SAP Basis, Security & BI Audit for Real Estate Company

SAP BASIS, Security and BI AUDIT

The Summary

Client has Approached AG Technologies for SAP Basis Audit Security Audit along with Audit of SAP Solution Manager, Saprouter audit and SAP BI general & Security audit.

The Client

Client is one of the leading real estate development groups in India. Client's focus is on the development of premium residential, commercial, retail, integrated townships, lifestyle gated communities and redevelopment projects primarily in the Mumbai Metropolitan Region (MMR) & Pune. The group is also undertaking projects in other key cities in India such as Hyderabad, Surat, Nagpur, Jaipur & Udaipur.

The Group has interests in real estate development, property and project management, engineering, procurement and construction (EPC) contracting for power transmission and infrastructure projects including road projects, warehousing and logistics.

The Business Requirement

Client approached AG Technologies for SAP Basis & Security Audit for R/3 ECC 6.0 along with SAP Solution Manager Audit, SAP saprouter Audit and SAP BI 7.0 general & Security Audit.

The Solution

AG Technologies Audit reports contains detailed analysis & report on each area with parameters AGT's Observation, Business impact of observations noted, AGT Recommendations and Approved Recommendation with symbolic indicator for Approved Recommendations showing whether it is Security implication / Document should maintained / Process change / Achievement.

Project Summary

Industry: Real Estate

Client Profile: One of the leading real estate development groups in India.

Solution: AG Technologies has done SAP Basis, SAP Security, SAP Solution Manager and SAP BI general and security Audit.

Solution Benefit:

- Helps in implementing best industry practice.
- Daily health check helped customer to take preventive action before any disaster take place.
- SAP backup policy stabilized
- SAP backup policy stabilized

Solutions highlight are as follow:

A) SAP Basis Audit :

1. Only Authorized person will have access to process and administer batch jobs and background session in SAP.
2. It will ensure that the frequency of health checkup is correct and proper checkup documents are maintained for R3 & BI landscape. It will also ensure that the corrective measures are taken post health check up.
3. The process will ensure Proper Transport Management routing & flow of request and even correct client distribution on R/3 & BI landscape for development, quality and production is implemented.
4. It will identify policy & regularly update on SAP support Packs & SAP Kernel Stacks.
5. Limited user id will be provided to end users on the bases on SAP agreement.
6. It will ensure that latest Oracle Patch is installed & correct tool is used to perform Database activity.
7. It will ensure that correct file system is created and even environment variables are correctly maintained as per SAP recommendation.

B) Security Audit :

1. It will ensure that Security Audit Log is activated.
2. Process will ensure correct user license Usage is performed and proper password protected file is maintain with the entire Admin user password. Only the basic Administrator will be authorized for user creation, deletion & updating Activity.
3. It will make sure that only authorized employees are having appropriate access and will disable the access to employee those who had left the organization.

C) SAP Solution Manager Audit :

1. It will ensure MOPZ is configured for downloading patch & Early Watch Report is configured.
2. The process will make sure that only authorized person is having appropriate access and correct user license are maintained.

D) SAP saprouter Audit:

1. It will ensure that correct restrictive entries are inserted in Saproutlab.

E) SAP BI 7.0 General Audit:

1. Process will check whether existing process chain & dependency between chains & documents are correct.
2. Process will check and control whether the growth of data does not affect the system usability in future after growth of historical data.
3. Process will check that the data failure is reported to Management for review & corrective steps are taken.
4. It will ensure any patch upgrade in ECC and its effects on BI system is documented.
5. It will ensure & review if any change done in data flow/BI architecture/New Report Design follows Change Management Process.
6. It will ensure any changes done BI Objects follows Change Management Process guidelines and New BI Objects follow the proper naming convention.

F) SAP BI SECURITY AUDIT - BI 7.0

1. Review of User Roles/Authorization objects & Controls to protect against unauthorized visibility of critical data in BI Reports.
2. Ensure only authorized developer can delete the data from BI Objects like Cube/DSO/PSA etc. and to ensure business critical data is not deleted by unauthorized person.
3. Controls to ensure that only authorized person can create or delete objects in BI Development server
4. Safeguard against unauthorized deletion of BI Objects in Productive environment/Development environment
5. Controls to ensure unauthorized modification of BI Objects in Production /Development
6. Infoarea design review for better control over BI object data security and redesigning of Infoareas for better control over BI Objects data security

Technology:

SAP Solution	**:** SAP ECC 6.0
Operating System	**:** AIX P Series 5.3
Database	**:** Oracle 10G

The Solution Benefit

- Helps in implementing best industry practice.
- After audit client started to do daily health checkup. Daily health check helped customer to take preventive action before any disaster take place.
- Customer Patched there SAP technical patches to latest release, which help them to remove security loops of the system.
- Authorization stabilized, previously many users where having full rights of SAP, audit has removed all these loop holes.
- SAP backup policy stabilized.
- System database growth was very high, after audit we found there was DBTABLOG table which was not required. We have truncated the table to reduce the database size and stopped the table logging.
- OS level authorization stabilized, all employee of client were able to telnet the server, we have suggested customer to provide the access of OS to restricted people.