International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Role of Audit Teams and 3rd Party Assessors in Maintaining the Risk Posture of the Organization

Pranith Shetty

Information Security and Risk Officer, Morgan Stanley, New York

Abstract: ***Risk posture of the organizations are a culmination of a lot of factors, risks identified over the course of various assessments internally, vulnerabilities & incidents, financial appetite, risk appetite, tolerance and many more. Internal security teams are very diligent in maintaining the risk posture and protecting the firm from external and internal threats. Risk reports from these teams are also communicated to leadership and management. However, teams like Internal audit and third party assessors bring in an unbiased perspective onto the findings. Because of the industry exposure, these teams have a unique and learned inputs into their projects. Third party teams reduce the compliance overhead and significantly fast track the certification roadmap, consumers have trust and faith on external attestors since they have a pre - conceived notion that internal assessment teams might be biased and might not serve external interests. Internal Audit teams on the other hand provide in depth and identify critical risks which in some cases might not have been selected due to macro factors pitching in and affecting the risk assessment teams.***

Keywords: Internal Audit, Risk Posture, 3rd party, third party attestation, Cybersecurity, Risk management

1. Introduction

The advancement in information technology and systems has massively helped business to not only sustain but scale new heights. The technology and the security risk landscape is never the same, it constantly evolves. With rise of new technologies and the way we do business has given rise to a whole new world of cybersecurity threats like malware, nation state actors, cybercrimes, even social engineering techniques have evolved. The need for cybersecurity professionals is now more than ever, firms and businesses are building their dedicated security teams reporting to the CISO (Chief Information Security Officer) and these teams do ensure secure design, creation and operations of their products and / or services. There is a need of an independent review or attestation of some kind that ensures an unbiased opinion of the current state of security infrastructure and services.

This independent review can be performed by either an Internal Audit team meaning an assessment team of full time employees hired by the business with reporting line (Head of Audit) to board of directors so that there is no conflict of interest and the assessment report stays clear of department heads. This review can also be performed by an Independent auditor or team outside the firm, contracted by board or senior management.

[1] An information systems security audit (ISSA) is an independent review and examination of system records, activities and related documents. This assessment results in a report that usually has findings and recommendations to improve the risk posture of the firm. Internal Audit teams by providing this report help in communicating an independent and unbiased opinion of the risk posture to Leadership and Senior management. However, there are some cases where even the Internal Audit teams wont suffice, for example: Regulators and federal bodies more often than not rely on a 3rd party or Independent attestation for some of the regulations like SOX (Sarbanes Oxley) [2], PCI DSS (Payment Card Industry Data security standards [3], especially in the financial services sectors that are publicly listed businesses so they are bound by transparency, privacy and related regulations like the NY - DFS Cybersecurity (New York Department of Financial Services). Some Customers usually request for independent attestations by renowned accounting and audit firms to ensure the product not only meets their required specifications but also complies with federal, state and local policies etc.

These independent attestations are a major contributor in maintaining, improving and communicating the risk posture of firms across involved staff, stakeholders and leadership.

2. Audit framework

Generally, prior to the Audits, a formal intention letter is drafted and shared with the Auditees to prepare for the audit and ensure availability of key resources, this process is usually followed so as to not overwhelm production staff and also to ensure minimal business impact to the daily operations. [1] These audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes. For Audits, usually COSO framework [5] is adopted by businesses and they are modified slightly to accommodate their mode of operations and organization structure.

There is also a mix of COBIT (Control objectives for information technology) framework and similar that's included especially for Technology related audits.

The following visual figure 1, will help understand the Audit framework and process flow end to end, especially in the Cybersecurity and Technology space [1] [6] [7].

This is how any Audit performed by the internal Audit team, post the Audits, the responsibility and accountability lies now on the executives who were scoped in as part of the Audit to ensure findings are remediated as per the specified timelines by the audit team or before the next review, deferred to the

Audit team's judgement. If they cannot be remediated within the SLA (Service Level agreements), date extensions need to be signed off by the Audit team and they would have to be presented at the Steering committee reviews. Date extensions are very serious and not granted for critical findings by the steering committee members since Critical risks need to be remediated as soon as possible to limit the exposure and attack surface. For the rest of them, Audit team usually grants extensions based on the detailed rationale and only after their approval, it can be then presented in the Governance forums for extensions. The audit timeline stretches for months in some cases since these are very detailed and needs a lot of planning & resource commitments.

Sharing of draft report is a crucial step since this gives the auditees a peek on the findings and gives them a chance to provide more evidence to negate those findings or reduce the risk rating, also if there are any findings that are duplicate or not accurate, auditees can contest those with evidence, this helps in better summarizing the risk posture and helps the firm in the long run.

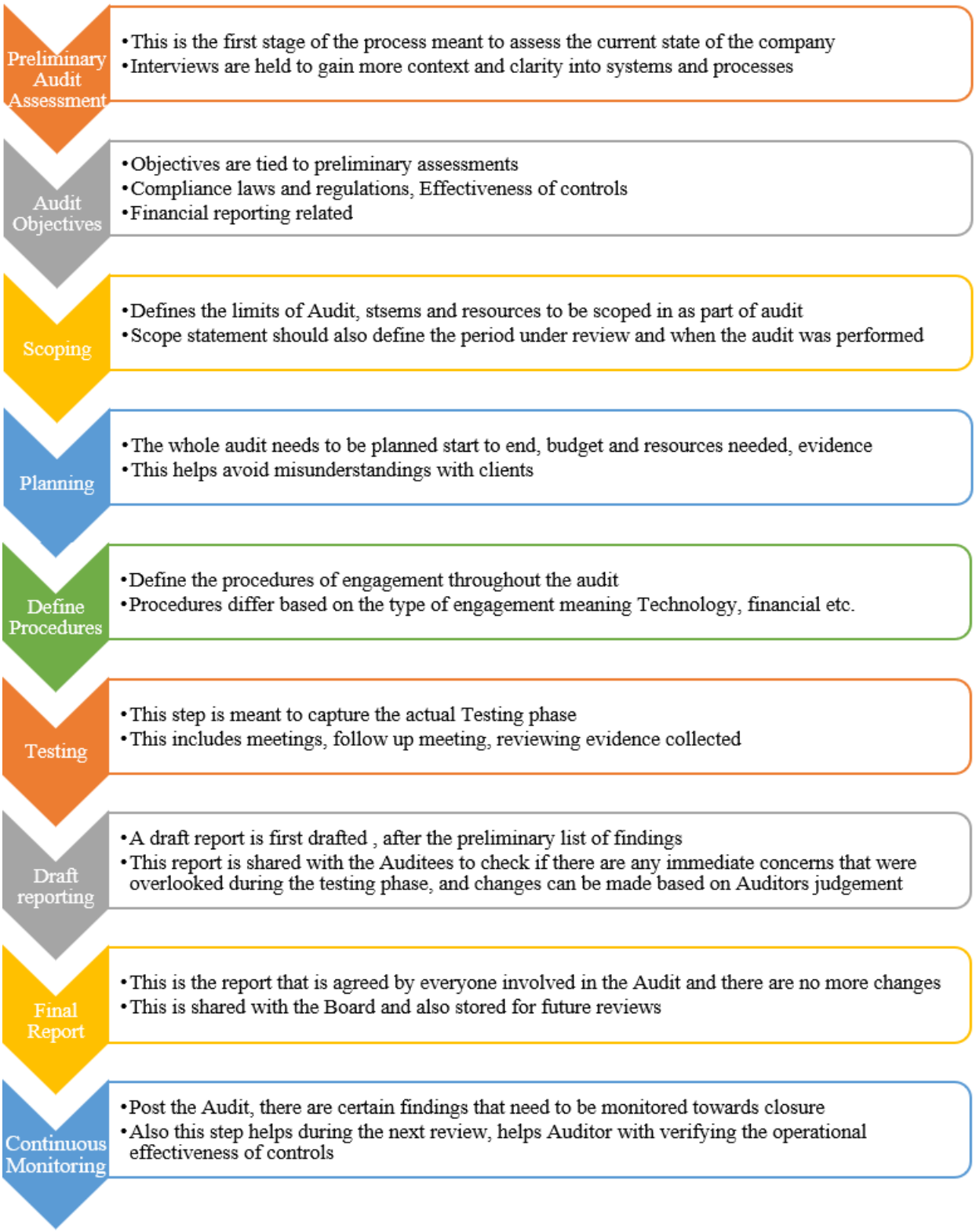
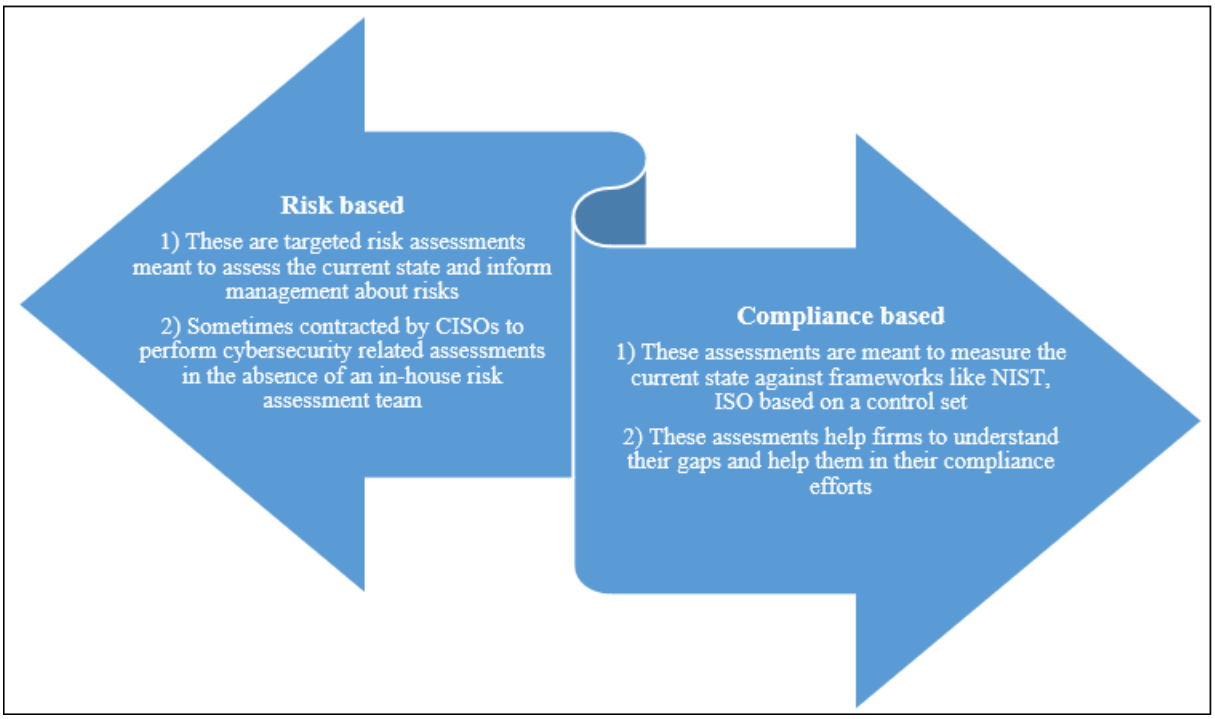


Figure 1: Audit process flow

3. 3rd party assessments

Third party assessments are independent evaluations performed by a security vendor [10]. The main difference between and Audit and these assessments are that these are designed to be collaborative. These are not meant to uncover any findings but rather help the firm achieve a benchmark or make informed decisions. These are typically Risk based or Compliance based.



Both these assessments help the organizations in their business objectives, 3rd party risk assessments help in the annual control requirements as per certain regulations and policies, including internal ones, while Compliance related assessments help products with "Go to Market" strategies and sales.

4. Discussion

Every business should have an in-house internal audit team as a third line of defense, an independent investigative team that can review the policies and procedures, inspect systems and processes. This process ensures the whole organization is in check and operates within the boundaries defined. The Audit function also ensures that a comprehensive set of risks are identified and the organization is not blindsided. Audit teams when functioning as per charter and ensuring all assets are scoped in an annual cadence, can significantly help organizations improve the risk posture, if not all, most of the risks identified would have been on the remediation track with rest of them being accepted by the firm based on their risk appetite.

All the steps followed by the audit team as part of their framework is to make sure there is no business impact as a result of the audit.

Third party assessments are also key to get an independent review of a certain area in businesses, since most of the 3rd parties work with many customers, businesses, they have varied insights into the nuances of risks within the industry. This insight proves valuable especially if the end goal is compliance to certifications. These assessments are very helpful to identify risks that normally would have been challenging for in house teams because of the varied skillsets that these teams bring. Regulators in most cases prefer 3rd party attestation to verify accuracy of the findings and risks in the risk register. For example – Around 2017/18, many financial firms reached out to 3rd party assessors to measure current state and identify target state to implement NY - DFS [4] related compliance steps. Similarly, 3rd party assessors are also called in to verify the accuracy of SEC - 10Q reporting, SOX [2] compliance, PCI DSS [3] and many more. Third party assessors are equally held accountable for any inaccuracies in these attestations.

Senior Management has access to reports from both internal audit teams and 3rd party attestors if contracted, these reports alongside internally generated data dashboards provide a complete holistic risk posture about the firm, this helps them in making business decisions, divert budget, resources, review their risk appetite and accordingly provide risk response

5. Conclusion

[6] Cybersecurity risks affect the annual revenues, profits, sales and more. It can drive up costs and affect revenue. Innovation and Customer recurrences are also impacted, apart from having internal security teams who continuously identify risks, work on measures to remediate them, and provide risk reporting. It's very important to have an independent perspective on risk posture by the firms.

An internal audit team reporting directly to the board will not be influenced by any other senior leader and at the same time won't be affected by any micromanagement related tactics, the report would provide a comprehensive view of findings, risks resulting from those and the recommendations that would help mitigate these findings.

At the same time, 3rd party assessors are needed when firms aim for compliance certifications for market access or compliance to industry frameworks and regulations, since these assessing organizations bring in with them varied skill sets and experience from other clients from the same sector that might prove helpful in navigation of challenges. An independent and unbiased perspective is very crucial for the firms and businesses to maintain their risk posture.

References

[1] "Information Systems Security Audit: An Ontological Framework, " *www.isaca. org*. [Online]. Available: https: //www.isaca. org/resources/isaca - journal/issues/2016/volume - 5/information - systems - security - audit - an - ontological - framework
[2] "The Sarbanes Oxley Act, " *sarbanes - oxley - act. com*. [Online]. Available: https: //sarbanes - oxley - act. com
[3] PCI Security Standards Council, "PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1 For merchants and other entities involved in payment card processing, " Jul.2018. [Online]. Available: https: //listings. pcisecuritystandards. org/documents/PCI_DSS - QRG - v3_2_1. pdf
[4] "Cybersecurity Resource Center, " *Department of Financial Services*. [Online]. Available: https: //www.dfs. ny. gov/industry_guidance/cybersecurity
[5] "Internal Control, " *COSO*. [Online]. Available: https: //www.coso. org/guidance - on - ic
[6] "IS Audit Basics: Auditing Cybersecurity, " *www.isaca. org*. [Online]. Available: https: //www.isaca. org/resources/isaca - journal/issues/2019/volume - 2/is - audit - basics - auditing - cybersecurity
[7] "Auditing Applications Part 1, " *ISACA*, 2012. [Online]. Available: https: //www.isaca. org/resources/isaca - journal/past - issues/2012/auditing - applications - part - 1
[8] "Your Audit Reports Have Consequences, " *ISACA*. [Online]. Available: https: //www.isaca. org/resources/news - and - trends/isaca - now - blog/2020/your - audit - reports - have - consequences
[9] "Monitoring and verifying cybersecurity controls effectiveness, " *Bakertilly. com*, 2017. [Online]. Available: https: //www.bakertilly. com/insights/monitoring - and - verifying - cybersecurity - controls - effectiveness
[10] S. Falconi, "Third - Party Assessments: What to Expect and Why They Can Benefit You, " *Delta Risk*, Feb.07, 2019. [Online]. Available: https: //deltarisk. com/blog/third - party - assessments - what - to - expect - and - why - they - can - benefit - you/