Back to Basics: Audit Trail and Log

The excerpts from the Indian Companies Act for audit trail and log, and management and auditor responsibility to comply and report is as below;

Proviso to Rule 3(1) of the Companies (Accounts) Rules, 2014 (hereinafter referred as "the Account Rules") states that 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 the books of account along with the date when such changes were made and ensuring that the audit trail cannot be disabled.

Text of Rule 11(g) of Companies (Audit and Auditors) Rules, 2014 Whether the company, in respect of financial years commencing on or after the 1st April, 2022, has used such accounting software for maintaining its books of account which has a feature of recording audit trail (edit log) facility and the same has been operated throughout the year for all transactions recorded in the software and the audit trail feature has not been tampered with and the audit trail has been preserved by the company as per the statutory requirements for record retention.

In today's environment, the majority of the books of accounts are maintained with the help of computer software. The software could be more advanced with all the functions integrated such as ERP or there are various software/applications used for recording, processing, and reporting financial transactions. The auditor (internal/external) while assessing the compliance with the above rules needs to review, check and understand the following to ensure that the organization complies with the above rules;

- The accounting software used by the organization, whether it is ERP or multiple software for processing the transactions;
- The list of all the users and the access level in the software with rights;
- Mapping of all the financial/business transactions from end to end, such as order to cash, procure to pay, journal entries, fixed assets, month-end process, expenses cycle with reference to users/manual input/system processing, with authorization level defined in the system;
- The system processed and posted transactions with time intervals (daily, weekly, monthly, and yearly) and manually posted transactions;
- Understand the park and post, single authorization, and queue system of approval at various levels in the system;
- Understand the master updates of critical fields in the software;
- In the case of shared service or outsourced operations, the processing of transactions by shared service users vis-à-vis in-house users;
- The manual or system file upload and interfaces processing;
- Understand the system terminology for audit trail or log maintenance with various abbreviations defined as per the system design and how to interpret the audit trail or log.
- Review the system downtime process and how the transactions were processed once the system is running again;
- The Access to the system database regarding confidentiality, integrity, and availability;
- Review the exceptions report for overriding the user access for completing/posting the transactions;
- The backup of the database with other applications used for financial reporting;
- Back-dated posting after month-end and year-end closing, access levels to change the reported financials;
- Review of priority access levels with super users' rights in the system;
- Assessment of COI/SOD process by the management and action taken;
- Record retention of system data with history of audit trail/log;
- Change of priority levels of users and reinstating the same after a short period or after posting a specific transaction;

The above checks are not exhaustive, the list may be expanded depending on each auditor's experience, knowledge, and professional skepticism. In the case of an ERP system, this will not be challenging where a process exists to identify and records each transaction with the audit trail/log. In the case of multiple software used by the organization, this will be challenging as transactions will flow through each software with or without audit trail/log functionality. The auditor needs to be aware of the system abbreviations managed to record the audit trail/log with financial impact and users' details.

Vijay N Trivedi