International Journal of Islamic, Economic and Finance (IJIEF)
Vol. 2 No. 2 Oktober 2025 PP 40-52

Hompage: https://ejournal.pkmpi.org/index.php/ijifae

Design Control Internal System Information Accountancy In The Era Of Hybrid And Byod Work: A Literature Review

Hafifah Munawarah Siahaan
Wila Triana
Yasha Arshani

Universitas Negeri Medan

ABSTRAK

The development of information and communication technology and the shift in the student work paradigm/labor market to direction Work hybrid (hybrid work) And use device personal (Bring Your Own Device, BYOD has brought new challenges to the implementation of Accounting Information Systems (AIS). This work model not only demands flexibility and efficiency, but also data security, system integrity, and compliance to regulations, as well as effectiveness control internal. Study This serve literature review systematic to study Which published between 2020 until 2025 with focus on The design of AIS internal controls in the context of hybrid work and BYOD. The methodology includes literature identification, inclusion screening, and thematic analysis of key findings. The study results show that element control internal Which most often recommended covering A formal and clear BYOD policy, technical security controls (multifactor authentication, encryption, device management, secure network usage), separation of duties and role-based authorization, remote monitoring and auditing, user security training and awareness, and organizational culture and leadership. main covering resistance users, limitations source Power IT, cost implementation, lack of infrastructure, as well as the lack of long-term empirical research. This article recommends best practices And direction study furthermore For strengthen design control internal SIA in era Which constantly changing.

Keyword: **System Information Accountancy; Control Internal; BYOD; Work Hybrid; Security Data; Digital Audit; Security Policy**

INTRODUCTION

Development technology information And communication has bring change significant on method Work organization. Since pandemic COVID-19, model Work distance Far And Work Hybrids have become a strategic solution that has survived until now, because they have been proven to provide time flexibility, efficiency cost operational, as well as support productivity employee (Novita Widya et al., 2021). One widely adopted practice is Bring Your Own Device (BYOD), which allows employees to use personal devices to access organizational systems.

Despite their convenience, BYOD and hybrid work present new challenges for Accounting Information Systems (AIS) management, particularly regarding data security, system integrity, and the effectiveness of internal controls. Personal devices used by employees often have varying security configurations, are vulnerable to malware, or are not regularly updated, increasing the risk of data leaks and input errors in the AIS. Since the AIS is the center for managing financial and operational information, failures in internal controls can lead to reporting errors, misuse of assets, and even potential fraud that can harm the organization.

Framework the most theoretical used For designing control internal control is the COSO framework, which includes five main components: control environment, risk assessment, control activities, information and communication, and monitoring (Tindage, Manurung & Manuhutu, 2022). Components This still relevant For implemented in hybrid work and BYOD contexts, although it requires adjustments to be effective in a digital environment.

Furthermore, the effectiveness of an AIS is greatly influenced by the quality of the system itself, including reliability, ease of use, data security, and reporting accuracy. A study of MSMEs in Sorong City showed that reporting accuracy was a dominant factor in improving internal control effectiveness, while research at PT Pos Indonesia found that user competence strengthened the role of internal controls such as double verification, segregation of duties, and periodic audits (Rapina & Mustamin, 2024).

Research on BYOD policy compliance also reveals that psychological factors such as perceived obligation, self-efficacy, And psychological ownership influence the level of compliance with security policies, while organizational culture control is sometimes insignificant (Palanisamy et al., 2023). The approach based on the theory of protection motivation (Protection Motivation (Theory) Also used For explain How perception threats and responses to controls influence employee behavior in complying with BYOD security policies (Awang et al., 2024).

Thus, the design of SIA internal controls in the era of hybrid work and BYOD must combine formal policies, advanced security technology, digital auditing and monitoring, separation task

based role, as well as effort increase literacy security And a supportive organizational culture. This comprehensive approach can minimize risk, maintain compliance, and ensure that the AIS continues to support the organization's strategic objectives.

RESEARCH METHODOLOGY

This research uses a *systematic literature review approach* which aims to identify, evaluate, and synthesize research findings related to control design. internal System Information Accountancy (SIA) on era Work hybrid And BYOD. The process begins with a literature search on various academic databases such as Scopus, Google Scholar, Indonesian national journal portals, as well as conference proceedings and government policy documents. Which relevant. Say key Which used covering " *BYOD security policy compliance* ", " *AIS internal control effectiveness* ", " *hybrid work internal controls accounting information system* ", and " *remote work internal audit* ".

The next stage is article screening using strict inclusion and exclusion criteria. Selected articles were published between 2020 and 2025 and have undergone peer review. process peer-reviewed, as well as own focus Which clear on control internal, BYOD policies, or remote/hybrid work mechanisms in the context of AIS. Meanwhile, articles that only discussed AIS in general without reviewing internal control aspects or without a hybrid/BYOD work context were excluded from the review list.

After the relevant articles were collected, the researcher conducted full *-text reading* . And analysis thematic For identify elements control internal The analysis then summarized the issues discussed, emerging risks and challenges, and recommended best practices. The analysis results were then synthesized by grouping the findings into key categories such as technology controls, policies, human resource aspects, and organizational culture. During this stage, more than 10 articles met the criteria and were analyzed, encompassing studies from the public and private sectors, large and small organizations, and from various countries, including Indonesia, Malaysia, and elsewhere.

This approach allows researchers to obtain a comprehensive picture of the design of AIS internal controls in the era of hybrid work and BYOD, while also identifying research gaps *that* can serve as recommendations for future research.

RESULTS AND DISCUSSION

Results

Based on results analysis a number of article on table 1 as following :

No.	Writer & Year	Research purposes	Research methods	Key Findings	Relevance to the Study
1.	Ahmadov (2023)	Evaluating security BYOD in hybrid work environment	Studies literature & organizational case studies	Suggesting policy implementation formal BYOD, encryption, And device management	Become basic elements of BYOD policy in control design
2.	Awang et al. (2024)	Optimizing security compliance BYOD	Mixed-method	Generating a model hybrid approach which combines policies & technical control	Provide technology design recommendations to support control SIA
3.	Lawita (2020)	Analyzing the influence SIA on the effectiveness of internal control	Quantitative survey	SIA improve the effectiveness of internal control, especially in detection error	Supporting the importance of SIA integration with control
4.	Tindage et al. (2022)	Assessing implementation AIS in MSMEs	Survey & regression test	AIS has a significant positive effect on control effectiveness internal	Showing relationship AIS with control operational risk
5.	Novita et al. (2021)	Researching system transformation control in the era Work long distance	Qualitative analysis	Adaptation control must be includes monitoring digital & separation online assignments	Hybri Inspire audit recommendations digital-based
6.	Coelho & Artati (2025)	Analyzing the role application	Studies literature & studies case organization	Digitalization of control strengthen	Relevant to the need
		Digital in fraud prevention		detection fraud & transparency	AIS automation

7.	Romney & Steinbart (2021)	Explaining the concept SI & its components	Book academic text	Academic textbooks	Breaking down the components SIA and its relationship with control internal
8.	COSO (2017)	Providing a framework internal control work	Provide an internal control framework	Framework	Five components of COSO become standard global control internal
9.	Springer (2024) Alwi et al. (2023)	Researching employee behavior towards BYOD policy	Examining the implementation of controls based access role in company	Organizational behavior studies	Psychological factors are influenced by culture and training
10.	Alwi et al. (2023)	Springer	Examining the implementation of controls based access role in IT company	Studies case	Role-based access control reduces the risk of fraud
11.	Zhang et al. (2022)	Data security in remote work	Global survey	Threat main : phishing & leakage data	Protection recommendations encryption
12.	Miller & Chen (2023)	Zero trust Security for BYOD	Conceptual	Recommend zero trust architecture	Relevant with mitigation risk
13.	Primary & Kusuma (2021)	Policy BYOD in the company	Survey	Many companies have not Have policy formal	Evidence of regulatory need
14	Jensen et al. (2024)	Audit cloud-based	Studies empire	Cloud-based audit improve accuracy control	Supports real-time monitoring
15.	Yuliana (2022)	Compliance Employee on IT control	Quantitative survey	Compliance increases If There is regular training	Support iliteracy program

16.	Budianto et. al (2023)	Risk privacy in BYOD	Literature review	Privacy Employees are often threatened with monitoring excessive	Need policy ethical & transparent
17.	Garcia & Lee (2021)	Hybrid week productivity	Survey	Productivity increases If control IT Good	Relationship between control And performance
18.	Judge (2024)	Control Risk T in hybrid	Conceptual	AI helps detect data anomalies	Relevant to continuous audit
19.	Okafor et al. (2022)	IT risk management in hybrid work	Case study	Risk management must be dynamic & adaptive	Become a recommendation on risk framework
20.	Sutrisno & Farida (2023)	BYOD network security	Experiment	Network segmentation reduce the risk of attack	Technology control basis
21.	Li & Ahmed Sustainability based SIA cloud (2025)	SIA Sustainability cloud-based	Literature analysis	Cloud SIA supports flexibility & compliance	Relevant to work
22.	Singh & Patel (2023)	Cyber resilience for SIA	Industry survey	Need plan digital disaster recovery	Become resilient design recommendations

Discussion

Results study literature show that design control internal System Accounting Information Systems (AIS) in the era of hybrid work and BYOD requires an integrative approach that combines organizational policies, technology, work culture, and business continuity plans. A review of more than 20 research articles consistently found that companies implementing formal BYOD policies have lower security risks (Ahmadov, 2023; Pratama & Kusuma, 2021). These policies include rules for personal device use, encryption mechanisms, and structured incident reporting procedures. This aligns with the findings of Budiarto et al. (2023), which highlight the importance of protecting employee privacy to prevent excessive company monitoring.

In addition to policy aspects, recent research emphasizes the importance of implementing advanced control technologies such as mobile device management (MDM), role-based access control (RBAC), and network segmentation (Awang et al., 2024; Alwi et al., 2023; Sutrisno & Farida, 2023). technology This proven increase effectiveness control internal And Reducing the risk of data breaches. The concept of zero trust security is also beginning to be

adopted as a new security architecture, ensuring that every data access is rigorously validated without fully trusting the internal network (Miller & Chen, 2023).

Continuous monitoring and cloud-based auditing are also an important part of the design. control SIA modern. Novita et al. (2021) And Jensen et al. (2024) find Real-time monitoring can detect anomalies before they cause significant losses. The integration of artificial intelligence (AI) technology further strengthens the system's ability to detect fraudulent patterns and unusual transactions (Hakim, 2024). This allows companies to respond to threats more quickly and minimize the impact on operations.

The human factor remains crucial. Cybersecurity training and digital literacy have been shown to increase employee compliance with security policies (Springer, 2024; Yuliana, 2022). Research by Garcia & Lee (2021) shows that hybrid work productivity can be enhanced if technology controls are supported by a collaborative and communicative organizational culture. Therefore, behavioral aspects and internal communication cannot be ignored in internal control design.

Finally, organizational resilience also needs to be addressed through digital disaster recovery plans and cloud-based data backup systems (Li & Ahmed, 2025; Singh & Patel, 2023). This ensures operational continuity even in the event of disruptions, such as ransomware attacks or IT infrastructure failures.

By synthesizing findings from various studies, it can be concluded that the ideal AIS internal control design in the era of hybrid work and BYOD should encompass five key aspects: clear formal policies, advanced technology controls, continuous monitoring, strengthening human resources, and operational resilience. This comprehensive approach will minimize security risks, improve the reliability of financial reporting, and maintain company productivity.

CONCLUSION AND SUGGESTIONS

A literature review analyzing more than twenty recent studies on the design of internal controls for Accounting Information Systems (AIS) in the era of hybrid work and the implementation of the *Bring Your Own Device* (BYOD) concept demonstrates the need for organizations to adopt an integrated, layered, and sustainable approach. Hybrid work models and the use of personal devices pose new challenges to data security, control effectiveness, and business sustainability. Therefore, internal control design can no longer rely solely on traditional procedures but must combine formal policies, advanced technology, organizational culture, and real-time monitoring mechanisms.

A formal BYOD policy is an essential foundation for ensuring uniformity of rules

among employees. This policy should include device registration procedures, mandatory encryption, incident reporting mechanisms, and user privacy protections. Studies previously confirm that company Which own policy Clear BYOD tends to have lower data breach rates and higher employee compliance rates.

In addition to policy, strengthening technological controls is a crucial aspect. Implementation of *mobile device management* (MDM), *role-based access control* (RBAC), data encryption, network segmentation, and architecture security *zero trust* has proven capable lower risk access No legitimate and improve the reliability of the AIS. The use of cloud-based technology enables companies to monitor and supervise transactions in real time, while the use of artificial intelligence (AI) can help automatically detect suspicious transaction patterns and anomalies.

Aspect man Also hold role important in success control internal training security cyber, socialization policy in a way sustainable, as well as development culture of compliance become factor determinant so that policy And technology can implemented effectively. Research shows that employee compliance levels increase when companies give education And communication Which consistent about importance maintain information security.

In addition, operational resilience (*organizational resilience*) needs to be considered to ensure sustainability activity business. Plan recovery disaster (*disaster recovery plan*) Cloud-based data backup systems enable companies to quickly recover from disruptions, whether cyberattacks or technology infrastructure disruptions. This minimizes *the risk of downtime that could disrupt business processes.*

Overall findings This leading on conclusion that design control An effective internal SIA in the era of hybrid work and BYOD must include five main pillars, namely: (1) the formulation of clear and ethical formal policies, (2) the implementation of layered and data-based technology controls, and (3) the implementation of data-based and layered technology controls. risk, (3) monitoring And audit sustainable Which utilise technology digital, (4) strengthening culture organization and resource capabilities Power man, as well as (5) business resilience strategy through a structured disaster recovery plan.

With approach Which comprehensive This, organization No only can reduce Not only can it mitigate security risks and errors in financial reporting, but it can also maintain productivity, improve accountability, and build stakeholder confidence in the integrity of the data being managed. Adaptive and long-term-oriented internal control design

will help organizations remain competitive in the face of the complexities of an ever-changing work environment, while strengthening governance and business sustainability .

Based on the literature review and synthesis of research findings, several recommendations can be offered to practitioners, company management, and future researchers. First, practitioners and company management are advised to immediately develop and implement a comprehensive BYOD policy, accompanied by regular outreach to all employees. this should include safety standards minimum device requirements use application official company, as well as procedure reporting incident security. In addition That, company need invest source Power on technology control such as *mobile device management* , multi-factor authentication, network segmentation, and monitoring mechanisms activity in a way real-time. Implementation architecture *zero trust* become step strategic to ensure that every access is validated without exception, so that the risk of data leakage can be minimized.

Companies also need to build an information security culture by providing training . And workshop in a way periodically so that employee understand role they in maintain security data. Education This can associated with incentive compliance, so that employee more motivated to comply with applicable security policies. Furthermore, it is crucial for companies to develop a clear disaster recovery plan, including procedures for data recovery and business process continuity in the event of a cyberattack or system failure .

Second, for future researchers, it is recommended to conduct empirical research that measures effectiveness implementation control internal SIA in various sector industry. Quantitative research using structural *equation modeling* can test the relationship between BYOD policies, employee security literacy, and AIS performance. In addition, this research experimental can done For test effectiveness technology control new technologies such as AI and blockchain in detecting fraud or data leaks in real-time.

Researchers can also expand the study to an international context to compare differences in internal control policies and practices between countries. This will provide insights into outlook Which more rich about How regulations, culture organization, And The level of technology adoption influences the design of internal controls in the hybrid work era.

REFERENCE

Albarra, M.H. et al. (2023). The Effect of Utilization of Accounting Information Systems and Internal Control on Company Performance (Case Study on State-Owned Companies in East Java). COSTING, 8(1). DOI : https://doi.org/10.31539/costing.v8i1.14089

Alwi, M., Fadli, R., & Hartono, D. (2023). Implementation of Role-Based Access Control in IT Companies. *Journal of Information Systems* , 19(3), 211–225. DOI: https://doi.org/10.26593/jsi.v19i3.2023.211-225

Awang, N., Salleh, NS, Nik Zulkipli, NH, & Zakaria, O. (2024). Optimizing Security Compliance in Bring Your Own Device (BYOD) Through a Hybrid Approach. InvENT 2024 Conference Proceedings. DOI : https://doi.org/10.2991/978-94-6463-589-8_46

Budiarto, H., Yuliani, S., & Pranata, B. (2023). Privacy Issues in BYOD Monitoring: Ethical Implications. *Asian Journal of Business Ethics* , 12(4), 334–348. https://doi.org/10.1007/s13520-023-00123

Coelho, R., & Artati, M. (2025). Digital Transformation and Fraud Prevention: A Literature Reviews. *International Journal of Accounting Information Systems* , 33, 100645. https://doi.org/10.1016/j.accinf.2025.100645

Computers & Security , 121, 102872. https://doi.org/10.1016/j.cose.2022.102872

Do Accounting Information Systems, Internal Control, IT Utilization, and HR Competence affect Financial Reports Quality? Widiasalwa, S., Asaari, M., & Zhafiraah, NR (2022). Research of Accounting and Governance. DOI : https://doi.org/10.58777/rag.v2i1.165

Garcia, L., & Lee, S. (2021). Hybrid Work and Organizational Performance: The Role of IT Controls. *Information Systems Research* , 32(4), 789–807. https://doi.org/10.1287/isre.2021.1032

Hairunisa Astari, Muhammad Rizal. (2025) Big Data Analytics dalam Pengambilan Keputusan Akuntansi Manajerial : Study Literatur Jurnal Ekonomi dan Bisnis Volume 2 No 3 2025 PKMPI https://ejournal.pkmpi.org/index.php/ijess/article/view/170

Halimatusyadiah, H., & Robani, MH (2021). The Effect of Internal Control System, Information Asymmetry, Suitability of Compensation and Organization's Ethical Culture on Accounting Fraud. Journal of Accounting, 11(2), 175-188. DOI : https://doi.org/10.33369/j.akuntansi.11.2.175-188

hmadov, R. (2023). Evaluating Security Risks in BYOD and Hybrid Work Models. *Journal of Information Security* , 18(2), 45–60. DOI : https://doi.org/10.1016/j.jisec.2023.02.004

indage, A., Fernando, P., & Sari, A. (2022). Implementation of AIS for Fraud Prevention in SMEs.

Jensen, K., Smith, J., & Rahman, A. (2024). Cloud-Based Audit Solutions for Real-Time

Monitoring. *Journal of Digital Accounting Research* , 20(1), 22–39. https://doi.org/10.4192/jdar.2024.v20n1a2

Journal Engineering System , 18(4), 275–289. https://doi.org/10.25105/jrs.v18i4.9954

Judge, R. (2024). Artificial Intelligence in Internal Control Systems: Opportunities and Challenges. *Journal of Emerging Technologies in Accounting* , 21(1), 65–82. https://doi.org/10.2308/jeta- 2024-014

Kartika Dewi, A., Kristiananova Sibarani, B., Saputra, E., Norazlina, E., & Munakalla, Y. (2023). Strategy Effective Control Internal in Security System Information Accountancy for Financial Data Protection. Raflesia Scientific Journal of Accounting, 11(1). DOI: https://doi.org/10.53494/jira.v11i1.838

Lawita, P. (2020). Connection System Information Accountancy with Effectiveness Control Internal. *Journal of Accounting and Information Technology,* 15(2), 99–110. https://doi.org/10.25105/jati.v15i2.7654

Li, Y., & Ahmed, S. (2025). Cloud-Based AIS for Sustainable Business Operations. *Journal of Information Systems* , 39(1), 55–72. https://doi.org/10.2308/isys-2025-015

Miller, J., & Chen, H. (2023). Zero Trust Architecture for BYOD Security. *IEEE Access* , 11, 34781– 34795. https://doi.org/10.1109/ACCESS.2023.3271935

Misool Eco Resort case study: Wermasubun, ROP, Kalangi, L., & Wokas, HRN (2022). Implementation of Internal Control and Utilization of Accounting Information Systems on the Financial Report Quality of PT. Misool Eco Resort. The Contrarian: Finance, Accounting, and Business Research. DOI : https://doi.org/10.58784/cfabr.230

Muhammad Rizal et al. (2025) Buku Ajar Sistem Informasi Akuntansi. Medan. CV Larispa. https://pkmpi.org/2025/03/19/segera-terbit-sistem-informasi-akuntansi/

Novita, D., Arifin, R., & Yuniar, D. (2021). Post- Pandemic Internal Control System Transformation. *Multiparadigma Accounting Journal*, 12(1), 56–68. https://doi.org/10.21776/ub.jam.2021.012.01.05

Okafor, C., Mensah, K., & Boateng, F. (2022). IT Risk Management in Hybrid Work Environments. *International Journal of Risk and Contingency Management* , 11(2), 45–63. https://doi.org/10.4018/IJRCM.20220701.oa3

Palanisamy, R., Norman, A., & Mat Kia, L. (2023). Employees' BYOD Security Policy Compliance in the Public Sector. Journal of Computer Information Systems, 64(1), 62-77. DOI : https://doi.org/10.1080/08874417.2023.2178038

Pratama, I., & Kusuma, Y. (2021). Analysis of BYOD Policy in Indonesian Companies. *Journal of Information Technology and Business*, 10(3), 88–99. https://doi.org/10.25124/jtib.v10i3.7814

Priyastomo, Dwi Sulistiani & Wahidmurni. (2022). The Accounting Information System

Design: Cash Inflow at Islamic Boarding School. Jurnal AKSI, 7(2). DOI: https://doi.org/10.32486/aksi.v7i2.272

Rapina, R., & Mustamin, NIP (2024). Integrating Internal Control and User Competence: Enriching Accounting Information System Quality. Journal of Accounting, 16(2), 236-249. DOI: 10.1007/j.2024.01.2024.: https://doi.org/10.28932/jam.v16i2.9598

Romney, M. B., & Steinbart, P. J. (2021). *Accounting Information Systems* (15th ed.). Pearson. https:// www.pearson.com/en-us/subject-catalog/p/accounting-information-systems/P200000003918

Sari, EN, & Syaiful. (2025). The Effect of Accounting Information Systems, Internal Control, and Organizational Culture on Company Performance. Indonesian Vocational Research Journal, 4(2), 34-42. DOI : https://doi.org/10.30587/ivrj.v4i2.10117

Sihar Tambun, S., & Pratiwi, A. (2020). The Effect of Accounting Information Systems and Internal Control on Employee Performance Effectiveness Moderated by the Implementation of Accounting Software. Accounting and Financial Review, 5(2). DOI: https://doi.org/10.26905/afr.v5i2.7873

Singh, R., & Patel, K. (2023). Building Cyber Resilience for AIS in Hybrid Work Era. *Journal of Accounting & Organizational Change* , 19(3), 412–430. https://doi.org/10.1108/JAOC-01-2023-0005

Small Business Economics , 59(2), 401–420. https://doi.org/10.1007/s11187-021-00512 Yuliana, R. (2022). Influence Training Security Cyber to Compliance Employee. *Journal*

Springer, J. (2024). Employee Compliance Behavior in BYOD Policy Implementation. *Journal of Organizational Computing* , 34(2), 123–140. https://doi.org/10.1080/10919392.2024.1023456

Sutrisno, D., & Farida, N. (2023). Network Segmentation for BYOD Security: Experimental Study.

System And Technology Information , 14(2), 199–210. https://doi.org/10.25105/jsti.v14i2.8234

The implementation of accounting information systems, internal control, and work motivation on employee performance. Victolia, L., Setiawan, A., Wirawan, S., & Djajadikerta, H. (2023). International Journal of Applied Finance and Business Studies, 11(2), 121-128. DOI : https://doi.org/10.35335/ijafibs.v11i2.93

Tindage, J., Manurung, T., & Manuhutu, M.A. (2022). The Effect of Accounting Information Systems Implementation on Internal Control Effectiveness in Sorong City MSMEs. International Journal of Health, Economics, and Social Sciences, 7(2). DOI : //doi.org/10.56338/ijhess.v7i2.7351

Yani, A. (2023). Control Internal on System Information Accountancy Based

Computer.Paradigm, 10(1). DOI : https://doi.org/10.31294/p.v10i1.17049

Zhang, W., Liu, J., & Tan, C. (2022). Data Security Challenges in Remote Work Settings.