J I T E T
ISSN: 2303-0577
JURNAL INFORMATIKA DAN TEKNIK ELEKTRO TERAPAN

AUDIT OF TRADING PLATFORM INFORMATION SYSTEM FROM THE PERSPECTIVE OF INFORMATION SECURITY GOVERNANCE IN COMMODITY FUTURES TRADE

Syifaurachman[1], Muhamad Ihsan Ashari[2], Galuh Oka Safitri[3]

[1,2,3] Department of Information Systems, Faculty of Computer Science, Universitas Pamulang; South Tangerang City, Banten Province, Indonesia.

Keywords:
information systems audit;
information security;
trading platform;
commodity futures trading.

Corespondent Email:
dosen03181@unpam.ac.id

Abstract. *Information system-based trading platforms play an important role in supporting real-time, high-value, and high-risk commodity futures trades. With their complex designs, huge transaction volumes, and reliance on digital technology, information system security is crucial to operational reliability and stakeholder confidence. Weak security measures can result in financial losses, service disruptions, and reputational damage. This study employs an information system audit approach to assess the efficacy of information system security controls on a commodity futures trading platform. A descriptive qualitative approach with a case study at Company X was used. Data were gathered by analyzing security audit reports, internal policies, and operational processes, conducting interviews with system management and supervisory people, and observing platform activities. Data analysis involved comparing real system circumstances to information system audit best practices and digital transaction security standards. The findings indicate that security procedures have been widely implemented but are only partially compliant. Key holes were detected in risk planning that is not frequently updated, insufficient documentation of operational controls, flaws in human resource competency management, and a lack of comprehensive continuous monitoring and improvement processes. These findings emphasize that effective information system security necessitates not just the establishment of controls, but also consistent implementation, thorough documentation, and alignment of technology controls with business operations.*

1. INTRODUCTION

The digitalization of business processes has driven significant transformation in the commodity futures trading sector through the use of information system-based trading platforms. These platforms enable fast, integrated, and real-time transaction execution, but at the same time increase system complexity and exposure to various information security risks [1], [2]. In the context of commodity futures trading, which involves high-value transactions and directly impacts market stability, information system security is a critical element in maintaining operational reliability and market participant confidence.

Previous research has demonstrated that security threats to digital transaction systems, such as data leaks, access misuse, cyberattacks, and service outages, can result in considerable financial losses and reputational risks for enterprises that operate digital platforms [3], [4]. These dangers are increasing as network and cloud-based technologies become more prevalent, expanding the attack surface and necessitating more adaptive security controls [5].

The literature on information security governance and management highlights the value of maturity in managing information system security. Organizations with low security maturity typically use reactive controls, are inadequately documented, and lack continuing evaluation processes [6], [7].

Information systems audits are regarded as an important tool for assessing the efficacy of security controls, information technology governance, and information systems risk management. Audits are used not only to evaluate compliance, but also as a strategic tool to improve system reliability and organizational performance. [8], [9].

Although various studies have been completed on information systems audits, empirical research on commodity futures trading platforms has been very restricted [10]. This study attempts to examine information systems security on commodities futures trading platforms through an information systems audit technique, utilizing a case study of Company X.

2. LITERATURE REVIEW

2.1 Digital Transformation and Information System Security Challenges

According to the literature on information systems auditing and security, digital transformation in the banking and e-commerce industries has increased organizations' reliance on complex, integrated information systems. Digital platforms that handle high-value transactions, such as commodity futures trading, have considerable hurdles in terms of information security, technological governance, and information system risk management [1, 2]. Data breaches, unauthorized access, cyberattacks, and service outages have been cited as critical variables affecting the operational stability and financial performance of digital enterprises [3], [4].

As network and cloud technologies become more widely used, the attack surface for information systems grows and becomes more dynamic. This circumstance necessitates a more flexible, organized, and risk-based approach to security controls [5]. Previous research has demonstrated that failing to consistently manage information security risks can result in reoccurring security incidents and erode user trust in digital services [6].

2.2 Information System Security Maturity and Risk Management

Measuring the level of information system security maturity is critical for determining an organization's readiness to meet increasing cyber threats [7]. Low levels of maturity are typically characterized by reactive controls, inadequately documented systems, and a lack of continuing review processes. In contrast, firms with higher levels of maturity tend to have a structured, documented, and integrated security approach with business strategy.

2.3 Information System Audits as a Security Evaluation Mechanism

Information system audits are regarded as a strategic tool for assessing the efficacy of security controls, information technology governance, and information system risk management. Audits are used not just to ensure compliance with standards and rules, but also to improve system dependability and overall organizational performance [8], [9]. In e-commerce and trading platform contexts, information system audits are critical for verifying that security measures support service continuity and the integrity of digital transactions [10].

Modern information system auditing methodologies highlight the need of incorporating policies, processes, and technical controls into an information security management framework. Organizations with mature information security management systems typically include thorough documentation, regular evaluations, and organized continuous improvement procedures [11]. In contrast, ineffective audit planning and risk management can diminish the effectiveness of detecting errors and controlling weaknesses in digital-based information systems [12].

2.4 Implementation Gap and Best Practices in Security Audits

Studies on information security audit practices reveal a discrepancy between the current condition of information systems and recommended best practices. Although security controls have been adopted, they are frequently uneven, incompletely documented, and unsupported by continuing evaluation [13], [14]. This scenario exemplifies prevalent issues in adopting information system security governance in complex digital corporate environments.

Empirical research in a variety of industries indicates that integrated information system audits can improve the quality of security measures and information technology governance. However, many companies are still in the governance strengthening stage, in which controls are in place but have not yet reached an appropriate level of maturity [15], [16]. This gap is often associated with immature risk planning, poor operational documentation, and a lack of human resource expertise in information security aspects [17][18]19].

2.5 Security Monitoring and the Relevance of Previous Studies

Aside from technical aspects, the literature highlights the value of proactive monitoring and evaluation of information system security. Reactive monitoring systems are thought to be less successful at detecting possible threats early and preventing large-scale security incidents [20]. As a result, integration of technological controls and business processes is a critical prerequisite for improving information system security, particularly in high-value digital transaction systems.

According to research on framework-based information system audits and governance, operational and security controls are frequently functional but need to be strengthened in documentation, periodic evaluation, and continuous improvement. Based on [21] found that, while operational domains and security services have been implemented in web-based information systems, management capability remains at an intermediate level, necessitating stronger governance to ensure the sustainability and effectiveness of security controls.

3. RESEARCH METHOD

This study followed a rigorous methodological methodology to achieve a thorough and structured assessment of information system security on the trading platform. The first part of the research was determining the audit scope, which attempted to establish the boundaries of the information system, business processes, and security issues that would be evaluated. Determining this scope is critical to ensuring that the audit process is targeted and consistent with the characteristics of the commodity futures trading platform.

The following stage was data collecting, which included a documentary evaluation of information system security audit reports, internal policies, and operational processes, as well as interviews with information system management and oversight stakeholders. Furthermore, firsthand observation of the trading platform's operational processes was carried out to analyze the alignment between documented policies and their actual implementation. The collected data was then used as the foundation for the information system evaluation procedure.

The information system evaluation focused on three key areas: information system governance, operational procedures, and technology and security controls. At this point, each facet was examined to determine the efficacy of the applied security controls. The evaluation results were then utilized to determine the level of compliance of information system security controls, which were divided into three categories: conformity, partial conformity, and nonconformity. The third part of the research involves assessing the findings and synthesizing the audit results in order to uncover patterns of weaknesses and root reasons that affect information system security. Based on this analysis, the report reached conclusions and made recommendations for changes to commodity futures trading platforms' security controls and information system governance.

This study employs a descriptive qualitative approach and a case study methodology to acquire a thorough understanding of the implementation of information system security measures on the X Company trading platform. An information system audit is a framework for evaluating the efficiency of security measures, identifying control flaws, and auditing risks in digital-based systems [11, 12].

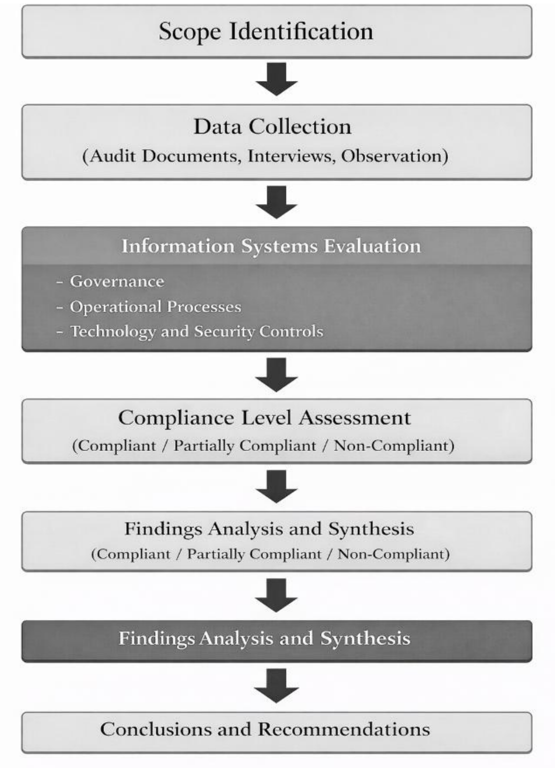
Scope Identification
Data Collection
(Audit Documents, Interviews, Observation)
Information Systems Evaluation
- Governance
- Operational Processes
- Technology and Security Controls
Compliance Level Assessment
(Compliant / Partially Compliant / Non-Compliant)
Findings Analysis and Synthesis
(Compliant / Partially Compliant / Non-Compliant)
Findings Analysis and Synthesis
Conclusions and Recommendations

Figure 1. Research Methodology Stages

4. RESULT AND DISCUSSION

4.1 General Results of Information System Audit

The results of the information systems audit show that Company X's trading platform includes an information security control architecture that facilitates the execution of commodity futures trading operations. The presence of policies, responsibility structures, and operational processes reveals that the business understands the significance of information system security in facilitating high-value, real-time transactions. This finding is consistent with the results of an examination of information system security in the digital business environment, which revealed that most firms have adopted basic to intermediate security controls [14].

However, the audit results revealed that the vast majority of security controls did not fully meet the compliance standards. Only the leadership and governance parts of information technology were deemed compliant among the seven audit aspects reviewed, with the remaining six deemed somewhat compliant. This shows that controls have been functionally implemented, but there are still gaps in implementation consistency, documentation completeness, and procedures for evaluation and ongoing improvement, as shown in Table 1.

Table 1. Summary of Trading Platform Information System Audit Results

No	IS Audit Aspect	Status of Implementation	Findings Notes	Clause ISO 27001:2022 Relevan	Requirement
1	Context and scope of the system	Partial compliant	The scope has not been updated regularly	*Clause 4.3 (Determining the scope of the ISMS)*	Defining ISMS boundaries and relevance to the organizational context
2	IT leadership and governance	Compliant	Roles and responsibilities have been defined	*Clause 5.1 & 5.2 (Leadership and commitment; Policy)*	Leadership is responsible for ISMS, establishing policies and responsibilities.
3	Information system risk planning	Partial compliant	Risk documentation is not consistent	*Clause 6.1 & Annex A.5-A.8 (Risk assessment and treatment, Information security objectives)*	Risk planning, threat evaluation, and mitigation according to business context
4	Resource management	Partial compliant	Security training is not structured	*Clause 7.2 (Competence), Clause 7.3 (Awareness)*	Employees should be competent and aware of information security through training.
5	Operational and control systems	Partial compliant	Procedure is not fully documented	*Clause 8.1 (Operational planning and control), Annex A.5 - A.8*	Technical controls and operational procedures must be documented and implemented.
6	Security monitoring and evaluation	Partial compliant	Follow-up of monitoring results is not yet systematic	*Clause 9.1 & 9.2 (Monitoring, measurement, analysis and evaluation; Internal audit)*	Periodic evaluation of ISMS performance, internal audits, and risk monitoring
7	Continuous improvement	Partial compliant	Perbaikan belum terdokumentasi formal	*Clause 10 (Improvement)*	Continuous improvement, corrective action and enhancement of ISMS

4.2 Distribution of Compliant Levels

The distribution of conformance levels across audit results shows that partial conformity predominates in all evaluated aspects. Six of the seven information system audit elements, or 86%, are classified as partial conformity, with only one aspect (14%) classified as conformity. No aspects are non-conformant.

This predominance of partial conformance suggests that information system security controls on Company X's trading platform are in place and operational, but have not yet reached an appropriate level of maturity. This distribution pattern reflects the overall state of companies in the security governance strengthening phase, where measures have been installed but have yet to be thoroughly documented and regularly reviewed. Table 2 details the conformance level dispersion.

Table 2. Summary of Distribution of Compliant Levels

Category	Total Findings	Persentase
Compliant	1	14%
Partial Compliant	6	86%
Non-Compliant	0	0%

4.3 Key Audit Findings

Several important results from the information systems audit could have an impact on the effectiveness of the trading platform's security procedures. The first finding is that information systems risk planning has not been updated on a regular basis. This condition could prevent new hazards or changes in the risk profile from being discovered in a timely manner.

The next finding was the lack of documentation for standard operating procedures (SOPs) guiding information system security measures. This insufficient documentation has the potential to cause inconsistencies in control application, especially when there are system modifications or people rotations. Furthermore, the audit discovered that information systems security training had not been structured, raising the risk of operational and human errors.

Monitoring and evaluation processes were in place, but follow-up on monitoring outcomes was inconsistent and not documented. Table 3 provides an overview of the important findings and their potential implications for information system security.

Table 3. Summary of Key Findings and Potential Impact

Clause and/or Annex Control	Findings	Dampak Potensial
CL.6.1.2 (Information security risk assessment) CL.6.1.3 (Information security risk treatment)	Risks have not been updated regularly	New risks were not identified in time
A.5.2 (Information security roles and responsible), A.8.32 (Change management)	IT Operational Procedure is not fully documented	Inconsistency in the application of controls
A.6.3 (Information security awareness, education, and training)	Security training is not structured	Operational errors and human error
CL.9.1.1 (Monitoring, measurement, analysis and evaluation)	Follow-up is not consistent	Repeated security flaws

4.4 Validity of Audit Result Data

The utilization of properly recorded primary data sources supports the legitimacy of this study's audit data. All audit tables and analyses are created using information system audit reports maintained in an internal audit spreadsheet. Each finding and conformance categorization can be linked to appropriate audit data.

This approach assures that the research conclusions are based on verifiable empirical facts, which increases the findings' credibility and dependability in the context of the Company X case study. As a result, the audit results reported accurately reflect the current level of information system security measures during the evaluation period.

4.5 Information System Technology Control Evaluation

The examination of technology controls revealed that Company X's trading platform has incorporated several technology controls to support transaction security, such as user access rights management, system infrastructure security, and a system activity recording mechanism. The presence of these controls shows that technology has been a major priority in information system security management.

However, the audit results showed that all aspects of technological controls remained in partial compliance. User access rights were not regularly checked, infrastructure security testing was limited, and system log analysis was not performed on a regular basis. Furthermore, technological risk management and incident response procedures were in place, but they were not supplemented by regular simulations and assessments. Table 4 presents an overview of the technology control evaluation results.

Table 4. Summary of IT Aspect Findings

Technology Security Aspect	Status	Finding
A.5.15 Access Control System	Parsial Compliant	Access rights have not been reviewed periodically
A.8.29 Security testing	Parsial Compliant	Protection exists, testing is limited
A.8.15 Logging & Monitoring	Parsial Compliant	Logs available, analysis not regularly
CL.6.1 IT Risk Management	Parsial Compliant	Technical risks have not been updated
A.5.24 and A.5.26 IT Incident Response and Recovery	Parsial Compliant	Procedures exist, simulations have not been performed

The table shows that technological controls are functionally in place, but have not yet reached the level of maturity expected for high-value transaction systems such as trading platforms.

4.6 Integration of Technology and Business Process Control

The audit results show that information system technology controls are still not properly linked with commodity futures trading business activities. Access control mechanisms, for example, are not adequately integrated with users' business roles and responsibilities, which increases the danger of access abuse. Furthermore, system monitoring techniques remain reactive, focusing on recording occurrences rather than early identification of anomalies or prospective cyberattacks. This circumstance demonstrates that technological controls are still viewed as an operational support role rather than an inherent part of business risk management. These findings indicate that increasing the integration of technology and business processes is a critical topic for strengthening the security of trading platform information systems.

4.7 Discussion

According to the study's findings, the majority of information system security safeguards are only partially compliant. This finding is consistent with prior study, which found that digital companies generally have security policies in place but encounter issues with documentation, implementation consistency, and continuing review.

Risk planning gaps suggest that information system risk management has not been implemented in an adaptive manner. This circumstance has the ability to impede companies from detecting emerging risks in dynamic digital transaction systems.

Weaknesses in operational control documentation highlight the significance of documentation as a critical component in the sustainability and accountability of information system security controls. Furthermore, the lack of structured security training suggests that technology measures should be balanced against increasing human resource competency.

Regarding monitoring, audit results show that information system security is still reactive and has not fully integrated into the continuous improvement cycle. However, proactive monitoring is essential for ensuring system reliability and market trust.

5. CONCLUSION

This analysis states that while information system security controls on Company X's commodity futures trading platform have been deployed as part of the system's operations, they have yet to reach an ideal level of maturity. The audit results show that, while security controls are in place and implemented, most are only partially compliant, particularly in areas such as risk planning, which has not been updated on a regular basis, incomplete operational control documentation, human resource competency that is not supported by structured security training, and mechanisms for continuous monitoring and improvement that have not been systematically implemented.

The findings of this study demonstrate that the presence of technological security controls does not ensure the effectiveness of information system security, especially on trading platforms with real-time and high-value transactions. Information system audits have proven to be a useful evaluation tool for identifying gaps between policy, implementation, and operational practices, as well as providing a foundation for developing more specific and risk-based improvement recommendations.

Practically, the findings of this study have implications for commodity futures trading businesses looking to improve the integration of technology controls, information system governance, and business processes. This improvement is intended to increase system reliability, reduce security threats, and maintain market participant confidence. More research is needed to combine information system audits with quantitative techniques, security maturity level measures, or security analytics to achieve a more comprehensive and impartial assessment.

REFERENCES

[1] M. Alshaikh, “Developing cybersecurity audit maturity models,” *Int. J. Inf. Manage.*, vol. 54, p. 102145, 2020.

[2] L. M. Fonseca and J. P. Domingues, “Information security governance and risk management,” *J. Ind. Inf. Integr.*, vol. 19, p. 100150, 2020.

[3] S. E. Chang, Y. C. Chen, and C. S. Lin, “Exploring information security governance in critical information systems,” *Inf. Syst. Front.*, vol. 22, pp. 1309–1324, 2020.

[4] J. Kwon and M. E. Johnson, “Security practices and financial performance in digital platforms,” *J. Cybersecurity*, vol. 7, no. 1, 2021.

[5] O. Ali, A. Shrestha, V. Osmanaj, and S. Muhammed, “Cloud computing security audit challenges,” *J. Cloud Comput.*, vol. 10, no. 1, pp. 1–18, 2021.

[6] I. A. Tøndel, M. B. Line, and M. G. Jaatun, “Information security incident management,” *Comput. Secur.*, vol. 92, p. 101746, 2020.

[7] C. Vroom and R. von Solms, “Towards cyber security maturity evaluation,” *Comput. Secur.*, vol. 105, p. 102242, 2021.

[8] P. F. Hsu, H. J. R. Yen, and J. C. Chung, “Assessing information security governance,” *Inf. Comput. Secur.*, vol. 29, no. 1, pp. 45–63, 2021.

[9] P. Ifinedo, “Security audit practices and organizational performance,” *Inf. Manage.*, vol. 58, no. 4, p. 103439, 2021.

[10] S. Al-Dhahri and A. Al-Sarti, “Auditing information systems in electronic trading environments,” *Int. J. Account. Inf. Syst.*, vol. 48, p. 100604, 2023.

[11] A. Ahmad, S. B. Maynard, and G. Shanks, “Information security management systems: A maturity perspective,” *Comput. Secur.*, vol. 105, p. 102237, 2021.

[12] B. Betri and D. Maidiana, “Pengaruh keefektifan audit sistem informasi dan risiko audit terhadap deteksi kesalahan,” *Balance*, vol. 10, no. 1, pp. 1–12, 2025.

[13] A. Ab Rahman and K. K. R. Choo, “Information security auditing: Trends and future directions,” *IEEE Access*, vol. 10, pp. 10411–10425, 2022.

[14] M. Alim, M. Rasyid, and A. P. Juledi, “Evaluasi keamanan sistem informasi dalam lingkungan bisnis digital,” *J. Ilmu Komput. Sist. Inf.*, vol. 7, no. 1, pp. 328–332, 2024.

[15] S. Serliana and J. N. Utamajaya, “Pendekatan terintegrasi audit sistem informasi,” *J. Ilm. Sains Teknol. Inf.*, vol. 3, no. 2, pp. 45–58, 2025.

[16] R. Wijaya and H. Santoso, "Evaluasi pengendalian keamanan informasi," *J. Inf. Syst. Eng.*, vol. 9, no. 1, pp. 15–28, 2024.

[17] A. Purnomo and Y. Nugroho, "Audit keamanan sistem informasi pada layanan transaksi elektronik," *J. Sist. Inf.*, vol. 20, no. 2, pp. 89–102, 2024.

[18] A. Alruwaili and S. R. Gulliver, "Information systems risk assessment in financial platforms," *J. Inf. Secur. Appl.*, vol. 65, p. 103102, 2022.

[19] E. Sutisna, "Evaluating security risks and the impact of analytic technology on the audit process," *Adv. Manag. Audit Res.*, vol. 3, no. 1, pp. 30–43, 2025.

[20] S. Choi and J. Lee, "Governance mechanisms for secure digital transaction systems," *Electron. Commer. Res.*, vol. 23, pp. 421–445, 2023.

[21] R. G. Faradilla, "AUDIT SISTEM INFORMASI MENGGUNAKAN COBIT 5 DOMAIN DSS001 DAN DSS005 (STUDI KASUS PERPUSTAKAAN UPN VETERAN JAWA TIMUR)", *JITET*, vol. 13, no. 1, Jan. 2025.