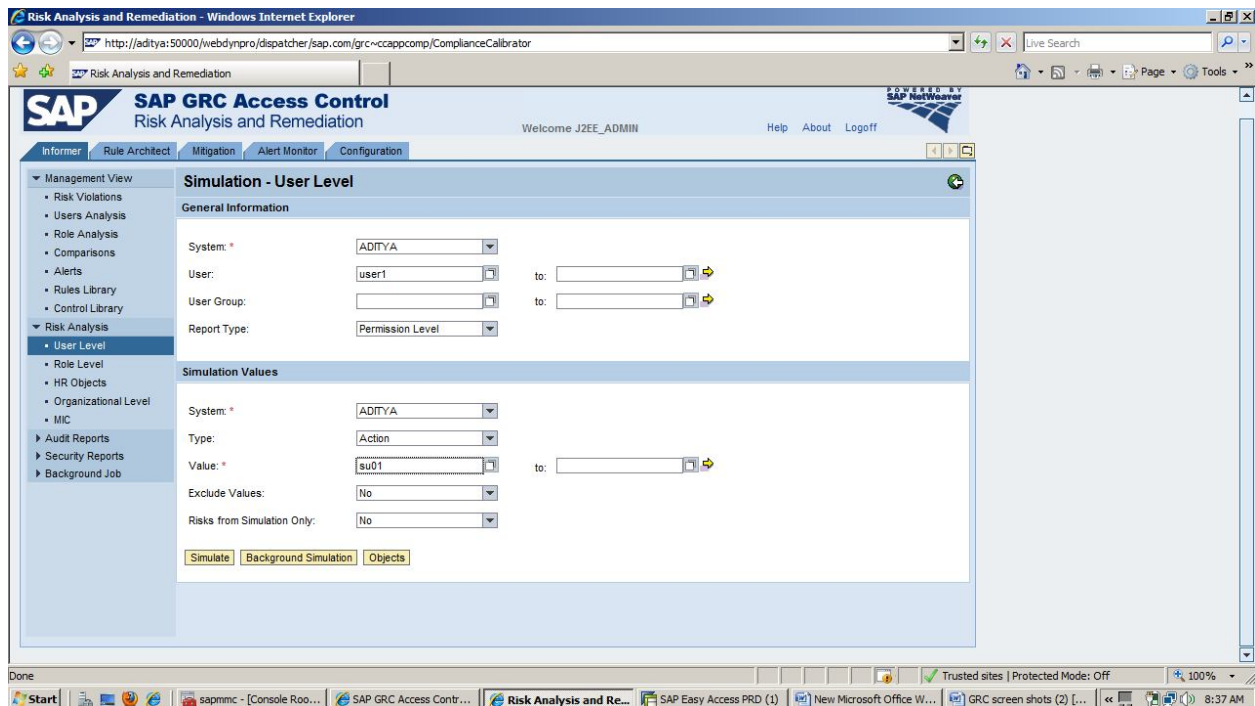
GO to Risk Analysis → User Level Give the **system** details and **user name**.

Check the below screen shot



PREPARED BY  
ADITYA JOSYULA

Then Click on **simulate**



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Here fill the required details & Under the Simulation Values give the value which you want to add, Here the value is nothing but Tcode.

Then click on Simulate

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The main content area shows a 'User Analysis at Permission Level - Summary Report' for user 'USER1' in system 'ADITYA'. The report includes selection criteria and a table of conflicting actions.

**Selection Criteria**

System:	PRD	User Type:	Dialog
User:	USER1	Ignored Users:	Locked and Expired
User Group:		Exclude Mitigated Risk:	Yes
Custom Group:		Offline Analysis:	No
Risks by Process:	All		
Risk Level:	All		
Risk ID:			
Rule Set:	GLOBAL		
Report Type:	Permission Level		

**Conflicting Actions**

Conflicting Actions	Risk Description	Level	Business Process
Client Administration (SCC4) and User Maintenance (SU01)	B0111BD01: Security Administration & Client Administration	High	Basis
Local Client Copy (SCCL) and User Maintenance (SU01)	B0111BI01: Security Administration & Client Administration	High	Basis

Here the value which we have used is SU01 to the user and its showing the risk in High Level.

So this clarifies the value which we have used shouldn't be assigned to the user.

But if the business wants to allow this risk to the user we can do it by using Mitigation Control Option.

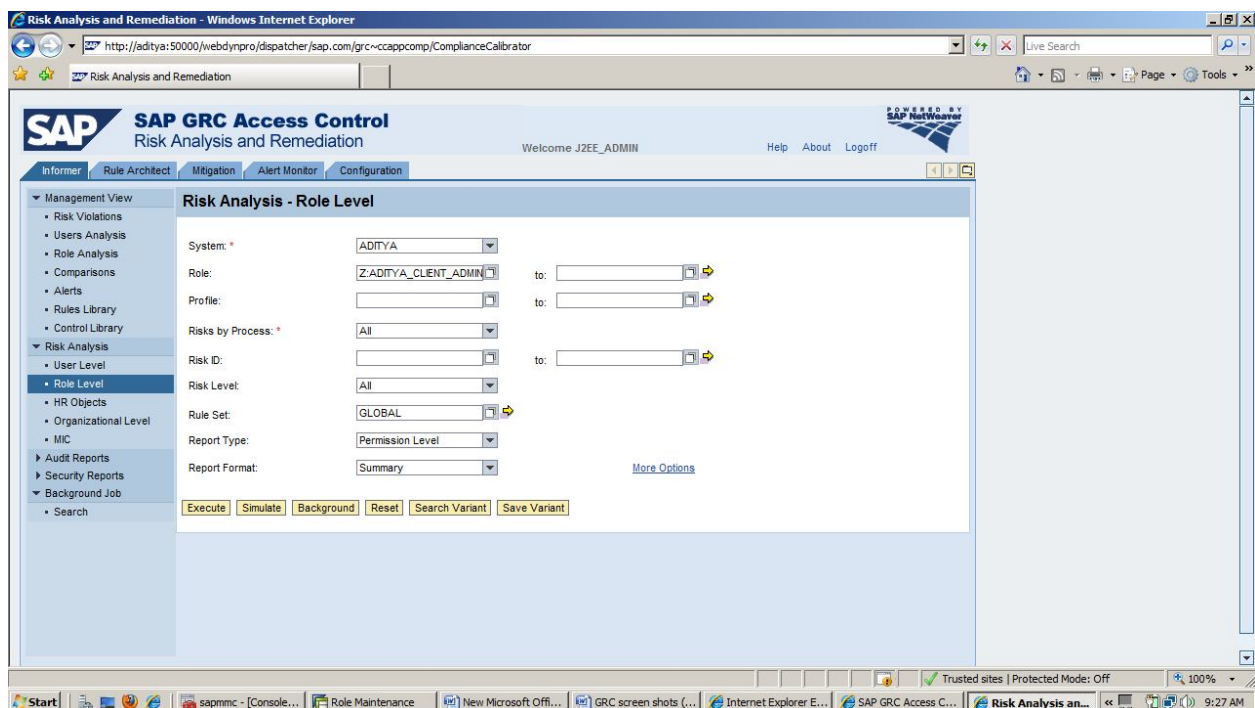
UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

## Steps for Simulation at Role Level

GO to Risk Analysis → Role Level Give the **system** details and **Role name**.

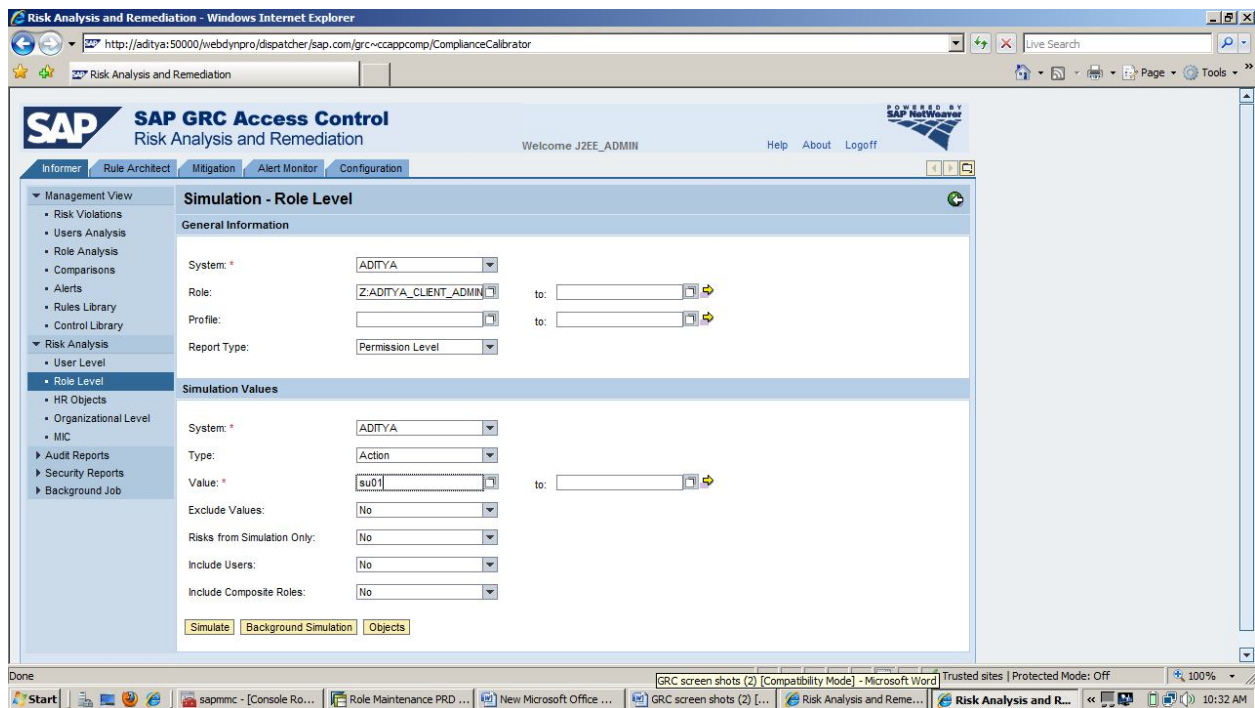
Check the below screen shot



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Then click on Simulate



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Here fill the required details & Under the General Information mention the system & role name. Under the Simulation Values give the value which you want to add, Here the value is nothing but Tcode.

Then click on Simulate

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The main window shows a 'Role Analysis at Permission Level - Summary Report' for the role 'CLIENT\_ADMIN (Z-ADITYA\_CLIENT\_ADMIN)' in the system 'ADITYA'. The report includes a table of conflicting actions with the following data:

Conflicting Actions	Risk Description	Level	Business Process
Client Administration (SCC4) and User Maintenance (SU01)	B0111BD01: Security Administration & Client Administration	High	Basis
Local Client Copy (SCCL) and User Maintenance (SU01)	B0111BI01: Security Administration & Client Administration	High	Basis

The interface also shows a left-hand navigation menu with options like 'Management View', 'Risk Violations', 'Users Analysis', 'Role Analysis', 'Comparisons', 'Alerts', 'Rules Library', 'Control Library', 'Risk Analysis', 'User Level', 'HR Objects', 'Organizational Level', 'MIC', 'Audit Reports', 'Security Reports', and 'Background Job'. The top navigation bar includes 'Informer', 'Rule Architect', 'Mitigation', 'Alert Monitor', and 'Configuration'. The bottom status bar shows the system is in 'Protected Mode: OFF' and the time is 10:32 AM.

Here the value which we have used is SU01 to the Role and its showing the risk in High Level.

UNDER THE GUIDANCE OF  
RASHEED AHMED



PREPARED BY  
ADITYA JOSYULA

So this clarifies the value which we have used shouldn't be assigned to the Role.

But if the business wants to allow this risk to the Role we can do it by using Mitigation Control Option.

### **Mitigation:**

Allowing the risk by using or creating the Mitigation Control ID's as per the Business.

You can use Mitigation Controls to associate controls with the Risk, and assign them to Users, Roles, Profiles, or HR Objects.

Make individuals as Control Monitors or Approvers and then assign them to Controls.

### **Steps for Creating Mitigation**

Here we are creating a Mitigation Control for the below Screen Shot.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

**SAP GRC Access Control**  
Risk Analysis and Remediation

Welcome JZEE\_ADMIN

Management View  
Risk Analysis  
User Level

System: ADITYA  
User: USER1  
User Group:  
Custom Group:  
Risks by Process: All  
Risk ID:  
Risk Level: All  
Rule Set: GLOBAL  
Report Type: Permission Level  
Report Format: Summary

Execute Simulate Background Reset Search Variant Save Variant

**SAP GRC Access Control**  
Risk Analysis and Remediation

Welcome JZEE\_ADMIN

Management View  
Risk Analysis  
User Level

**User Analysis at Permission Level - Summary Report**

Selection Criteria

System: PRD  
User: USER1  
User Group:  
Custom Group:  
Risks by Process: All  
Risk Level: All  
Risk ID:  
Rule Set: GLOBAL  
Report Type: Permission Level

User Type: Dialog  
Ignored Users: Locked and Expired  
Exclude Mitigated Risk: Yes  
Offline Analysis: No

Run Date/Time: 2013-10-08 11:27:15

User: USER1 (USER1)      User Group:      System: ADITYA

Conflicting Actions	Risk Description	Level	Business Process
Client Administration (SCC4) and User Maintenance (SU01)	B0111BD01: Security Administration & Client Administration	High	Basis
Local Client Copy (SCCL) and User Maintenance (SU01)	B0111BI01: Security Administration & Client Administration	High	Basis

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



**Version IT**

Now click on the Risk Description -B0111BD01.

Check the below screen shot

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The main content area shows a 'User Analysis at Permission Level - Summary Report' for user USER1. The report includes selection criteria such as System (PRD), User (USER1), and Risk Level (All). A table of conflicting actions is shown below, listing two instances of 'Security Administration & Client Administration' with a 'High' risk level and 'Basis' business process.

Conflicting Actions	Risk Description	Level	Business Process
Client Administration (SCC4) and User Maintenance (SU01)	B0111B001: Security Administration & Client Administration	High	Basis
Local Client Copy (SCCL) and User Maintenance (SU01)	B0111B010: Security Administration & Client Administration	High	Basis



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

After clicking the Risk Description -B011BD01, you will find the Risk information. You need to concentrate on the Risk ID & Business Process.

Check the below screen shot.

The screenshot shows the SAP GRC Access Control interface in a Windows Internet Explorer browser. The page title is "SAP GRC Access Control Risk Analysis and Remediation". The user is logged in as "JZEE\_ADMIN". The main content area displays the "Risk Information" for Risk ID "B011".

Risk ID:	B011
Risk Type:	Segregation of Duties
Risk Level:	High
Risk Owner:	
Risk Description:	Security Administration & Client Administration
Detailed Description:	An individual could inappropriately modify roles and assignments and reflect this change to the production's mirror copy eliminating the chance to revert to the appropriate setup.
Control Objective:	
Business Process:	Basis
Relevant Function(s):	BS05 - Client Administration and BS10 - Security Administration

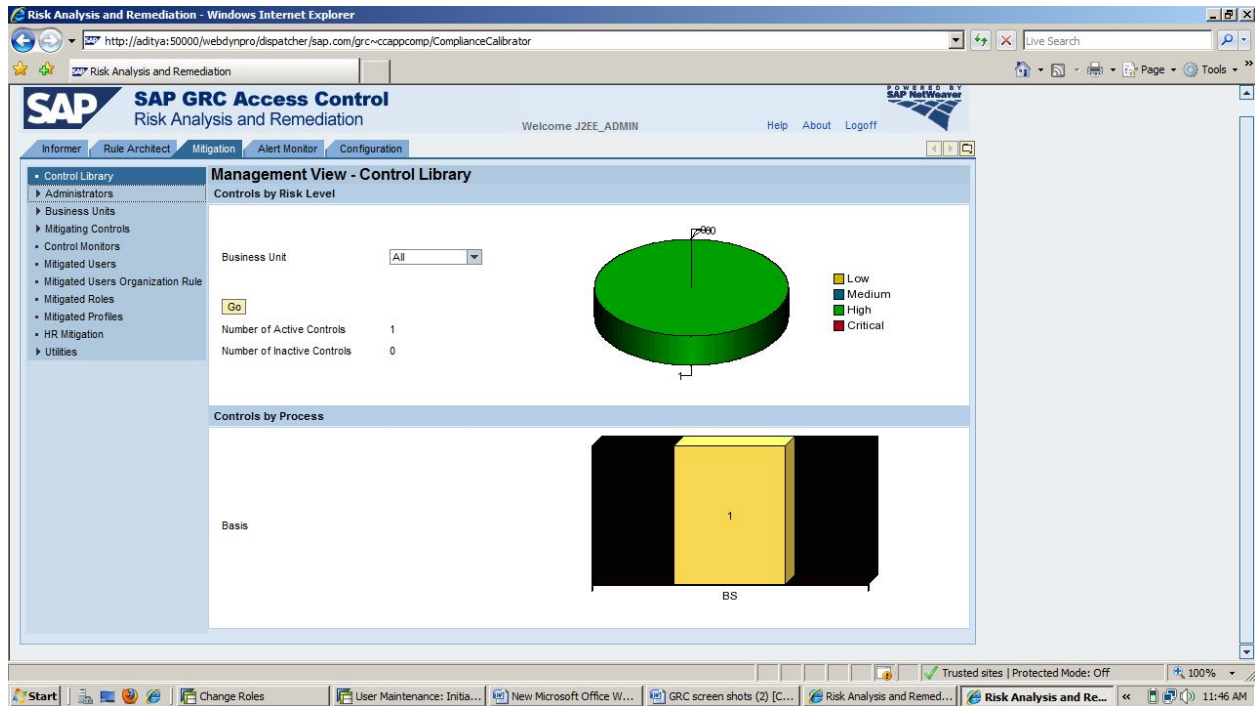
Below the table, there is a "Change History" button.

Version 17

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Now go to Mitigation Tab, Check the below screen shot.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Here we have to create the Approvers, Monitors, Risk Owners, Business Unit, Mitigating Control ID, Control Monitors and Mitigated Users.

Check the below screen shot for the process.

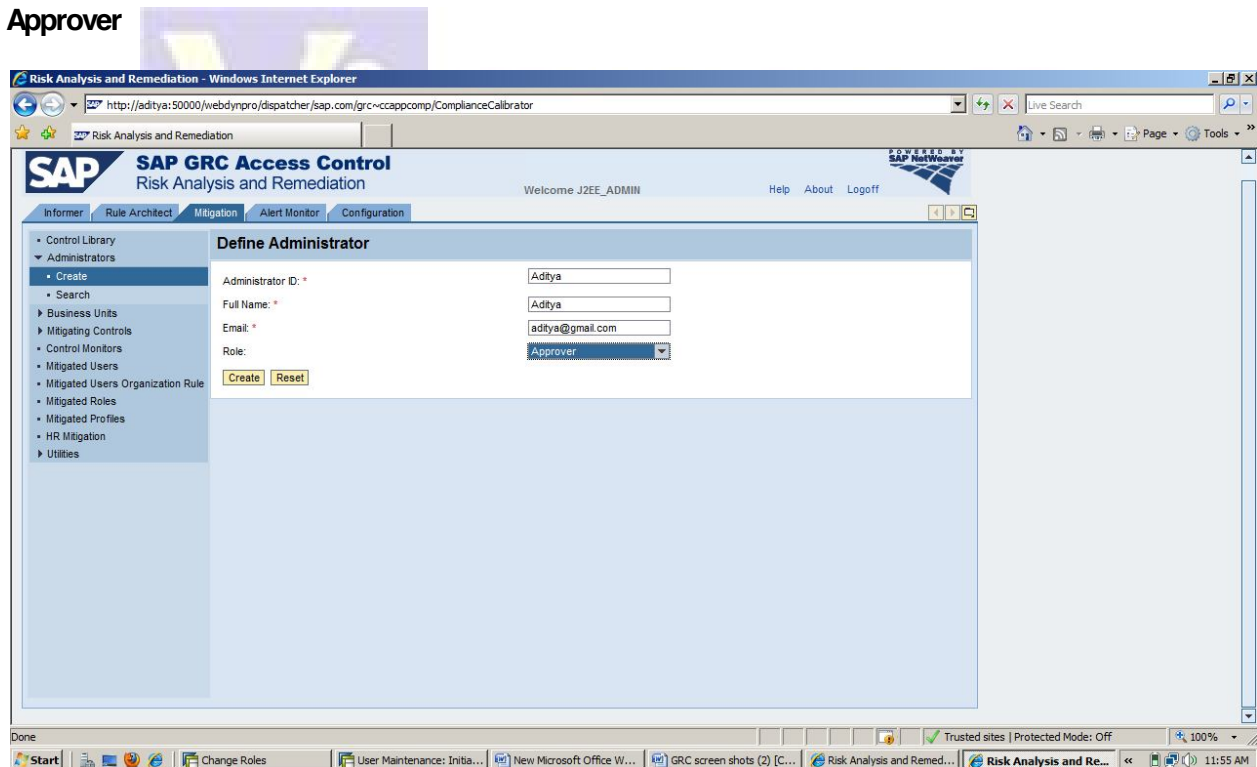
### STEP1:

In this Administrator Tab we are going to create Approvers, Monitors, Risk Owner ID's.

Goto Administrators→Click on Create→ then fill the required details.

Check the below screen shots.

### Approver



The screenshot shows the SAP GRC Access Control interface in a Windows Internet Explorer browser. The page title is "SAP GRC Access Control Risk Analysis and Remediation". The user is logged in as "JZEE\_ADMIN". The navigation menu on the left includes "Control Library", "Administrators", "Business Units", "Mitigating Controls", "Control Monitors", "Mitigated Users", "Mitigated Users Organization Rule", "Mitigated Roles", "Mitigated Profiles", "HR Mitigation", and "Utilities". The "Administrators" section is expanded, showing "Create", "Search", and "Business Units". The "Define Administrator" form is displayed with the following fields: "Administrator ID" (Adtya), "Full Name" (Adtya), "Email" (aditya@gmail.com), and "Role" (Approver). There are "Create" and "Reset" buttons at the bottom of the form. The browser's address bar shows the URL: "http://aditya:50000/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCallibrator". The Windows taskbar at the bottom shows several open applications, including "Change Roles", "User Maintenance: Initia...", "New Microsoft Office W...", "GRC screen shots (2) [C...", "Risk Analysis and Remed...", and "Risk Analysis and Re...". The system clock shows "11:55 AM".

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

## Monitor

The screenshot shows the SAP GRC Access Control interface in Internet Explorer. The browser address bar shows the URL: `http://aditya:50000/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator`. The page title is "Risk Analysis and Remediation". The main header includes the SAP logo, "SAP GRC Access Control Risk Analysis and Remediation", and a welcome message "Welcome J2EE\_ADMIN". The navigation menu includes "Informers", "Rule Architect", "Mitigation", "Alert Monitor", and "Configuration". The left sidebar contains a tree view with categories like "Control Library", "Administrators", "Business Units", "Mitigating Controls", "Control Monitors", "Mitigated Users", "Mitigated Users Organization Rule", "Mitigated Roles", "Mitigated Profiles", "HR Mitigation", and "Utilities". The main content area is titled "Define Administrator" and contains the following form fields:

- Administrator ID: \* (Text input: Addy)
- Full Name: \* (Text input: Addy)
- Email: \* (Text input: addy@gmail.com)
- Role: (Dropdown menu: Monitor)

Below the form are "Create" and "Reset" buttons. A status message at the bottom of the page reads "Administrator successfully created". The Windows taskbar at the bottom shows several open applications, including "Change Roles", "User Maintenance: Inita...", "New Microsoft Office W...", "GRC screen shots (2) C...", "Risk Analysis and Remed...", and "Risk Analysis and Re...". The system clock shows 11:56 AM.

## Risk Owner

The screenshot shows the SAP GRC Access Control interface in Internet Explorer, similar to the previous one. The browser address bar shows the URL: `http://aditya:50000/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator`. The page title is "Risk Analysis and Remediation". The main header includes the SAP logo, "SAP GRC Access Control Risk Analysis and Remediation", and a welcome message "Welcome J2EE\_ADMIN". The navigation menu includes "Informers", "Rule Architect", "Mitigation", "Alert Monitor", and "Configuration". The left sidebar contains a tree view with categories like "Control Library", "Administrators", "Business Units", "Mitigating Controls", "Control Monitors", "Mitigated Users", "Mitigated Users Organization Rule", "Mitigated Roles", "Mitigated Profiles", "HR Mitigation", and "Utilities". The main content area is titled "Define Administrator" and contains the following form fields:

- Administrator ID: \* (Text input: Adi)
- Full Name: \* (Text input: Adi)
- Email: \* (Text input: adi@gmail.com)
- Role: (Dropdown menu: Risk Owner)

Below the form are "Create" and "Reset" buttons. A status message at the bottom of the page reads "Administrator successfully created". The Windows taskbar at the bottom shows several open applications, including "Change Roles", "User Maintenance: Inita...", "New Microsoft Office W...", "GRC screen shots (2) C...", "Risk Analysis and Remed...", and "Risk Analysis and Re...". The system clock shows 11:56 AM.

UNDER THE GUIDANCE OF  
RASHEED AHMED



PREPARED BY  
ADITYA JOSYULA

**STEP2:**

Business Unit is based upon Business Processes for Functions Identification. Here Business Unit ID is a unique ID which was picked by our own.

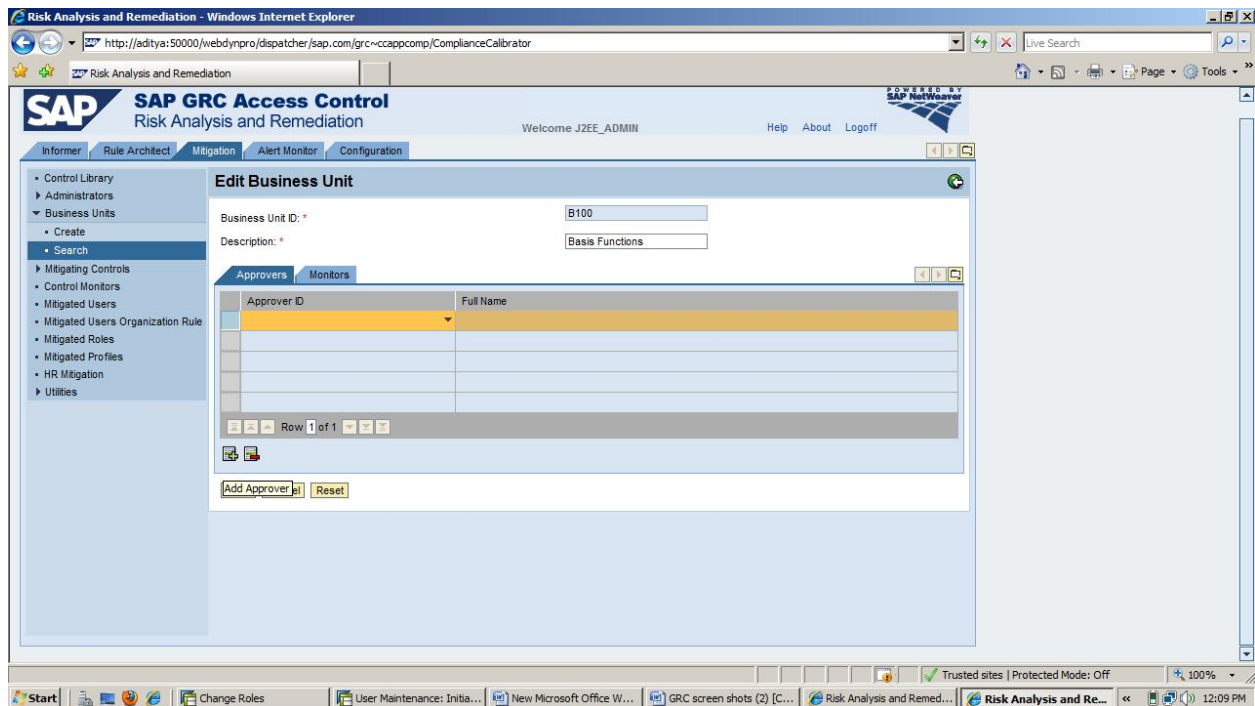
EX:B100

Goto Business Unit → Click on Create → then fill the required details.

→ Give the Business ID, Description and add the Approver & Monitor.

→ Click on Save.

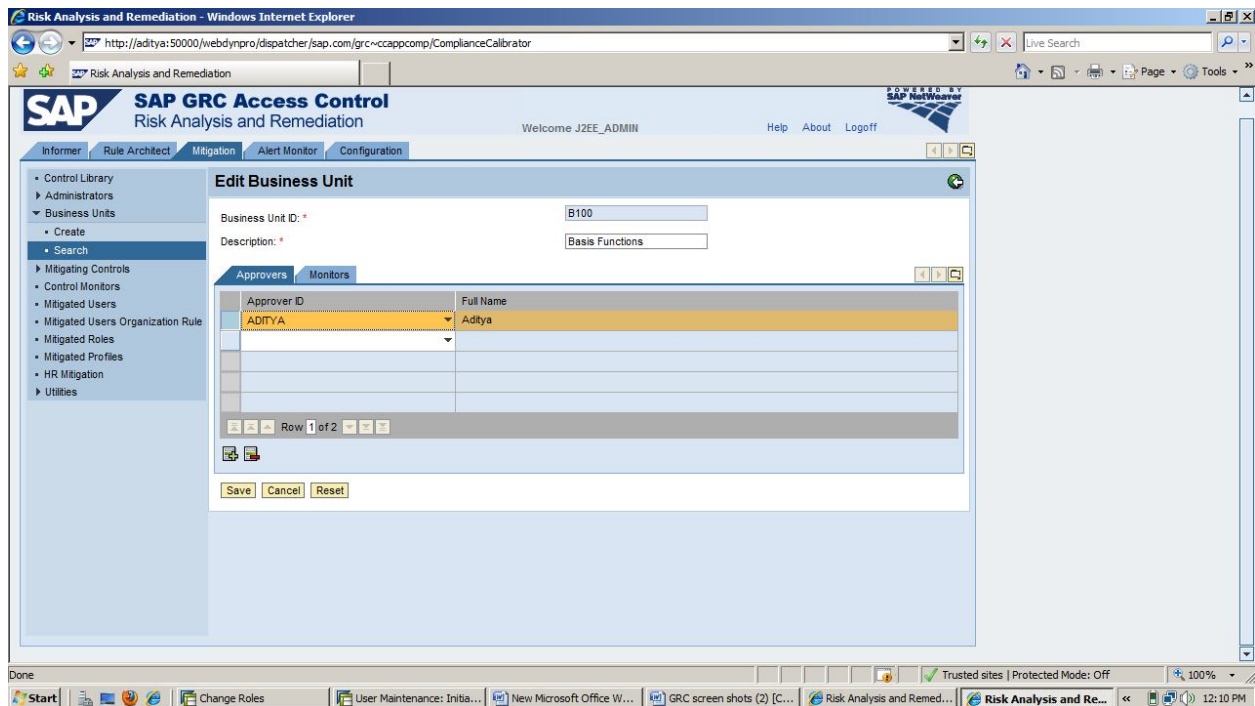
Check the below screen shots.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on the Plus(+) button to add the Approver.



The screenshot displays the SAP GRC Access Control interface in a Windows Internet Explorer browser. The page title is "SAP GRC Access Control Risk Analysis and Remediation". The user is logged in as "J2EE\_ADMIN". The main content area is titled "Edit Business Unit" and contains the following fields:

- Business Unit ID: \* (Text input: B100)
- Description: \* (Text input: Basis Functions)

Below these fields is a table with two tabs: "Approvers" and "Monitors". The "Approvers" tab is active, showing a table with the following data:

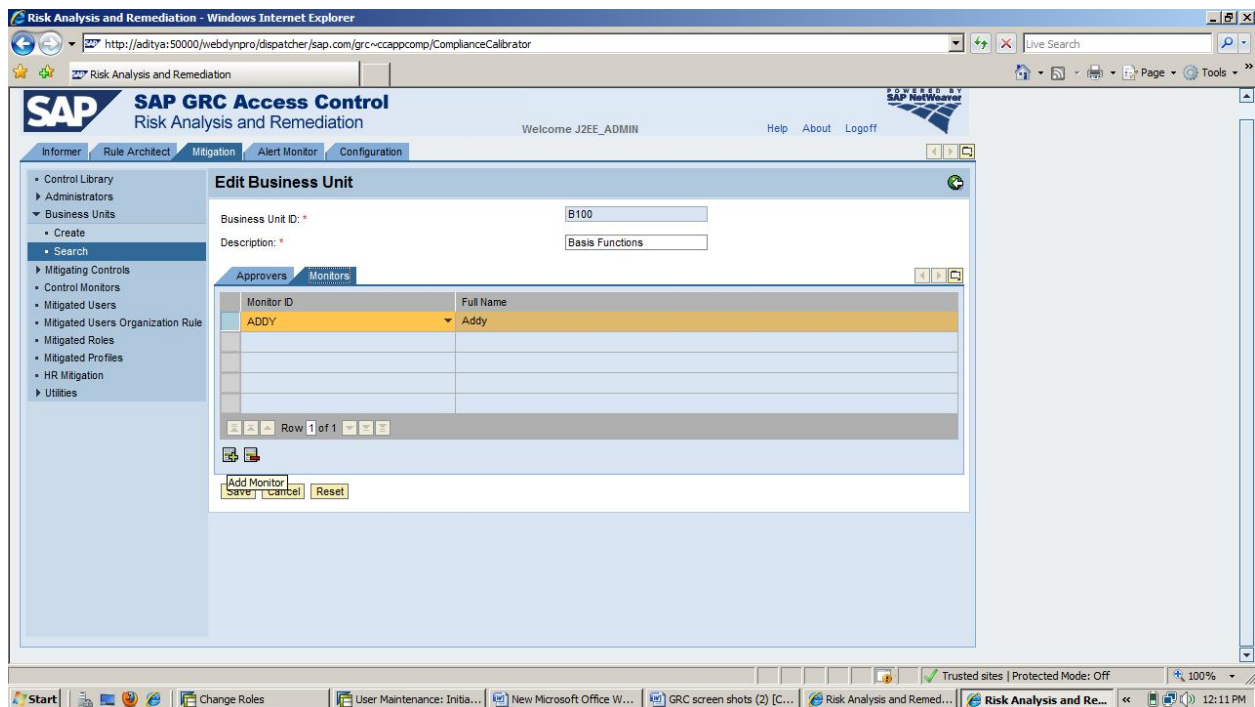
Approver ID	Full Name
ADITYA	Aditya

At the bottom of the table, there is a status bar indicating "Row 1 of 2". Below the table are "Save", "Cancel", and "Reset" buttons. The browser's address bar shows the URL: "http://aditya:50000/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator". The Windows taskbar at the bottom shows several open applications, including "Change Roles", "User Maintenance: Initia...", "New Microsoft Office W...", "GRC screen shots (2) [C...", "Risk Analysis and Remed...", and "Risk Analysis and Re...". The system clock shows "12:10 PM".

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

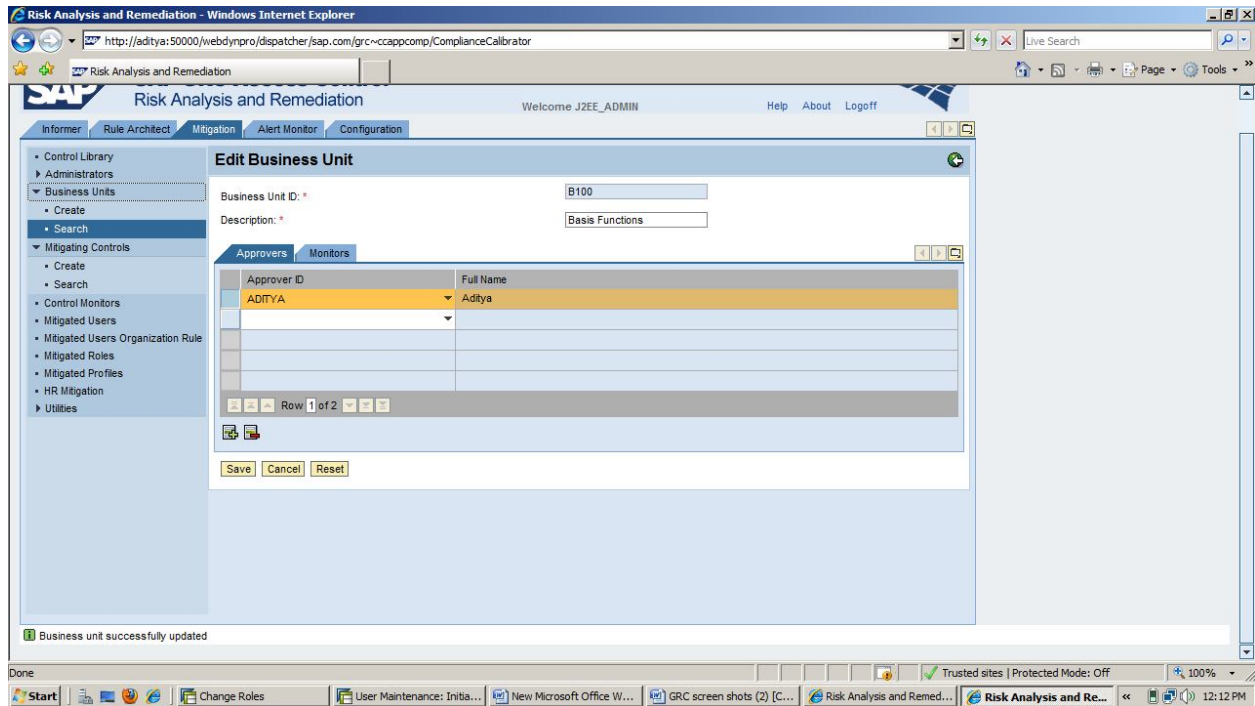
Go to Monitor Tab & Click on the Plus(+) button to add the Monitor.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on Save.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

STEP3:

Mitigating Controls is based upon Risk IDs for Identification. Here Mitigating Control ID is a unique ID which was picked by our own.

EX:B200

Goto Mitigating Controls → Click on Create → then fill the required details.

→ Give the Mitigating Control ID, Description, Business Unit, Management Approver.

→ Add the Associated Risk ID & Monitor.

→ Click on Save.

Check the below screen shots.

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

**SAP GRC Access Control**  
Risk Analysis and Remediation

Welcome J2EE\_ADMIN

Informer | Rule Architect | Mitigation | Alert Monitor | Configuration

Control Library  
Administrators  
Business Units  
Mitigating Controls  
Control Monitors  
Mitigated Users  
Mitigated Users Organization Rule  
Mitigated Roles  
Mitigated Profiles  
HR Mitigation  
Utilities

### Create Mitigating Controls

Mitigating Control ID: \* B200  
Description: \* Mitigation For USER1  
Business Unit: \* Basis Functions  
Management Approver: \* ADITYA

Risk ID	Description	Risk Level
B011	Security Administration & Client Administration	High

Row 1 of 1

Add Risk | Save | Reset

**SAP GRC Access Control**  
Risk Analysis and Remediation

Welcome J2EE\_ADMIN

Informer | Rule Architect | Mitigation | Alert Monitor | Configuration

Control Library  
Administrators  
Business Units  
Mitigating Controls  
Control Monitors  
Mitigated Users  
Mitigated Users Organization Rule  
Mitigated Roles  
Mitigated Profiles  
HR Mitigation  
Utilities

### Create Mitigating Controls

Mitigating Control ID: \* B200  
Description: \* Mitigation For USER1  
Business Unit: \* Basis Functions  
Management Approver: \* ADITYA

Monitor ID	Full Name	Email
ADDY	Addy	addy@gmail.com

Row 1 of 1

Add Monitor

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA



Click on Save.

**Version IT**

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

The screenshot displays the SAP Risk Analysis and Remediation web interface in Internet Explorer. The browser address bar shows the URL: `http://aditya:50000/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator`. The page title is "Risk Analysis and Remediation" and the user is logged in as "J2EE\_ADMIN".

The main content area is titled "Create Mitigating Controls" and contains the following fields:

- Mitigating Control ID: \*
- Description: \*
- Business Unit: \*
- Management Approver: \*

Below the form is a table with the following columns: Monitor ID, Full Name, and Email. The table is currently empty, and the status bar below it indicates "Row 0 of 0".

At the bottom of the form, there are "Save" and "Reset" buttons. A message at the bottom of the page states: "Mitigating control successfully created".



UNDER THE GUIDANCE OF  
RASHEED AHMED

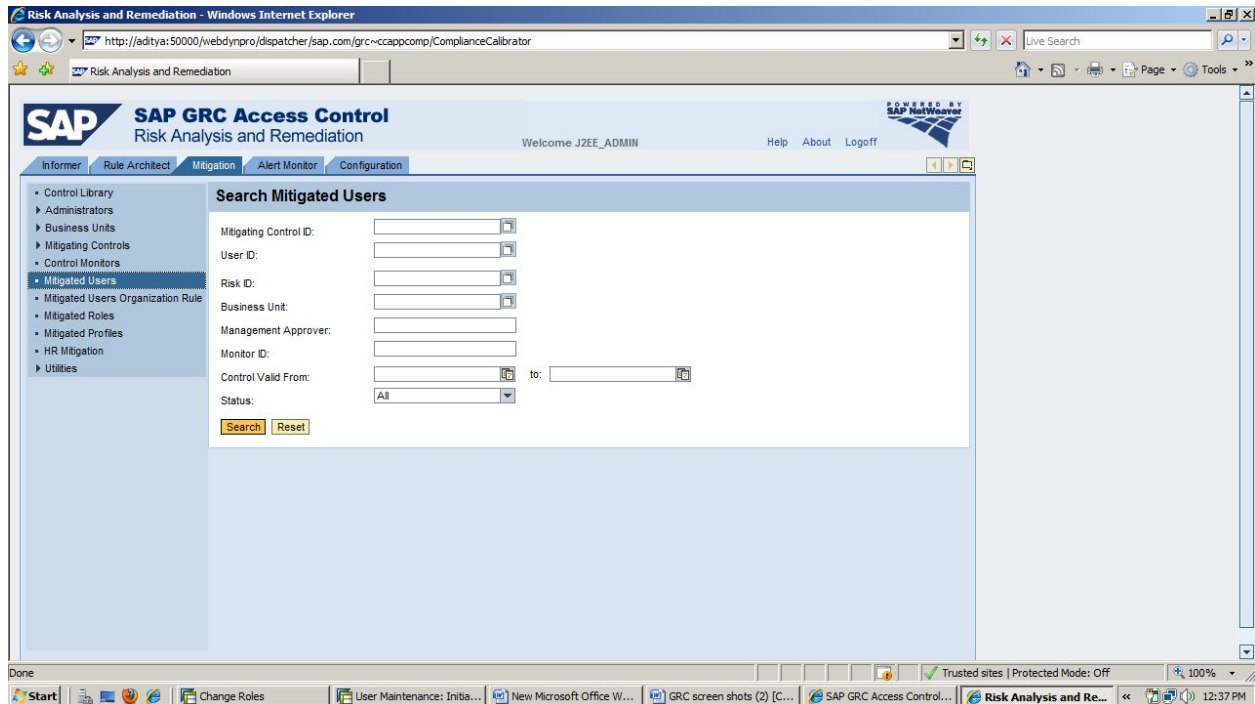


PREPARED BY  
ADITYA JOSYULA

STEP4:

Mitigated Users is used for assigning the Mitigating Control ID's to the User to allow the Risk.

Goto Mitigated Users



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

→Click on Search.

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation web application. The browser window title is "Risk Analysis and Remediation - Windows Internet Explorer". The address bar shows the URL: <http://aditya:50000/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator>. The application header includes the SAP logo, "SAP GRC Access Control Risk Analysis and Remediation", and the user name "Welcome J2EE\_ADMIN". The navigation menu on the left includes: Control Library, Administrators, Business Units, Mitigating Controls, Control Monitors, Mitigated Users (selected), Mitigated Users Organization Rule, Mitigated Roles, Mitigated Profiles, HR Mitigation, and Utilities. The main content area is titled "Search Results - Mitigated Users" and contains a table with the following columns: User ID, Name, Mitigating Control ID, Risk ID, Valid From, Valid To, Monitor, and Status. The table is currently empty. Below the table, there are navigation controls showing "Row 0 of 0" and buttons for "Add", "Change", and "Delete". The Windows taskbar at the bottom shows several open applications, including "Change Roles", "User Maintenance: Inita...", "New Microsoft Office W...", "GRC screen shots (2) [C...", "SAP GRC Access Control...", and "Risk Analysis and Re...". The system clock shows "12:38 PM".

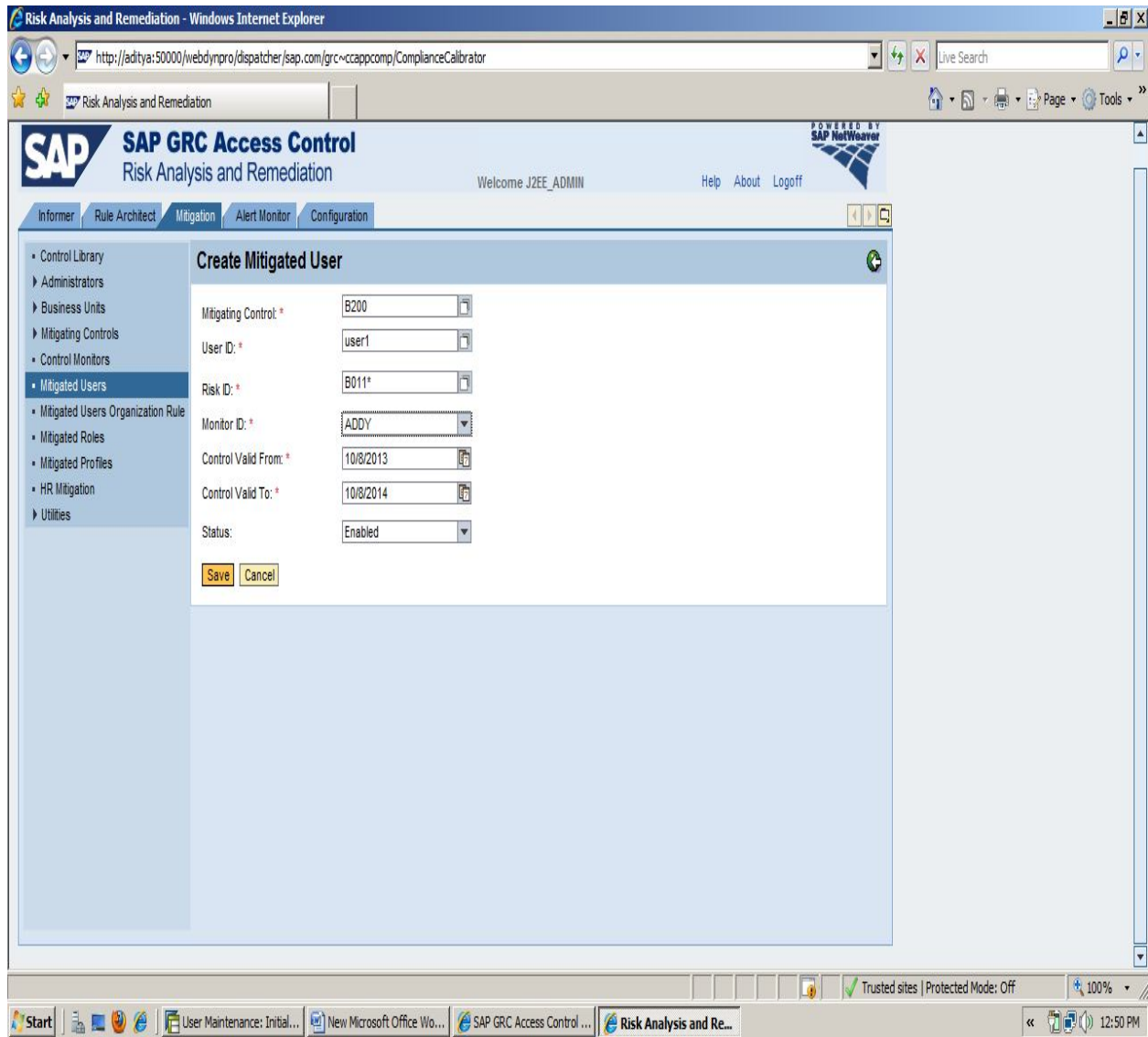
User ID	Name	Mitigating Control ID	Risk ID	Valid From	Valid To	Monitor	Status

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Here click on the add button, then give the Mitigating Control, User ID, Risk ID & Monitor ID.

Here we need to give the Risk ID-B011\* Manually because the Risk ID for the both violations is the same.



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on Save.

The screenshot shows the SAP Risk Analysis and Remediation web interface. The browser window title is "Risk Analysis and Remediation - Windows Internet Explorer". The URL is "http://aditya:50000/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator". The page title is "Risk Analysis and Remediation" and the user is logged in as "J2EE\_ADMIN".

The main content area displays "Search Results - Mitigated Users" with a table containing the following data:

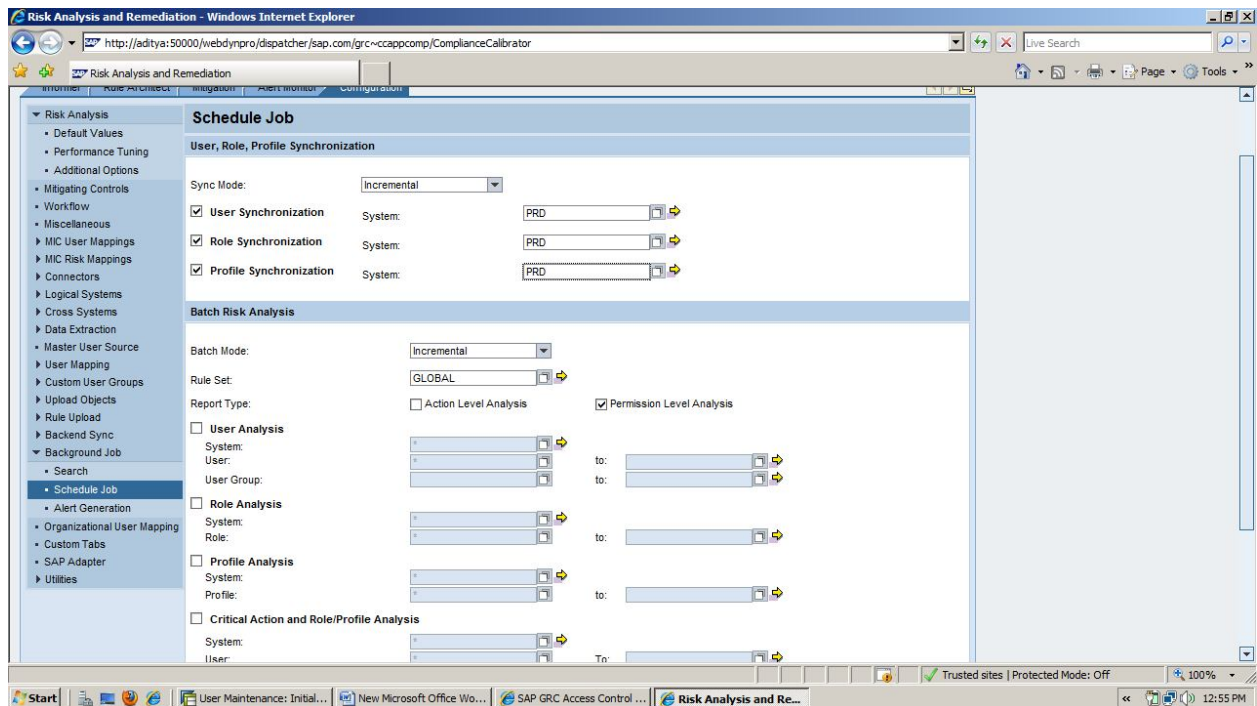
User ID	Name	Mitigating Control ID	Risk ID	Valid From	Valid To	Monitor	Status
USER1	USER1	B200	B011*	10/8/2013	10/8/2014	ADDY	

Below the table, there is a navigation bar showing "Row 1 of 1" and buttons for "Add", "Change", and "Delete". A message at the bottom left of the interface states "Mitigated User created successfully".

UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

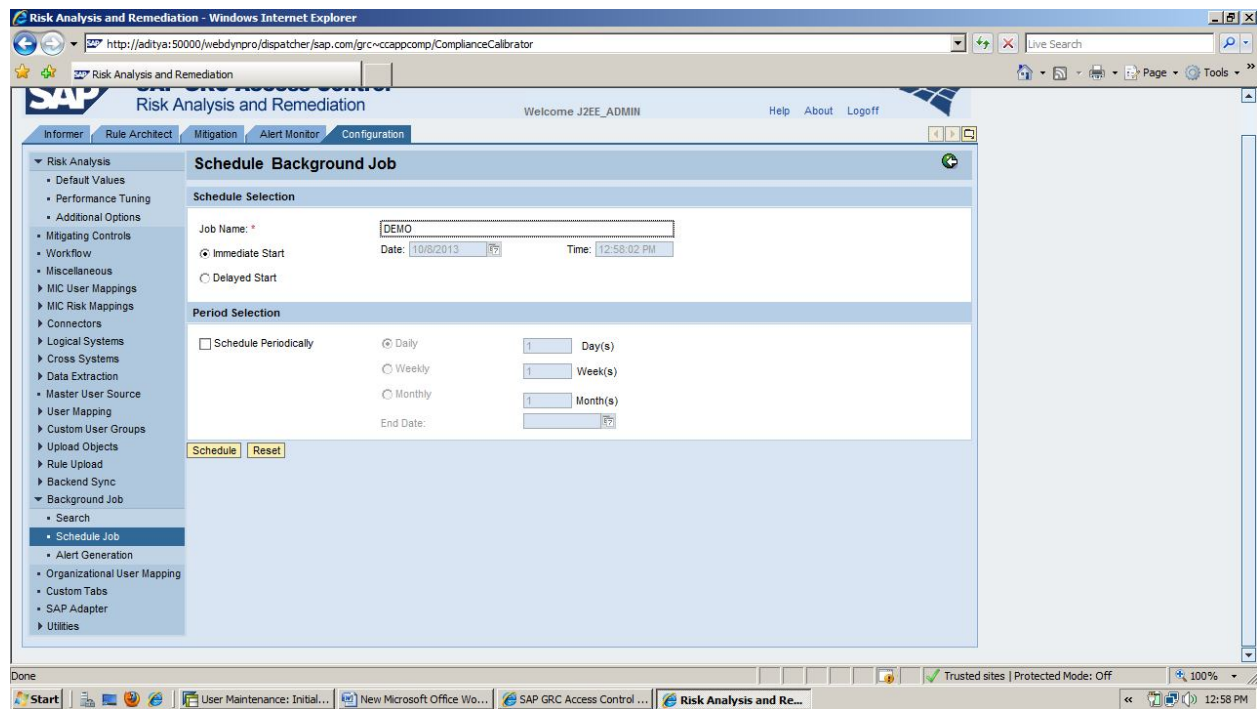
Now Schedule the Background Jobs. Check the below Screen Shot



UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Click on Schedule.

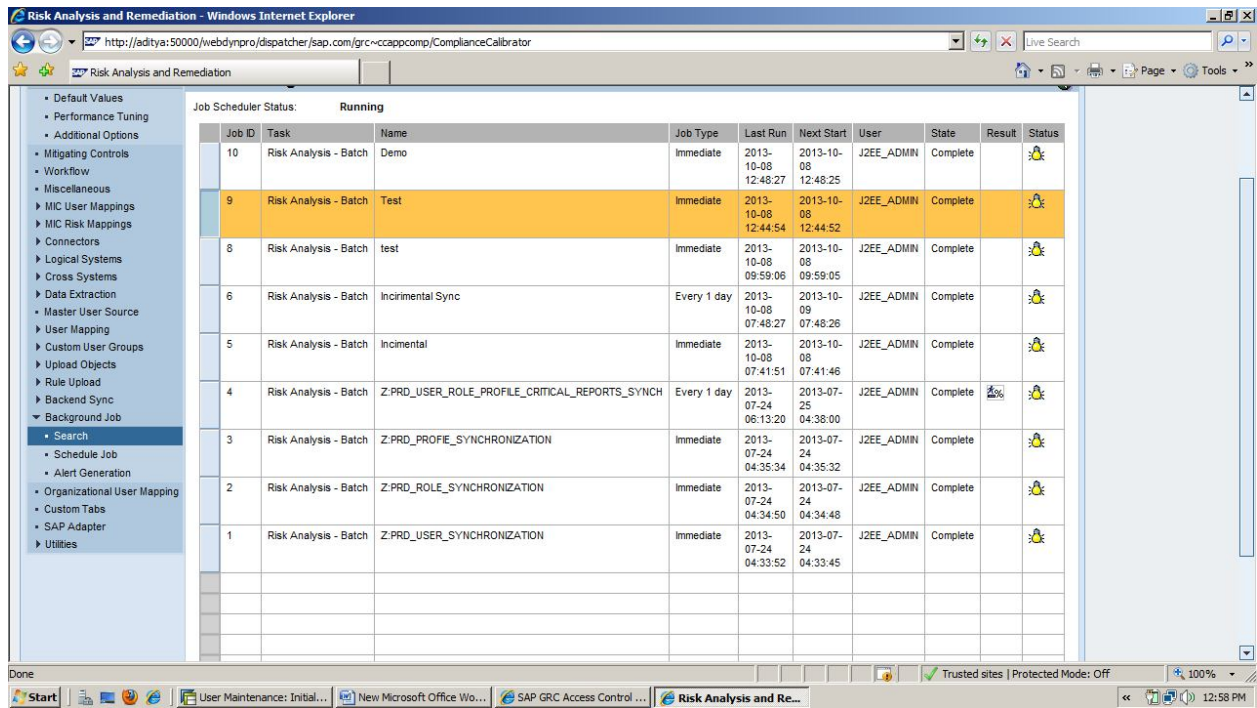


UNDER THE GUIDANCE OF  
RASHEED AHMED

PREPARED BY  
ADITYA JOSYULA

Here give the Job Name & Click on Schedule.

After that check the Job States.



The screenshot shows the 'Risk Analysis and Remediation' job scheduler interface. The 'Job Scheduler Status' is 'Running'. The table below lists the jobs and their current states.

Job ID	Task	Name	Job Type	Last Run	Next Start	User	State	Result	Status
10	Risk Analysis - Batch	Demo	Immediate	2013-10-08 12:48:27	2013-10-08 12:48:25	JZEE_ADMIN	Complete		
9	Risk Analysis - Batch	Test	Immediate	2013-10-08 12:44:54	2013-10-08 12:44:52	JZEE_ADMIN	Complete		
8	Risk Analysis - Batch	test	Immediate	2013-10-08 09:59:06	2013-10-08 09:59:05	JZEE_ADMIN	Complete		
6	Risk Analysis - Batch	Incremental Sync	Every 1 day	2013-10-08 07:48:27	2013-10-09 07:48:26	JZEE_ADMIN	Complete		
5	Risk Analysis - Batch	Incidental	Immediate	2013-10-08 07:41:51	2013-10-08 07:41:46	JZEE_ADMIN	Complete		
4	Risk Analysis - Batch	Z.PRD_USER_ROLE_PROFILE_CRITICAL_REPORTS_SYNCH	Every 1 day	2013-07-24 06:13:20	2013-07-25 04:38:00	JZEE_ADMIN	Complete		
3	Risk Analysis - Batch	Z.PRD_PROFIE_SYNCHRONIZATION	Immediate	2013-07-24 04:35:34	2013-07-24 04:35:32	JZEE_ADMIN	Complete		
2	Risk Analysis - Batch	Z.PRD_ROLE_SYNCHRONIZATION	Immediate	2013-07-24 04:34:50	2013-07-24 04:34:48	JZEE_ADMIN	Complete		
1	Risk Analysis - Batch	Z.PRD_USER_SYNCHRONIZATION	Immediate	2013-07-24 04:33:52	2013-07-24 04:33:45	JZEE_ADMIN	Complete		

The State would be COMPLETE

UNDER THE GUIDANCE OF  
RASHEED AHMED

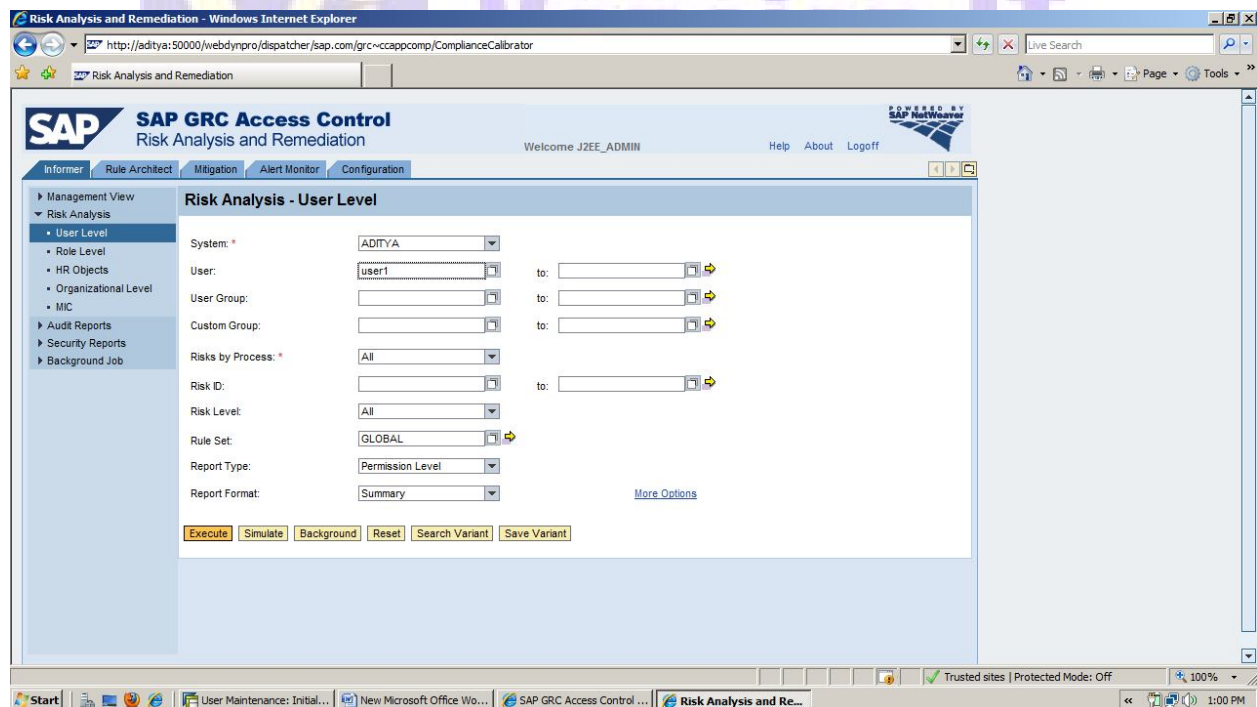
PREPARED BY  
ADITYA JOSYULA

Now Go back to the Informer Tab and find out the Risk to that User ID:USER1

GO to Risk Analysis → User Level.

Mention the System and User name.

Check the below screen shots.



UNDER THE GUIDANCE OF  
RASHEED AHMED



PREPARED BY  
ADITYA JOSYULA

Click on Execute.

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The main heading is "User Analysis at Permission Level - Summary Report". The interface includes a navigation menu on the left with options like Management View, Risk Analysis, User Level, Role Level, HR Objects, Organizational Level, MIC, Audit Reports, Security Reports, and Background Job. The main content area shows selection criteria and a table of results.

**Selection Criteria**

System:	PRD	User Type:	Dialog
User:	USER1	Ignored Users:	Locked and Expired
User Group:		Exclude Mitigated Risk:	Yes
Custom Group:		Offline Analysis:	No
Risks by Process:	All		
Risk Level:	All		
Risk ID:			
Rule Set:	GLOBAL		
Report Type:	Permission Level		

Run Date/Time: 2013-10-08 13:00:51

User: USER1 (USER1)      User Group:      System: ADITYA

Conflicting Actions	Risk Description	Level	Business Process
No Violations Found			

Now you won't find any Violations.

UNDER THE GUIDANCE OF  
RASHEED AHMED