International Journal of Business Quantitative Economics and Applied Management Research
Volume-6, Issue-12, 2021 ISSN No: 2349-5677

IT AUDIT OF ORACLE APPLICATIONS UNDERSTANDING, PREPARATION AND EXTRACTION

Rajalakshmi Thiruthuraipondi Natarajan
rajalan11@gmail.com

Abstract

IT Audit is done to review the organization's technology landscape and its functioning to reaffirm its compliance to the laws and policies defined by the government and the company. The significance of a successful audit is providing confidence that company is operating as expected and there are no major deviations. The IT audit can range anywhere from access to data security and from initiation to decommissioning and everything in between. It is essential that there is a healthy balance between the defined policies and organization's capabilities, since any exorbitant rule might prove to be costly and unsustainable. All policies should consider the entire organization and should not conflict with each other, nor should restrict the application form best serving the organization within the legal limits.

Oracle Applications, which can either be a part of the IT profile or the entire profile by itself, has multiple parts, such as server, database, application, and each eligible for its own audit activity and a careful planning and execution needs to be in place both while defining the rules and its implementation and by extension the external systems that interact with Oracle.

IndexTerms—IT Audit, Technical Audit, Separation of Duties, Access Management, Application Policies.

I. INTRODUCTION

Audit, by definition, is "an official inspection of an individual or an organization's accounts, typically by an independent body" – Oxford Dictionary. However, in a broader sense, it is a process of evaluating a part of or an entire organization (or individual's) to ensure that it adheres to the rules and regulations defined. While it is very commonly heard in financial domains, it is done in pretty much every walk oof a company. It acts as periodic check to ensure there are no unacceptable deviations. Any anomalies identified as part of the audit are documented and reported in detail and it is an obligation that these be addressed by the respective departments with utmost urgency or risk failing the audit. For this reason, and rightly so, the entire department or organization goes into high-alert mode during audit and spends long strenuous hours to check and recheck everything that will be audited.

While the impact of an audit is immediately evident in the stock market, where an audit failure can send a stock sharply down (or a mere announcement of an audit) or vice versa, an IT audit is no less critical, since it shows how well the technologies used by the organization is inline with

the company's policies and the laws laid down by the government. It can also expose vulnerabilities in the operations, security and reliability, which can not only impact the company's productivity, but can also lead to potential legal and ethical issues, causing irreparable damage financially and repute. Additionally, this provides a valuable opportunity to revisit the internal policies, and tune them in accordance to the market.

II. UNDERSTANDING THE SCOPE OF AUDIT

An audit, like any other project should start with the requirement. In this case, understand what the scope of the audit is. Having a clear understanding of the focal point would greatly help in collecting the relevant data, else there is a risk of either providing incorrect information or over-producing the details, neither of which is good for a successful audit. Also, there needs be an awareness of who has initiated the audit, since different teams might be focusing on different areas of interest though the source system might be the same.

A Government Audit, as the name implies, is initiated by the government to check if the IT systems are compliant with the rules laid by the government. Tax audit is a prime example of a government-initiated audit which happens periodically. However, in special cases, they can impose additional audits, to ensure that the customer and national interests are not compromised. For instance, banks and other financial institutions undergo various kinds of government audit to ensure that there is no mishandling of customer's funds or money laundering, etc. An IT audit initiated by the government, typically to ensure the security and data maintained by the corporations and by extension, parties that these organizations interact with are in line with the government rules. For example, per the EU's GDPR law, no organization can retain customer data any longer that it is needed, and it is the obligation of the collecting organization to delete the data to be compliant with this law. Any complaints from the customer or any other source might trigger an audit. These audit, obviously, are not controlled by the companies and there is little to no room for compromise and might result in legal issues and penalties.

Next is the Internal Audit or Private Audit, where the company initiates an audit as means of self-check to make sure that they are operating as per the rules laid by the government and by themselves. These are usually done periodically to reaffirm the sanctity of the process and to impart confidence to themselves and its customers and suppliers that they are operating effectively and are paying by the rules. These audits might be done by internal auditors or external auditing companies depending on the need and it can range anywhere between their financial transactions to the IT systems to employee's expenses to suppliers and customers. For instance, a company can perform an internal audit to review the accesses of certain application to make sure that right personal have right kind of access and each access have a proper approval flow. Unlike government audit, there is a bit of a wiggle room in internal audit and at times the policies do get modified based on the audit findings and the ability of an organization to adhere to the rules. Hence, these types of audit acts as validation of the processes and a chance to revisit the organizational policies and procedures to fine tune them as needed.

While the above section provides an insight on whom the audit is for, next is what can be included as part of an IT audit. The answer is anything and everything in the technical landscape can be added in scope of an audit, may it be an application or the interfaces which talk internally and externally to security protocols and the data that is maintained. When it comes to Oracle Applications, they have a potential presence in every part of the company's system architecture.
From a product standpoint, any or all of the following can be part of auditing related to Oracle E-Business Suite Applications –
Infrastructure Audit, as the name implies is an audit of the base hardware upon which the application or database is installed. This audit is to make sure that the hardware is up to the mark and can support the application in the near and long run and to check the changes that might have happened since the last audit and the changes are properly documented. There can also be a software component to this audit, which is used to check reliability of the software like the operating system version that is uses and if it supported and if the security patches are applied and in terms of network, if the transportation protocol used is secure and is compliant with the industry standards, etc.
Database Audit is done where the data is actually sored. There is a wide range of audit that can be done part of database audit. Apart from the obvious audit such as the version used, bug-fix and security patches, maintenance audit, etc., there can also ne some additional audit for continuance like, data grown, storage consumption, access either by end users or integrating systems and strategic planning such as back-up, data retention, encryption methodology, archival activity, etc.
Finally, Application Audit is to review and confirm that the application is functioning efficiently and securely. While the usual suspects, like patches and security are audited, the main intent of an application audit is usually to ensure that the processes and flows in the application functions as per the business flow documented by the organization. By tracking a data through a flow and auditing it at different milestones, the auditors can document evidence that the data flows as intended and there is no unauthorized modifications made in the due course to achieve the desired result. Not only is the data eligible for audit, but also who performs the actions and when and confirm that there is no one who isn't authorized is acting on the data.
The next step is to know what section is getting audited based on the functionality. There are several functionalities that overlap between different components listed above, yet, once needs to be aware that though the focus area is the same, the evidences or the success conditions might be different based on which component is being audited. Some of the key IT audit areas include –

2.1 Access Audit

One of the most frequent audits that an organization performs. This audit is to check if all access provided, modified or removed has followed the required review and approval process. Any unauthorized access is flagged and investigated, and swift corrective actions are done, since this can potentially be the first and last line of defense of an application. This audit is mainly to ensure that any one user or a group is not over-burdened with excessive responsibility or ability that becomes unmanageable or has a ability of cause damage. Leaving the intricacies aside, the access levels can be broadly classified as-

- Admins - These are the administrative users, who maintain the overall health of the application and there will be ana admin in each component like server (e.g. root), database (e.g. SYSDBA) and application (e.g. SYSADMIN). This is usually the most powerful user, and the access needs to be limited to few handfuls of administrators.
- Super User - This is a functional category of user who control the way the application or a portion of the application works. These are typically used at the time if initial set-up or as fire-fighter id in case certain process needs to be modified or override a step. This type of user is typically provided to a controller, who has an executive authority over the application.
- Regular User - These are regular operational user who have access to perform a specific set of tasks based on their job code. Most users will fall under this category, and users confined to a limited capability. This can either be an internal user or an external user, i.e., user outside the organization, who might access the applications for informational and transactional purposes..
- Inquiry User - These are the users with least capabilities. This type of user can only view data and cannot perform any transactions. However, it is important to ensure that the ability to view is also restricted based on the role, so that no sensitive data is visible to any unauthorized users.

Based on the above levels, the requirements and policies such as password complexity, retention policy, password change policy, etc. can be different and the strictness to adhere to these predefined rules might differ.

2.2 Data Audit

There is a huge variety of audits that can happen on the data such from the time it enters the organization until it is deleted from all storage, and sometimes even beyond that. This audit is critical to ensure the organization is operating efficiently and securely and data integrity is not compromised. Some of the common data audits performed are –

- Data Processing Audit - Every organization is bound by the government and industry laws on how to collect, retain, process and discard the data, in addition to the self-governing laws laid by the organization. Thes audits are in place to make sure that these rules are followed in every walk of the business. Any requirements such as SOX, PII, and any other compliance needs are properly met and stored accordingly. It also ensures that any collected data is processed only as per the committed need and retained only until it is legally allowed.
- Data Trail Audit - This is the process of tracking the evolution or transformation of data from its original from to its current form. With this audit, the company tracks the list of data influencers and the subsequent modifications that the source data underwent in different stages. These are usually done on master data or set-up data which can significantly alter the way the system operates.
- Data Security Audit - this is yet another critical audit to make sure that the there is no unauthorized access or transfer of data from or to the application systems. It is done in every level of the application like server level, database level, network level,

application level and even in the integrating system level. The checks can range from access level to the data encryption to data-scrambling and even the way it is safely deleted from the system, since any vulnerabilities in security might cause data leaks and might cause irreparable damage to the organization and their trading partners.

III. PREPARATION FOR AUDIT

It goes without saying that the team responsible for providing audit evidence needs to be well prepared to collect and present the details needed by the audit team, depending on the type of audit, as mentioned in the section above. It is important that the IT team keeps itself up to date on the application that they handle, and the teams involved so that they can collaborate amongst themselves to face the audit.

Firstly, the team needs to be aware of the audit obligations that they need to deliver. While it is the auditor's job to ask for detailed evidence, the support team needs to be aware if the requests fall within the scope of their duty and even if it does, what is the level of information that can be shared with the auditors. If any request is beyond the scope of audit, it can always be pushed back with relevant evidence. Also, this prevents over sharing of information which might be a breach of compliance or too much irrelevant information.

Once the scope is identified, the relevant team needs to identify and coordinated, since more often, the required evidence might have to come from different teams, at times third party companies, that needs to be consolidated and presented to the auditors. Along with identifying the teams, the required access to retrieve and document evidence needs to be identified and ensure that requests are raised and acquired. Failing this step, might result in unwanted hassle and run around between teams and members and causing delay in the audit completion.

Another important part is knowing the exception process. There should always be an assumption that there is a possibility that there might be a deviation in the agreed process. One should be aware of any such potential scenarios and the company's policy in addressing such anomalies. There usually will be an exception approval process, which will be acquired either before or after the anomaly. Also, need to take into account the worst possible scenario where the process was missed with no valid reasoning. All such scenarios should be taken into consideration and discussed with the management and the legal team, be prepared with the solution to minimize any unpleasant surprises.

IV. EVIDENCE COLLECTION FOR AN AUDIT

Once the auditors submit their requests, the support team need to gather evidence to support and back the claims. A concise and clear audit document would minimize, if not eliminate the need to clarifications or further discussions on the topic. Unlike a financial audit, which is usually done by auditors who are charted accountants or well versed in the financial domain, IT auditors most likely do not possess the technical knowledge of the application to know the architecture or its functioning. They largely rely on the evidence provided by the teams for their

auditing. Hence it is extremely important that the document has a seamless flow with each evidence connecting to the prior.

To gather the details, either top-down or bottom-up approach can be employed and the needs to be determine which is best path to take. For instance, for user access, most organizations, usually employ an access management tools such as idM or Service-Now, etc., and each user access which follows a workflow to finally provide access. While gathering evidence, unless specified by the auditor, the team can decide to with looks for requests in these tools and track the flow all the way to the access provided in the application or take a particular user from the application and trace it back to the request from access management tools. This way, there will be a clear flow indicating the process has been followed.

Also, it is advisable that the evidence be properly grouped, so that it is easy for the auditors to trace it, instead of providing it as big chunk of data, which makes it difficult for the auditors to reconcile. Example, when retrieving transactional data for a trial balance, it is best to have the document grouped by period or by accounts and use a consistent naming for the balances file and the transactional file. This makes it easier for the auditor to know which file to look into for evidence for a particular journal or balance, instead of browsing through several files to find a transaction.

V. CONCLUSION

Auditing, while is an unavoidable activity, need not be a stressful or a complex activity. It is pretty much making sure that the company is operating as per the policy defined, in most cases it will. While this article provides some of the practices that the team can adopt to minimize the hassle and increase the chances for successfully completing the audit, it is important to remember that every organization is different and so is the audit needs. Hence having a clear understanding the general policies, along with what sets your organization apart can make things easier for getting the right evidence for audit. Also, once needs to accept the fact that there will be limitations both technical and operational, which might affect proper auditing. However, with proper planning and execution, any team should be able to check most of the boxes and get through without major escalations or concerns which might have ripple effect both internally and in the market.

REFERENCES

1. Information technology audit, https://en.wikipedia.org/wiki/Information_technology_audit#:~:text=The%20primary%20functions%20of%20an,dispense%20information%20to%20authorized%20parties
2. IS Audit Basics: The Core of IT Auditing. https://www.isaca.org/resources/isaca-journal/past-issues/2014/is-audit-basicsthe-core-of-it-auditing
3. Information Technology Control and Audit - Fifth Edition, https://www.researchgate.net/publication/327312550_Information_Technology_Control_and_Audit

4. Oracle® E-Business Suite Security Guide - Enabling Oracle E-Business Suite Audit Trail, https://docs.oracle.com/cd/E26401_01/doc.122/e22952/T156458T663771.htm, p. 22
5. Embracing technology in the audit, https://www.journalofaccountancy.com/issues/2022/feb/embracing-technology-audit.html, Feb-2022
6. IT Audit Perspectives o today's top Technology risks, https://www.protiviti.com/sites/default/files/2022-09/10th-annual-IT-audit-technology-risks-survey-isaca-protiviti.pdf, Sep-2022
7. Laura Tate Zannucci, CISA, CISM, CDPSE, The Increasing Importance of IT Audits to the BoD, https://www.isaca.org/resources/news-and-trends/industry-news/2023/the-increasing-importance-of-it-audits-to-the-bod