

Lessons from the Warning Signs Before October 7th, 2023 Failure, Strengthening Board and Auditor Oversight

Keren Bar-Hava

Business Administration School

Hebrew University

Working Paper March, 2024

Abstract

Incomplete information analysis and overreliance on technology can create a "fog" obscuring financial risks. This paper argues that professional auditors, like informed and accurate intelligence forces, are essential for companies' survival. We draw an analogy between intelligence failures, where warnings are missed, and auditors who overlook red flags. The paper examines potential pitfalls in auditing work that mirror the failures evident in the October 7th attack, emphasizing the need for a risk-based approach and clear communication. The importance of the audit procedures is heightened in light of catastrophic events. Our goal is to emphasize the importance of audit procedures, taking a holistic view, and balancing critical thinking with technology to ensure that auditors, in conjunction with the board of directors, prevent financial disasters.

Keywords: Internal Control, Audit Failures, CAAT, Intelligence Failures, Financial Risk, Risk-Based Auditing, Corporate Governance Quality

Introduction

Auditors play a critical role as safeguards of companies, serving as a cornerstone of effective corporate governance. They act as a vital line of defense against errors, fraud, and other financial risks. Breakdowns in the auditing process, however, can also lead to significant financial disasters (Cullinan, 2004). However, the public perception of an audit's role often differs from the auditor's actual responsibilities, this gap, known as the audit expectation gap (Koh, and Woo ,1998). Accounting scandals and corporate failures have highlighted the widening expectation gap (Dennis, 2010; Gold et al., 2012; Hassink et al., 2009; Pourheydari and Abousaiedi,2011). This emphasizes the need for transparency throughout the audit process, including clear communication with the Board of directors.

The paper explores the critical role of expert auditors in an environment characterized by rising information asymmetry and a growing dependence on sophisticated technological tools. By drawing parallels between the intelligence force failures and potential undetected financial risks, we argue for the continued necessity of human expertise alongside technological advancements in the auditing process.

A recent Israeli intelligence failure where a surprise attack was missed, serves as a stark reminder of the dangers of incomplete information. The “October 7, 2023 Attack”, began on that day, early in the morning, when Hamas-led Palestinian militant groups launched a surprise offensive against Israel named "Operation Al-Aqsa Flood". The attack began with a barrage of rockets targeting Israel, while around 3,000 militants penetrated the Gaza–Israel barrier and attacked nearby Israeli communities and military bases. During this violent attack, 1,139 people were killed, of whom 766 were civilians. The violent attack included cases of rape, brutal abuse and Abduction of civilians, including babies and elders.

The analogy between intelligence failures, to notice Hamas's preparations or adequately prepare for the terror group's October 7, 2023 and auditing process catastrophes is particularly relevant in today's complex financial landscape. Companies operate in a dynamic environment with ever-evolving risks. Incomplete or inaccurate information can create a "fog" that obscures potential financial vulnerabilities. Expert auditors, similar to effective intelligence force, are essential to "see through the smog" and ensure the accuracy of the financial data.

This paper argues that an effective and complete audit process, incorporating a risk-based approach and clear communication channels, is crucial for mitigating financial risks and preventing costly mistakes. By drawing parallels with the intelligence force failures of October 7, 2023, we can identify potential weaknesses in auditing practices and advocate for a more proactive and vigilant approach. The paper explores these themes and emphasize the crucial role of auditors and boards as gatekeepers and fostering trust in the economy. We also discuss the risk of overreliance on artificial intelligence (AI) and other advanced technologies, in the auditing process, as a new threat that auditing needs to address in light of the October 7th event.

The remainder of this paper structured as follows. In section II, we briefly provide review of the role of the auditor and effective corporate governance. Section III describes audit failure and internal Control Weaknesses. In section IV. We document the intelligence force failure of October 7, 2023. Section V leverages the above-mentioned intelligence force failure as a case study with potential auditor failures. Section VI provide analysis and recommendations. Finally, Section VII concludes the study with key takeaways and potential implications.

II. Literature Review - Auditor and Effective Corporate Governance

Auditors play a critical role in safeguarding the financial stability and transparency of companies. Their core functions act as a vital line of defense against financial risks, including fraud (Sapiri, 2024). Through risk assessment, internal control evaluation and understanding complex financial instruments, auditors identify errors, deter fraud, and enhance transparency. However, research by Dechow et al. (1996) highlights the challenges of detecting earnings management, a form of financial misstatement. This underscores the importance of robust auditing procedures to mitigate audit failures. Additionally, Becker et al. (1998) find that larger audit firms (Big 6) tend to provide higher quality audits.

Auditors Responsibilities:

Verifying the Accuracy of Financial Statements: Auditors meticulously examine a company's financial records, supporting documentation, and underlying transactions to ensure they accurately reflect the company's financial position and performance (Hirst, 1994). This verification process helps identify discrepancies that might indicate intentional misstatements or errors. To ensure the reliability of financial information and the effectiveness of the audit process, auditors must maintain independence and objectivity in their assessment. This means that auditors should be free from any conflicts of interest that could compromise their judgment. They should not be influenced by the company's management or have any financial ties to the company they are auditing. Furthermore, auditors should approach their work with a neutral and unbiased perspective. They should base their conclusions solely on the evidence gathered during the audit process and not be swayed by external pressures or personal opinions.

Assessing the Effectiveness of Internal Controls: A robust internal control framework, evaluated by the auditors, helps prevent fraud by establishing clear procedures and segregation of duties. Auditors assess these controls to ensure they are designed and implemented effectively to safeguard assets, prevent errors, and promote adherence to regulations.

Identifying Potential Risks of Fraud or Errors: Auditors generally assess and evaluate the quality of internal control system of intended company to determine and plan the extent and process of audit work (Gaumnitz, Nunamaker, Surdick and Thomas, 1982). While the primary responsibility for preventing and detecting fraud falls on management, auditors can play a positive role in deterring such misconduct through their work (Bunget, (2009)). Through risk assessment procedures, auditors pinpoint areas susceptible to financial misstatements due to fraud or unintentional mistakes. This proactive approach allows them to focus their efforts on areas with the highest potential for problems (Ramos (2003)).

The Rise of Artificial Intelligence (AI) in Auditing:

The auditing profession is at a crossroads. Technological advancements, particularly in AI, are transforming the way businesses operate and generate financial data. This evolving landscape presents both challenges and opportunities for auditors, who face increasing pressure to improve efficiency and effectiveness while maintaining the integrity of financial reporting.

CAAT refers to Computer-Assisted Audit Technique. earlier studies explain the meaning of the term for the auditing profession: Braun and Davis (2003) defined CAATS as any use of technology to support the speed and efficiency of the

audit process. Similarly, Sayana (2003) described it as using certain software by the auditor to perform audits and to achieve the goals of auditing.

As technology continues to evolve, Aksoy and Gurol (2021) state that Digital transformation is the modification that bring forth new opportunities technological advancements used in audit activities. These new technologies used in audit activities are called Computer Assisted Audit Tools and Techniques (CAATTs). Those have emerged to help auditors look for anomalies in data files and to enable additional analyses to be done in less time with more evidence at a lower risk level. CAATTs can assist auditor with tasks like data analysis and identifying patterns, potentially improving the efficiency and effectiveness of the audit process. This can lead to improved audit quality, allowing auditors to dedicate more time to complex areas requiring human expertise. They also document that some researchers are skeptical since professional judgment of the auditor can be ignored with the utilization of AI.

According to Kokina and Davenport (2017), the Big Four accounting firms have made significant investments in artificial intelligence (AI) and data analytics for auditing purposes. This includes automating tasks like physical inventory counting through robotics, and using analytics to identify potential risks and trends.

Recent research by Fedyk et. al (2022) show that invest in AI helps improve audit quality, decreases fees, and eventually relocates human auditors, although the effect on labor takes several years to materialize. their empirical analyses are supported by in-depth interviews with 17 audit partners representing the BIG 8 U.S. public accounting firms, which show that AI is developed centrally, widely used in audit and that the primary goal for using AI in audit is improved quality, followed by efficiency.

The Importance of Board Oversight and the Audit Committee

The board of directors have the primary responsibility for the provision of useful and meaningful information for investors and other users of the financial statements, and a strong audit process is essential for achieving this objective. Thus, the board plays a vital role in managing expectations by fostering transparency about the nature and limitations of the auditor role. The effectiveness of the audit process hinges not only on the auditors themselves, but also on the quality of the board of directors. Research by Beasley (1996) provides empirical evidence that boards with a higher proportion of outside directors are less likely to see financial statement fraud. These outside directors bring objectivity and independence to the board's oversight role.

Beyond board composition, the audit committee plays a critical role in ensuring a strong audit process. Appointed by the board, this committee directly supervises the auditors and safeguards their independence (Dyer & Dalton, 1988). Al-Shaer and Zaman (2021) further highlight the importance of the audit committee's communication function. Their research suggests that the tone and content of these reports can influence the overall quality of financial reporting.

The audit committee can also oversee the risk assessment process and ensures clear communication channels between management, internal audit, and external auditors.

Directors and, specifically, the audit committee, play a critical role in fostering a robust and effective audit process. This extends beyond simply appointing the independent auditor. By establishing a culture of transparency and accountability, the

board can actively encourage a thorough and constructive audit. Key strategies include maintaining open communication with the auditors, ensuring adequate resources are allocated, and critically reviewing the audit report and findings. Through this active engagement, the board empowers the auditors to perform their duties diligently, ultimately strengthening the company's financial reporting and risk management practices.

As Council (2008) highlights, the audit committee serves as a crucial governance body overseeing the integrity of a company's financial reporting. Its multifaceted responsibilities include monitoring financial statements and announcements, scrutinizing significant judgments within them. Furthermore, the committee reviews the company's internal financial controls and, in the absence of a dedicated risk committee, the broader internal control and risk management systems. Additionally, it oversees the internal audit function. A crucial aspect of the committee's role involves recommending the appointment of the external auditor to the board for shareholder approval, as well as approving the auditor's remuneration and engagement terms. Maintaining auditor independence and objectivity, alongside the effectiveness of the audit process, also falls within the committee's purview. They are responsible for crafting policies regarding the external auditor's provision of non-audit services, adhering to ethical guidelines. Finally, the committee reports to the board, highlighting areas requiring action or improvement, and suggesting necessary steps. They also report on their own fulfillment of these responsibilities.

Bhasin (2016) state that an effective auditing committee can be a key feature of a strong corporate governance culture, bringing significant benefits to an organization. The effectiveness of the auditing committee is based on the

characteristics of independence, financial expertise and diligence. The audit committee complements the work of auditors and strengthens the overall corporate governance framework.

III. Audit Failure and Internal Control Weaknesses

This paper examines the multifaceted nature of audit failure, focusing on the various internal control deficiencies that can contribute to such breakdowns. We posit that audit failures often stem from a combination of factors, including:

Risk Misassessment: Auditors may fail to adequately identify and assess inherent and control risks within an organization. This can lead to a misallocation of audit resources and an inability to detect significant control weaknesses.

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.

Communication Silos: Ineffective communication between management, internal audit functions, and external auditors can hinder the timely identification and escalation of control weaknesses.

Systemic Design Flaws: Internal control systems themselves may be inherently flawed, lacking the necessary robustness to detect and prevent fraud or errors.

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.

By acknowledging 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 to mitigate the risk of audit failure and promote the effectiveness of the internal control environment.

III. The Case Study of October 7, 2023 Failure

Terrible massacre carried out by Hamas on the seventh of October, 2023. On the border on October 6, there was all the best technology. Hamas's infiltration into Israel was made possible by a series of security failures.

Frantzman (2023), state that there were observation towers and soldiers observing Gaza. Israel also has drones and observation balloons. However, what no one knew was that Hamas had thousands of terrorists ready to step off the line at around six in the morning and attack more than 29 locations 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.

Bergman and Kingsley (2023), document in their research the security failures of that day, the dreadful day in the history of the State of Israel. Here are the details:

- The 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;

- Clustering of commanders in a single border base that was overrun in the opening phase of the incursion, preventing communication with the rest of the armed forces;
- a willingness to accept at face value assertions by Gazan military leaders, made on private channels that the Palestinians knew were being monitored by Israel, that they were not preparing for battle.

Salhani (2023), document that an overreliance on technology by Israel's intelligence agencies and military has continued to shape the current conflict in Gaza, analysts say, while also being partially responsible for the failure to detect the Hamas attack on October 7. Israeli security services are understood to have collected more than enough data to anticipate an imminent Hamas attack. Indeed, Israeli intelligence was aware of plans for an impending Hamas attack up to one year beforehand, according to a report in the New York Times. Billions of dollars invested in high-tech defenses like border walls and security cameras around Gaza were believed to be enough to stop any attack. But the technological reliance led to a false sense of security. Comprehensive intelligence gathering requires a number of sources: open source, intercepted communications, satellite imagery and tracking are all crucial factors in intelligence gathering before putting together an analysis,. But the human intelligence aspect is also crucial.

IV. Analysis and Recommendations

The goal of the paper is to compare between the October 7th failure and audit process weakness. We use the October 7th security failure to offer a stark case study in how a confluence of internal control Deficiencies can lead to disastrous consequences. Similarities can be drawn between the intelligence failures that unfolded on that day and the factors contributing to audit breakdowns explored in this paper. Here are the failures of October 7th in terms of auditing controls:

Risk Misassessment: Just as Israeli intelligence over-relied on monitored communications and underestimated Gazan intentions, auditors can also fall victim to confirmation bias, neglecting to adequately assess all potential risks. Similar to the intelligence force failures on October 7th, auditors can be susceptible to risk misassessment, particularly when they over-depend on automated tools and neglect other sources of information

Communication Silos: The October 7th attack highlighted the importance of information sharing between different military branches. Similarly, effective communication between the board members, audit committee, internal audit, and external auditors is crucial to identify and address control weaknesses.

Systemic Design Flaws: The reliance on easily disabled surveillance equipment by Israeli forces (Frantzman, 2023) mirrors the potential flaws inherent in poorly designed internal control systems. Both require continuous evaluation and improvement. For instance, overreliance on manual controls without proper automation or vice versa can create vulnerabilities.

Organizational Inertia: The reluctance of Israeli commanders to adapt their strategies reflects the challenge of overcoming organizational inertia in implementing robust internal controls. Both situations require a proactive approach to change. Companies must be agile and willing to challenge the status quo and embrace ongoing improvements to their internal control frameworks.

These parallels underscore the importance of proactive risk management and strong internal controls in preventing disastrous outcomes. By drawing lessons from the October 7th failure, auditors can enhance their procedures, foster open communication, and advocate for well-designed and adaptable internal controls. Only through a multi-faceted approach can we mitigate the risk of failures, be they in national security or financial oversight. The overdependence on monitored communications and technological surveillance by Israeli intelligence parallels the potential dangers of auditors placing excessive trust in automated audit tools.

These parallels underscore the importance of proactive risk management and strong internal controls in preventing disastrous financial outcomes. By learning from the October 7th failure, auditors can enhance their procedures in several ways:

Critical Thinking and Professional Skepticism:

Auditors must go beyond simply analyzing the data presented and employ strong critical thinking skills to assess the broader context and identify potential risks that may not be readily apparent.

Utilize a Multi-Source Approach:

Overdependence on technology can create blind spots. Auditors should leverage a variety of information sources, including internal audit reports, industry publications,

and discussions with management, to gain a holistic understanding of the company's risk profile.

Maintain Open Communication:

Effective communication is vital. Auditors must foster open communication channels with management and the audit committee to ensure all concerns and red flags are addressed promptly.

The Role of Collaboration in Strengthening Auditing Practices

The parallels between the October 7th attack and audit failures highlight the critical role of collaboration between the audit committee and external auditors in preventing financial disasters like insolvency.

An effective audit committee actively fosters a culture of open communication and transparency within the organization. This allows them to engage constructively with the external auditor, providing them with clear expectations and unfettered access to necessary information. By critically reviewing the audit report and maintaining a healthy skepticism, the audit committee empowers the external auditor to identify red flags and potential risks that could lead to insolvency.

AI in the Auditing Process

we argue that it's important to remember that AI is a tool, not a replacement. Human judgment and critical thinking skills remain essential for interpreting data, identifying potential risks that AI might miss, and maintaining professional skepticism throughout the audit process. Improvements in the auditing process should focus on leveraging a combination of human expertise and technological advancements. By embracing AI as a powerful tool, auditors can enhance their ability

to detect and deter fraud while maintaining the essential role of independent oversight.

V. Conclusion

The October 7th 2023 “controls failures” serve as 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, although audit firms are investing billions of dollars to develop artificial intelligence systems that will help auditors execute challenging tasks, the event of October 7, underscores the dangers of overdependence on technology. This emphasizes the need for a balance between human expertise and technology. It suggests that both aspects are crucial for effective auditing. Human expertise are crucial for interpreting data and identifying potential risks that might be missed by technology alone.

While this paper emphasizes the irreplaceable role of human auditors, it's important to acknowledge research by Fedyk et al. (2022) suggesting that advancements in AI may transform the auditing 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 must be proactive in fostering a culture of strong internal controls. By prioritizing preventative measures and understanding the immense value

of disaster prevention, companies can significantly improve their overall risk management and financial stability.

References

- Aksoy, T., & Gurol, B. (2021). Artificial intelligence in computer-aided auditing techniques and technologies (CAATTs) and an application proposal for auditors. In Auditing Ecosystem and Strategic Accounting in the Digital Era: Global Approaches and New Opportunities (pp. 361-384). Cham: Springer International Publishing.
- Al-Shaer, H. and Zaman, M. (2021), "Audit committee disclosure tone and earnings management", *Journal of Applied Accounting Research*, Vol. 22 No. 5, pp. 780-799.
- 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.
- 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.
- Bergman R. and Kingsley P.(2023);How Israel's Feared Security Services Failed to Stop Hamas's Attack, *New York Times*.
- Bhasin, M. L. (2016). Strengthening corporate governance through an audit committee: An empirical study. *Wulfenia Journal*, 23(2), 2-27.
- Braun, R. L., & Davis, H. E. (2003). Computer-assisted audit tools and techniques: analysis and perspectives. *Managerial Auditing Journal*, 18(9), 725-731.
- Bunget, O. C. (2009). The role of financial auditor in detecting and reporting fraud and error.
- Council, F. R. (2008). Guidance on audit committees. Hirst, D. E. (1994). The importance of financial statement audits. *Auditing: A Journal of Practice & Theory*, 13(2), 167-182.
- 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–
- Dechow, P. M., Sloan, R. G., & Sweeney, A. P. (1996). Detecting earnings management. *The Accounting Review*, 71(3), 349-376.
- Dennis I (2010). What do you expect? A reconfiguration of the audit expectations gap. *International Journal of Auditing* 14(2):130-146.
- Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process?. *Review of Accounting Studies*, 27(3), 938-985.

Frantzman, S., (2023). How did Israel fail to stop Hamas' October 7 attack? – comment. The Jerusalem Post.

Gaumnitz, B. R., T. R. Nunamaker, J. J. Surdick and M.F. Thomas. 1982. "Auditor Consensus in Internal Control Evaluation and Audit Program Planning." *Journal of Accounting Research*. Vol. Autumn : 745-755

Gold A, Gronewold U, Pott C (2012). The ISA 700 auditor's report and the audit expectation gap – do explanations matter? *International Journal of Auditing* 16(3):286-307.

Hassink HFD, Bollen LH, Meuwissen RHG, de Vries MJ (2009). Corporate fraud and the audit expectations gap: A study among business managers. *Journal of International Accounting, Auditing and Taxation* 18(2):85-100.

Koh, H. C., & Woo, E. S. (1998). The expectation gap in auditing. *Managerial auditing journal*, 13(3), 147-154.

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.

Lin ZJ, 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.

Nicolescu, O. (2007). The Economic Impact of Fraud. *Annals of the University of Craiova - Economics Series*, 35(1), 339-348.

Pourheydari O, Abousaiedi M (2011). An empirical investigation of the audit expectations gap in Iran. *Journal of Islamic Accounting and Business Research* 2(1):63-76.

Ramos, M. (2003). Auditors' responsibility for fraud detection. *Journal of Accountancy*, 195(1), 28-36.

Sapiri, M. (2024). A Qualitative Analysis on the Role of Auditors in Preventing Financial Crises. *Golden Ratio of Auditing Research*, 4(2), 89-106.

Sayana, S. A., & Cisa, C. (2003). Using CAATs to support IS audit. *Information systems control journal*, 1, 21-23.