LESSONS LEARNED FROM WARNING SIGNS BEFORE THE OCTOBER 7, 2023, FAILURE: STRENGTHENING BOARD AND AUDITOR OVERSIGHT

Keren Bar-Hava *

* The Hebrew University Business School, Jerusalem, Israel
Contact details: The Hebrew University Business School, Mount Scopus Campus, Jerusalem 9190501, Israel

OPEN ACCESS

How to cite this paper: Bar-Hava, K. (2024). Lessons learned from warning signs before the October 7, 2023, failure: Strengthening board and auditor oversight. *Corporate Board: Role, Duties and Composition, 20*(3), 54–61. https://doi.org/10.22495/cbv20i3art5

ISSN Online: 2312-2722
ISSN Print: 1810-8601

Received: 27.07.2024
Accepted: 18.10.2024

JEL Classification: M41, M42, G30, M48
DOI: 10.22495/cbv20i3art5

Abstract

This paper argues that incomplete information analysis and over-reliance on technology can obscure financial risks, drawing parallels between audit failures and intelligence lapses such as the October 7, 2023, attack. It asserts that professional auditors and proactive boards are essential for corporate survival. Emphasizing a risk-based audit approach, the study highlights the need for holistic use of technology, critical thinking, and effective communication. The research offers actionable guidance for boards to enhance collaboration with auditors, integrate safeguards into decision-making, and strengthen corporate governance. By focusing on robust internal controls and proactive risk management, this study provides a framework to prevent future financial disasters.

Keywords: Internal Control, Audit Failures, Technology in Auditing, Risk-Based Auditing, Independent Directors, Corporate Governance Quality

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Author declares that there is no conflict of interest.

1. INTRODUCTION

Audit failures and governance breakdowns have repeatedly been at the center of major financial crises, leaving permanent impacts on corporate stability and investor confidence. Despite the vital role that auditors and proactive boards play in safeguarding against financial risks, deficiencies in both audit practices and governance oversight continue to lead to costly failures. This article argues that the combination of audit failures, governance breakdowns, and the silence of key gatekeepers significantly contributes to systemic risk. It offers practical recommendations for boards to mitigate these risks and enhance corporate resilience.

Drawing upon the seminal studies of Dechow et al. (1995) and Becker et al. (1998), examining auditors' difficulties in detecting earnings management, this study broadens the discussion by focusing on how governance breakdowns, aggravated by audit failures and the silence of key gatekeepers like independent directors, escalate systemic risk. As Bar-Hava et al. (2021) noted, independent directors frequently resign without revealing crucial governance issues, thereby sustaining organizational risk and weakening transparency.

The State of Israel, much like a global corporation fortified with cutting-edge technology and sophisticated defence mechanisms, appeared impervious to threats. However, as the events of October 7, 2023, showed, even the most well-protected systems can fail catastrophically if early warning signs are ignored. This case study provides a unique lens through which we can view corporate governance failures. Just as Israel's advanced security apparatus faltered, large corporations with strong internal controls and advanced technologies are vulnerable to collapse when human oversight and proactive risk management are lacking.

In addition, this article provides practical recommendations for boards, auditors, and regulators. By drawing parallels between the intelligence failure of October 7, 2023, and common audit failures, this article demonstrates the need for a more proactive and vigilant approach to risk management. Both domains reveal how overreliance on technology and a failure to act on early warning signs can lead to disastrous outcomes. By addressing these issues, this research provides a framework for strengthening corporate governance and preventing future financial crises.

As Rasmussen and Svedung (2000) argue, proactive risk management is essential in today's complex and dynamic environment. By anticipating and addressing potential risks before they materialize, organizations can enhance their resilience and mitigate the negative impacts of unexpected events. This paper explores the implications of proactive risk management for corporate governance, focusing on the roles of auditors and boards in identifying, assessing, and mitigating risks.

The remainder of this article is structured as follows. Section 2 provides an overview of the auditor's role and the importance of effective corporate governance. Section 3 describes audit failures and internal control weaknesses. Section 4 presents the October 7, 2023, intelligence failure as a case study. Section 5 analyses the parallels between intelligence and audit failures. Section 6 offers a discussion, including recommendations and limitations. Finally, Section 7 concludes the study.

2. LITERATURE REVIEW: AUDITOR AND EFFECTIVE CORPORATE GOVERNANCE

This article examines procedures that necessitate cooperation between several safeguards, focusing on the leadership of the board and its interactions with auditors and other safeguards. Effective corporate governance depends not only on auditors' oversight but also on the active engagement of boards, audit committees, and external mechanisms. Each plays a crucial role in ensuring financial stability, transparency, and accountability. This section reviews the relevant literature on these key controllers, examining their individual roles as well as their collective contributions to corporate governance.

Auditors are central to safeguarding a company's financial integrity. They serve as a critical line of defense against financial misstatements and fraud, enhancing transparency through risk assessment and internal control evaluations (Sapiri, 2024). Dechow et al. (1995) highlights the challenges auditors face in detecting earnings management, which is a common form of financial misstatement aimed at manipulating reported earnings. Their findings underscore the importance of robust auditing procedures to prevent audit failures. Similarly, Becker et al. (1998) find that larger audit firms, often referred to as the Big Six (since 2001, the Big Four: Deloitte, Ernst & Young, KPMG, PwC), provided higher quality audits due to their access to more resources and greater expertise, further demonstrating the importance of audit firm size in maintaining audit integrity.

2.1. Responsibilities of auditors

The primary responsibility of auditors is to evaluate the quality of a company's internal control systems, which enables them to plan and perform audit work effectively (Gaumnitz et al., 1982). Auditors meticulously examine financial records and supporting documentation to ensure that a company's financial statements accurately reflect its financial position (Hirst, 1994). This verification process helps identify discrepancies that may signal intentional misstatements or errors. Independence and objectivity are critical for auditors, who must avoid conflicts of interest to maintain the integrity of their assessments. Auditors must approach their work neutrally, basing their conclusions on the evidence they gather and not being influenced by external pressures or personal biases.

2.2. Assessing the effectiveness of internal controls

A robust internal control system, evaluated by auditors, provides protection against fraud and errors. Auditors assess the design and implementation of these controls to ensure they are adequate to prevent fraud, protect assets, and promote regulatory compliance. The literature consistently emphasizes the importance of internal controls in maintaining the integrity of financial statements (Gaumnitz et al., 1982). Strong internal controls help to minimize the risk of financial misstatements and ensure the effective functioning of corporate governance.

2.3. Identifying potential risks of fraud or errors

While management has the primary responsibility for preventing and detecting fraud, auditors contribute to this effort by identifying potential risks through their assessments (Bunget, 2009). Auditors evaluate areas within an organization that may be particularly vulnerable to financial misstatements due to fraud or errors. Ramos (2003) argues that risk assessment procedures allow auditors to focus their efforts on areas with the greatest potential for problems to arise, ensuring that resources are allocated efficiently during the audit process.

2.4. The rise of artificial intelligence in auditing

The integration of artificial intelligence (AI) into the audit process has introduced both opportunities and challenges for the profession. AI tools, such as Computer Assisted Audit Techniques (CAATs), support auditors by enhancing the speed and efficiency of audit tasks (Braun & Davis, 2003). These tools allow auditors to analyse large datasets, identifying patterns and anomalies that might otherwise go undetected (Sayana & Cisa, 2003). As technology advances, auditors increasingly rely on AI to support their work. Aksoy and Gurol (2021) note that digital transformation, particularly the use of AI, has revolutionized the audit profession by providing auditors with new tools to improve the accuracy and efficiency of their audits.

Despite the advantages of AI, some researchers express concerns about the potential for overreliance on these technologies, which could reduce the role of professional judgment. Kokina and Davenport (2017) emphasize that while AI can enhance audit quality, human oversight remains essential. Auditors must continue to exercise professional scepticism and critical thinking to interpret AI-generated insights correctly. Fedyk et al. (2022) found that investment in AI has resulted in improved audit quality and lower fees, although the full impact of these technologies on the audit labour market and practice may take years to be realized.

2.5. Audit expectation gap

Lin and Chen (2004) discuss the audit expectation gap, which refers to the difference between what the public expects from auditors and the actual scope of their responsibilities. While the public may expect audits to guarantee the absence of errors or fraud, auditors provide only reasonable assurance through extensive testing procedures. This gap highlights the importance of clear communication between auditors and the board of directors, who play a key role in managing expectations and promoting transparency regarding the limitations of the audit.

2.6. Board oversight and the audit committee

The effectiveness of the audit process depends not only on the auditors, but also on the quality of the board of directors and the audit committee. Beasley (1996) demonstrates that boards with a higher proportion of independent outside directors are less likely to experience financial statement fraud. These independent directors bring objectivity and independence to the board's oversight role, which is essential for effective corporate governance. The audit committee, appointed by the board, is tasked with supervising the auditors and ensuring their independence (U.S. Securities and Exchange Commission, 1934, Section 10A; U.S. Securities and Exchange Commission, 2022, Section 301).

Al-Shaer and Zaman (2021) underscore the importance of the communication role of the audit committee. Their research indicates that the tone and content of communication between auditors and the audit committee can significantly affect the quality of financial statements. Transparent communication fosters an environment in which auditors can freely raise concerns, contributing to a more effective audit process.

2.7. The silence of the safeguards in financial crises

The silence of key safeguards, including auditors and independent directors, during financial crises can have severe implications for corporate governance. Sikka (2009) examines how auditors' failure to raise red flags during critical moments of financial distress contributed to several governance breakdowns. This silence, whether due to conflicts of interest, overconfidence, or passive compliance, exacerbates corporate failures by allowing financial misstatements and risky behaviours to go unchecked. Similarly, Bar-Hava et al. (2021) highlight that independent director, who play a pivotal role in corporate oversight, often resign without disclosing the governance issues they encountered, perpetuating the risks within the organization. The combined silence of both auditors and independent directors weakens the corporate governance structure and emphasizes the need for proactive risk management, transparency, and stronger safeguards to prevent financial crises.

3. AUDIT FAILURE AND INTERNAL CONTROL WEAKNESSES

This article analyzes the multifaceted nature of audit failure, focusing on the various internal control deficiencies that can contribute to such breakdowns. Auditors serve a critical function in ensuring the integrity of a company's financial reporting and governance structures, with internal controls being fundamental to this process. Internal control is designed to provide reasonable assurance regarding the reliability of financial reporting, compliance with applicable laws and regulations, and the effectiveness of operations (Kinney, 2000). However, when auditors fail to execute their responsibilities with due professional care, the likelihood of internal control weaknesses increases substantially. Such weaknesses can undermine a firm's ability to detect and prevent financial misstatements or operational inefficiencies, ultimately compromising both its financial health and reputation (Ge & McVay, 2005). Audit failures often stem from a combination of factors, including:

- *Inadequate risk assessment.* Auditors may fail to adequately identify and assess inherent and control risks in an organization. This can result in the misallocation of audit resources and an inability to detect significant control weaknesses. Professional skepticism is a cornerstone of effective auditing, yet auditors sometimes fall short of this standard, whether due to cognitive biases such as confirmation or optimism bias, or organizational pressures (Nelson, 2009). Risk misassessment frequently leads to audit failures, as demonstrated by Bell and Solomon (2002), who emphasize the need for a systematic approach to identifying risks early in the audit process.
- *Confirmation bias and cognitive biases.* Auditors may exhibit confirmation bias, leading them to disregard or downplay red flags that contradict their initial risk assessments. Additionally, optimism bias can prevent them from acknowledging the potential severity of control deficiencies. When auditors are overly optimistic, they may fail to recognize early warning signs of deeper control issues, allowing problems to persist undetected (Tversky & Kahneman, 1974). The tendency to succumb to such biases is well documented in the auditing literature, and steps to mitigate these biases are necessary for improving audit quality (Knechel & Salterio, 2016).
- *Communication silos.* Ineffective communication between management, internal audit functions, and external auditors can hinder the timely identification and escalation of control weaknesses. Internal control weaknesses arise from a confluence of

factors, including failures in communication among key stakeholders. Without open, structured communication channels, crucial information about control deficiencies may not reach decision-makers in time to prevent significant failures (DeZoort et al., 2002). Cohen et al. (2002) further explore the importance of audit committee involvement in fostering effective communication and governance, highlighting that communication failures exacerbate internal control deficiencies.

- *Systemic design flaws.* Internal control systems themselves may be inherently flawed, lacking the necessary robustness to detect and prevent fraud or errors. Poorly designed or outdated systems can severely limit an organization's ability to maintain an effective control environment. This is especially true in cases where companies have failed to invest in their control systems, leading to vulnerabilities that can be exploited by internal or external parties (Ashbaugh-Skaife et al., 2006). Ge and McVay (2005) note that firms with complex operations and weak internal systems are particularly susceptible to material weaknesses, emphasizing the need for ongoing investment in internal control structures.
- *Organizational inertia.* A reluctance to adapt or challenge existing processes can create an environment where control weaknesses persist. This can be exacerbated by a culture that discourages questioning or dissent. When companies are resistant to change, or when management does not encourage continuous improvement of internal controls, even obvious deficiencies may remain unresolved for extended periods (Hannan & Freeman, 1984). Organizational inertia, driven by deeply ingrained behaviors and structural resistance, can prevent timely responses to emerging risks and weaknesses, making the organization vulnerable to prolonged control issues.

The failure of auditors to adequately fulfill their oversight responsibilities can have far-reaching implications for the organization. Weaknesses in internal controls not only increase the risk of financial misstatements but also expose the company to regulatory sanctions, legal liabilities, and reputational damage (DeAngelo, 1981). The long-term consequences of audit failures can be severe, eroding investor confidence and undermining the firm's market position. Therefore, ensuring that auditors adhere to rigorous professional standards is critical in maintaining the effectiveness of the internal control environment and safeguarding the company's financial stability (Kinney, 2000).

By recognizing these interrelated factors, auditors can enhance their risk assessment procedures, improve communication channels, and advocate for the implementation of robust internal controls. This multifaceted approach can help reduce the risk of audit failure and enhance the effectiveness of the internal control environment. Auditors, by improving their risk assessment processes, maintaining professional skepticism (Nelson, 2009), and facilitating open lines of communication, play a pivotal role in identifying and addressing control deficiencies. This, in turn, strengthens the internal control environment and reduces the likelihood of audit failure.

4. THE CASE STUDY OF OCTOBER 7, 2023, FAILURE

The horrific massacre was carried out by Hamas on October 7, 2023. The most advanced technologies were used at the Israeli border on October 6, 2023. Hamas's infiltration into Israel was made possible by a series of security failures.

Frantzman (2023) states that there were observation towers and soldiers monitoring Gaza. Israel also has drones and observation balloons. However, no one knew that Hamas had thousands of terrorists ready to leave the line at around 6am and attack more than 29 points along the border fence. Videos show that Hamas used drones to attack various observation towers and observation points. They also attacked armored vehicles. This made it harder to contend with the attack.

- Intelligence officers failed to monitor key communication channels used by Palestinian attackers.
- Overreliance on border surveillance equipment that was easily shut down by attackers, allowing them to raid military bases and slay soldiers in their beds.
- Concentration of commanders in one border base that was captured early in the invasion, preventing communication with the rest of the military.
- Willingness to accept at face value claims by Gazan military leaders, made through private channels that the Palestinians knew were monitored by Israel, that they were not preparing for battle.

Salhani (2023) documents that an over-reliance on technology by Israel's intelligence agencies and military has continued to shape the current conflict in Gaza, while also being partially responsible for the failure to detect the Hamas attack on October 7, 2023. Israeli security services are believed to have collected more than enough data to anticipate an imminent Hamas attack. Indeed, according to Bergman and Goldman (2023), Israeli intelligence knew about the impending Hamas attack plans a year in advance. Billions of US dollars invested in high-tech defenses such as border walls and closed-circuit television cameras around Gaza were thought to be sufficient to stop any attack. But technological reliance has led to a false sense of security. Comprehensive intelligence gathering requires a range of sources: open-source code, intercepted communications, satellite imagery, and tracking. All of these are critical factors in gathering intelligence before producing an analysis, but the human intelligence aspect is also critical to critical thinking.

5. ANALYSIS

The intelligence failure on October 7, 2023, provides a stark example of how failure to respond to early warning signs can have disastrous consequences. This failure mirrors similar governance breakdowns in the corporate world, where audit processes and board oversight fail to address significant risks due to miscommunication, poor leadership, or a dysfunctional board culture. Drawing parallels between intelligence failures and audit failures reveals several critical areas of overlap: 1) risk misassessment, 2) communication silos, 3) systemic design flaws, and 4) organizational inertia.

A significant parallel is in misjudgement of risks. Israeli intelligence underestimated the threat posed by Hamas, just as auditors often miss significant risks due to confirmation bias or overconfidence (Tversky & Kahneman, 1974; Nelson, 2009). In both contexts, there is an overreliance on technology and established processes that create blind spots. Auditors, like intelligence officers, may fail to challenge their initial conclusions, leading to overlooked red flags within the organization (Bell & Solomon, 2002). This underscores the critical role that boards of directors must play in promoting accountability and critical oversight. Boards should lead by ensuring that auditors adopt a dynamic, questioning approach to risk assessment, continuously re-examining potential threats and refusing to settle for superficial analyses (Brown & Peterson, 2022).

Another critical reason for the failure of the October 7, 2023, attack was the breakdown in communication between intelligence and military branches. Failure to share important information in a timely manner has allowed attackers to exploit vulnerabilities (Frantzman, 2023; Bergman & Kingsley, 2023). Similarly, communication silos within corporations, whether between management, internal auditors, or the board, delay the identification of governance risks (Cohen et al., 2002). Dysfunctional cultures often stifle communication, especially when power imbalances prevent the free flow of information (Brown & Peterson, 2022). To mitigate these risks, boards must take proactive steps to remove communication barriers by creating an environment where stakeholders are encouraged to speak up and raise concerns freely. Regular and transparent communication between auditors, management, and the board is critical to identifying governance risks early and preventing organizational failure (Al-Shaer & Zaman, 2021).

Another parallel is the reliance on flawed internal systems. Israeli forces depended on technologies that were easily disabled by attackers, just as many organizations rely on internal control frameworks that fail to detect significant risks (Salhani, 2023). Silence, particularly the reluctance to question flawed systems, perpetuates these systemic flaws (Perlow & Williams, 2003). In corporate governance, boards of directors must take the lead in regularly reviewing and updating internal controls to reflect the evolving risks facing the organization. A culture of continuous improvement, driven by board leadership, is necessary to avoid governance failures on a large scale (Kinney, 2000).

Organizational inertia, or resistance to change in the face of clear risks, was another critical factor in the intelligence failure. Israeli commanders were slow to adapt to the evolving threat, reflecting the challenges corporate boards face in recognizing and addressing governance deficiencies (Hannan & Freeman, 1984). Dysfunctional cultures, particularly those characterized by power dynamics that discourage questioning, exacerbate this inertia (Brown & Peterson, 2022). Boards have a responsibility to counteract inertia by promoting a culture where critical oversight and questioning are valued. Governance frameworks must remain flexible and adaptable to changing risks and challenges, requiring regular reassessment and renewal (Rasmussen & Svedung, 2000).

Finally, failure to respond to early warning signs, whether in national security or corporate governance, is often compounded by a culture of silence. As Perlow and Williams (2003) note, silence driven by fear or complacency prevents necessary interventions. In corporate governance, dysfunctional board cultures characterized by passive compliance or fear of retaliation allow risks to grow unchecked (Brown & Peterson, 2022). To break this cycle, boards must foster a *culture of openness* and *proactive oversight*. Auditors need to feel empowered to raise red flags without fear of retaliation, and board members must lead by example, promoting transparency and accountability. By challenging the status quo and encouraging open dialogue, boards can prevent governance failures from escalating into larger crises (Sikka, 2009). For a comparative analysis between the October 7, 2023, case study and the corporate governance audit failures, see Table A.1 (in the Appendix).

6. DISCUSSION

In the context of corporate governance, critical thinking and professional scepticism are essential components of an effective audit. Auditors must go beyond simply analysing the financial data provided and take a broader risk assessment approach. By applying strong critical thinking, auditors can assess the broader context of an organization's operations and identify risks that may not be readily apparent. This approach is especially important when assessing complex governance issues, where surface-level data may obscure deeper problems within the organization.

Moreover, reliance on a single source of data can create blind spots that allow risks to go undetected. Overreliance on technology in auditing parallels the problems that arose from the October 7, 2023, intelligence failure, where overreliance on surveillance technology led to critical oversights. Therefore, auditors must adopt a multi-source approach, using a wide range of information, including internal audit reports, industry publications, and direct discussions with management. By synthesizing diverse sources of information, auditors can develop a more holistic understanding of the company's risk profile.

Open communication is another critical aspect of governance that should be a priority during the audit process. The parallels between communication breakdowns in intelligence failure and corporate governance failures highlight the importance of fostering clear, direct channels for sharing information. Auditors should maintain strong communication with management, the audit committee, board members, and other key stakeholders to ensure that concerns are addressed promptly and effectively. The ability to raise red flags early can mitigate potential governance risks before they escalate.

The role of collaboration between the audit committee and external auditors is fundamental in strengthening auditing practices and preventing financial disasters such as insolvency. An audit committee that promotes open communication and transparency creates an environment in which external auditors are empowered to provide objective assessments. This collaborative environment ensures that auditors have unfettered access to necessary information and are encouraged to maintain professional scepticism throughout the audit process. Healthy scepticism allows auditors to critically review financial reports and detect potential risks that may otherwise go unnoticed. The effectiveness of this collaboration can determine whether governance issues are resolved in time to avoid significant financial consequences.

A key problem in corporate governance is the widespread perception that auditors and other safeguards are a burden rather than a source of value. This conception needs to change. Just as a company invests in research and development to drive innovation, it should invest in the insights and oversight provided by auditors, compliance teams, and risk managers to protect and enhance corporate integrity. By repositioning these functions as essential contributors to strategic success, boards can not only enhance governance but also leverage these teams to create sustainable, long-term value.

As the October 7, 2023, incident demonstrates, failure to respond to early warning signs can have disastrous results. In the context of corporate governance, the board's responsibility to foster an environment that prioritizes transparency, critical thinking, and proactive risk management is essential to mitigating these risks. Synergy between auditors, audit committees, and the board is crucial to ensuring that risks are identified and addressed proactively.

7. CONCLUSION

The "Control Failures" of October 7, 2023, provide a stark illustration of the critical role that independent auditors with integrity and professional expertise play in the modern economy. Auditors must remain constantly vigilant, employing a robust set of critical thinking skills to not only analyze the financial data presented, but also to assess the broader context and identify potential risks that may not be readily apparent. Furthermore, while audit firms are investing billions of dollars in developing AI systems to help auditors perform complex tasks, the October 7, 2023, event highlights the dangers of over-reliance on technology. It highlights the need for a balance between human expertise and technology. It suggests that both are critical to an effective audit. Human expertise is critical to interpreting data and identifying potential risks that may be missed by technology alone

While this article highlights the indispensable role of human auditors, it is important to acknowledge the research by Fedyk et al. (2022) that suggests advances in AI could transform the audit landscape in the future. AI has the potential to improve audit quality and efficiency. However, even in a technology-driven future, strong human expertise will remain essential for critical thinking, interpreting data, and identifying risks that might be missed by automation alone.

Additionally, boards of directors must be proactive in creating a strong internal control culture. By prioritizing preventative measures and understanding the immense value of disaster prevention, companies can significantly improve their overall risk management and financial stability.

To prevent governance disasters, corporate boards and audit committees must take a proactive and integrated approach to oversight, particularly in their interactions with internal and external auditors. Here are several key actions boards need to take:

- *Strengthening auditor independence.* Boards of directors should take a more active role in ensuring the independence of internal and external auditors. This includes reviewing and approving audit hours, resources, and audit plans with genuine diligence, rather than as a mere formality. By doing so, boards demonstrate their commitment to thorough and independent auditing processes. Best practice dictates that the internal auditor should be subordinate to the chairman of the board, or ideally, the chair of the audit committee — an independent board member. This ensures that the auditor reports to a truly independent authority, rather than the chief executive officer (CEO), and is not viewed as just another employee. This structure enhances objectivity, reduces conflicts of interest, and improves the integrity of the audit process.
- *Listening and paying attention to auditors.* Auditors should be seen as vital partners in safeguarding the organization, not just as technical advisors. Boards must ensure that auditors' concerns are duly considered, especially when they raise red flags or express concerns. Regular, direct communication between auditors, the audit committee, and the board can ensure that critical issues are heard and addressed promptly.
- *Audit plan evaluation.* The board should carefully discuss and evaluate the audit plan to ensure it aligns with the company's most pressing risks. Boards need to move beyond surface-level approval and engage in detailed discussions with auditors about the rationale behind the audit plan, areas of concern, and potential blind spots.
- *Encouraging transparency and open communication.* Boards should create an environment where auditors feel empowered to speak freely and raise concerns. This can be supported by regularly scheduling sessions where auditors provide updates, even outside of formal board meetings, ensuring open communication throughout the year.
- *Monitoring and adjusting audit focus.* Governance risks evolve, and so should audit plans. Boards must regularly reassess and adjust audit plans based on emerging risks or changes in the organization. This dynamic approach ensures that audits remain relevant and effective in mitigating risks.
- *Changing the perception of safeguards.* Boards need to lead a cultural shift in how safeguards such as auditors, compliance officers, and risk management teams are viewed within the organization. Rather than viewing them as obstacles or a necessary evil, these key roles should be valued for the critical insights and protections they offer. By framing these functions as integral to the long-term success of the company, boards can foster a more collaborative relationship with these teams. This shift in perception encourages the view

that safeguards add value by protecting the organization's reputation, ensuring compliance, and preventing costly failures.

• *Integrating safeguards into strategic decision-making.* Safeguards should not be siloed away from strategic decision-making but should have a seat at the table when key corporate risks and opportunities are discussed. Their expertise in risk management and compliance can help the board make more informed, balanced decisions. By involving auditors and other oversight bodies in strategic discussions, boards can demonstrate the value they add beyond traditional financial or compliance roles. For key recommendations for improving board oversight and audit practices, see Table A.2 (in the Appendix).

This study primarily draws parallels between the October 7, 2023, intelligence failure and audit failures on corporation, focusing on the role of auditors and boards in mitigating risks. While the comparison offers valuable insights into governance breakdowns, the scope of the analysis is limited by its reliance on a single case study. The lessons of intelligence failure provide a useful framework, but broader conclusions should be made with caution, as organizational dynamics in national security may differ in key respects from corporate governance structures.

Additionally, while the study discusses the increasing role of technology in auditing, particularly the use of AI, it does not explore in depth the long-term implications of these technological advancements. Future research could focus on the evolving role of AI in auditing, its impact on audit quality, and the balance between human oversight and technological tools.

Furthermore, the focus on independent directors and auditors as key safeguards in governance may not capture the full spectrum of governance failures, particularly those stemming from management practices and internal politics. Expanding the scope to include these dimensions could offer a more comprehensive understanding of governance breakdowns.

REFERENCES

Aksoy, T., & Gurol, B. (2021). Artificial intelligence in computer-aided auditing techniques and technologies (CAATTs) and an application proposal for auditors. In T. Aksoy & U. Hacioglu (Eds.), *Auditing ecosystem and strategic accounting in the digital era: Global approaches and new opportunities* (pp. 361–384). Springer https://doi.org/10.1007/978-3-030-72628-7_17

Al-Shaer, H., & Zaman, M. (2021). Audit committee disclosure tone and earnings management. *Journal of Applied Accounting Research, 22*(5), 780–799. https://doi.org/10.1108/JAAR-12-2020-0243

Ashbaugh-Skaife, H., Collins, D. W., & LaFond, R. (2006). The effects of corporate governance on firms' credit ratings. *Journal of Accounting and Economics, 42*(1–2), 203–243. https://doi.org/10.1016/j.jacceco.2006.02.003

Bar-Hava, K., Huang, S., Segal, B., & Segal, D. (2021). Do independent directors tell the truth, the whole truth, and nothing but the truth when they resign? *Journal of Accounting, Auditing and Finance, 36*(1), 3–29. https://doi.org/10.1177/0148558X18780801

Beasley, M. S. (1996). An empirical analysis of the relation between the board of director composition and financial statement fraud. *The Accounting Review, 71*(4), 443–465. https://www.jstor.org/stable/248566

Becker, C. L., DeFond, M. L., Jiambalvo, J., & Subramanyam, K. R. (1998). The effect of audit quality on earnings management. *Contemporary Accounting Research, 15*(1), 1–24. https://doi.org/10.1111/j.1911-3846.1998.tb00547.x

Bell, T. B., & Solomon, I. (Eds.). (2002). *Cases in strategic-systems auditing* [Business Measurement Case Development and Research Program]. KPMG and University of Illinois.

Bergman, R., & Goldman, A. (2023, December 2). Israel knew Hamas's attack plan more than a year ago. *The New York Times.* https://www.nytimes.com/2023/11/30/world/middleeast/israel-hamas-attack-intelligence.html

Bergman, R., & Kingsley, P. (2023, October 10). How Israel's feared security services failed to stop Hamas's attack *The New York Times.* https://www.nytimes.com/2023/10/10/world/middleeast/israel-gaza-security-failure.html

Bhasin, M. L. (2016). Strengthening corporate governance through an audit committee: An empirical study. *Wulfenia Journal, 23*(2), 2–27. http://surl.li/vmbpaf

Braun, R. L., & Davis, H. E. (2003). Computer-assisted audit tools and techniques: Analysis and perspectives. *Managerial Auditing Journal, 18*(9), 725–731. https://doi.org/10.1108/02686900310500488

Brown, G., & Peterson, R. S. (2022). Causes of dysfunctional culture. In *Disaster in the boardroom: Six dysfunctions everyone should understand* (pp. 61–85). Springer. https://doi.org/10.1007/978-3-030-91658-9

Bunget, O.-C. (2009). *The role of financial auditor in detecting and reporting fraud and error.* Munich Personal RePEc Archive. https://mpra.ub.uni-muenchen.de/12888/

Cohen, J., Krishnamoorthy, G., & Wright, A. M. (2002). Corporate governance and the audit process. *Contemporary Accounting Research, 19*(4), 573–594. https://doi.org/10.1506/983M-EPXG-4Y0R-J9YK

Cullinan, C. (2004). Enron as a symptom of audit process breakdown: Can the Sarbanes-Oxley Act cure the disease? *Critical Perspectives on Accounting, 15*(6–7), 853–864. https://doi.org/10.1016/j.cpa.2003.06.007

DeAngelo, L. E. (1981). Auditor size and audit quality. *Journal of Accounting and Economics, 3*(3), 183–199. https://doi.org/10.1016/0165-4101(81)90002-1

Dechow, P. M., Sloan, R. G., & Sweeney, A. P. (1995). Detecting earnings management. *The Accounting Review, 70*(2), 193–225. https://www.jstor.org/stable/248303

DeZoort, F. T., Hermanson, D. R., Archambeault, D. S., & Reed, S. A. (2002). Audit committee effectiveness: A synthesis of the empirical audit committee literature. *Journal of Accounting Literature, 21*, 38–75. https://core.ac.uk/download/pdf/232842894.pdf

Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies, 27*(3), 938–985. https://doi.org/10.1007/s11142-022-09697-x

Financial Reporting Council (FRC). (2012). *Guidance on audit committees.* https://www.accaglobal.com/content/dam/acca/global/PFD-memberscpd/InternalAudit/Guidance-on-Audit-Committees-September-2012.pdf

Frantzman, S. (2023, October 13). How did Israel fail to stop Hamas' October 7 attack? — Comment. *The Jerusalem Post.* https://www.jpost.com/opinion/article-768059

Gaumnitz, B. R., Nunamaker, T. R., Surdick, J. J., & Thomas, M. F. (1982). Auditor consensus in internal control evaluation and audit program planning. *Journal of Accounting Research, 20*(2), 745–755. https://doi.org/10.2307/2490898

Ge, W., & McVay, S. (2005). The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizons, 19*(3), 137–158. https://doi.org/10.2308/acch.2005.19.3.137

Hannan, M. T., & Freeman, J. (1984). Structural inertia and organizational change. *American Sociological Review, 49*(2), 149–164. https://doi.org/10.2307/2095567

Hirst, D. E. (1994). Auditors' sensitivity to source reliability. *Journal of Accounting Research, 32*(1), 113–126. https://doi.org/10.2307/2491390

Kinney, W. R., Jr. (2000). Research opportunities in internal control quality and quality assurance. *Auditing: A Journal of Practice & Theory, 19*(s-1), 83–90. https://doi.org/10.2308/aud.2000.19.s-1.83

Knechel, W. R., & Salterio, S. E. (2016). *Auditing: Assurance and risk.* Routledge. https://doi.org/10.4324/9781315531731

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting, 14*, 115–122. https://doi.org/10.2308/jeta-51730

Lin, Z. J, & Chen, F. (2004). An empirical study of audit 'expectation gap' in The People's Republic of China. *International Journal of Auditing, 8*(2), 93–115. https://doi.org/10.1111/j.1099-1123.2004.00084.x

Perlow, L., & Williams, S. (2003). Is silence killing your company? *IEEE Engineering Management Review, 31*(4), 18–23. https://doi.org/10.1109/EMR.2003.24935

Ramos, M. (2003). Auditors' responsibility for fraud detection. *Journal of Accountancy, 195*(1), 28–36. https://www.journalofaccountancy.com/issues/2003/jan/auditorsresponsibilityforfrauddetection.html

Rasmussen, J., & Svedung, I. (2000). *Proactive risk management in a dynamic society.* Swedish Rescue Services Agency. https://rib.msb.se/Filer/pdf%5C16252.pdf

Salhani, J. (2023, December 9). Did Israel's overreliance on tech cause October 7 intelligence failure? *Al Jazeera.* https://www.aljazeera.com/features/2023/12/9/did-israels-overreliance-on-tech-cause-october-7-intelligence-failure

Sapiri, M. (2024). A qualitative analysis on the role of auditors in preventing financial crises. *Golden Ratio of Auditing Research, 4*(2), 89–106. https://doi.org/10.52970/grar.v4i2.393

Sayana, S. A., & Cisa, C. (2003). Using CAATs to support IS audit. *Information Systems Control Journal, 1*, 21–23. https://csbweb01.uncw.edu/people/ivancevichd/classes/msa%20516/extra%20readings%20on%20topics/caats/using%20caatts%20to%20support%20it%20audit.pdf

Sikka, P. (2009). Financial crisis and the silence of the auditors. *Accounting, Organizations and Society, 34*(6–7), 868–873. https://doi.org/10.1016/j.aos.2009.01.004

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

U.S. Securities and Exchange Commission. (1934). *Securities Exchange Act of 1934.* https://www.sec.gov/file/securities-exchange-act-1934-0

U.S. Securities and Exchange Commission. (2002). *Sarbanes-Oxley Act of 2002.* https://www.govinfo.gov/content/pkg/COMPS-1883/pdf/COMPS-1883.pdf

APPENDIX

Table A.1. Parallels between the October 7, 2023, case study and audit failures in corporate governance

Aspect of October 7, 2023, case study	*Audit failures*	*Comparative analysis*
Over-reliance on technology	Over-reliance on automated audit tools	Both cases show that excessive trust in technology, without human oversight, can lead to critical blind spots. Auditors, like intelligence agencies, must blend technological tools with professional scepticism to catch risks that automated systems may miss.
Failure to respond to early warning signals	Ignoring red flags in audits	In both intelligence and auditing, early signs of risk were present but ignored. In auditing, red flags may come from internal audits or minor discrepancies and ignoring them can lead to larger failures.
Breaking communication between agencies	Disconnect between auditors, management and the board	Just as intelligence agencies failed to communicate, auditors and boards often operate in silos, preventing critical information from being shared. Open communication is vital to catching and addressing risks early.
Systemic failures in assessing threat levels	Misjudgments in risk assessment	The intelligence community's misassessment of the threat posed by Hamas is similar to auditors underestimating the risk of financial misstatements. Both highlight the need for better risk evaluation processes.
Organizational inertia	Resistance to addressing governance issues	In both cases, organizational inertia delayed necessary responses. Boards and auditors must be vigilant and flexible enough to adapt quickly to emerging risks and governance challenges.

Table A.2. Key recommendations for board oversight

Recommendation	*Description*	*Expected outcome*
Strengthen auditor independence	Review and approve audit resource and plan with genuine diligence	Enhanced audit quality and objectivity
Foster open communication	Create an environment where auditors can speak freely	Early identification of potential risks
Dynamic audit planning	Regularly reassess and adjust audit plans	Audits remain relevant to evolving risks
Integrate safeguards in strategy	Involve auditors in strategic discussions	More informed, risk-aware decision making