CLAIMPROOF INSURANCE CASE STUDY

LOKESH BOLLINI

Operationalize steps required for the IT assurance for program change control process (a specific area)

Operationalization steps required for IT Assurance for Program change control process (PCC). Change control is a methodology used to manage any change requests that impact the baseline of your project. Some steps defined by IT Governance by COBIT is:

Refine the understanding of the IT assurance for claim proof insurance company:

- PCC will be implemented by assessing organisation scope and objectives that are approved by higher management.
- Identify where the changes are being done and allocate proper change management strategy by making a proper change management team.
- When a change is identified managing the change is important by taking action and implement plans according to it.
- After implementation of plans, documentation of final report, collect, analyse feedback, and implement proper actions by consulting with higher management team.

In an insurance company change are inevitable and occurs periodically, hence a proper change management control is necessary. IT assurance is important claim proof insurance company as it is required to protect customer data, prevent fraud, to maintain business activity and comply with regulatory requirements.

Refine the scope of key control objectives for the Program Change Control process assurance:

Key control objectives for PCC involves all the changes that will happen even if this is small or major change. Some of the changes are:

- Any changes that happen in the automated adjudication systems

- Documentation change of any testing, approval process and monitoring have to be maintained.
- Changes in financial strategies that affect the overall PCC process.
- Any management role changes should be document and reviewed by senior management.
- Testing of source code before production and checking the version controls
- Reviews of any changes that are made and place rollback procedures in case of any failures.

Test the effectiveness of the control design of the key control objectives.

Claim proof insurance can test the effectiveness of the control design by implementing KPI(Key Performance Indicators). KPI's are standard indicators in an organization that can track and measure the performance of any change or process adapted by the organization.

Some of the KPIs to be included to measure the control design are:

- Tracking change KPI: This KPI measures the number of incidents that occurs because of change. This is important for maintaining historical data and see the patterns.
- Fraud detection KPIs can help to measure the risks that claim proof is facing in current and can predict the future risk by implementing controls for the existing fraud activities.
- Tracking the number of unauthorised changes can give logs of users.
- Since there is a One time password already existing which confirms the ticket number, we can also add extra layer of protection for programmers to get the approval to the changes that are being done.

Testing the outcome of the key control objectives:

Outcome of key control objectives can be tested by following objectives:

- Reviewing change requests, test plans and monitoring reports
- Interviewing the stakeholders will provide valid feedback for the outcome of the key control objectives.
- We can test the systems by doing unauthorised access to the systems and test the systems.

- Testing of final production code before deploying it can provide valid feedback for any last-minute changes to the code.
- We can also analyse the automated adjudication system and compare with existing results.

Documenting the impact of control weaknesses:

There are certain loopholes and impacts of the control weaknesses implemented across the Claimproof insurance.

- There is no verification of the users/programmers who can make changes in the system without any stakeholder involvement or any logs. This could cause potential risks/threats to the existing adjudication system.
- During an initial interview, the administrator was asked whether further examination of off-hours changes was performed; the response was no. This is very critical as users can take advantage of this lack of observation in the process to access sensitive information and can lead to potential threats to the existing system.
- Programme change administrator is given the final opportunity to have the production code. Careful monitoring of this position needs to be taken care of as final code in a single user for long period of time can be a potential threat to any organization especially this claim proof insurance.

Develop and communicate overall conclusion and recommendations:

After assessing entire program change control the auditors of unqualified opinion ltd., can recommend and include the following in the audit report:

- Final production code deployment facility is given to a single change administrator which can cause potential risk and this needs to be addressed by providing rotational duties to this role.
- Off hour changes are not reviewed which can lead to improper changes in the system.
- Documentation of version control is not complete during the source code deployment.

- Implement a proper management to control the logs and changes made in the systems.
- There should be a rollback feature included incase if any changes are made incorrectly and should be reviewed by the higher management.
- Web controls like firewall and data loss prevention system should be in place for the system to prevent risks.

Based on the results of question 1 and your understanding of the control environment in the case study, identify 4 high-risk areas requiring audit attention.

Open-source test libraries: In claimproof insurance company, the test libraries that contain source and executable code are open to all programmers who can access them for the changes. There is no proper logging mechanism to track the changes made the any individual programmers too, this can cause serious setback in tracking the logs of changes made to the process. This can also leads to unapproved changes as access is open to everyone and there is high risk for improper changes that is unapproved by senior management.

Improper access control management: Once a programmer has completed testing, it is accessed by change administrator and moves the source executable code directly to the production team. There is no proper quality testing happening over here and any improper entries of code can be overlooked, and final production can be incorrect. Monitoring of the roles of administrator actions is preferred and rolling duties for these roles can prevent any unseen fraudulent activities.

No monitoring in off-hours: Generally, in organisations, major changes are being done in off-hours to limit down time in production hours. However, in claim proof insurance, off-hours changes are not being monitored. This is a high-risk area which can cause unapproved changes into the system. A proper audit is required by implementing logs of the changes that are made and the individuals that approved the changes for the upload. This can provide historical data for all the changes made in off – hours.

Reconciliation of Incident management: Difference between incident management and PCCS can happen due to the mismatch of data that is being tracked or reported. This have to be monitored regularly to avoid any incidents and avoid potential risk.

How would you assess the control design?

Assessing control design is important to implement a better change process than the existing one and this can be done in following ways:

- Checking if there are any process for identifying and approving change requests.
- Before source code deployment, we can check if there is any existing process to test the validity of the code.
- Similarly, after deployment of changes, monitoring the changes and collect, analyse the changes, and see if there is any process for it.
- Checking the effectiveness of existing controls that are available to identify, approve the change requests.
- Also checking is there any process that involves senior management to review and monitor the changes that are being made in the PCCS.
- Documentation of the PCCS
- Also, checking if the incident reporting system and PCCS to ensure they are reconciled on a regular basis to avoid any mismatch of data between both.
- Is there any process to get the feedback of senior management on the PCCS

How would you test the control effectiveness?

There are several ways to test the control effectiveness for PCCS.

- Monitor and check the access/logs of users that have access for production systems to find any unauthorized access.
- Review of documentation of PCCS for any mismatch entries in the system and access the logs for the same.

- Testing the final production code before deployment and review of the result for any errors.
- Review the mismatch data of incident management and reconciliation and tracking the data back to the source.
- Reviewing the KPIs and assess it against the existing control systems for any trends.
- Checking the program change administrator log access and the changes made by them and also overseeing the rotation of the duty by other users.
- Documentation of the changes made in off hours and the errors caused during the same time along with logs of the users that have access during the period.
- Checking if there is any synchronization between production source and executable code and whether any unauthorized changes are done in the production.

REFERENCES

- https://www.isaca.org/resources/cobit
- https://asana.com/resources/change-control-process