Software Program INC Case study

Brief description of the audit process required to satisfy the auditing of IT controls over financial reporting.

The audit process begins by understanding the organisation's structure and its financials. There is a code of professional ethics that IS auditors must comply with before starting any audit. For Software Program Inc, an audit charter is established which provides management's responsibility and objectives for the audit function. This audit charter also provides various financial, ethical, and authoritative guidelines for auditors to perform an IT audit.

Next, we (AuditGen PC) will collect information about Software Program Inc.'s policies, business objectives, and working environment. For a financial audit, we will check the existing controls and see if they are in compliance with industry standards. The organisation has research and development testing, and the distribution of production libraries occurs. Also, web operations, including call centres, are operating. Hence, a detailed audit process is required to check if the controls are in place to make sure these processes are following industry-standard guidelines. This organisation also contains digital streams, and transactions happen through credit cards; hence, an audit process is required to check if this is following PCI DSS. Also, when conducting a financial audit, we must check the organisation's controls against the US Sarbanes-Oxley Act of 2002, or SOX compliance, which focuses primarily on financial controls and reporting and requires the CEO and CFO to certify the accuracy of financial statements. Additionally, we must check our controls against the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, and the COBIT 5 framework is adopted by organization for governing and controlling IT.

After checking organization controls against industry standards, we will provide a final report to Hy Fenation from Software program Inc, and provide the necessary improvements required to be adopted by senior management and do periodical follow-ups to check the progress on the implementation of the controls.

Based on the presentations by the Software Program executives, perform a risk assessment of the infrastructure and applications to identify the processes that need to be included in the audit.

As explained by Dalton Walton, there are three different networks that are protected by firewalls, i.e., administrative systems, research and development, and web operations. For administrative systems, the main risks are due to web attacks like cross-site scripting (XSS) and SQL injection, which can cripple main business data and cause reputation and infrastructure damage on a high level. To overcome this risk, certain cyber security controls need to be implemented, like anti-malware software and security awareness training among employees.

In research and development, there is a potential chance of copyright infringement and data leaks, which can lead to the loss of intellectual property that can damage organization future growth. To overcome this, internal controls need to be in place, like providing access on a need-to-know basis for sensitive data and tracking the flow of data from development to distribution.

In web operations, there can be a potential chance of power outages that can disrupt IT access in call centre operations, which can lead to huge customer dissatisfaction. Also, periodic monitoring of the effectiveness of employees that are interacting with direct consumers can improve overall web operation controls.

In software development and testing, where different versions of the product are being tested and sent for final production, there will be potential errors in the version control of the software that is released in media and downloaded versions, or compatibility issues in downloaded versions. Also, there is a chance for the downloaded version to get pirated by cracking the files, which is a common issue for downloadable software. To overcome this, there should be controls that follow industry standards, like the Software Licence Management Association (SLMA) Framework, and some internal control measures like Digital Rights Management, Licensing, and activation to use, legal controls, and providing regular updates to the software.

We have to check whether the controls already existing in the organization are following the COSO and COBIT frameworks and evaluate the above risks. We must prioritise the controls that need to be executed as high, medium, and low risk for the next 3 years and provide this information to senior management for execution. We must ensure that no control has lapsed for more than 3 years and follow up with senior management to check if any progress is being made to mitigate potential risks.

Accounting System is a purchased application from PearTree Software, Inc. We have to check whether PearTree is following its service level agreement and its own controls. Data updates are being done on a daily or monthly basis, as per the process. There should be backup controls planned in the event of any IT issues at PearTree. Also, software programs are operated on multiple platforms, and updates are provided to all, which can lead to high maintenance on each platform whenever a new version is released. There should be a control to monitor every update across multiple platforms and document it.

Identify the processes you believe should be included in the evaluation of control design and operating effectiveness.

The processes that should be included in the evaluation of control design and operating effectiveness are:

1. Implement periodical review over important frameworks that an public company needs to follow and check if the organization is maintaining current industry standards.
2. Implement periodic reviews of important frameworks that a public company needs to follow and check if the organization is maintaining current industry standards.
3. Safeguarding intellectual property against competitors in a similar market using patents and avoiding any copyright infringement issues
4. Checking if our third-party services are following their controls or not.
5. Providing access to sensitive data on a need-to-know basis to employees with thorough background checks.
6. Installing up-to-date antimalware software or cybersecurity controls to overcome any potential data breach.
7. Maintaining transparent revenue tracking involves monitoring various income sources across the organization.
8. Maintaining periodic backups of sensitive data to trusted data servers.
9. Checking if Release to Manufacturing (RTM) is as per the business requirements and the same version is being sent to media and downloaded.
10. Keeping up-to-date inventory, which should be scalable as per the versions that are being produced,
11. Process of selling licences to end users and its access management.

12. Providing customer support for all platforms, like Windows, Linux, and Macintosh, whenever a new version is released, and proper documentation is provided for all the platforms.
13. Proper maintenance of databases on a server is important as multiple data is fed to the same system's network.
14. Adopting quality testing before releasing any application to platforms and maintaining up-to-date software.

- Lokesh Bollini