

Evaluating the Governance Execution Gap in the Customer Onboarding Process at PT XYZ: An Integrated Coso and three Lines Model Approach

Hanifa Shabila Putri Zulachir*, Vera Diyanty

Universitas Indonesia, Indonesia

Email: hanifashabilaputri@gmail.com*

Keywords:

internal control; COSO IC-IF 2013; three lines model; customer acceptance process; futures broker.

ABSTRACT

This study aimed to evaluate the implementation of internal control based on the COSO Internal Control–Integrated Framework (IC-IF) 2013 and the Three Lines Model (TLM) at PT XYZ, a BAPPEBTI-licensed futures brokerage company. The research was motivated by recurring procedural violations during 2022–2024, including non-WPB marketing personnel performing WPB functions, fund transfers prior to verification, unauthorized trading activities, and cash deposits. Using a qualitative case study approach, data were collected through in-depth interviews with nine cross-line informants (marketing, WPB, compliance, SPI, and the compliance director), document analysis, and limited observations. A gap analysis was conducted by comparing ideal conditions based on BAPPEBTI regulations, standard operating procedures (SOPs), COSO principles, and TLM principles with actual implementation conditions. The results showed that PT XYZ’s internal control system remained inadequate. Of the 11 main SOP procedures evaluated, five were consistently and repeatedly violated. All five COSO components demonstrated significant weaknesses. The implementation of the Three Lines Model was also ineffective: Line One was weakened by business target pressures, Line Two functioned primarily in an administrative capacity, and Line Three lacked consistency, with no routine coordination among the lines. The study identified 12 Design Gaps (including the absence of compliance KPIs, written sanction policies, a risk register, a whistleblowing system, and IMS alert features) and five Implementation Gaps (including non-WPB marketing personnel performing WPB functions, transfers before verification, unauthorized trading, cash deposits, and WPB accompaniment control gaps). The recommendations include redesigning KPIs with compliance-based weighting, implementing tiered sanctions, establishing a risk register, providing a whistleblowing system, developing IMS alert features, and strengthening top management commitment and cross-line accountability.



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

Copyright © 2026 by Author. Published by
Riviera Publishing

INTRODUCTION

The financial services industry is a sector with a high level of operational risk and regulatory compliance requirements; therefore, it requires an internal control system that is effectively designed and implemented. Various studies have shown that weak internal control quality contributes to increased risks of deviations and reduced organizational accountability,

even when formal control frameworks are already available (Alshaiti, 2023; Boulhaga et al., 2022). One financial services sector that plays a strategic role as a means of hedging, price discovery, and alternative investment in Indonesia is Commodity Futures Trading (PBK). However, the development of this industry has not been immune to public distrust and negative perceptions (Mugarura, 2016).

This negative perception has been further intensified by the increasing number of illegal investment fraud cases that often operate under the guise of futures brokerage companies. These illegal entities exploit public misconceptions by offering unrealistic fixed-income promises, which contradict the high-risk nature of futures investments (high risk–high return) (Medidjati & Heryana, 2024). Such fraudulent practices not only harm customers but also damage the reputation of legitimate futures brokerage companies licensed by the Commodity Futures Trading Supervisory Agency (BAPPEBTI). To further examine these issues, this study conducted a case study of PT XYZ. As a BAPPEBTI-licensed futures brokerage company, PT XYZ demonstrates a governance execution gap, namely a gap between formally established governance structures and their actual implementation in practice. Although the company has established Standard Operating Procedures (SOPs), an organizational structure, compliance functions, and internal audit mechanisms that reflect the implementation of the Three Lines Model (TLM), procedural violations continued to occur during the 2022–2024 period. This phenomenon reflects a governance paradox, in which governance elements are formally available but remain ineffective in preventing operational deviations due to weak execution, conflicts of interest, and misalignment between formal policies and actual practices (Ahmad & Mahmood, 2026; Araral, 2026; Eich, 2026; Furusa & Phahlane, 2026; Latchu & Singh, 2026; Li et al., 2026).

One clear indication of vulnerability in this industry is the increasing number of customer complaints reported to BAPPEBTI. Based on official BAPPEBTI data, 177 customer complaint cases against futures brokerage companies were recorded throughout 2023. Furthermore, the number of customer complaints increased to 230 cases in 2024, representing an increase of approximately 30% compared with the previous year. This condition presents a significant challenge because customer protection remains a critical concern, particularly due to gaps between service promises and actual practices. Many complaints are related to misleading marketing information, fixed-income guarantees, and misinterpretation of investment risks that result in significant customer losses (BAPPEBTI, 2024).

The high-risk characteristics of the Commodity Futures Trading (PBK) industry are multidimensional. First, from a product perspective, leverage mechanisms and price fluctuations have the potential to magnify losses within a short period. This risk is inherent to futures trading and is communicated to customers through the Futures Brokerage Representative (WPB) verification process. Second, from a customer protection perspective, structural vulnerabilities remain. Customer funds must be maintained in a segregated account that is legally separate from company assets (Bappebti, 2018; Marchellia, 2022). However, customers in the PBK industry do not have a customer fund protection scheme equivalent to the Deposit Insurance Corporation (LPS) mechanism available in the banking sector.

Amid the inherent risks of this industry, operational and compliance risks arising from internal weaknesses within companies require particular attention. These risks should be mitigated through effective internal control systems; however, procedural violations continue

to occur during the customer acceptance process at PT XYZ, including inappropriate product marketing practices, unauthorized transactions, and non-compliance with established verification procedures. This research specifically focuses on risks originating from the company's internal processes because these issues directly contribute to customer harm. Strengthening internal control at PT XYZ is expected to reduce avoidable risks and improve customer protection.

PT XYZ is a licensed futures brokerage company authorized by BAPPEBTI and is expected to maintain high standards of regulatory compliance. Based on the Decree of the Head of BAPPEBTI Number 8 of 2019 concerning Technical Provisions for Futures Brokerage Behavior, futures brokerage companies are required to establish SOPs for customer acceptance. These regulations form a fundamental basis for the ethical and operational practices of futures brokerage firms. Meanwhile, customer acceptance SOPs refer to the Decree of the Head of BAPPEBTI Number 9 of 2021, which provides technical guidelines to ensure that customer registration processes are conducted efficiently, effectively, and legally. Nevertheless, field findings indicate procedural inconsistencies and irregularities that reveal weaknesses in internal control implementation (BAPPEBTI, 2019; BAPPEBTI, 2021).

Furthermore, a comparison between the 11 main procedures in PT XYZ's Customer Acceptance SOPs and field findings, including BAPPEBTI audit results for the 2022–2024 period, revealed that five main procedures were consistently and repeatedly violated. These procedures include: (1) face-to-face obligations and product and risk explanations by the WPB as specified in SOP point 1; (2) the prohibition of marketing personnel requesting or receiving customer passwords as specified in SOP point 2; (3) WPB verification requirements before customers transfer funds as specified in SOP point 3; (4) the three-stage customer acceptance process consisting of initial registration, KYC verification by WPB, and proof-of-transfer upload as specified in SOP point 5, which was violated through fund transfers before WPB verification completion; and (5) the prohibition of cash deposits into segregated accounts as specified in SOP point 9. These violations were not isolated incidents. Based on Compliance Department estimates, fund transfers before verification occurred almost monthly, involving approximately 6%–17% of new customers. This condition indicates that the issue is not merely the existence of violations but also their high frequency and repetitive nature, reflecting systemic weaknesses in internal control implementation and supervision.

The Commodity Futures Trading industry is highly regulated to protect customers and maintain market integrity. However, comprehensive regulations do not always guarantee effective implementation. At PT XYZ, several procedural violations continued to occur in the customer acceptance process, including transfers of funds to segregated accounts before completion of WPB verification, profit promotions inconsistent with Fair Dealing principles, marketing activities conducted without WPB assistance, and indications of unauthorized trading through misuse of customer trust. Audit and compliance findings during the 2022–2024 period also demonstrated repeated violations despite the existence of established SOPs and regulations. This condition indicates that the primary issue is not the absence of rules but rather weaknesses in internal control implementation, supervision, and organizational compliance culture.

These violations demonstrate weaknesses in the internal control components described in the COSO Internal Control–Integrated Framework (IC-IF) 2013, including the control

environment, risk assessment, control activities, information and communication, and monitoring activities. In addition, these issues reflect weaknesses in accountability and coordination among supervisory functions. The first line has not consistently implemented procedures, the second line has not effectively performed preventive and monitoring functions, and the third line has not generated sustainable improvements. Therefore, evaluating only the internal control design is insufficient to explain the root causes of these problems, as an assessment of role distribution, responsibilities, and supervisory effectiveness through the Three Lines Model approach is also required.

Based on these conditions, this study proposes an integrated approach combining the COSO Internal Control–Integrated Framework (IC-IF) 2013 and the Three Lines Model (TLM) to evaluate the customer acceptance process at PT XYZ. The COSO IC-IF 2013 framework was used to assess the effectiveness of internal control design and implementation, while the TLM was used to evaluate role clarity, accountability, and coordination among supervisory lines. The integration of these two frameworks represents the research novelty because it evaluates not only what controls should exist but also who is responsible for implementing them. Through this approach, the study is expected to identify gaps between policies and practices and provide comprehensive recommendations to strengthen compliance, internal control effectiveness, and governance oversight in the customer acceptance process at PT XYZ.

METHOD

Research Design

This study employed a qualitative approach with a descriptive-evaluative case study design to examine the implementation of internal control and supervision mechanisms in the customer acceptance process at PT XYZ. This approach enabled an in-depth examination of organizational practices, processes, and behaviors through multiple data sources (Creswell, 2014; Yin, 2018). The research focused on evaluating internal control implementation based on the COSO Internal Control–Integrated Framework (IC-IF) 2013 and the Three Lines Model at PT XYZ as a futures brokerage company operating in a highly regulated industry. The study aimed to describe actual conditions, assess the effectiveness of internal control and the implementation of supervisory roles across defense lines, and identify gaps between policies and practices. Internal control effectiveness was evaluated based on the implementation of the five COSO components, while the effectiveness of the Three Lines Model was assessed based on the alignment of each line's roles with applicable governance principles (COSO, 2013; IIA, 2020).

Data Types and Sources

The data used in this study consisted of primary data and secondary data. Primary data was obtained through in-depth interviews with PT XYZ's internal resource persons who were directly involved in the customer acceptance process, namely Marketing, Futures Brokerage Representative (WPB) Marketing, WPB Verification, Settlement, Dealing, Compliance and Customer Complaints, AML/PPT Desk, Internal Supervision System (SPI), and Compliance Director. Meanwhile, secondary data was obtained through a documentation study of various relevant company documents, such as Standard Operating Procedures (SOPs) for customer admission, organizational structure and work guidelines, compliance policies including AML/PPT and KYC/CDD, internal audit reports and compliance monitoring, account opening

forms, verification checklists, proof of approval, and other administrative documents. In addition, this study also utilizes academic literature in the form of scientific journals and professional institution reports related to COSO IC-IF 2013 and the Three Lines Model as a theoretical and comparative basis in the analysis of research findings.

Data Collection Techniques

The data collection techniques in this study were carried out through interviews, documentation studies, and field observations. Semi-structured interviews were conducted with first-line, second-line, third-line representatives, and Compliance Directors to gain an in-depth understanding of the implementation of internal controls and the Three Lines Model in the customer onboarding process. The documentation study is carried out by examining various relevant documents, such as customer acceptance SOPs, compliance policies, internal audit reports, compliance monitoring reports, organizational structure, job descriptions, and administrative documents related to the customer acceptance process. In addition, non-participant observations are carried out to directly observe the implementation of the customer acceptance process, starting from document checking, KYC verification, issuance of user IDs and passwords, checking deposits, activating trading accounts, to the use of the company's information system. The three techniques are used in an integrated manner to obtain comprehensive data, verify consistency between policies and actual practices, and support the triangulation process in research.

Data Analysis Techniques

The data analysis in this study uses a qualitative approach with the gap analysis method to identify the gap between ideal conditions and actual conditions in the implementation of internal control as well as the Three Lines Model in the customer acceptance process at PT XYZ. The evaluation focused on two main axes, namely internal control based on the five components of the COSO Internal Control–Integrated Framework (IC-IF) 2013 and the implementation of the Three Lines Model which includes the role of the first, second, and third lines. Data analysis is carried out through the stages of data reduction, data presentation, and conclusion drawing according to the Miles and Huberman model, then followed by thematic coding to group the data into COSO component categories, Three Lines Model elements, implementation gaps, and improvement recommendations. Furthermore, gap analysis is carried out by determining ideal conditions based on BAPPEBTI REGULATIONS, PT XYZ SOP, the principles of COSO IC-IF 2013, and the Three Lines Model, then comparing them with the actual conditions obtained through interviews, observations, and documentation studies. The gaps found were classified into design gaps and implementation gaps, then mapped into COSO components and the Three Lines Model defense line to identify the root of the problem and develop integrated improvement recommendations.

RESULTS AND DISCUSSION

Gap Analysis

After evaluating the implementation of internal controls based on the COSO IC-IF 2013 and the Three Lines Model, the next step is to identify the gap between ideal conditions and actual conditions. However, before analyzing the gap in detail, it is necessary to first explain the characteristics of the data available at PT XYZ. The company does not have a centralized record-keeping system for all procedural violations. The quantitative data that can be obtained

is only limited to estimates from Compliance for violations of fund transfers prior to verification as well as specific findings in BAPPEBTI's audit for unauthorized trading and cash deposits. Meanwhile, violations such as non-WPB marketing that performs WPB functions are only documented qualitatively in audit reports and interview results. Therefore, the following gap analysis remains possible due to the nature of qualitative research that prioritizes depth of contextual understanding, but the reader needs to be aware of the limitations of quantitative data for some types of violations. And as explained in chapter 4, the analysis in this subchapter only covers the process of accepting new customers electronically online. Dormant accounts were not analyzed because they were outside the scope of the study.

Based on the evaluation in subchapters 5.1 and 5.2, it was found that 43 criteria (32 COSO criteria and 11 TLM criteria) were not met or partially met, indicating a gap between ideal conditions (regulations, SOPs, COSO principles, and Three Lines Model) and actual conditions in the field. In order to focus more on the root of the problem, these criteria are grouped into 17 main findings summarized in the Integrated Gap Analysis Matrix in Table 5.3.

The gaps identified are divided into two types, namely design gaps (design gaps, occurring due to the absence of policies, procedures, or systems that should exist) and implementation gaps (implementation gaps, occurring because policies, procedures, or systems are already available but not implemented consistently). This sorting is important to identify the root of the problem precisely: whether the problem stems from the absence of a design that should exist, or from the failure to execute an existing design.

1. Design Gap

The design gap is the gap between the supposed ideal conditions (based on BAPPEBTI regulations, internal SOPs, COSO principles, best practices, and the Three Lines Model) and the design of policies, procedures, or systems set by PT XYZ. This gap occurs because companies don't have the design policies, procedures, or systems that they should have. Design weaknesses make the internal control system inherently incapable of preventing deviations, because the design itself does not encourage compliance or does not have adequate control mechanisms. Based on the analysis of documents and interviews, 12 design gap findings were found, which are narratically described as follows.

a. Marketing KPIs without compliance indicators

The ideal conditions according to COSO Principle 5 (criterion 1.13) demand that performance appraisals should reflect not only the achievement of business targets but also compliance with procedures and ethical values. Best practices also emphasize that KPIs must be balanced between business outcomes and compliance. PT XYZ's SOPs and jobdesc do not include compliance indicators. The actual condition found is that marketing KPIs are only based on the amount of funds raised, without the weight of compliance. Thus, this gap is classified as a design gap because the company does not design a performance appraisal system that encourages compliance. This inherently wrong design makes marketing tend to ignore SOPs in order to achieve targets. Improvement requires redesigning KPIs in terms of company policies.

b. Compliance has no monitoring parameters

Ideal conditions according to COSO Principle 16 (criterion 5.1) and TLM L2-2 require the compliance function to have measurable indicators to conduct effective monitoring. The compliance SOP does not include monitoring parameters. Actual conditions show that

compliance is monitoring monthly but without specific parameters or indicators, relying only on the number of complaints. This gap is a design gap because the design of the compliance function is not equipped with a compliance measuring tool, so monitoring is reactive. Fixes require setting monthly parameters such as transfer percentage before verification, number of unassisted marketing, and verification compliance level.

c. Sanctions for violations are not strict

The ideal conditions according to COSO Principle 1 (criterion 1.2) require strict and documented sanctions to create a deterrent effect. The company's SOP does not have a written sanction policy, there is only the practice of giving SP. The actual conditions show that the sanctions given are only SP without a clear level. This gap is a design gap because companies do not design a multi-tiered and documented sanction system. Weak sanctions design inherently does not sufficiently change the behavior of offenders. Improvements require the preparation of a multi-level sanction policy (SP1, SP2, SP3, layoffs) plus bonus deductions.

d. No risk register for the customer acceptance process

Ideal conditions according to COSO Principle 7 (criterion 2.2) and risk management best practices require companies to have formal risk documentation (risk register) that identifies, analyzes, and mitigates risks. The SOP does not include risk registers. The actual condition is the absence of a risk register for the customer acceptance process. This gap is classified as a design gap because the company does not design formal risk documentation, so risk identification and mitigation are only reactive. Improvement requires the establishment of a risk register that contains the main risks such as mis-selling, unauthorized trading, transfers before verification, cash deposits.

e. No whistleblowing system

Ideal conditions according to COSO Principle 14 (criterion 4.4) and financial industry best practices emphasize the importance of secure and independent breach reporting channels for early detection. The SOP does not cover a whistleblowing policy. Actual conditions indicate the absence of a dedicated reporting channel. This gap is a design gap because the company did not design a mechanism that allows employees to report violations without fear of retaliation, so violations are not detected internally. Repairs require the provision of a whistleblowing channel (email/hotline) with a guarantee of anonymity.

f. Marketing recruitment and WPB do not filter ethics and compliance

The ideal conditions according to COSO Principle 4 (criterion 1.12) emphasize that recruitment criteria should include an understanding of ethics, integrity, and compliance. In companies, they have not paid special attention to the ethical aspect in recruitment. The actual condition is the absence of ethical questions or integrity background checks in the recruitment process. This gap is a design gap because the design of recruitment criteria is incomplete, causing companies to recruit marketers who do not have a WPB license and lack understanding of the limitations of authority. Improvements require the addition of interview questions about ethics and integrity background checks.

g. There are no marketing written guidelines (code of ethics & code of conduct)

The ideal conditions according to Perba BAPPEBTI No. 4/2018, COSO Principle 1 (criterion 1.1) and COSO Principle 14 (criterion 4.3), as well as TLM L2-1 require written guidelines on behavior and authority limits that are clearly communicated. The SOP does not contain specific guidelines for marketing. Actual conditions indicate the absence of written

guidelines on what information can and cannot be conveyed. Socialization is only oral. This gap is a design gap because the design of policy communication is incomplete. Improvement requires the creation of a written Marketing Code of Conduct that is socialized and signed.

- h. There is no regular coordination forum between L1, L2, L3

The ideal conditions according to the TLM Coordination Principles (K-1 Coordination criteria) require a regular coordination forum between Line 1, Line 2, and Line 3 to discuss risks, findings, and process improvements. The SOP does not regulate routine meetings. The actual conditions show that coordination only occurs when there is a case or after there are BAPPEBTI audit findings, without a fixed schedule. This gap is a design gap because the company does not design a scheduled coordination mechanism, so each line works in silos. Fixes require quarterly forums with minutes and action items.

- i. There is no alert system on IMS

Ideal conditions according to COSO Principle 11 (criterion 3.8) and COSO Principle 16 (criterion 5.2) require the system to have features that support preventive control such as alerts for suspicious activity. The technical SOP does not require such a feature. The actual condition indicates that the STI does not have an alert. This gap is a design gap because the system design is incomplete to support control, leading to a reliance on manual coordination. The fix requires the development of automation features in IMS.

- j. Low Compliance Independence (only recommendations, decisions in the hands of the directors)

Ideal conditions according to COSO Principle 2 (criterion 1.6) and TLM L-2 require the compliance function to have sufficient independence and authority to recommend sanctions and stop the violating process. The compliance SOP only mentions "assisting the Compliance Director" and "submitting a report". The actual condition is that compliance only submits a report, the final decision remains in the hands of the board of directors, and does not have the authority to decide for itself. This gap is a design gap because the design of the compliance authority structure is weak, causing the Second Line to be unable to force improvements. Improvements require the granting of compliance authority to recommend sanctions and reporting channels directly to the Compliance Director.

- k. SPI has never assessed the effectiveness of internal control

Ideal conditions according to COSO Principle 17 (criterion 5.4) and TLM L3-4 require SPI to assess the effectiveness of internal controls on a regular basis and monitor follow-up on repeated findings. SPI's SOP regulates the preparation of action plans. However, actual conditions show that SPI has never formally assessed the effectiveness of internal controls, does not have an assessment methodology (such as maturity level), and recommendations are only socializing. This gap is a design gap because the company did not design a measurable internal control effectiveness evaluation mechanism. Improvements require SPI to assess the effectiveness of internal control by a measured method (maturity level), and the results are reported to the board of directors and commissioners.

- l. WPB and non-WPB marketing does not receive adequate AML/PPT training

The ideal condition according to Perba BAPPEBTI 2/2016 requires AML/PPT education for all employees, including marketing. SOP does not have a special training program. The actual conditions show that marketing only gets verbal "sounding" without formal training for all SOPs in the company. This gap is an implementation gap because

regulations already require it, but companies do not implement it. Improvements require mandatory AML/PPT training every year for all Non-WPB and WPB marketing, accompanied by certificates and comprehension tests.

This design gap is entirely within management's control to be corrected through changes in policies, procedures, systems, and organizational structures. Without design improvements, efforts to strengthen implementation will be difficult to succeed because the system inherently does not encourage compliance and does not have adequate early detection mechanisms.

1. Implementation Gap

Implementation gap is a gap between the Standard Operating Procedures (SOPs) that have been designed and the actual practices that occur in the field. This gap occurs because SOPs, policies, or systems are already available by design (as per regulations, COSO principles, and the Three Lines Model), but are not implemented consistently in the field. Based on the analysis of interviews and documents, it was found that PT XYZ has a very wide implementation gap in various aspects of customer acceptance, which is the main cause of repeated violations and the findings of the 2022–2024 BAPPEBTI audit. The following is a narrative description for the 5 identified implementation gap findings.

a. Non-WPB marketing performs WPB functions

The ideal conditions in design have been met: SOP point 1 and Perba BAPPEBTI 4/2018 Article 2 require only WPBs to be allowed to have direct contact with potential customers. Non-WPB marketing jobs also only mention "making promises". However, actual conditions show that non-WPB marketing still explains products, risks, and prospects without WPB assistance, with repeated violations in the 2023–2024 BAPPEBTI audit. The cause is target pressure where there is the same target for WPB and Non-WPB in the same position and weak supervision. This gap is an implementation gap because SOPs already exist but are not implemented. Improvements require strengthening supervision, monitoring parameters, and strict sanctions.

b. Transfer funds before WPB verification is completed

The ideal conditions in terms of design have been met: SOP points 3 and 5.3 and Perba BAPPEBTI 9/2021 point 3 require the sequence of procedures (simulation → registration → verification → transfer). The actual condition shows that many customers transfer funds before the verification is completed. Based on Compliance estimates, these violations occur in around 5%–20% of the number of new customers every month. The reason is that marketing personnel sometimes lack to educate customers to follow the flow of the process sequence correctly and compliance does not proactively monitor the activities of marketing personnel in the field. Because SOPs already exist, this gap is an implementation gap. Improvements require periodic socialization to marketing personnel and strict monitoring by compliance.

c. Unauthorized trading (marketing accepts passwords and transactions on behalf of clients)

The ideal conditions in design have been met: Customer Agreement points 6, Jobdesc WPB points 17–18, and Perba BAPPEBTI 4/2018 prohibit this practice. Actual conditions show that real cases are still occurring, with indications of transactions by brokers in the 2022 and 2024 BAPPEBTI audits (proof of office IP). The cause is light sanctions, in this case only SP and inadequate customer education. This gap is an implementation gap because policies already exist but the implementation of supervision and sanctions enforcement has failed.

Improvements require strict and documented sanctions (SP1–PHK), IP address monitoring, and customer education.

d. Cash deposits by customers

The ideal conditions in design have been met: Perba BAPPEBTI 2/2016, Perba 4/2018 Article 7 letter c, SOP item 5.3, and Internal Memo which prohibits cash deposits. The actual condition shows that there are still cases of customers making cash deposits, and the practice still occurs after the memo is issued. This gap is an implementation gap because the policy already exists but the implementation of the ban fails due to weak supervision and education. Improvement requires real-time monitoring and re-education.

e. WPB companionship control gap

The ideal conditions in design have been met: the SOP mentions mandatory face-to-face by the WPB, and Perba BAPPEBTI 4/2018 requires assistance. The actual condition shows that the mentoring mechanism is carried out by marketing to meet potential customers first, and then bring WPB to the next meeting. WPB was not present during the initial interaction discussing the product, and there have been no strict sanctions if procedures are violated. This gap is an implementation gap because procedures are not consistently applied to close the gap. Improvement requires WPB to be present in every interaction that discusses products/risks, interaction recordings, and sampling monitoring. In addition, periodic monitoring by compliance is needed for all marketing activities that occur in the field by enforcing forms that must be filled out by marketing personnel signed by customers and attaching documentation evidence to be reported to compliance.

All of the implementation gaps above show that PT XYZ has an adequate foundation of policies, SOPs, and regulations by design, but the implementation in the field fails due to several reasons such as target pressure, weak supervision, light sanctions, and lack of management commitment. The root of this implementation gap is the weak control environment such as non-compliance KPIs, light sanctions and target pressure, and the ineffectiveness of the monitoring functions of Line 2 and Line 3. As a result, the most dominant and recurring violations from year to year (as recorded in the 2022–2024 BAPPEBTI audit) continue to occur. Without improvements to the control environment and strengthening the supervisory function, the implementation gap will continue to recur.

Integrated Gap Analysis Matrix

To summarize all the gap findings that have been described in subchapters 5.3.1 (design gap) and 5.3.2 (implementation gap), an Integrated Gap Analysis Matrix is prepared in Table 5.1. This matrix maps 17 key findings based on the type of gap, related BAPPEBTI regulations, company SOPs, actual conditions (interview and audit results), weak COSO components, failed Three Lines Model lines, and initial recommendations for improvement. This matrix serves as an integrative summary that links all findings to the evaluation framework that has been established in Chapter 3.

Table 1. Integrated Gap Analysis Matrix of PT XYZ Customer Acceptance Process

Yes	Findings/Violations	Regulations & SOPs	Evidence/Actual Conditions	Gap	COSO	TLM	Recommendations
1	Non-WPB marketing	Perba 4/2018	Marketing explains the	IG	CA	L1,L2	Mandatory WPB assistance,

Yes	Findings/Violations	Regulations & SOPs	Evidence/Actual Conditions	Gap	COSO	TLM	Recommendations
	describes products without WPB	Ps.2; POS item 1	product because of the target; Audit Findings 2023–2024				monitoring, multi-level sanctions
2	Transfer before WPB verification	Perba 9/2021; POS 3 & 5.3	Transfers take precedence before verification; 6–17% of new customers/month	IG	CA	L1	Tighten marketing monitoring and education
3	Unauthorized trading (customer password provided to marketing)	Perba 4/2018; Agreement No.6	Password case is given; Audit Findings 2022 & 2024	IG	CA	L1,L2	IP monitoring, periodic password changes, strict sanctions
4	Deposit cash to segregated account	Perba 2/2016; POS 5.3	Cash deposits are still common;	IG	CA	L1,L2	Real-time monitoring and refunds
5	Funds-based KPIs	Best Practice COSO	There are no compliance indicators in the KPI	DG	CE	L1	Add compliance weights $\geq 20\%$
6	Compliance without monitoring indicators	Best Practice COSO	Relying only on the number of complaints	DG	AND	L2	Set monthly monitoring KPIs
7	Sanctions are only SP	Internal regulation	There is no level of sanction	DG	CE	L2	SP1–SP3, layoffs, and bonus deductions
8	No risk register	Best Practice COSO	Not yet available	DG	DATE	L2,L3	Compile a risk register of the customer acceptance process
9	No whistleblowing system	Not yet required	No reporting channels	DG	IC	L2	Form an independent whistleblowing channel
10	Recruitment has not assessed ethics & compliance	Best Practice COSO	There is no ethical aspect in the selection	DG	CE	L1,L2	Add ethics and integrity tests
11	There are no written marketing guidelines	Perba 4/2018	Oral briefings only	DG	IC	L2	Susun Marketing Code of Conduct

Yes	Findings/Violations	Regulations & SOPs	Evidence/Actual Conditions	Gap	COSO	TLM	Recommendations
12	TLM coordination is reactive	Three Lines Model	No regular forums	DG	COORD	COORD	Quarterly Coordination Forum
13	AML/PPT training is inadequate	Perba 2/2016	Just a short socialization	DG	CE	L1,L2	Annual training and competency tests
14	No alert system	Best Practice	Detection is still manual	IG	CA	L1,L2	Develop alert features on IMS
15	WPB was not present at the initial interaction	Perba 4/2018	Assistance was carried out later	IG	CA	L1	Required attendance and documentation of meetings
16	SPI has not assessed the effectiveness of control	COSO Principles	Only socialization recommendations	DG	AND	L3	Annual control effectiveness audit
17	Low compliance independence	COSO/TLM Principles	Only recommend	DG	CE	L2	Strengthen authority and reporting pathways

Recommended Improvements

Based on all analyses in subchapters 5.1 to 5.3, it was found that PT XYZ's internal control weaknesses were systemic and layered. The root of the main problems are: (1) the absence of compliance indicators in marketing KPIs so that business targets take precedence over compliance; (2) the absence of a written and tiered sanction policy so that there is no deterrent effect; (3) the low independence of the Second Line (Compliance) because the final decision remains in the hands of the board of directors; (4) the absence of risk management infrastructure and early detection systems (whistleblowing system, risk register, measurable monitoring parameters and alert features in the IMS system); and (5) the ineffectiveness of the internal audit function (SPI) in assessing and ensuring follow-up improvements, as well as the absence of routine coordination on the line.

The implication of the root of this problem is: the same violations (non-WPB marketing carrying out WPB functions, transfers before verification, unauthorized trading, cash deposits) continue to be repeated from year to year, as recorded in the 2022–2024 BAPPEBTI audit. Therefore, the success of all the technical recommendations in this study is highly dependent on strengthening the commitment of top management (Tone at the Top) as the main foundation. Management's statement of concern about the risk of margins being threatened if procedures are implemented too tightly confirms that compliance has not been positioned as the organization's top priority. Without a paradigm shift in management to put integrity above short-term target achievement, technical improvements such as information system features or SOP revisions will not have a lasting impact.

Based on the five root problems above, the following improvement recommendations are prepared in an integrated manner. Recommendations 1 to 5 are aimed at addressing the root of problems 1 and 2, namely the absence of compliance indicators in marketing KPIs and weak

sanctions and compliance culture. Recommendation 6 is aimed at addressing the root of problem 3, namely the low independence of the Second Line (Compliance). Recommendations 7 to 10 are aimed at addressing the root of problem 4, namely the absence of an early detection system in the form of risk registers, monitoring parameters, whistleblowing, and supporting system features. Recommendations 11 to 13 are aimed at closing the implementation gaps in the field that stem from the root of problems 1 and 2 (target pressure and weak supervision). Recommendations 14 and 15 are aimed at strengthening the oversight function, which is related to the root of problems 3 and 5 (low compliance independence and ineffectiveness of SPI's internal audit function). Recommendation 16 is aimed at addressing the root of the fundamental problem, namely the lack of tone at the top management commitment that consistently puts compliance above short-term business targets.

Improvement of the Control Environment (Strengthening Tone at the Top and Culture of Compliance)

1. Redesign of marketing KPIs with compliance indicators

Marketing KPIs have so far only focused on the amount of funds raised, without measuring compliance with procedures. This encourages non-WPB marketing to go beyond the limits of authority to achieve the target. The company needs to add a compliance weight of at least 20% of the total performance assessment, with indicators including: (a) not receiving or requesting customer passwords, (b) not conducting unauthorized trading, (c) compliance with WPB assistance procedures, and (d) no proven customer complaints related to mis-selling. These new KPIs must be communicated in writing, evaluated monthly by Compliance with direct marketing supervisors, and integrated into promotion and deposition policies.

2. Firm and documented implementation of tiered sanctions

So far, there has been no written sanction policy, and the sanctions are only in the form of warning letters with no deterrent effect. The company must prepare a written sanction policy that regulates the level of punishment: Warning Letter (SP) 1 for the first minor offense; SP2 for a second minor offense or a first moderate offense; SP3 for the first serious violation; and Termination of Employment (PHK) for repeated gross violations or violations that significantly harm customers (e.g. unauthorized trading). Additionally, include annual bonus deductions for moderate and above category violations. This policy must be socialized with proof of the signature of all employees.

3. Buat pedoman tertulis Marketing Code of Conduct

So far, there are no written guidelines on what marketing can and cannot convey. The Company must prepare a Marketing Code of Conduct document that contains in detail: (a) information that may be submitted (company profile, passive income opportunities without the promise of fixed income); (b) information that should not be disclosed (fixed income promises, specific "buy" or "sell" analysis, profit guarantees); (c) limitations of authority (not allowed to accept passwords, not to make transactions on behalf of customers, not to explain product technicalities without WPB); (d) consequences of violations (referring to the tiered sanctions policy). Every marketing and WPB is obliged to read, understand, and sign the commitment. This document is socialized annually.

4. Add ethical and compliance aspects to the recruitment process

Marketing and WPB recruitment has so far not filtered the understanding of ethics and compliance. Companies need to add interview questions about ethics, integrity, and case

studies of compliance violations. Do a background check on the job history of the prospective marketer. For non-WPB marketing candidates, provide an early understanding of the limits of authority and the consequences of violations.

5. Conduct mandatory compliance training every year

There is currently no regular compliance training, and marketing only gets verbal "sounding". Companies must create an annual compliance training program for all marketing and WPB. The material includes: prohibition of mis-selling, prohibition of unauthorized trading, AML/PPT obligations, correct procedures for WPB assistance, and consequences of violations. Graduation certification is a prerequisite to still be able to carry out tasks. Document the implementation of the training with attendance lists, materials, and photos.

6. Strengthen the independence of the Director of Compliance and Compliance

Compliance currently only acts as a recommender, with the final decision remaining in the hands of the board of directors. The Company needs to authorize Compliance to: (a) recommend sanctions in writing to the Compliance Director; (b) temporarily suspend the process of accepting customers who are proven to be in violation of the SOP (e.g. transfers before verification or cash deposits) without having to wait for the approval of the board of directors for emergency measures; and (c) a direct reporting pathway to the Director of Compliance without intervention from other directors for cases of obvious violations. The compliance function must also be protected from pressure from business targets with a written policy that Compliance performance evaluation is not associated with the achievement of target margins or the number of new customers.

Improved Risk Assessment and Monitoring (Building Early Detection and Measurable Parameters)

1. Form a risk register for the customer acceptance process

The company does not yet have formal risk documentation. The risk identification process can be carried out through brainstorming involving representatives of Line 1 (marketing, WPB, Settlement), Line 2 (Compliance, AML/PPT), and Line 3 (SPI) which is carried out periodically (for example, every year or every 6 months according to the evaluation cycle carried out by SPI), as well as whenever there is a change in BAPPEBTI regulations or significant changes in business processes. This team is tasked with mapping key risks such as: mis-selling, unauthorized trading, transfers before verification and cash deposits. For each risk, it is necessary to document a description of the risk, causes, impacts, probabilities, mitigation plans, persons in charge, and evaluation schedule. This risk register must be reviewed and approved by the President Director and the Compliance Director as a form of top management commitment, then socialized to all related lines.

2. Set compliance monitoring parameters for Compliance

Compliance so far has only relied on the number of complaints without measurable parameters. The company must establish monthly compliance performance indicators, for example: (a) the percentage of new customers who transfer before verification (target <5%); (b) the number of non-WPB marketing that is proven to interact without WPB assistance (target 0); (c) WPB verification compliance level (100% pre-deposit verification target); (d) the number of customer complaints per 100 new customers (the target decreases every quarter). Report these parameters monthly to the Compliance Director and discuss them in the quarterly coordination forum.

3. Provide a safe and independent whistleblowing system

The company does not yet have a violation reporting channel. Form a whistleblowing channel that is managed by an independent party (it can be Compliance with a guarantee of anonymity, or outside the structure if possible). Use a dedicated email address or hotline that doesn't track the identity of the whistleblower. Ensure the confidentiality of the whistleblower's identity and protection from retaliation. Socialize the presence of this channel to all employees through posters, email blasts, and internal memos.

4. Develop alert features on IMS systems

The current IMS system does not have automatic alerts to detect procedural violations. Add the following features: (a) automatic alerts to Compliance and marketing managers if there is a deposit attempt before verification is complete; (b) automatic notification to the customer in the 11th and 12th months that the account will be closed if there is no activity; (c) alerts for login activity from unknown IP addresses or from office IPs for specific customer accounts (to detect potential unauthorized trading).

Improvement of Control Activities (Closing Implementation Gaps)

1. Require WPB assistance in every interaction that discusses products or risks

Revised SOPs so that non-WPB marketing is strictly prohibited from explaining products, risks, or transaction mechanisms without the assistance of WPB who are physically present or via video call (recorded). Require interaction documentation in the form of a video call recording or a written summary (form) signed jointly by WPB and the customer that explains the product or risk is WPB. Compliance conducts sampling monitoring of at least 10% of the total interactions every month. Apply tiered sanctions for marketing that violates.

2. Strengthen supervision and enforcement of sanctions for violations that already have policies

Violations such as transfers before verification, unauthorized trading, and cash deposits already have policies prohibiting them, but the implementation of oversight is weak. The Company must: (a) conduct real-time monitoring by Compliance of new customer deposits; (b) follow up on any violations with sanctions in accordance with the multi-level sanctions policy; (c) re-educate marketing and customers on a regular basis about prohibitions and consequences; (d) for unauthorized trading, add suspicious IP address monitoring.

3. Improve SOP communication documentation

All changes to new SOPs, guidelines, and regulations must be communicated in written form (not just verbally). Keep proof of socialization (attendance lists, minutes, screenshots of email delivery) in a shared folder that can be accessed by all interested employees. Especially for non-WPB marketing, create a one-page summary of "Do's and Don'ts" that is pasted in the work area and emailed every time there is a change.

Internal Audit Function (SPI) Improvements to Ensure Continuous Improvement

1. SPI is required to conduct periodic assessments of the effectiveness of internal control

SPI has never formally assessed the effectiveness of internal control. SPI must develop a measurable assessment methodology, for example using a maturity level (scale 1–5) for each COSO component. Conduct an assessment at least once a year. The results of the assessment are reported to the President Director and the Board of Commissioners, and become the basis for policy and procedure revisions. SPI must also specifically monitor follow-up on repeated

findings; if the same findings arise for more than two consecutive periods, SPI is obliged to investigate the root of the problem and recommend sanctions to management.

2. Hold quarterly coordination forums L1, L2, L3

So far, coordination has only been reactive (when there are cases). The form of a fixed agenda for quarterly meetings attended by representatives of Line 1 (marketing, WPB, Settlement), Line 2 (Compliance, AML/PPT), and Line 3 (SPI). The mandatory agenda: (a) evaluation of the findings of violations in the previous period; (b) discussion of risk trends from the risk register; (c) follow-up audit recommendations; (d) Procedure improvement plan. Document minutes and action items with a clear person in charge and deadlines. The follow-up of the action item is verified in the next forum.

Cross-Line Improvement and Strengthening Management Commitment

1. Strengthening the commitment of top management (tone at the top) and affirming the accountability of compliance directors

The main person in charge of compliance implementation at PT XYZ is the Director of Compliance. Therefore, strengthening the culture of compliance requires not only commitment from all employees, but also a strong commitment from top management as the party that determines the direction, values, and culture of the organization. Top management (President Director and Compliance Director) need to issue a written policy that explicitly states that compliance with regulations and SOPs should not be sacrificed for the sake of achieving business targets. This policy must be communicated consistently to all employees as part of strengthening the company's tone at the top and compliance culture. In addition, the performance evaluation of the Director of Compliance and Compliance should not only be based on administrative compliance, but also consider the effectiveness of the compliance function in preventing and reducing the occurrence of repeated violations. Evaluation indicators can include a decrease in the frequency of fund transfers before verification, an increase in compliance with WPB assistance, and a reduction in repetitive findings in BAPPEBTI audits.

In accordance with the principles of the Three Lines Model, the Board of Commissioners as a supervisory body has the responsibility to ensure that the governance, risk management, and internal control structures run effectively. In this context, the Board of Commissioners not only plays a role in evaluating the company's overall performance, but also ensures that the compliance function under the responsibility of the Compliance Director is able to carry out its role effectively as a second line of defense. Thus, the effectiveness of the compliance function is part of the accountability of the Director of Compliance which needs to be accounted for to the Board of Commissioners. This accountability can be carried out through the submission of performance reports on the compliance function, the results of supervision, the follow-up of audit findings, and the progress of the implementation of the improvement program that has been set. (The Institute of Internal Auditors, 2020b)

As a form of implementing the supervisory function, the Board of Commissioners is advised to conduct periodic evaluations of the effectiveness of the compliance function and the achievements of improvements that have been made. If there is no significant improvement in the repeated findings during the evaluation period, the Board of Commissioners may consider more comprehensive corrective actions and re-evaluate the effectiveness of the structure, resources, authority, and leadership of the compliance function to identify the root cause of the

non-optimal implementation of the compliance function. This step is important to ensure that the compliance function is not only formally present in the organizational structure, but is truly able to carry out its role effectively, independently, and accountably in strengthening PT XYZ's internal controls.

Recommendation Feasibility Analysis

Not all recommendations have the same level of ease of implementation. Here's a brief analysis of the eligibility:

1. Recommendations with high feasibility, where these recommendations require low costs and do not require complex approval, include: redesign of marketing KPIs, implementation of multi-level sanctions, addition of ethical aspects in recruitment, creation of a Marketing Code of Conduct, mandatory compliance training every year, determination of compliance monitoring parameters, provision of a whistleblowing system through special emails, improvement of SOP communication documentation, and the establishment of a quarterly coordination forum. This recommendation only requires changes to policy documents and management commitments, so that it can be implemented immediately.
2. Recommendations with moderate feasibility, where these recommendations require investment or cultural change, include: the establishment of a risk register, the development of alert features in the IMS system, the obligation to assist WPB, the strengthening of supervision for violations of existing policies, and the obligation of SPI to assess the effectiveness of internal control. This recommendation takes time and cost, especially for the development of IT systems, but it is still feasible to implement.
3. Recommendations with low feasibility, where these recommendations require a change in commitment from top management, include: strengthening the independence of Compliance, strengthening the tone at the top, and the accountability mechanism of the Director of Compliance. This recommendation is challenging because it requires the willingness of the board of directors to relinquish some authority and change the paradigm from target-oriented to compliance-oriented. Nonetheless, these recommendations remain important to create sustainable improvements.

Companies are advised to implement recommendations gradually, starting from recommendations with high feasibility as the first step for improvement, then progressively moving on to recommendations with medium and low feasibility in line with strengthening internal commitments.

All of the above recommendations are interrelated. The success of its implementation relies heavily on top management's commitment to putting integrity above short-term targets. Companies are advised to prepare an action plan with clear deadlines, assign a person responsible for each recommendation, and conduct periodic evaluations of implementation progress. Without fundamental changes to culture and accountability, technical improvements will not have a lasting impact.

CONCLUSION

This study concluded that the implementation of internal control and the Three Lines Model in the customer onboarding process at PT XYZ was not yet fully effective despite the existence of regulatory requirements and internal procedures. The findings identified 17 gaps, consisting of 12 design gaps and 5 implementation gaps, which indicated weaknesses across

all five COSO components, particularly in the control environment and monitoring activities. Recurring violations, including marketing personnel operating beyond their authorized roles, fund transfers before verification, unauthorized trading, and cash deposits, demonstrated that the primary issue was not the absence of rules but rather weaknesses in enforcement, monitoring, accountability, and organizational commitment to compliance.

Furthermore, the Three Lines Model had not functioned optimally due to weak coordination among the three lines, limited independence of the compliance function, and the absence of effective internal audit evaluations of control effectiveness. Therefore, strengthening tone at the top, integrating compliance indicators into performance measurement systems, enhancing compliance authority, implementing structured monitoring mechanisms, and improving coordination among governance functions are essential steps toward achieving sustainable improvements in internal control effectiveness and customer protection within the commodity futures brokerage industry.

REFERENCES

- Ahmad, Z., & Mahmood, Z. (2026). Institutionalising corporate governance: Contradictions, negotiated compromises and unintended consequences. *Journal of Accounting in Emerging Economies*, 1–21.
- Alshaiti, H. (2023). Influences of internal control on enterprise performance: Does an information system make a difference? *Journal of Risk and Financial Management*, 16(12), 518. <https://doi.org/10.3390/jrfm16120518>
- Araral, E. (2026). *Agency theory in public administration: A comparative study of the US, China, and EU*. Cambridge University Press.
- BAPPEBTI. (2016). *Regulation of the Head of Commodity Futures Trading Regulatory Agency (BAPPEBTI) No. 2 of 2016 concerning knowledge customers principle by futures broker*.
- BAPPEBTI. (2018). *Perdagangan berjangka komoditi* (pp. 1–20). BAPPEBTI.
- BAPPEBTI. (2019). *Surat Keputusan Kepala BAPPEBTI Nomor 8 Tahun 2019*. BAPPEBTI.
- BAPPEBTI. (2021). *Surat Keputusan Kepala BAPPEBTI Nomor 9 Tahun 2021*. BAPPEBTI.
- BAPPEBTI. (2023). *Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Republik Indonesia Nomor 6 Tahun 2023*.
- BAPPEBTI. (2024). *Laporan kinerja BAPPEBTI 2024*. BAPPEBTI.
- Boulhaga, M., Bouri, A., & Elbardan, H. (2022). The effect of internal control quality on real and accrual-based earnings management: Evidence from France. *Journal of Management Control*, 33(4), 545–567. <https://doi.org/10.1007/s00187-022-00348-5>
- Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework*. Committee of Sponsoring Organizations of the Treadway Commission.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- Eich, M. (2026). *Strategic corporate governance and the architecture of decision and control structures*. Auremont House.
- Furusa, S. S., & Phahlane, M. (2026). Interplay of flawed ICT governance and contextual realities: A systematic review of e-government project failures in Africa. *Computers*, 15(8), 490.
- Latchu, A., & Singh, S. (2026). State Information Technology Agency (SITA) and the paradox of centralized ICT procurement: Reform or redundancy in South Africa's public sector. *The African Journal of Information Systems*, 18(1), 1.

- Li, L., Xu, Y., & You, L. (2026). Systemic failure and distorted feedback: A study on the implementation dilemma of local government's cross-Strait agricultural cooperation from a political systems theory perspective. *Systems*, 14(3), 262.
- Marchellia, S. N. (2022). Klausula baku pada perjanjian berjangka dan perlindungan hukum bagi investor perdagangan berjangka komoditi. *Journal of Trade Development and Studies*, (8). <https://doi.org/10.52391/jcn.v6i1.677>
- Medidjati, R. A., & Heryana, T. (2024). *Investasi bodong: Fenomena, bias perilaku investor dan dampaknya di Indonesia*. Penerbit Adab.
- Mugarura, N. (2016). The juxtaposition of success and failure of corporate governance procedures: The interplay between rules and practice. *Journal of Financial Crime*, 23(2), 379–413.
- The Institute of Internal Auditors. (2020). *The IIA's three lines model*. The Institute of Internal Auditors. <https://iia-indonesia.org/three-lines-model-dari-iaa/>
- Yin, R. K. (2018). *Case study research and applications: Design and methods*. SAGE Publications.