Practices of IT Audit in Dual-Class Share Companies: A Case Study of Alphabet Inc.

Chaoyue Li
Fox School of Business, Temple University, Beijing 101312, China

Keywords: Dual-Class Share Structure, IT Audit, COSO Framework, COBIT Framework.

Abstract: This paper explores the IT auditing practices of technology-driven enterprises operating under a dual-class share structure, using Alphabet Inc. as an illustrative case study. It examines the significance of IT auditing within this governance model and the unique challenges that arise due to its inherent characteristics. By introducing the COSO Internal Control Framework, the COBIT IT Governance Framework, and Agency Theory, the paper provides a comprehensive analysis of how dual-class share structures influence the independence and transparency of IT audits. The dual-class structure grants founding teams prolonged control over the company, which, while advantageous for strategic stability, can result in diminished audit quality and reduced governance transparency. Drawing from the practical example of Alphabet Inc., this paper elaborates on the ways in which external audit mechanisms and robust risk management strategies can strengthen the independence and compliance of IT audits. It also offers best practice recommendations for optimizing IT governance and auditing procedures, ensuring that strategic stability is preserved without compromising the effectiveness of IT control and transparency.

1 INTRODUCTION

In modern corporate governance, the dual-class share structure has become a widely adopted strategy by many large technology companies, such as Alphabet Inc. This structure, which allows different classes of shares with unequal voting rights, ensures that founding teams retain control over the long-term strategic direction of the company even when holding a lower equity percentage. With the growing complexity of information technology, dual-class structures present unique challenges for IT audit. IT audit is a comprehensive evaluation of information technology systems and their control measures, aimed at ensuring system security, integrity, and compliance. By combining expertise in auditing and information technology, IT audits identify and manage potential risks, ensuring data accuracy and supporting business objectives, and thus serve as a crucial tool in corporate risk management. This paper aims to discuss the importance of IT audit in the context of dual-class share structures, analyzing its key role in safeguarding corporate information security and ensuring the effectiveness of internal controls, and using the real-world example of Alphabet Inc. to explore how best to implement IT audit practices in this governance environment.

Recent years have seen increased research on the impact of dual-class structures on corporate governance, particularly in the field of IT audit. While the dual-class structure can ensure that founding teams retain control, it often leads to decreased transparency in corporate governance, thereby increasing audit risk. Moreover, empirical studies have indicated that dual-class structures significantly affect audit quality, particularly in cases of a wide divergence between voting rights and cash flow rights. Such structures can result in management choosing lower-quality audit services, further exacerbating challenges to audit independence (Liu, 2020; Springer, 2020). Therefore, exploring IT audit practices under such structures holds important theoretical and practical significance.

2 THEORETICAL FRAMEWORK

In the context of a dual-class structure, IT audit faces unique challenges. To address these challenges, this

Li, C.
Practices of IT Audit in Dual-Class Share Companies: A Case Study of Alphabet Inc..
DOI: 10.5220/0013225900004568
In *Proceedings of the 1st International Conference on E-commerce and Artificial Intelligence (ECAI 2024)*, pages 344-349
ISBN: 978-989-758-726-9

paper will analyze the topic based on three key theoretical frameworks: the COSO Internal Control Framework, the COBIT Framework, and Agency Theory. These theoretical models not only provide a foundation for IT audit but also offer practical guidance for ensuring the independence and effectiveness of audits under complex governance structures.

2.1 COSO Internal Control Framework

The COSO Internal Control Framework serves as the foundation for the design and evaluation of internal control systems, and it is widely applied in the governance practices of various organizations. The framework includes five key components: control environment, risk assessment, control activities, information and communication, and monitoring (Ren, 2019). For companies with a dual-class structure, the COSO framework is particularly useful for ensuring the independence and transparency of IT audits within a control environment heavily influenced by the founding team. By applying the COSO framework, companies can establish a solid internal control environment that clearly delineates the independence of the audit function while using risk assessment to identify and manage potential threats to information system security. For instance, large global technology companies often face multiple data center security risks, and applying the COSO framework can effectively ensure the security and compliance of information systems.

2.2 COBIT Framework

The COBIT framework provides a set of control objectives and best practices specifically for IT governance. It emphasizes balancing IT risks and business value in corporate governance, particularly in maintaining audit independence and impartiality in IT audits, thereby preventing audit results from being affected by undue interference from management or founding teams (Gu, 2023). For companies with a dual-class structure, the COBIT framework offers guarantees for the independence of IT audits and governance transparency. As technology companies make substantial investments globally, the complexity of IT audit has also increased significantly. Applying the COBIT framework allows for effective identification and management of IT risks, ensuring the rational allocation and use of IT resources.

2.3 Agency Theory

Agency Theory addresses conflicts of interest between management (agents) and shareholders (principals), particularly under conditions of information asymmetry. The theory posits that management may engage in behaviors detrimental to shareholders, thus necessitating independent audit to mitigate these conflicts (Forst and Hettler, 2019). In the context of a dual-class share structure, with founders holding significant control rights, agency issues can become even more complex. Alphabet Inc. mentioned in its 10-K report that 53% of the company's global revenue in 2023 came from international markets (Alphabet, 2023). In such a globalized operational context, agency problems can be more pronounced. Therefore, by incorporating Agency Theory, this paper further analyzes how IT audit can function in such a structure to balance the interests of founders and other shareholders.

3 THE ASSOCIATION BETWEEN DUAL-CLASS STRUCTURE AND IT AUDIT

Alphabet Inc. has adopted a dual-class share structure, wherein its founders maintain long-term control of the company through Class B shares with high voting rights. Although this control provides strategic stability, it also presents unique challenges for IT audit. Studies have shown that companies with dual-class structures often perform poorly in terms of audit independence and transparency, thereby increasing audit risk.

Specifically, Alphabet Inc.'s 2023 10-K report highlights the increasing complexity of cybersecurity threats and data protection challenges faced by the company. To address these challenges, the company must ensure the security and compliance of its information systems, making IT audit particularly important. In this context, IT audit must ensure not only the security and compliance of information systems but also that audit independence is not compromised by founder control.

4 CASE ANALYSIS: IT AUDIT PRACTICES AT ALPHABET INC.

4.1 Maintaining Independence and Transparency in IT Audit

Under a dual-class structure, audit independence and transparency are key challenges. Alphabet Inc.'s founders retain significant control through Class B shares, which may influence audit independence to some extent (Harvard Law School Forum, 2022). However, Alphabet Inc. has taken several measures to maintain the independence of IT audit. For instance, the company regularly invites independent third-party audit firms to conduct comprehensive audits of its IT systems, ensuring the objectivity and impartiality of audit results. Third-party audits cover not only traditional financial information systems but also include reviews of the security and compliance of cloud infrastructure. Through external audits, Alphabet Inc. effectively reduces the risk of management overstepping during the audit process, thereby enhancing the independence of IT audit.

Furthermore, Alphabet Inc. enhances audit transparency by publicly disclosing audit results and related risk management measures. For example, in its 10-K report, the company provided detailed information on major cybersecurity threats, including cyberattacks, data breaches, malware, ransomware, and supply chain security issues, as well as corresponding strategies. This transparency not only increases shareholders' trust in management but also improves overall corporate governance (Alphabet, 2023).

4.2 Application of the COSO Framework at Alphabet Inc.

The COSO Internal Control Framework forms the foundation of Alphabet Inc.'s internal control system. Specifically, the company has established a dedicated internal control environment to ensure that its information systems are strictly monitored throughout their lifecycle. Risk assessment is a key component of the COSO framework, and Alphabet Inc. regularly conducts risk assessments to identify potential threats to information system security and implements corresponding control measures. For instance, the company continuously updates and tests its disaster recovery plan to ensure that information systems can be quickly restored during emergencies, such as cyberattacks or natural disasters (Forst and Hettler, 2019; Qalaai, 2023).

Additionally, Alphabet Inc. emphasizes the information and communication aspect of the COSO framework in its IT audit practices. The company ensures smooth internal information flow between departments and communicates audit results and critical IT risks to external stakeholders through regular shareholder reports and press releases. This approach not only complies with the COSO framework's requirements for information and communication but also strengthens the transparency and accountability of the company's IT audit.

4.3 IT Governance under the COBIT Framework

The COBIT framework emphasizes balancing IT risks and business value within corporate governance, which has been fully reflected in the IT audit practices of Alphabet Inc. To address an increasingly complex IT environment, Alphabet Inc. has adopted COBIT framework best practices to establish a complete IT governance structure. Through this structure, the company can effectively identify and manage IT risks, ensuring the rational allocation and use of IT resources. For example, the company has implemented strict access control and regular security audits for its key cloud computing and data storage systems to prevent unauthorized access and potential data breaches (Mambu et al., 2024).

Within the context of a dual-class share structure, the COBIT framework also helps Alphabet Inc. ensure the independence of IT audits. Specifically, the company has set up an independent IT audit committee responsible for supervising the IT audit process and reporting directly to the board of directors. This arrangement ensures that the audit process is free from direct influence by management or founders, thereby enhancing the credibility of audit results.

4.4 Practical Application of Agency Theory

Agency Theory examines conflicts of interest between management and shareholders, which can be particularly complex under a dual-class share structure. Alphabet Inc.'s management holds significant control rights, which might, in certain cases, lead to decisions that are unfavorable to common shareholders (Alphabet, 2023). To mitigate such conflicts, IT audit becomes a crucial mechanism. Through independent IT audit, Alphabet Inc. can ensure that the operation and management of its information systems align with the interests of all shareholders, not just those of the founding team.

For instance, in response to increasingly severe cybersecurity threats, Alphabet Inc. has leveraged IT audit to identify and mitigate potential agency issues. The company has introduced advanced monitoring technologies and real-time risk assessment tools to ensure that all management decisions undergo rigorous audit and evaluation, preventing management from making decisions that favor their own interests due to information asymmetry.

4.5 The Impact of Dual-Class vs. Single-Class Share Structures on IT Audit: A Comparative Analysis of Alphabet Inc. and IBM

4.5.1 Cybersecurity and Risk Management

In its 2023 10-K report, Alphabet Inc. provided a detailed description of its cybersecurity and risk management strategies. The company employs advanced technological methods, including artificial intelligence and big data analytics, for real-time monitoring and response to potential security threats. Additionally, Alphabet has highlighted its defenses against common cyberattacks, supply chain vulnerabilities, and state-sponsored cyberattacks, particularly noting the heightened importance of security amidst global political tensions (Alphabet, 2023).

In contrast, IBM also emphasizes the importance of risk management in its cybersecurity strategy, especially in highly regulated industries such as finance, healthcare, and government. IBM has adopted a multi-layered security defense system based on the NIST (National Institute of Standards and Technology) cybersecurity framework and uses overlapping controls to defend against cyberattacks. IBM also faces the challenges of global cyber threats and has explicitly stated that, despite implementing various measures, it cannot entirely eliminate cybersecurity risks (International Business Machines Corporation, 2023).

4.5.2 Internal Control and IT Audit

Alphabet Inc. relies on the COSO framework, conducting both external and internal audits to ensure the independence and security of its IT systems. The company particularly emphasizes the role of external audit firms in monitoring information systems and cybersecurity, thereby ensuring the transparency of internal controls and audits. The audit also includes assessments of AI system security to avoid risks arising from technological malfunctions (Alphabet, 2023).

Similarly, IBM's internal control and IT audit also rely on the COSO framework, combined with its global standardized processes to ensure compliance and business transparency. Additionally, IBM's audit covers complex industries and regions, encompassing data processing, cloud services, and the storage and transmission of various types of sensitive information (International Business Machines Corporation, 2023).

4.5.3 Data Privacy and Compliance

Regarding data privacy, Alphabet Inc. ensures compliance through strict user data protection policies and continuous adaptation to privacy regulations such as GDPR. The company has implemented features such as data encryption and user-controlled privacy settings on a global scale and continually updates its IT audit procedures to comply with increasingly stringent global privacy regulations (Alphabet, 2023).

IBM faces even more complex global compliance challenges concerning data privacy. Its clients come from highly regulated industries, and IBM must ensure the security and compliance of customer data worldwide through strict internal controls and audit processes. IBM's risk management and compliance checks cover all its products and services, ensuring transparency and security in data processing (International Business Machines Corporation, 2023).

4.6 Future Outlook and Continuous Improvement

While Alphabet Inc. has established a comprehensive IT audit system, continuous improvements are needed as technology evolves and external threats change. In the future, Alphabet Inc. may further enhance the automation and intelligence of its IT audit, leveraging artificial intelligence and big data analysis tools to improve the accuracy of risk identification and audit efficiency. Moreover, as shareholders demand greater transparency in corporate governance, the company may need to disclose its IT audit results more frequently and in greater detail to boost investor confidence and market trust.

Through its comprehensive IT audit practices, Alphabet Inc. demonstrates how to maintain audit independence and transparency in an environment of significant managerial control. The company has implemented several measures, including regular internal and external audits, security reviews of cloud infrastructure, and compliance checks, to ensure that its IT systems can withstand external threats. Furthermore, the introduction of third-party audit firms enhances audit independence, ensuring that the founders' control does not compromise the objectivity of audit results.

5 CONCLUSIONS

Although the dual-class share structure provides a stable long-term governance framework for companies, it also poses unique challenges for IT audit. Companies like Alphabet Inc., with dual-class structures, have demonstrated how to maintain audit independence and transparency in an environment with significant managerial control through comprehensive IT audit practices. Drawing from the case of Alphabet Inc., the following best practice recommendations for IT audit in dual-class companies are proposed:

(1) Ensuring IT Audit Independence: Under a dual-class structure, management's control may pose a potential threat to audit independence. Therefore, companies should ensure that IT audits are conducted by independent third parties and further strengthen the role of the audit committee to prevent excessive management interference in the audit process.

(2) Enhancing Audit Transparency: Companies should establish mechanisms to regularly disclose IT audit results to shareholders. It is recommended that key findings and countermeasures from IT audits be reported to shareholders at least quarterly. Specific steps include identifying key risks during the audit, categorizing them, detailing the potential impact of each risk and management measures in the quarterly report, and setting a disclosure schedule to ensure timely communication. Companies should also hold an annual IT governance transparency meeting to communicate audit results and governance improvement plans directly with shareholders, thereby enhancing trust and engagement.

(3) Strengthening Risk Management and Emergency Response: Dual-class companies should place special emphasis on risk management for information systems and conduct regular cybersecurity tests and emergency response drills. IT audits should cover these areas to ensure that companies can respond swiftly and effectively to information security threats, thereby minimizing losses and compliance risks.

(4) Continuous Monitoring and Improvement: IT audit should not be limited to annual audits but should be a process of continuous improvement. Companies should regularly review and optimize their IT audit processes to ensure that audit practices can keep pace with rapidly evolving technological changes and constantly emerging security challenges.

By adopting these best practice recommendations, dual-class companies can more effectively address the unique challenges of IT audit, enhancing audit independence and transparency. In the future, as technology and regulations continue to change, companies will need to continuously monitor and improve their IT audit practices to ensure that their governance structures do not negatively impact the independence of the audit process.

In conclusion, while the dual-class share structure provides a guarantee of long-term control, it raises new issues regarding audit independence and transparency. By drawing on the IT audit practices of Alphabet Inc. and adopting the above best practice recommendations, companies can maintain stable governance structures while optimizing their IT audit processes. Future research could further explore how different types of dual-class companies implement IT audit in complex governance environments to provide more targeted audit strategies.

REFERENCES

Alphabet Inc., 2023. Form 10-K Annual Report for the Fiscal Year Ended December 31, 2023. United States Securities and Exchange Commission.

Forst, A., Hettler, B. R., 2019. Disproportionate Insider Control and the Demand for Audit Quality. *AUDITING: A Journal of Practice and Theory*, 38(1):171-191.

Gu, Y., 2023. Research on Enterprise Information System Audit Based on COBIT Framework. *Market Weekly*, (10): 158-161.

Harvard Law School Forum on Corporate Governance. 2022. Re-Thinking The Hostility Towards Dual-Class Share Structures. *Harvard Law School Forum on Corporate Governance*.

International Business Machines Corporation., 2023. Form 10-K Annual Report for the Fiscal Year Ended December 31, 2023. *United States Securities and Exchange Commission*.

Liu, S., 2020. Research on the correlation between dual ownership structure characteristics and audit quality: based on empirical evidence of US dual ownership structure listed companies. *National Circulation Economy*, (24): 128-132

Mambu, J. Y., Wulyatiningsih, T., Adam, S., 2024. Applying COBIT 2019 to Design a Tailored IT Governance System for PT. Telekomunikasi Seluler Manado Branch. Jurnal Informasi dan Teknologi, 6(2): 229-237.

Qalaai, Z., 2023. The COSO Framework: Implications of Internal Control Components on Organisational Performance. Lebanese French University - Erbil, Kurdistan.

Ren, L., 2019. Analysis of Enterprise Risk oriented Audit Model Based on the New COSO Framework. *Audit Perspective Audit Observation*, (31): 78-81.

Springer., 2020. Voluntary Disclosure and Ownership Structure: Dual-Class Share Firms. *Journal of Management and Governance*.