By OnlineInterviewQuestions.com

GRC Interview Questions

GRC is abbreviated as Governance, Risk and Compliance solution which can be defined as a body that helps various organizations in managing regulations. It also helps in removing any risk that may harm the organizations' vital operations. GRC basically performs a list of activities that help organizations to manage their guidelines and keeps auditing inappropriate documents, spreadsheets, files, etc as organizations may face legal issues due to external auditors if GRC is not present in an organization or company. GRC has various advantages and applications like :

- GRC is less complex and thus activities can be easily managed.
- It helps in improving risk identification, risk evaluation, and management activities.
- It contributes to planning strategies that help in corporate management and policy management activities.
- Measures to ensure guarantees conventionality with laws, policies, and formalities of organizations.
- GRC is a wide collection of activities rather than a single activity constructed for achieving high standards.

GRC is divided into various modules that perform a particular activity to reduce risk in any organization. Some of its modules are GRC Access Control, SAP GRC Process Control and Fraud Control Management, SAP GRC Risk Management, SAP GRC Audit Management, SAP GRC Global Trade Services and many more. Below are mostly asked **GRC Interview Questions**.

Q1. What is the SAP GRC?

SAP GRC abbreviated as System, Applications, and Products (SAP), Governance, Risk and Compliance (GRC) which is an integrated body combining of various activities which unite help the organizations to regulate several policies and reduce various risks. It is made up of three different terms viz. Governance, Risk, and Compliance which has specific definitions in this field which is as follows :

- **GOVERNANCE:** Governance is the combination of various processes which are established by various members of the board to automate various rules and conventions.
- **RISK:** Risk management is the proper procedure of managing risks in an organization and predicting future risks to run the organization smoothly and in a hassle-free manner.
- **COMPLIANCE:** Compliance focuses on following various rules regarding the company's policies, procedures, laws, rules and regulations and many more.

Q2. What is UME and how it works?

UME stands for the user management system. When A user tries to access a tab whose access is not with them, the tab will not display when the user tries to access that tab. A user can only access a function when a UME

action is assigned for a tab for that particular user.

In the tab "Assigned Actions" of Admin user, all the available standard UME actions for CC tabs can be found.

Q3. What are the key activities that Process control shares with Access control in GRC?

Risk control needs to be performed as a part of compliance and regulation practice, it is required to mitigate risk in an organization.

A critical part of managing risk in an organization is to define the responsibilities clearly, managing role provisioning and managing access for the superuser.

Q4. What is the Audit Risk Rating(ARR)?

To define the criteria for an organization so that risk rating can be found and ranking for risk rating can be established, Audit Risk Rating is used. As per management feedback, each audible entity is rated in Audit Risk Rating (ARR). ARR can be used to perform the tasks given below:

- Set of audible entities and risk factor can be found out
- Risk score for a risk factor in each auditable entity can be defined and evaluated.
- The auditable entity can be rated as per risk score.
- By comparing risk scores for different auditable entities users can also generate an Audit plan from Audit Risk Rating (ARR).

Q5. What is the difference between preventive mitigation controls and detective mitigation controls?

Difference between preventive mitigation controls and detective mitigation controls

Preventive Mitigation Controls	Detective Mitigation Controls
Preventive mitigation control measures are basically used to lessen the effect of risk even before the risk actually occurs.	Detective Mitigation Controls measures are used when an alert of a risk is already generated which means when the risk occurs.
Various activities to be performed under this process are: Configuration, user exits, security, defining workflow and custom objects.	Various activities to be performed under this process are activity reports, alert information, budget reviews and comparisons between plans made and reviews generated.
Preventive mitigation helps in releasing strategies and authorization limits.	Detective Mitigation Controls help in deducing and analyzing various risks.
It also contributes to preventing future risks and encourages the development of the company.	It also helps in analyzing the sole reason for risk and measures of preventing it in the future for the sake of the organization.

Q6. Explain the various advantages of using Global Trade Services?

The advantages of using Global Trade Services are described below:

1. The cost and effort of managing compliance for global trading can be reduced by using Global Trade Services.
2. It can help in improving productivity and can also ease time-consuming manual tasks.
3. The penalties for trade compliance violations can be reduced by using it.
4. It can improve the quality of services and can yield better customer satisfaction.
5. To avoid trade with sanctioned or denied parties and to create and improve the brand and the image Global Trade services are very helpful.
6. By performing customs clearance, it fastens the inbound and outbound processes. It can also help in removing unnecessary delays.

Q7. Can super user act as Firefighter?

Yes, superusers can act as Firefighters and they have the following additional capabilities:

1. To perform tasks outside of their normal role or profile, it can be used in the case of an emergency situation.
2. Firefighter ID's can be assigned only by certain individuals (owner).
3. It can create an auditing layer to monitor and record usage. An extended capability is allowed for it.

Q8. What is Internal Audit Management(IAM)?

Internal Audit Management allows a user to process the information from Risk management and from process control to use it in audit planning. The proposals of audit can be transferred to audit management for processing whenever required and the issues for reporting can be generated by using the audit items. Internal Audit Management provides the users with space where they can perform complete audit planning, create audit items, define audit universe and create and view audit reports and audit issues.

Q9. What is an Audit Universe?

Audit Universe is that space which contains audit entities which can be classified as Business units, Lob's or departments. The audit planning strategies are defined by audit entities and these can be linked to Process control and Risk management to find risks, controls, etc.

Q10. Explain the use of Report and Analytics Work Center in GRC.

Process control, Risk management, and access control share the Reports and Analytics Work center. The Risk

and Analytics Work Center mainly work under certain verticals like Access Dashboards, Access Risk Analytics Report, Security reports, role management reports, Audit Reports, and Superuser Management Reports. This sections perform a certain group of activities and then submit their report to the board for analysis. This body acts as a central location for displaying reports and dashboards like user analysis and various other reports.

Q11. What is SoD Risk Management?

SoD Risk can be defined as the risk that causes or may cause problems to the members of a particular organization. due to its working operations and projects, Segregation of risk management starting from Risk recognition to rule building validation and various other risk management activities to follow continuous compliance, it is required in every business. There is no need to perform segregation in the GRC system if the roles are different.

Q12. Briefly explain the common roles and key duties of GRC based on SoD.

These are the following common roles and their key duties based on SoD:

Business Process Owner:

- Identifying and approving risks for monitoring.
- Approving remediation that involves user access.
- Designing controls to mitigate conflicts.
- Communicating about role changes or access assignments.
- Performing proactive continuous compliance.

Senior officers:

- Approving or rejecting risks between business areas.
- Approving mitigation risks for selected areas.

Security Administrator:

- Assuming the ownership of GRC tools and security processes.
- Designing and maintaining rules to identify the risk conditions
- Customizing GRC roles to enforce roles and responsibilities.
- Analysing and remediating SoD conflicts at the role level.

Auditors:

- Performing risk assessment on a regular basis.
- Providing specific requirements for audit purpose.
- Performing periodic testing of rules and mitigation controls
- They act as a liaison between external auditors.

SoD Rule Keeper:

- Performing GRC tool configuration and administration.
- Maintaining controls over rules to ensure integrity.
- They act as a liaison between basis and GRC support center.

Q13. How do you perform risk classification? What is the difference between low, medium and high-risk classification?

The risks should be classified as per the policy of the company. There are various risk classifications that can be defined as per risk priority and company policy:

Critical-

For risks that contain the company's critical assets that may be compromised by fraud or system disruptions, Critical Classification is done.

High-

Physical or monetary loss or system-wide disruption includes fraud, loss of any asset or failure of a system are included.

Medium-

Multiple system disruptions like overwriting master data in the system are included in this.

Low-

These are the risks in which either productivity losses or system failures are compromised by fraud or system disruptions. In this, the loss is said to be minimum.

Q14. Explain the use of GRC risk management.

GRC Risk Management is used to manage and control all types of risks occurring or going to occur in the future. There are several uses of GRC Risk Management. Some of them are as follows :

- The main focus of Risk Management is on organizational alignment towards various factors like the risks which need immediate concern, risk mitigation, and associated thresholds.
- Risk Management systems perform qualitative and quantitative analysis of risks to figure out the level of risk to decide for the organization whether to take it or not.
- It also comprises of various solutions to risks.
- It identifies risks in an organization.
- It performs both preventive mitigation controls and detective mitigation control methods.

Q15. What is SAP GRC fraud management?

SAP GRC fraud management is a body that helps to discover frauds and prevent them at an early stage to minimize any type of loss that can occur to the organization.

Q16. Explain the use of the following commands: RSECADMIN & RSECADMIN

RSECADMIN is used to maintain authorizations for reporting users.

RSECADMIN is used to maintain analysis authorization and role assignment to a user.

Q17. How do you implement Firefighters ID in the SAP GRC system?

Following steps are followed to implement firefighter ID's:

- For each business area, create a firefighter ID.
- The next step is to assign the necessary roles and profiles to carry the firefighting tasks.
- The profile SAP_ALL should not be assigned.

Q18. Define Derived role in GRC?

The role that is already existing is known as the **derived roles**. They are generally seen as the menu structure that contains certain functions to provide services like- transactions, reports, Web-links and so on. But an existing role can only inherit as a menu or function if it was never assigned with transaction codes until now.

They have a very proper way of maintaining roles, now those roles they do not differ in their functionality; like the menus and the functions provided by them. They just follow different characteristics when in contact with different organization levels.

Q19. Define the Composite role in GRC?

A group of several different roles is collected in one container and that container is known as a **composite role**. It can be also called as roles. Now, these roles do not deal with authorization data. So for changing authorizations that are represented by the composite roles, we just need to maintain each role separately for maintaining the data which is time-consuming.

Q20. How many authorizations fit into a profile?

The **maximum number of authorizations** that can be fit into a profile is **150**. A number of profiles for the role is being generated when the total number of authorizations exceeds that maximum marker level and this process is done by the Profile Generator.

Total characters in a name that consists of a profile are 12 and the first 10 characters can be changed when it is being generated for the first time.