



Report of the State Comptroller of Israel | May 2024

The Defense System

---

# **Prevention of Fraud and Embezzlement at Israel Aerospace Industries Ltd.**





# Prevention of Fraud and Embezzlement at Israel Aerospace Industries Ltd.

## Background

Israel Aerospace Industries Ltd. (IAI or “the Company”) is a government-owned corporation as defined in the Government Companies Law, 1975. IAI, one of Israel's largest defense industries, operates through four business divisions: Missile and Space Systems Division, Military Aircraft Division, Aviation Division, and Military Electronics Division, whose activity is carried out through Elta Systems Ltd., a government subsidiary under full IAI ownership. As of the end of 2022, IAI had about 13,800 employees, 5,100 suppliers, and 46 held corporations, 26 of which were overseas, and its annual revenue was about USD 4.97 billion.

Embezzlement and fraud can cause severe organizational damage, such as financial losses, damage to reputation, regulatory sanctions, and loss of customers. According to an ACFE study<sup>1</sup>, organizations lose about 5% of their annual revenue due to embezzlement and irregularities. Every organization is vulnerable to embezzlements and fraud, and it is impossible to eliminate the risk of their occurrence. However, organizations can mitigate this risk through various measures, including fostering a proper organizational culture and raising awareness among employees and managers at all levels; developing a structured plan for detecting and addressing embezzlement and fraud, as well as preventing them; and implementing dedicated controls and specialized systems within the organization designed to manage these risks.

In January 2020, the Government Companies Authority issued a circular regarding corporate risk management in government-owned companies and subsidiaries (Circular on Risk Management 2020), which stipulates that the risk management of each company should address at least several types of risks noted in the circular, including risks of embezzlement and fraud.

<sup>1</sup> The Association of Certified Fraud Examiners (ACFE) is an international organization.



Key Figures

**USD 4.97 billion**

annual revenue turnover of IAI in 2022

**83**

where fraud and embezzlement were rated in the latest corporate IAI risk survey in 2020 out of 85 risks\*

**26%**

of employees in the procurement field do not comply with company guidelines to rotate between roles every five years

**130**

the internal audit recommendations received by the company's management were implemented a year behind the time set. Among these, 81 were implemented with a delay of over two years (as of December 2022), including fraud and embezzlement recommendations

**about 34% (814)**

respondents (IAI employees) to the State Comptroller's Office questionnaire\*\* did not know whom to approach if they wanted to report integrity breaches

**about 23%—33% (557–787)**

respondents (IAI employees) to the State Comptroller's Office questionnaire believed that various types of fraud and embezzlement can be perpetrated in the company, including misappropriation of equipment, supplier fraud, and falsified attendance reports

**about 55% (1,305)**

respondents (IAI employees) to the State Comptroller's Office questionnaire were unaware of the existence of a "hotline" for reporting complaints openly or anonymously

**about 11% (264)**


10% of respondents (IAI employees) to the State Comptroller's Office questionnaire did not know if they would report fraud or embezzlement occurring in the company if they had information about it, and about 1% of respondents said they would not report the issue

\* On a scale where "1" reflects the highest risk and "85" the lowest. According to IAI, the corporate risk survey determines risks whose realization could endanger the corporation, and based on the company's experience, instances of fraud do not usually reach significant financial amounts and do not fall into the category of key corporate risks.

\*\* During the audit (in May 2023), the State Comptroller's Office distributed a questionnaire regarding fraud and embezzlement risks among the company's employees.




## Audit Actions

 From January to July 2023, the State Comptroller's Office examined the IAI, the Government Companies Authority, and the Director of Security of the Defense System (MALMAB) regarding fraud and embezzlement at IAI in 2019–2022 (on specific issues, the audit applied to the period ending on June 30, 2023). The audit examined the company's risk management system, focusing on the management of fraud and embezzlement risks: evaluating the control environment for risk management, assessing monitoring and handling the risks, handling cases of fraud and embezzlement by MALMAB, and supervision by the Government Companies Authority on this matter. The audit was conducted at IAI, ELTA, the Government Companies Authority, and MALMAB.

Moreover, (conducted in May 2023), the State Comptroller's Office distributed a questionnaire among 14,126 IAI employees on fraud and embezzlement risks within the company. 2,411 employees (about 17%) fully answered the questionnaire.

The subcommittee of the Knesset State Audit Committee decided not to submit to the Knesset and not publish some data from this audit report to safeguard the security of the state under section 17 of the State Comptroller Law, 1958, [consolidated version].

## Key Findings

 **Management of Fraud and Embezzlement Risks at IAI** – although IAI has formulated a document titled "Fraud and Embezzlement Risk Prevention Policy," the topic is not anchored in a separate procedure. Handling these risks is divided among various factors within the company and defined in numerous regulations. It was found that the division of authority and responsibility defined in IAI's regulations for dealing with fraud and embezzlement risks and incidents is unclear, with overlaps between different factors. Moreover, the required internal reporting mechanisms when such incidents occur, including reporting to the chief risk officer, are ambiguous.

No factor in IAI, including the chief risk officer, has a central comprehensive database of fraud and embezzlement incidents detected within the company in 2019–2022, which can undermine the management and handling of embezzlement and fraud risks.

From January 2019 to June 2023, incidents of fraud and embezzlement occurred at IAI, including cases of false reporting, abuse of authorization for changes in information systems, theft or personal use of company property, and falsification of expense



reimbursements. However, the risks associated with these incidents were not ranked among the top twenty risks in the company's 2021 fraud and embezzlement risk survey, which could cast doubt on the quality of the risk likelihood assessment.

- 📌 Appointment of a Chief Risk Officer and his Responsibility for Managing Fraud and Embezzlement Risks** – according to the Government Companies Authority's 2020 Risk Management Circular, in a government company classified as 9 and above (IAI's classification), the Chief Risk Officer should not hold other positions. Contrary to this circular, and despite the numerous tasks of the Chief Risk Officer as defined in the Risk Management Circular, which require significant attention and resources, the company's board of directors appointed the company's Chief Financial Officer (CFO) as Chief Risk Officer in July 2021. The CFO position is complex by itself and entails responsibility for all financial aspects of the company. This appointment could compromise the independence of the Chief Risk Officer and create a conflict of interest between his different roles.


From 2010 until the end of the audit (July 2023), responsibility for managing fraud and embezzlement risks at IAI was transferred between various factors. Since 2021, this responsibility has been held by the CFO, who also serves as Chief Risk Officer.


- 📌 Meeting of the Board's Risk Management Committee** – in 2018–2022 (except for 2020), the Board's Risk Management Committee failed to meet every quarter as stipulated in IAI's corporate risk management policy document and corporate risk management procedure. In addition, there were periods of time during these years, from six months to a year, at which the committee did not convene, such as from July 2018 to July 2019.


- 📌 Rotation in Sensitive Positions** – one of the main controls that can reduce embezzlement is the rotation of employees in key positions with access to company funds and assets, such as buyers, accounting and finance personnel. Rotating employees in these positions can hinder employees wishing to embezzle company assets. However, IAI has not mapped out sensitive positions for rotation. The procurement area lacks a structured and managed rotation process, and about 26% of procurement employees do not adhere to the rotation logic established by company management guidelines from 2011 and updated in 2017. In addition, no rotation is performed in the finance area, with some employees holding their positions for many years, including 45 employees (about 8% of all finance employees) who have been in their roles for over 15 years.

- 📌 "Hotline" for Submitting Anonymous Complaints and Employee Inquiries on Integrity Issues** – one of the most common methods for detecting irregularities and felonies within a company is through information from various sources such as employees, customers, and suppliers. One mechanism for receiving such information is a "hotline" reporting system, which allows for effortless transfer of information and complaints from within and outside the organization, even anonymously if desired.

However, the State Comptroller's Office survey raised that 55% of respondents were unaware of the existence of the "hotline." Employees in the ELTA and Missile and Space Systems divisions were less aware of the "hotline" than employees in other divisions (37% and 42% respectively, compared to 52%). The engineering sector was less aware of the "hotline" than other sectors (38% compared to an average of about 51%). Furthermore, employees who have been with the company for 6–20 years were less aware of the "hotline" (an average of 38.5% compared to 50%).

 **Preventing Conflict of Interest** – according to the company's Conflict of Interest Prevention Procedure, employees in certain positions must sign a conflict of interest declaration form every two years. The list of positions includes, among others, employees of a certain rank and above (department head level), accounting supervisors, members of procurement and tender committees, various employees who engage in business with building contractors, those who determined specifications for suppliers, or members of a negotiation team with suppliers. It was found that IAI is aware that its 2018 Conflict of Interest Procedure does not reflect the actual work process and that the company's process for preventing conflicts of interest among its employees, implemented through a dedicated system first introduced in August 2021, is neither efficient nor effective, hence requiring substantial changes. It should be noted that IAI is revising this procedure, still it was not completed as of July 2023.

 **Supervision and Control of Subsidiaries** – at the end of 2022, the Company had 46 subsidiaries, 26 of which are abroad. 17 of these subsidiaries (37%) are wholly owned by the Company, nineteen (41%) are not wholly owned but are consolidated in IAI's financial statements, and ten (22%) are less than 50% owned by IAI. According to IAI's December 31, 2022 financial statement, the Company's most significant subsidiary is ELTA. It was found that only in 2021 did the Company begin to define its control mechanisms for managing risks in its subsidiaries, and in 2022, it started to advance a risk management process in them, as well as a SOX process in four of them. Out of these, the documentation of processes and writing of controls have been completed in two subsidiaries. At the end of the audit (July 2023), gaps exist in IAI's control over some of its subsidiaries, including the failure to adopt a risk management mechanism and insufficient reporting. This is despite IAI identifying gaps in the oversight and control of its subsidiaries in the 2015 fraud and embezzlement risk survey, including those related to fraud and embezzlement risks. These gaps were also noted in risk surveys conducted in 2017 and 2021 and in the company's internal audit reports, which recommended to close these gaps, including the implementation of SOX in the subsidiaries.

 **Implementation of Internal Audit Recommendations** – at the end of 2022, 130 internal audit recommendations at IAI had been accepted by company management. However, their implementation was delayed by over a year, of which 81 recommendations were delayed by over two years. Among the recommendations postponed by over a year were those relevant to IAI's corporate risks, including regulatory compliance, business intelligence, intellectual property management, and



compliance program implementation. In addition, there were controls for preventing fraud and embezzlement recommendations, such as authorization and database management.

**👎 MALMAB's Procedure on Criminal Investigations** – IAI and ELTA are entities guided by MALMAB, in charge of matching the reliability of employees in the defense system and those employed by it, to their duties including in the guided entities, as well as conducting criminal investigations within the defense system entities. IAI must comply with MALMAB's instructions on various issues, including handling criminal incidents that occur within it. Since 2007, the MALMAB criminal investigations procedure in defense system bodies has not been updated, and the MALMAB operates differently from the established procedure. This is reflected in a draft procedure that has yet to be approved. As long as no updated procedure is approved, the decision-making process within MALMAB regarding whether or not to investigate a matter brought before it remains unformalized.

**👎 Supervision and Monitoring by the Government Companies Authority** – until the end of the audit (July 2023), the Government Companies Authority had partially automated the system it planned to establish in 2022 to support its work processes. Automation of the receipt and monitoring of reports from government companies, including risk management reports such as risk surveys and failure events, has not yet been completed. The Government Companies Authority has not reviewed the implementation of its guidelines in the 2020 risk management circular, following the recommendations of the State Comptroller's report on "Prevention of Embezzlement in Government Ministries and Government Companies" from 2022, nor have these guidelines been updated. In addition, the Authority has not follow-up the implementation of controls in this matter in government companies, nor does it send update notifications to the entities it oversees about discovered embezzlement cases or publish recommendations to reduce exposure to embezzlement risks.







**The Legal Advisor's Activity in Establishing a Forum for Information Sharing on Integrity Issues** – the legal advisor's establishment of a regulators' forum within the company is commended. In addition to the legal advisor herself, this forum includes the internal auditor, the chief risk officer, the VP of Human Resources, and the security officer whose role is to address integrity, improve the flow of information, and provide updates on the various relevant factors within the company.

**Internal Auditor's Enhancement of Risk Management Control in the Company** – the internal auditor's method of developing a risk-based work plan is commended.





## Key Recommendations

-  Given the central role of the company's chief risk officer, who guides and supervises various company risk holders, and the importance of its independence in the main processes conducted within the company, it is recommended that the company's board of directors appoint a chief risk officer who meets the requirements of the Government Companies Authority's circular.
-  It is recommended that IAI review its various procedures, including the Code of Ethics, handling complaints and public inquiries, human resources organization, and the risk management, and make the necessary adjustments. This includes defining the responsibilities and authority of each role in the company handling, reporting, and sharing information about fraud and embezzlement incidents, including of the chief risk officer. It is further recommended that the chief risk officer coordinate all fraud and embezzlement incidents within the company. In addition, given the ethical and organizational importance of integrity, it is recommended that the company management review the criteria defined for ranking the severity of fraud and embezzlement risks, including the handling of embezzlements involving amounts that are insubstantial to the organization, as well as the required controls in these processes.
-  It is recommended that IAI enhance measures to reduce fraud and embezzlement risks, including allowing company management to map sensitive positions for approval by the board. This mapping should encompass roles with access to the company's funds and assets, especially those in procurement and finance. Additionally, a policy regarding rotation within these positions should be developed and enforced. In addition, it is recommended that the company increase awareness among all its employees about reporting through the "hotline," especially in cases of integrity breaches. This is due to the importance that the company attaches to managing complaints and inquiries from employees and the public to improve business management, enhance the controls it implements, and foster its reputation and image. The "hotline" is crucial for detecting irregularities, increasing trust between employees and the company, and deterring employees from engaging in prohibited activities. Furthermore, IAI should continue addressing gaps to prevent conflicts of interest among all relevant employees and prioritize the resolution of these gaps among employees at management levels and unique groups such as procurement staff. It is also recommended that IAI complete the process changes to prevent conflicts of interest among its employees, update its relevant procedures, and assimilate these changes into its information systems.
-  It is recommended that IAI enhance supervision and control over the divisions and directors acting on behalf of the held companies; implement a risk management mechanism in them, as prescribed, including embezzlement and fraud risks; and expand the scope of SOX implementation in additional held companies. In addition, given the centrality of the role of directors in the held companies, including in risk management, it is recommended that



IAI ensure the training of directors appointed by it at a time close to their appointment and provide relevant and targeted training in the subject, including in the prevention of fraud and embezzlement. It is also recommended that IAI examine the directors' ability to perform this role properly in several held entities in addition to their role in the company, emphasizing subsidiary companies.

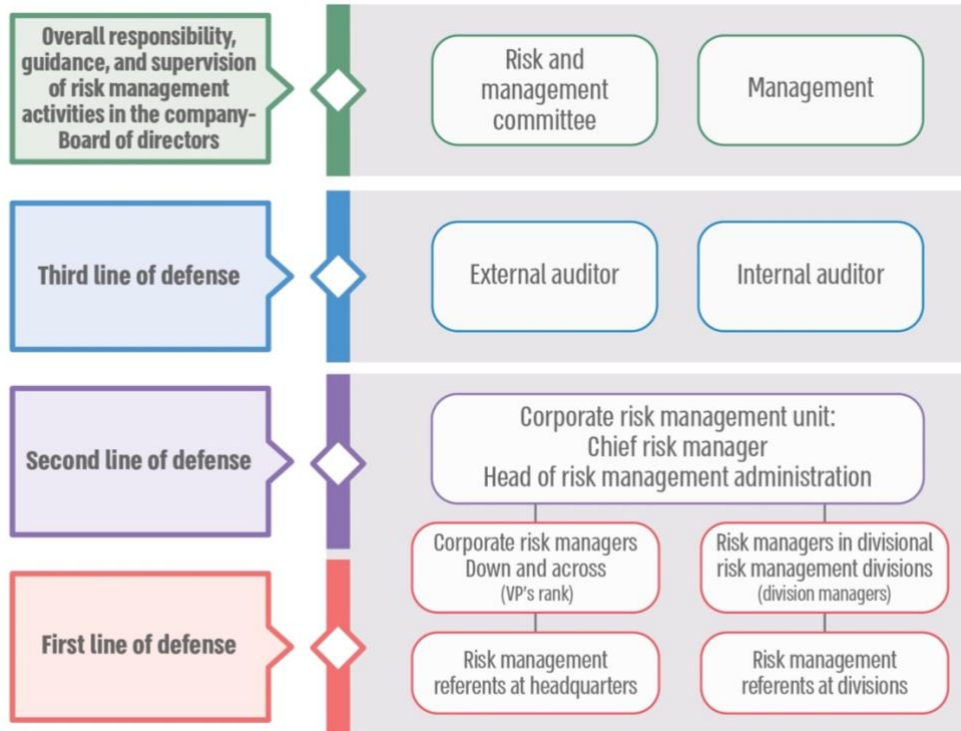


It is recommended that MALMAB promptly approve updated procedures regarding criminal investigations within defense system bodies and bring them to the guided bodies' attention, including IAI. Furthermore, given the urgency of taking steps by the guided body, including internal investigation of the incident and establishing controls to prevent recurrence, it is recommended that the evolving procedure also update the relevant factors in the guided body as early as possible.



It is recommended that the Government Companies Authority complete the automation of work processes and interfaces with government companies, including receiving company reports on risk surveys procedures, failure events, and significant failure events. In addition, it is recommended that the authority expand reporting obligations, including detailing incidents classified as medium or low severity. The Authority should require government companies to immediately report significant failure events, including incidents involving officeholders in the government company. It is also recommended that the Government Companies Authority receive detailed reports from IAI on such events, even if they are not significant in the Israel Securities Authority and do not require reporting to it.

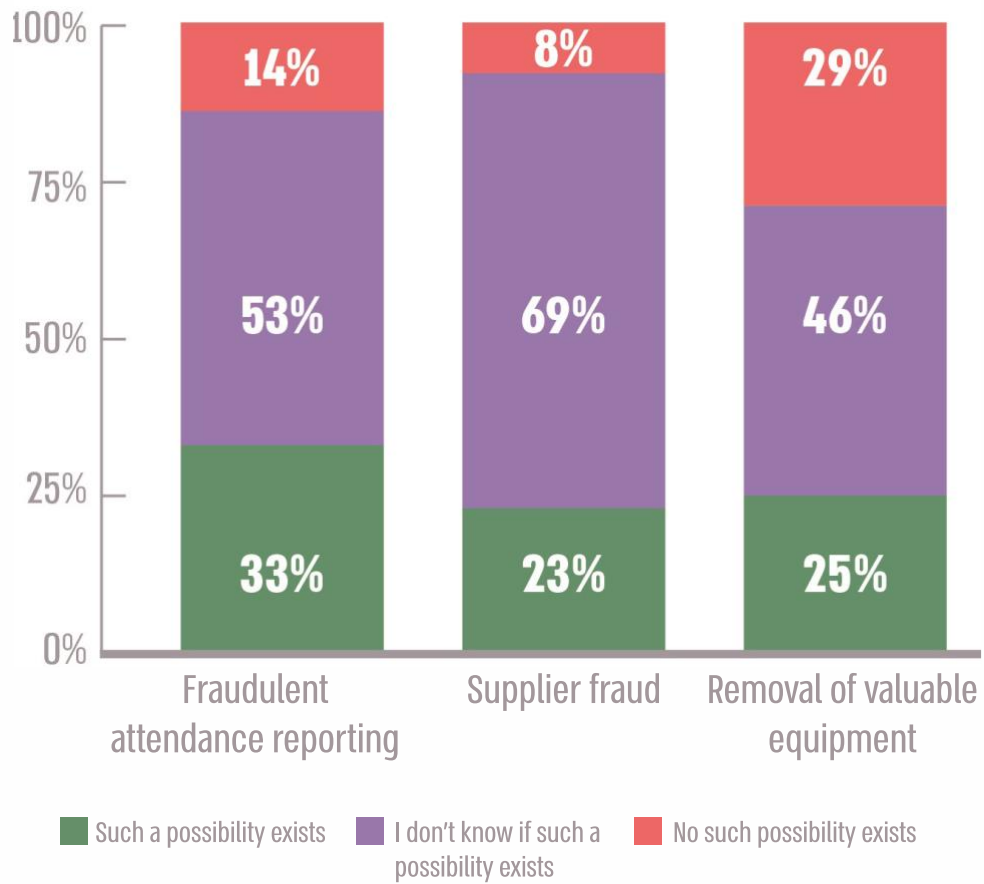
## Mechanism of Authority and Responsibility in Risk Management – Lines of Defense at IAI



According to IAI's 2023 policy document, processed by the State Comptroller's Office.



**Distribution of IAI Employees' Assessments Regarding the Likelihood of Embezzlement and Fraud Events Occurring, by Type**



Based on responses from IAI employees to a State Comptroller's Office questionnaire.



---

---

## Summary

Israel Aerospace Industries (IAI), one of the largest defense industries in Israel, is a wholly state-owned government company. Given the large scale of its financial activity (with revenues of about USD 4.97 billion in 2022), the complexity of its operations, and its large number of employees (around 13,800) and suppliers (around 5,100), it is exposed to embezzlement and fraud risks that need to be managed and mitigated. The audit found deficiencies, including in the appointment of the Chief Risk Officer and the exercise of his responsibilities. Gaps were found in the controls and measures to reduce embezzlement and fraud incidents within the company, including mapping sensitive positions and formulating a rotation policy, supervising conflicts of interest among employees, and supervising and controlling subsidiaries. In addition, an ambiguity was found in the division of authority and responsibility in handling embezzlement and fraud incidents and the prevention of their recurrence.

Embezzlement and fraud incidents can cause financial damage to any company and harm its image and organizational culture. IAI is a government-owned defense company engaged in the core of Israel's defense activity, where the reliability of its employees and suppliers is critical, including from a security perspective. This importance is further heightened given its large number (46) of subsidiaries, its widespread geographical distribution, and its limited control over some of them. To optimally prevent embezzlement and fraud incidents, IAI should improve the necessary controls, including those over the operations of its domestic and international subsidiaries, considering the report's findings and recommendations.

