

Compliance with Section 128 of the Companies Act

Audit Trail and Daily Backup

Pune Branch of WIRC
March 20, 2025

Note

- I will be sharing the presentation slides through the Branch office
- Ask questions – I may answer them immediately or park the question for Q&A



Background

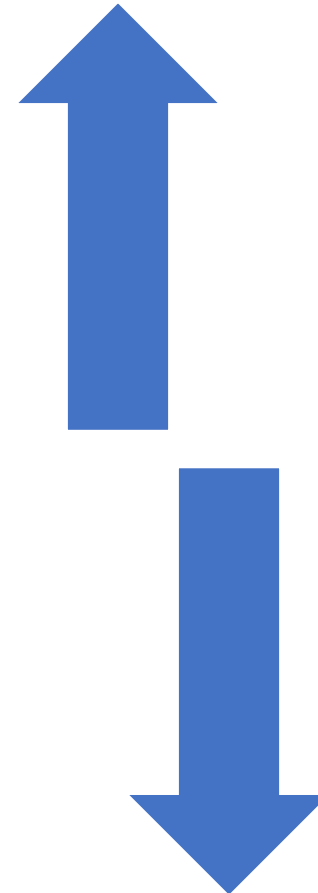
Information Technology is a **Monster** on our shoulder Agree?

It is up to you how you look at this Monster

Technology is inevitable ... specially after Corona

Even Government is using technology

Audits cannot be done without technology ...



Pre Corona

- Physical evidences
- Physical audit visits

Post Corona

- Electronic evidence
- Virtual audits

Compliance with Section 128 of the Companies Act

Audit Trail and Daily Backup

Session Objective –

1. Understanding the regulatory requirement – daily backup and audit trail
2. Management & Auditors' responsibilities
3. Reporting compliance and consequences of non-compliance
4. Checklist for auditors
5. Testing guidance – Tally and SAP ERP

Daily Backup



Regulatory Requirement – Daily Backup

What led to Daily backup .. Backup in India

- Large corporates with global presence, started consolidating IT resources including servers and data – economy of scale and better security
- What resulted in insisting data backup
 - Instances where data stored outside India, where access is not made available to regulators
 - Instances of data beach – resulting non availability of data for investigations

Regulatory Requirement – Daily Backup

The Requirements of Daily backup under Section 128 of the Companies Act, 2013, and the Companies (Accounts) Rules, 2014 -

- The Ministry of Corporate Affairs (MCA) has tightened its grip on data security with the "Companies (Accounts) Fourth Amendment Rules, 2022," announced in August 2022. These amendments **mandating daily backups of all electronic books of account and relevant documents**. This replaces the earlier, less stringent "periodic backup" requirement and took effect immediately on 11th August 2022.
- Backup is scheduled on daily basis
- Backup on servers physically located in india .. regardless of where the primary data resides.

Regulatory Requirement – Daily Backup

The Requirements in nutshell –

- **Books of accounts & Electronic records** - maintain books of account, including ledgers, journals, **and other documents**, on a daily basis.
- **Secure storage** - The backups must be stored in a secure manner, with encryption & access controls.
- **Multiple copies** - maintain multiple copies of the backups, including at least one off-site copy.
- **Data integrity** - ensure the integrity of the electronic records and backups,
- **Retention period** - The backups must be retained for a minimum period of 8 years.

Regulatory Requirement – Daily Backup

Management Responsibility -

- **Ensure daily backups** - ensure that the company's electronic records, including financial data, are backed up daily.
- **Designate backup responsibility** - designate a responsible person to oversee the daily backup process.
- **Ensure Secure Storage** - backups are stored in a secure manner, using encryption and access controls.
- **Verify Backup Integrity** - verify the integrity of the backups periodically through restoration testing.
- **Maintain backup records** – maintain records of the backups, including date, time & details of the backup.

Regulatory Requirement – Daily Backup

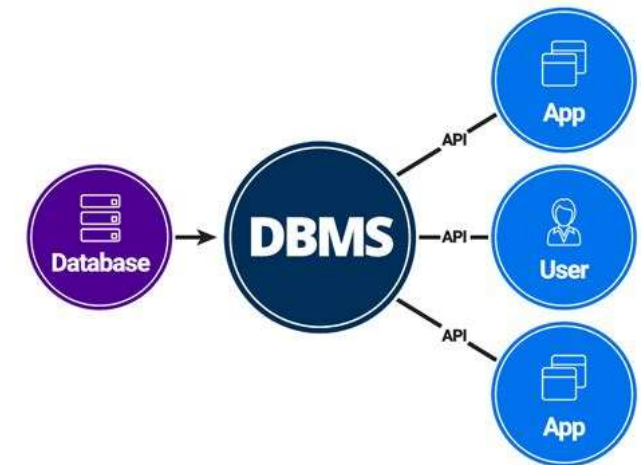
Auditors Responsibility –

- **Review backup procedures** - review the company's backup procedures for adequacy & effectiveness.
- **Test backup integrity** - test the integrity of the backups to ensure they can be restored in case of a disaster.
- **Evaluate backup security** - evaluate the security measures in place to protect the backups.
- **Report backup deficiencies** - report any deficiencies or weaknesses to the management
- **Check Retention of backup** is as per requirements
- Can management **reproduce the books** from backed-up data?

Regulatory Requirement – Daily Backup

Methods of Backup

- What is critical for auditors
 - Frequency, Format & Verification
- Incremental Back up Vs full Backup
 - Grand Father – Father – Son Technique
 - Full backup
- Backup of – Data and / or Server
 - Tally data is part of Tally folder on user machine or server
 - Large ERP data is huge and separate than the application



Regulatory Requirement – Daily Backup

Checklist for Auditors

- What constitutes “**Books of Accounts**” – important to include **relevant papers**
- Is Backup policy amended to include requirements of daily back-up?
- Whether Backup and Restoration testing is part of management exercise?
- Whether backup is manual or automated (through tools)?
- Has management demonstrated restoration during the year?
- Whether backed-up data is retained for 8+ years?

Audit Trail



Regulatory Requirement – Audit Trail

What led to “Audit Trail” requirement ...

- **Stock Market Scam 1990s to 2000** – audit trail to prevent authorised access
- **Satyam Scandal 2009** – need of audit trail to prevent and detect corporate frauds
- **Current scenario 2010 onwards**
 - Data Breaches -
 - Increasing Cyber Attacks

Instances led to requirement of “Audit Trail” ...

- IT Act 2000
- RBI Guidelines for Banks
- DPDP Act 2023

Regulatory Requirement – Audit Trail

“Audit Trail” ... how it helps

- **Accountability** – organisations are accountable for their actions
- **Transparency** – transparency in processing data, tracking & monitoring
- **Security** – detect and prevent unauthorised access
- *Now Compliance – to demonstrate compliance*

Regulatory Requirement – Audit Trail

Section 128 of the Companies Act 2013 read with Rule 3 of the Companies (Accounts) Rules, 2014.

Audit Trail feature in accounting software from 1st April 2023.

For the financial year commencing on or after the 1st day of April 2023, every company which uses **accounting software** for **maintaining its books of account**, shall use only such accounting software which has a **feature of recording audit trail of each and every transaction**, creating an **edit log of each change** made in books of account along with the **date when such changes were made and ensuring that the audit trail cannot be disabled**.

Regulatory Requirement – Audit Trail

Key Requirement of Sec 128 (Audit Log)

Electronic Maintenance of Books of Account – applies to company maintaining its books of account and other **relevant books** and **papers** in electronic mode.

Audit Trail - ensure availability of :

- Source documents, Accounting entries, Adjustments & Deletions.

Integrity and Security - Protection against **unauthorized access**, data **tampering** & Data **backup and recovery**.

Retention Period - The company must retain the electronic records for a minimum period of 8 years.

Regulatory Requirement – Audit Trail

What constitutes Audit Trail or Log

- **Date and time** of each transaction.
- **Nature** of each transaction (e.g., addition, deletion, modification).
- Details of the **person** making the transaction.
- Details of the changes made to the books of account and other relevant **books and papers**.

Who, When and What

Regulatory Requirement – Audit Trail

Management Responsibility

- Ensuring that the audit log is maintained
- Ensuring that the audit log is accurate, complete, and tamper-proof.
- Ensuring that the audit log is protected from unauthorized access.
- Ensure audit log is retained as per requirement

Regulatory Requirement – Audit Trail

Auditors Responsibility (Rule 11(g)) ... Verification and Reporting

- Whether the audit trail feature is configurable (i.e., if it can be disabled or tampered with)?
- Whether the audit trail feature was enabled/operated throughout the year?
- Whether all transactions² recorded in the software are covered in the audit trail feature?
- Whether the audit trail has been preserved as per statutory requirements for record retention

Regulatory Requirement – Audit Trail

Checklist for Auditors

- **List of applications** to be covered for audit trail – applications covering financial transactions and reporting
- Is audit trail enabled?
- Whether log includes – who, when, and what?
- Has management done any testing of availability of Audit trail?
- Whether logs are non editable?
- Whether backed-up data which is retained for 8+ years also includes audit trail or Audit logs? (Retention Testing – applicable from this year)

Regulatory Requirement – Audit Trail

Reporting by auditors

- ICAI guide provides templates for reporting
- Exceptions which needs to report
 - Audit log data is editable resulting difficulty in whether the same is tempered during the year
 - Audit log not operational throughout the year
 - Operations are outsoared resulting non availability of information for audit trail or daily backup
 - Evidence of daily back-up is not available

Exclusions from Scope of Books of accounts

- Application used in isolation with no interface with manual log maintained

Consequences of Non-Compliance with Sec 128

Non Maintenance of Books of Accounts as per Section 128 of the Companies Act, 2013.

Managing director, whole-time director in charge of finance, Chief Financial officer or such other person of the company shall be punishable with imprisonment for a term which may extend to 1 year or with fine which shall not be less than Rs. 50,000/- but which may extend to Rs. 5,00,000/- or with both

Examples - Audit Trail



Tally ERP

Audit Trail - (EL Version 5.1)



Tally – Checking Audit Trail & Daily backup

Tally ERP – version before EL were non-compliant

Tally Prime v2.1 have option to enable edit log

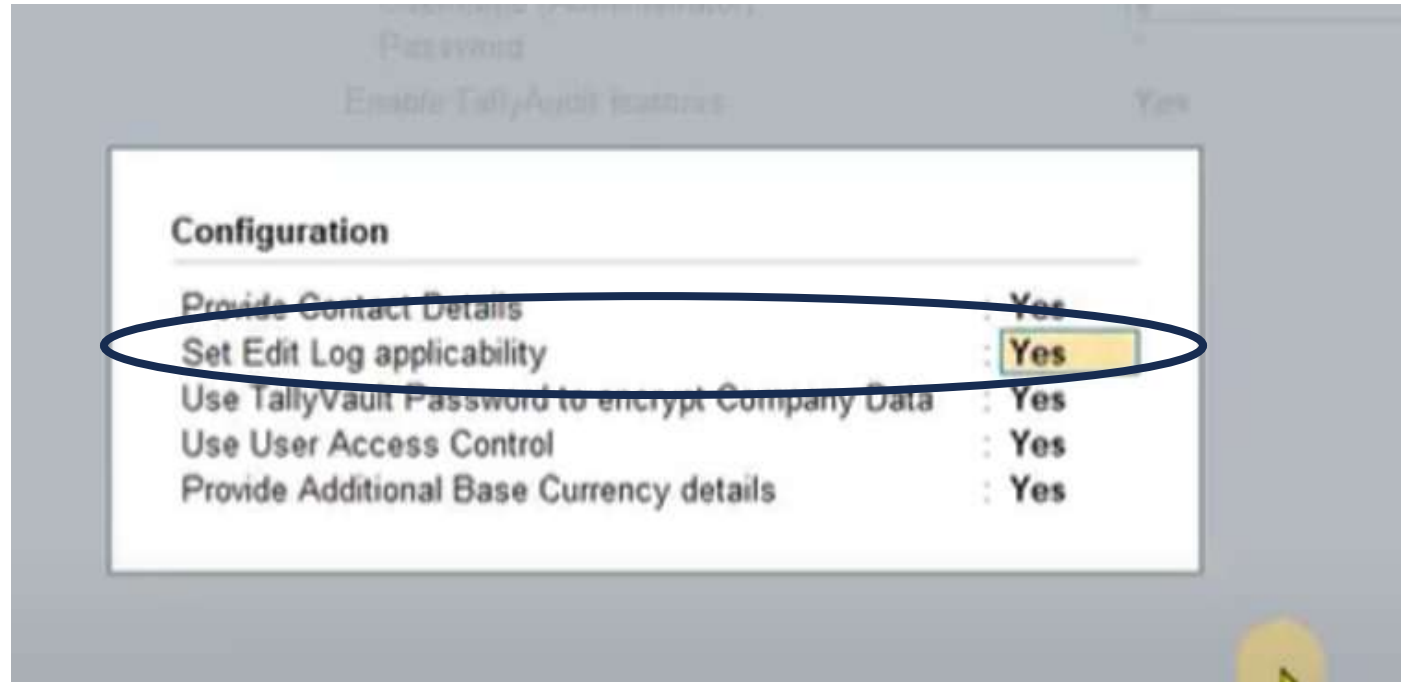
Tally Prime 5.1 – Logs are by default

Tally – Checking Audit Trail & Daily backup

Tally Prime Normal version - Audit trail feature is configurable, i.e., It can be enabled or disabled.

Check configuration through F12.

Hence his is not completely Compliant



Tally – Checking Audit Trail & Daily backup

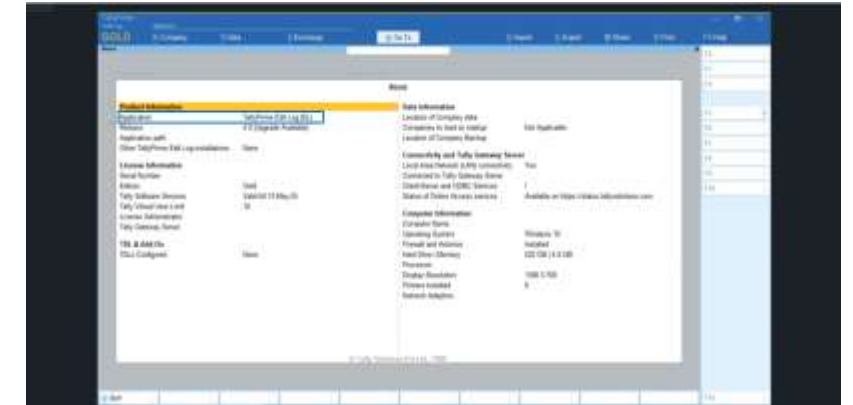
Tally Prime “Edit Log” version – logs enabled by default

There is no option to enable and disable



Tally – Checking Audit Trail & Daily backup

Tally Prime 5.1 – Logs are by default

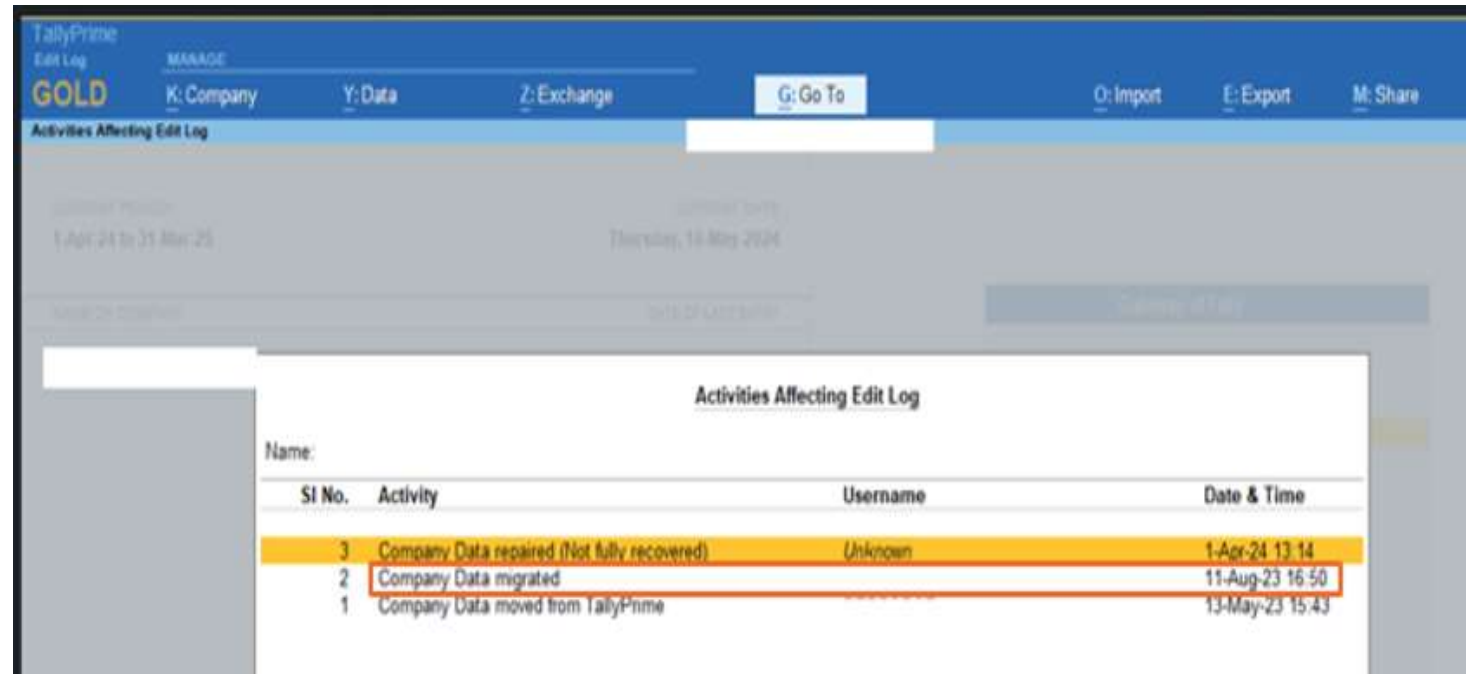


Tally – Checking Audit Trail & Daily backup

Migration of Tally during the year

- Select Button – Company (Alt+K),
- Navigate to option - Edit Log

In the screenshot, entity had moved from Tally Prime to Tally Prime Edit log version on May 13, 2023.



The screenshot displays the TallyPrime Edit Log interface. At the top, there is a navigation bar with options like 'MANAGE', 'G: Go To', 'O: Import', 'E: Export', and 'M: Share'. Below this, the 'Activities Affecting Edit Log' section is visible. A table lists the activities, with the following data:

Sl No.	Activity	Username	Date & Time
3	Company Data repaired (Not fully recovered)	Unknown	1-Apr-24 13:14
2	Company Data migrated		11-Aug-23 16:50
1	Company Data moved from TallyPrime		13-May-23 15:43

Tally – Checking Audit Trail & Daily backup

Changes in log visible in Tally

In the screenshot, entity had moved from Tally Prime to Tally Prime Edit log version on May 13, 2023.



The screenshot displays the 'Activities Affecting Edit Log' window in Tally Prime. The window title is 'Activities Affecting Edit Log'. Below the title, it shows 'Name: Excellent Enterprises'. The main area contains a table with four columns: 'Sl No.', 'Activity', 'Username', and 'Date & Time'. The table lists four activities, with the first one highlighted in yellow.

Sl No.	Activity	Username	Date & Time
4	Company Data moved from TallyPrime	Ranbir	9-May-23 14:14
3	Edit Log disabled	Ranbir	9-May-23 14:13
2	Company Data moved from TallyPrime Edit Log	Ranbir	9-May-23 14:11
1	Company Data moved from TallyPrime	Ranbir	9-May-23 14:06

Tally – Checking Audit Trail & Daily backup

How to check Logs in Tally

Step 1: Go to Day book and then navigate to Basis of Value

Step 2 – Select altered vouchers to obtain list of modified / altered vouchers in the Edit log report.

Step 3 – Select the deleted voucher option to obtain list of deleted vouchers in the Edit log report.

Step 4: From the list altered master record, navigate to the individual record and use (ALT+Q) for detailed Edit log report generated:





SAP : Audit Trail

SAP - Standard Functionality

SAP software provides a full audit trail, logging and evaluating all changed data in the system. Accounting documents are recorded for all business transactions. To ensure a comprehensive audit trail, SAP provides the following standard functionality:

- 1. No posting without a created document** – A posting document or journal entry must be stored in the system for every transaction. Each posting document carries the document date, a time stamp, as well as information about the user who has posted this document.
- 1. Changes to posting documents** – A posting document cannot be changed, but additional information can be added, such as a reference or a comment. Again, these additions are tracked. To reverse a posting, a new document including all audit-relevant data is created.
- 2. Unique identification of a posting** – An accounting document is identified by the company code, the document number, and the fiscal year.

SAP - Standard Functionality

4. **Authorization concept** – A detailed authorization concept for the company can be set up to ensure that only authorized users can make document postings.
5. **Consistency checks** – The system verifies whether the balance of debits and credits is zero and also determines whether all mandatory fields are filled. For General Ledger account master data SAP provides a standard functionality to display changes in General Ledger Account Master Data, to keep control of all changes.
6. **Transport of changes** – Configuration in the production system cannot be changed directly, instead the configurations are transported to the production system from the development system for ECC and S/4HANA On Premise and for S/4HANA Cloud from the Quality system through the Transport Requests. These Transport Requests are used further to track the changes of the configurations performed in the Production system



SAP Audit Trail – Application Level

Display of changed Documents

Transaction codes used for Display of “Changed Documents” in SAP.

Extract **document change details** from standard SAP report – **S_ALR_87012293**.

The above lists all changes in the documents in the period selected

Master data change log details available in standard SAP report – **S_ALR_87012308**.

*The above lists all changes in the **Masters** in the period selected*

The screenshot shows the SAP 'Display of Changed Documents' report selection screen. It is divided into several sections:

- Document type:** Includes radio buttons for Documents (selected), Recurring Entry Documents, Sample Documents, Parked Documents, Docs which were once parked, and External Documents.
- General Selections:** Includes fields for Company Code (1000), Document Number, Fiscal Year, Receiving Company Code, Changed on (01.01.2011), and Changed by. Each field has a corresponding 'to' field and a search icon.
- Further Selections:** Includes checkboxes for Document Header Data and Line Item Data. Below these are fields for Document Type, Posting Key, Special G/L Indicator, and Field Group, each with a corresponding 'to' field and a search icon.
- Output Control:** Includes a field for Layout.

Changes captured at Table Level

Logs are recorded within the table:

- CDHDR Table: Change document header
- CDPOS Table : Change document items

For customized tables called Z Tables are – check if the Z Tables are forming part of the Audit Trail

Changes captured at Table Level

CDHDR: Change document header – shows all documents where there is change

Program Edit Goto Settings System Help L6P (3) 430

Data Browser: Table CDHDR: Selection Screen

✓ [] Number of Entries Cancel

OBJECTCLAS to

OBJECTID to

CHANGENR to

USERNAME to

UPDATE to

UTIME to

TCODE to

Table: CDHDR

	MANDANT	OBJECTCLAS	OBJECTID	CHANGENR	USERNAME	UPDATE	UTIME	TCODE	PLANCHNGNR	ACT_CHNGNR
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1356961069	WF-BATCH	05.09.2023	12:35:34	FB02		
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1359365724	EE3046	14.09.2023	18:55:18	FBL1N		
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1360778397	EN7792	20.09.2023	15:22:57	FBL1N		
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1361057658	EN7792	21.09.2023	14:00:48	FBL1N		

Unique
document
No

Changes captured at Table Level

CDPOS: Change document items – shows for a document Old value, New value, etc.

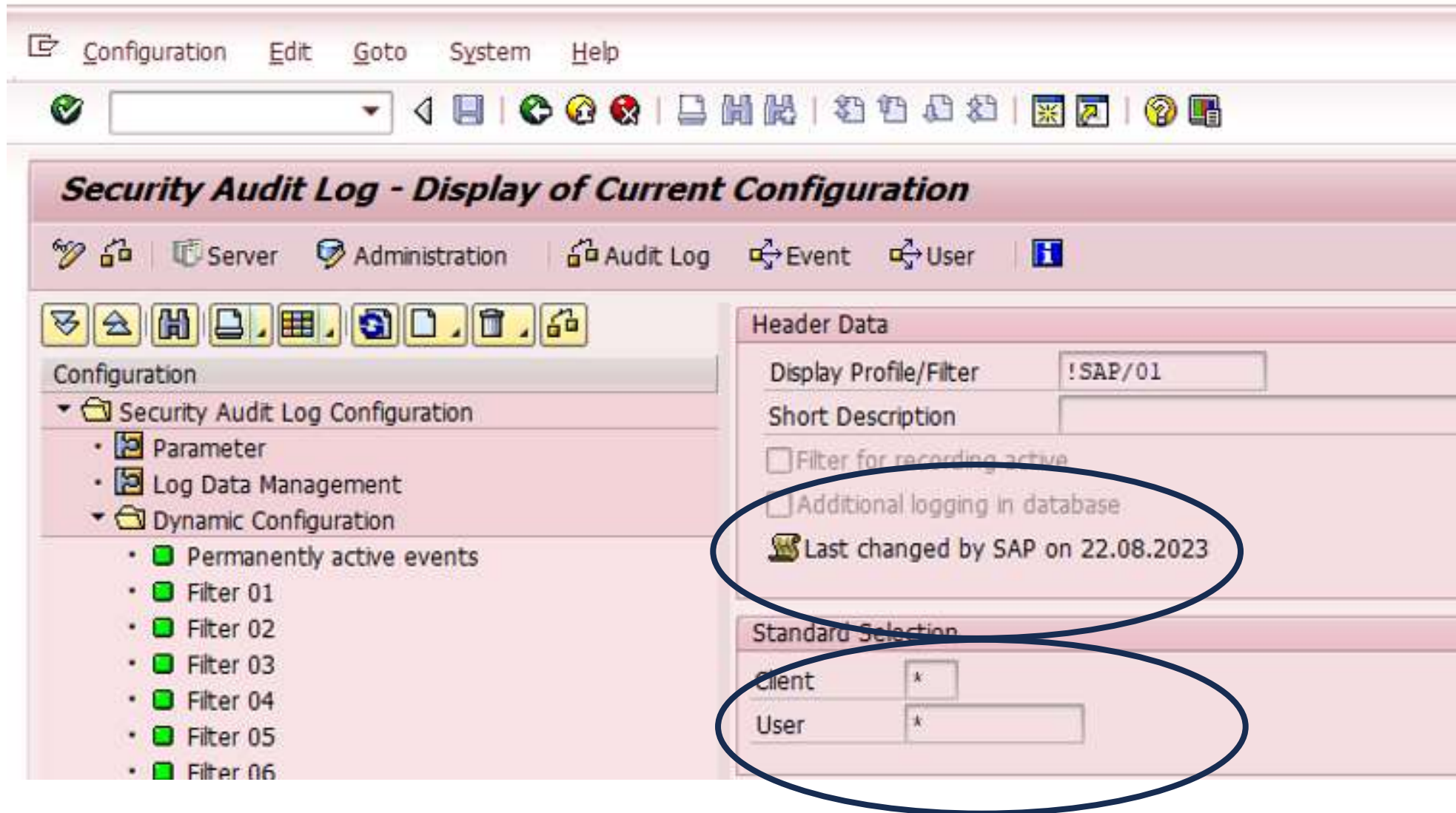
<input type="checkbox"/>	MANDANT	OBJECTCLAS	OBJECTID	CHANGENR	TABNAME	TABKEY	FNAME	CHNGIND	TEXT_CASE	UNIT_OLD	UNIT_NE...	CUKY_OLD	CUKY_NEW	VALUE_NEW	VALUE_OLD	_DATAAGIN...
<input type="checkbox"/>	430	<input type="checkbox"/> BELEG	430295 65402483452024	1356961069	BKPF	430295 65402483452024	AEDAT	U	1					20230905	00000000	
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1356961069	BSEG	430295 65402483452024001	FDLEV	U	1					XX	F1	
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1356961069	BSEG	430295 65402483452024001	ZLSPR	U	1					E		
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1359365724	BKPF	430295 65402483452024	AEDAT	U	1					20230914	20230905	
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1359365724	BSEG	430295 65402483452024001	ZLSCH	U	1					2		
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1359365724	BSEG	430295 65402483452024001	ZUONR	U	1					COF9970-23	9970-23	
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1360778397	BKPF	430295 65402483452024	AEDAT	U	1					20230920	20230914	
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1360778397	BSEG	430295 65402483452024001	ZLSPR	U	1					C		
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1361057658	BKPF	430295 65402483452024	AEDAT	U	1					20230921	20230920	
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1361057658	BSEG	430295 65402483452024001	FDLEV	U	1					F1	XX	
<input type="checkbox"/>	430	BELEG	430295 65402483452024	1361057658	BSEG	430295 65402483452024001	ZLSPR	U	1						C	

Customized Tables: Changes captured at Table Level

When SAP is customized – “**Z Tables**” are configured. One needs to check if the Z Tables are forming part of the Audit Trail. The same was checked from **Table DD09L**, where Log is enabled manually by marking "X".

Table Name	Ac	Vers	SC	Dt.Cl	B	Genkey	Log	S	Author	Date	Time
ZACMST	A	0	0	APPL0		0			AJAIN	06.08.2022	13:51:18
ZARS_BUYER_MAST	A	0	4	APPL0		0			SPLDEVELOPER	15.11.2022	18:35:22
ZARS_CONFIG	A	0	1	APPL1		0	X		SPLDEVELOPER	12.12.2022	18:55:32
ZARS_LOG_TAB	A	0	3	APPL0		0			SPLDEVELOPER	15.11.2022	18:30:24
ZART_CF_PRDCT	A	0	0	APPL0		0			ARTERIAUSER	06.08.2022	08:04:53
ZART_TDS_GL_ACC	A	0	0	APPL0		0			ARTERIAUSER	11.04.2023	09:33:15

SAP – SM19





SAP Audit Trail – Database Level

Changes captured at Table Level

- Access to database could be through PAM (Privilege Access Management) tool or direct access
- Access to PAM tool is restricted and only “Privilege users are allowed access.
- In case of PAM tool, logs are generated and recorded in media file. Which covers recording of actions done by the user.
- Maintaining of recording is crucial – often not retained for more than 3 to 6 months due to size of recording is high

Auditor need to take precaution in verifying and ensuring that the recordings are retained for retention period

To conclude ...

CA cannot say “I do not understand technology”

New Mantra for Auditors

Use Technology

Evaluate technology

Report on Technology

Questions ?

Thank you

CA Jitendra Barve

Email jbarve@gmail.com

Mobile +91 8380037800