SAP Access / Authorization Issue

Category: Access/Account

Sub-Category: User Account

Group: Access/Authorization to SAP Systems and Apps

Step No.	Action	Details / Sub-Steps	Expected Outcome
1	Validate User Access Request	- Confirm user details (Employee ID, Department, Role). - Validate request type: **standard, developer, or business role**. - Ensure proper approval via **GRC/ITSM workflow** if applicable.	User request validated with correct justification.
2	Check Role Assignment	- Run SU01 → Roles tab to review assigned roles/profiles. - Verify if standard access roles already include **SE38** or **RSUSR100N** authorization. - Check role validity dates.	User's assigned roles identified.
3	Assign Standard Roles	- If missing, assign pre-approved **standard roles** for transaction access. - Ensure changes align with **role catalog** and SoD compliance.	Standard roles assigned successfully.
4	Verify Access in SE38	- Have user retry SE38 → Run program **RSUSR100N**. - If denied, proceed with trace analysis.	Access test confirms role sufficiency or indicates missing authorization.
5	Analyze Missing Authorizations	- Execute **ST01** or **SU53 (Authorization Check)** to capture missing objects. - Identify which authorization object is blocking access. - Note TCODEs like SE38, SPRO, LTMC, or custom objects.	Missing authorization objects identified.
6	Apply Custom Roles/Objects	- Modify or assign **custom role** in **PFCG** with required authorization objects. - Adjust **field values (Auth fields)** per	User receives access with correct custom

		business requirement. - Re-generate and transport roles.	objects.
7	Review Security Policy	- Ensure assignment complies with **org security policies**. - Validate segregation of duties (SoD) using **SAP GRC Access Control**. - Escalate to security team if high-risk transaction.	Role assignment is compliant and risk-free.
8	Implement Workflow Controls	- If recurring, configure **GRC Firefighter ID** or temporary elevated access workflow. - Use **IdM workflows** to streamline request/approval process.	Automated approval workflow in place.
9	Re-Test & Confirm	- Confirm successful execution without authorization error.	User gains expected access.
10	Document & Close	-Document actions taken. - Mark resolution type as **Access/Authorization Provided**.	Ticket documented and closed successfully.