Analysis of Academic Scheduling Management Using ISO/IEC 27001:2022 People Controls

Yolan Dita Dewi Pramudita[1], Wiwin Sulistyo[2], Irwan Sembiring[3]
Department of Information Systems, Faculty of Information Technology
Satya Wacana Christian University, Salatiga, Indonesia
[1]972022016@student.uksw.edu, [2]wiwinsulistyo@uksw.edu, [3]irwan@uksw.edu

Abstract— User behaviour plays a critical role in determining the effectiveness of academic information system management, particularly in processes requiring high data accuracy and timeliness, such as academic scheduling. Despite system support, inconsistencies in data provision and updates indicate that information reliability is influenced by how users perform their responsibilities. This study evaluates People Controls based on ISO/IEC 27001:2022 Annex A.6 and integrates COBIT–CMMI to measure capability levels from a behavioural perspective. A qualitative approach was employed through observation and structured interviews with key stakeholders involved in academic scheduling. User activities were mapped to Annex A.6 controls to identify implementation gaps, followed by capability level assessment using COBIT–CMMI. The results show that control implementation is largely informal and habit-based, with an overall capability level of Level 2 (40%). User behaviour demonstrates basic control execution but lacks consistency and standardization, particularly affecting data accuracy and timeliness, which leads to misalignment between data availability and operational needs. These findings emphasize that improving information security requires strengthening consistent user behaviour, role accountability, and structured practices, alongside technical system support.

Keywords— Academic scheduling management, COBIT–CMMI, ISO/IEC 27001:2022, User behavior

I. INTRODUCTION

User behavior in carrying out responsibilities when using academic information systems constitutes a critical factor influencing the effectiveness of service management in higher education institutions [1], [2], [3]. The reliability of a system is influenced not only by technological aspects, but also by users' compliance with procedures, accuracy in data management, and ability to maintain information integrity [4], [5]. This indicates that users are not only involved in operational activities but also play a critical role in determining the quality and reliability of academic information at the institutional level [6].

The management of course scheduling involves intensive interactions among users with diverse roles within the academic information system [7], [8], [9]. This process involves coordination in schedule arrangement, lecturer assignment, and classroom allocation. Course scheduling in higher education institutions in Indonesia is a complex administrative process that relies on the accuracy, timeliness, and discipline of users in operating academic information systems. Indonesian universities have increasingly adopted integrated academic information systems to improve scheduling efficiency and support academic decision-making. However, operational challenges remain common across institutions, including delays in data entry and inconsistencies in schedule updates [10], [11], [12], [13]. The issues collectively affect

the quality of academic information services and the effectiveness of institutional operations.

Similar challenges are also observed at Satya Wacana Christian University. Although the implementation of SIASAT (Satya Wacana Academic Information System), the university's integrated academic information system, has contributed to improved scheduling efficiency, similar issues persist, particularly regarding the timeliness of data provision and the accuracy of data entry. These conditions subsequently affect information quality, coordination effectiveness, and the continuity of academic services.

This condition indicates that the effectiveness of academic scheduling management does not solely depend on the capability of technical systems, but also on the consistency of user behavior in maintaining data integrity in accordance with their respective roles and responsibilities. Initial interview findings reveal the presence of dynamics in the execution of processes by involved parties during the course data management period, which influence the smoothness of the registration process and constitute part of the feedback on academic service delivery. Misalignment between the availability of course data in the academic information system and the student registration period is still observed in certain cases, resulting in information that is expected to be available not being fully accessible.

In addition, class capacity planning based on projected participant numbers in some cases requires further adjustment, as some students have not obtained classes that meet their needs and are required to submit additional requests. This condition indicates opportunities for improvement in data management and inter-role coordination to support the integration of the academic scheduling process. It further highlights that behavioral aspects and coordination patterns among roles contribute significantly, and therefore should be incorporated into a systematic evaluation based on a human-centered information security control framework to identify gaps and areas for improvement.

Several studies in the field of information security indicate that human factors constitute a key element, particularly in aspects of security awareness, role clarity, and policy compliance [14], [15], [16], [17], [18]. This becomes particularly critical in environments such as academic scheduling, where data accuracy and timeliness are directly dependent on consistent user behavior. Within the SIASAT environment, examined information security management from a risk management perspective by assessing risks related to infrastructure, software, hardware security, and human resources [19]. Nevertheless, the behavioural aspects of information security control implementation, particularly those related to user responsibilities and behavioural consistency, were not specifically addressed. This limitation is also reflected in the broader literature, which predominantly focuses on policies, technical controls, and risk management rather than People Controls from a behavioural perspective [20], [21], [22], [23].

ISO/IEC 27001:2022, particularly within the People Controls domain (Annex A.6), emphasizes the importance of human-related controls in supporting information security [24], [25]. This approach positions humans as a key element in maintaining the confidentiality, integrity, and availability of information through aspects such as security awareness, training, and behavior in performing responsibilities in accordance with established policies [26]. However, the standard primarily evaluates control implementation from a compliance perspective and does not explicitly measure

ISSN 2442-7888 (online) DOI 10.24167/Sisforma

how consistently these controls are enacted through user behaviour [27]. To address this limitation, the COBIT–CMMI capability model is employed to provide a structured mechanism for assessing the maturity of control implementation, particularly in capturing behavioural consistency in practice, ranging from initial conditions to managed and optimized processes [28]. The integration of these two frameworks results in an evaluation approach that not only focuses on the implementation of controls, but also on the systematic and consistent measurement of their implementation capability levels.

The context of academic scheduling within academic information systems presents inherent complexities, as it involves coordination across multiple roles and depends significantly on data accuracy and timeliness [29]. In this context, the reliability and availability of information are closely associated with how users execute their assigned responsibilities.

While prior studies predominantly focus on technical security controls, policy compliance, and system performance, limited research has specifically examined People Controls from a behavioural perspective within Indonesian higher education institutions. This study addresses that gap by integrating ISO/IEC 27001:2022 People Controls (Annex A.6) with the COBIT–CMMI capability model to assess the consistency and maturity of user behaviour in academic scheduling management. By highlighting the role of behavioural implementation, this study contributes a more human-centric approach to information security assessment in higher education environments.

This study aims to analyze the implementation of People Controls with a focus on user behaviour. It provides an assessment of capability levels and establishes a basis for formulating recommendations to enhance information security and improve the reliability of academic scheduling management.

II. METHOD

A. RESEARCH DESIGN

This study was conducted using a qualitative approach to evaluate the implementation of information security controls based on the ISO/IEC 27001:2022 standard, with a focus on the People Controls domain (Annex A.6). The evaluation was focused on user behavior in carrying out roles and responsibilities within the management of academic scheduling.

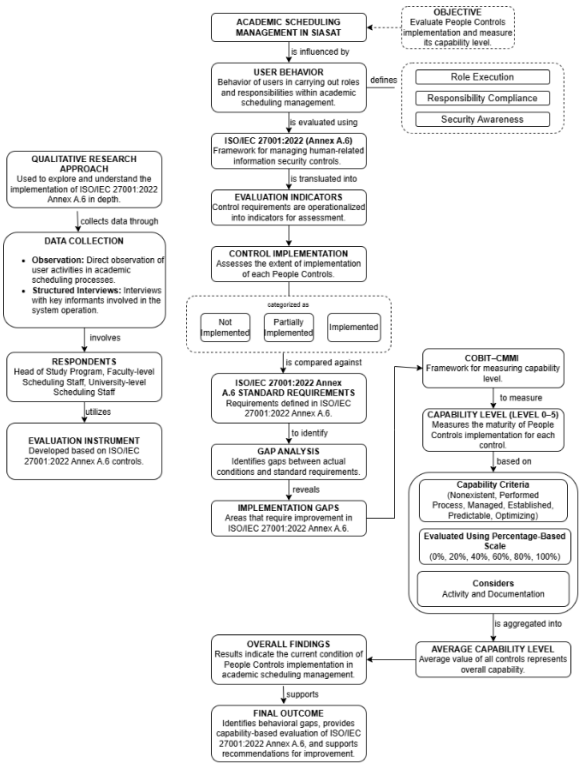

Figure 1. Concept Map of the Research Framework

Figure 1 illustrates the conceptual framework of the study, highlighting the relationships among the main components, with user behavior positioned as the central aspect within the ISO/IEC 27001:2022 People Controls domain (Annex A.6). The standard is applied to evaluate the implementation of behavior-based controls

ISSN 2442-7888 (online) DOI 10.24167/Sisforma

and to identify gaps between current practices and defined requirements. The identified gaps are subsequently assessed using the COBIT–CMMI approach to determine the capability level of control implementation. This representation outlines the integration of compliance-based evaluation and capability-based assessment within the proposed research framework.

B. DATA COLLECTION

The research object was located within the Faculty of Information Technology at Satya Wacana Christian University. Data were collected through direct observation of user activities and structured interviews with individuals involved in the operation of the academic information system. The interviews were conducted with three respondents, namely the Head of Study Program, faculty-level scheduling staff, and university-level scheduling staff, who were selected based on their direct involvement in the academic scheduling process.

The selected informants possess direct authority, operational responsibility, and decision-making involvement in the academic scheduling process. The three selected roles—Head of Study Program, faculty-level scheduling staff, and university-level scheduling staff—represent different layers of responsibility, including academic planning, faculty-level operational execution, and university-level coordination for general course management. This role-based selection provides comprehensive insights into user behaviour across hierarchical functions, thereby strengthening the validity and depth of the findings.

The instrument consisted of 25 questions developed based on ISO/IEC 27001:2022 Annex A.6 controls and mapped into evaluation indicators to identify the implementation of user roles and responsibilities, including aspects of security awareness and compliance with procedures.

C. DATA ANALYSIS

Analysis was conducted by mapping academic scheduling management activities to the controls defined in ISO/IEC 27001:2022 Annex A.6. Each control was translated into evaluation indicators to assess the implementation of People Controls. The level of control implementation was measured using the categories not implemented, partially implemented, and implemented, which represent levels of adoption ranging from absence of implementation to consistent application.

The assessment results were then used to identify gaps between the actual conditions and the established standards. The detailed control mapping is presented in Table 1.

Table 1. Mapping of ISO/IEC 27001:2022 Annex A.6 Controls

Annex A.6	Assessment
Screening	Ensuring that individuals involved demonstrate integrity and possess the required competencies in performing their assigned roles.
Terms and Conditions of Employment	Adherence to work regulations and consistency in task execution
Information Security Awareness, Education, and Training	Compliance with standard operating procedures (SOPs), accuracy of data entry, and awareness of data errors
Disciplinary Process	Adherence to organizational policies and responsiveness to system-generated corrections
Responsibilities After Termination or Change of Employment	Compliance with responsibility transfer procedures and prevention of unauthorized access
Confidentiality or Non-Disclosure Agreements	Compliance with data confidentiality requirements and avoidance of unauthorized information disclosure
Remote Working	Adherence to secure access practices and accuracy in remote data entry
Information Security Event Reporting	Timely reporting response and awareness of data anomalies

D. CAPABILITY ASSESSMENT

The results of the gap analysis were subsequently integrated with the COBIT–CMMI approach to measure the capability level of each control. The measurement was conducted using a Level 0 to Level 5 scale, which represented the maturity level of control implementation.

Capability values were obtained by converting the results of the control implementation evaluation into COBIT–CMMI capability levels based on process maturity criteria. The conversion process was carried out by mapping the level of activity execution for each control against COBIT–CMMI indicators (Level 0–5), which included aspects of activity existence, level of management, and process documentation.

The final value for each control was calculated based on this mapping to represent the maturity level of People Controls implementation individually.

Subsequently, the average capability value was calculated by summing all control values and dividing the result by the total number of controls analyzed. This average value was used to represent the overall capability level of People Controls implementation in academic scheduling management.

The obtained values indicated the capability position of each control as well as the overall implementation condition as a basis for evaluating People Controls. The assessment scale used is presented in Table 2.

Table 2. COBIT–CMMI Capability Level Assessment Scale

Level	Name	Description	Assessment	Percentage
0	Nonexistant	Controls are not implemented in the academic scheduling management process	No procedures, activities, or evidence of control implementation are present	0
1	Performed Process	Control implementation is performed in a reactive manner without formal planning	Activities depend on individuals and lack clearly defined standard operating procedures (SOPs)	20
2	Managed	Control activities are performed repeatedly but are not formally documented	Recurring work patterns exist but are not consistently applied across users	40
3	Established	Standard operating procedures (SOPs) have been established and implemented in the academic scheduling process	SOPs are available and used as a reference for task execution	60
4	Predictable	Control implementation is monitored and measured on a regular basis	Monitoring, evaluation mechanisms, and control performance indicators are established	80
5	Optimizing	Control activities are continuously improved based on performance measurement results and organizational learning.	Measurement results are regularly reviewed and used to enhance procedures, user behaviour, and control effectiveness.	100

III. RESULTS AND DISCUSSION

A. RESULTS

A.1 GAP ANALYSIS (ISO/IEC 27001:2022 ANNEX A.6)

The initial analysis was conducted based on ISO/IEC 27001:2022 Annex A.6 to identify the current state of People Controls implementation from a user-behaviour perspective. The results indicate that the application of human-related controls is predominantly characterized by informal practices and individual-based habits. This is reflected in user behaviour that relies heavily on personal understanding, direct communication, and organically developed working practices, without being fully supported by structured and formalized mechanisms.

Furthermore, user interactions are largely driven by short-term operational needs rather than consistent adherence to policy-based controls. This suggests that behavioural compliance is not yet fully embedded as a standardized practice across users, leading to variability in how information security-related responsibilities are enacted.

Table 3 presents the Gap Analysis results for People Controls under ISO/IEC 27001:2022 Annex A.6, focusing on user behaviour in the execution of assigned responsibilities.

Table 3. Gap Analysis of People Controls (ISO/IEC 27001:2022 Annex A.6)

Annex A.6	Findings	Annex A.6 Assessment	Gap
Screening	The assignment of personnel is conducted by the faculty. The selection criteria include a minimum bachelor's degree qualification, basic proficiency in spreadsheet tools (e.g., Microsoft Excel), and general data processing capabilities.	User assignment is established based on formal criteria, including information security-related considerations.	Personnel assignment does not yet incorporate information security-related considerations, such as awareness of data accuracy, information availability, and the impact of inaccurate data handling on system reliability, as the selection process is primarily based on academic qualifications and technical skills.
Terms and Conditions of Employment	Terms and conditions of employment are not formally documented; instead, they are communicated verbally.	Compliance with organizational work regulations and consistent execution of assigned tasks.	The absence of formally documented employment terms results in limited standardization of role expectations, despite consistent task execution and regulatory compliance.
Information Security Awareness, Education, and Training	Information security awareness and training activities are primarily focused on system updates and do not address risks associated with data accuracy.	Accuracy in data input and awareness of potential data errors.	Training content does not comprehensively cover data accuracy risks, resulting in limited integration of data integrity considerations within awareness activities.
Disciplinary Process	The disciplinary process is handled informally through direct communication.	Compliance with established organizational policies.	The disciplinary mechanism is insufficiently formalized, indicating limited alignment with structured policy enforcement practices.
Responsibilities After Termination or Change of Employment	The use of shared accounts and the transfer of access privileges between users without a formal authorization mechanism.	Adherence to responsibility transfer procedures and prevention of unauthorized access.	Access transition practices are not governed by a controlled authorization mechanism, indicating limited formal control over account and privilege management during employment changes.
Confidentiality or Non-Disclosure Agreements	No formal Non-Disclosure Agreement (NDA) is established; however, an understanding of confidentiality is present at the operational level.	Maintenance of data confidentiality and prevention of unauthorized information disclosure.	The absence of formally established confidentiality agreements indicates limited contractual reinforcement of confidentiality obligations at the organizational level.
Remote Working	All activities are conducted entirely within the faculty environment.	Use of secure access mechanisms in accordance with established requirements.	Secure access requirements are not explicitly defined for non-faculty or remote environments, limiting clarity of control implementation beyond physical premises.
Information Security Event Reporting	Data accuracy-related errors are corrected directly within the system, whereas information security incidents are reported to BTSI through informal channels.	Availability of a formal and documented information security incident reporting mechanism.	Incident handling practices are not fully standardized under a formal reporting mechanism, as reporting varies depending on the type of incident and relies on informal communication channels.

A.2 CAPABILITY LEVEL ASSESSMENT (COBIT–CMMI)

Based on the gap analysis of ISO/IEC 27001:2022 Annex A.6, a capability level assessment was subsequently conducted using the COBIT–CMMI framework to evaluate the maturity of People Controls from a user behaviour perspective. This assessment focuses on the extent to which information security control activities are

integrated into work habits, the consistency of user actions, and the level of formalization in practices that support information security.

The results indicate that the overall capability is at Level 2 (Managed), with an average score of 40%. At this stage, user behaviour in implementing information security controls demonstrates basic and relatively consistent execution; however, it is still largely shaped by individual habits and informal interaction patterns rather than standardized organizational structures.

Table 4 presents the results of the capability level measurement for People Controls based on the COBIT–CMMI framework, summarizing the assessment outcomes across all Annex A.6 control areas.

Table 4. Results of Capability Level Measurement for People Controls (COBIT–CMMI Framework)

Annex A.6	Capability Level	Percentage	Capability Level Description
Screening	2	40	Personnel selection is based on basic qualifications and technical skills, with limited inclusion of information security-related considerations in the selection process.
Terms and Conditions of Employment	2	40	Employment conditions are communicated verbally and are not formally documented within standardized employment agreements or procedures.
Information Security Awareness, Education, and Training	2	40	Awareness and training activities are conducted with primary focus on operational updates, with limited coverage of structured information security behavioural topics.
Disciplinary Process	2	40	The disciplinary process is executed through informal communication without formalized procedural documentation or standardized enforcement workflow.
Responsibilities After Termination or Change of Employment	2	40	Access and responsibility changes are managed without a formal authorization workflow for approval and documentation of access transfer activities.
Confidentiality or Non-Disclosure Agreements	2	40	Confidentiality expectations exist informally and are not established through formal Non-Disclosure Agreements or documented commitments.
Remote Working	2	40	Remote working controls are not defined and no formal mechanisms for remote access security are established.
Information Security Event Reporting	2	40	Incident reporting is performed through informal communication channels without a fully standardized reporting procedure or formal documentation structure.
Average Capability Level		**40**	

To achieve Level 3 (Established), control activities should be consistently guided by formally documented procedures and reinforced through clearly defined role-based responsibilities embedded within organizational practices. This level represents an established and consistently communicated condition, where control-related practices are formally approved, understood, and applied across users rather than relying on individual discretion. As a result, users demonstrate more uniform behaviour in carrying out their responsibilities, which strengthens consistency, enhances accountability in practice, and improves the reliability of daily operational activities.

B. DISCUSSION

The findings indicate that the implementation of People Controls in academic scheduling management remains at Capability Level 2 (Managed), where user behaviour reflects the execution of basic control-related activities but is not yet fully supported by standardized behavioural structures within the organization. Control execution is still influenced by individual habits and situational communication patterns rather than consistent adherence to formal procedures.

This condition is significant given that the academic scheduling process involves intensive interactions among users with diverse roles. In this context, consistency in user behaviour plays a critical role in maintaining coordination and ensuring information reliability. Although the academic information system supports process efficiency, its effectiveness depends on how consistently users perform their assigned responsibilities. These patterns indicate an interaction between organizational culture and user cognitive tendencies. In the absence of sufficiently formalized controls and clearly defined accountability structures, such conditions are associated with variations in data entry and update practices. This suggests that the observed inconsistencies are not solely procedural in nature, but are also influenced by organizational norms, individual perceptions of responsibility, and habitual work practices that shape user behaviour in practice.

Compared to Level 3 (Established), current user practices do not yet fully reflect the implementation of institutionalized procedures. This is evident in variations in data management and updates, particularly in terms of timeliness. Such conditions align with the observed misalignment between data availability and the registration period,

highlighting the direct influence of user behaviour on information quality and availability.

Overall, these findings emphasize the importance of strengthening People Controls through more consistent behavioural practices, clearer role-based responsibilities, and reinforced accountability mechanisms within the organization. To support both immediate operational improvements and long-term organizational development, the recommended improvements are categorized into short-term operational improvements and long-term strategic improvements. The mapping of these recommendations based on ISO/IEC 27001:2022 Annex A.6 is presented in Table 5 and Table 6.

Table 5. Short-Term Recommendations for ISO/IEC 27001:2022 Annex A.6

Annex A.6	Recommendation	Expected Impact
Screening	Define basic information security-related considerations, such as awareness of data accuracy, information availability, and the impact of inaccurate data handling on system reliability, into personnel selection and assignment criteria.	Personnel demonstrate initial awareness of information security responsibilities and the importance of accurate academic scheduling data handling from the beginning of role assignment.
Terms and Conditions of Employment	Establish formally documented terms and conditions that clearly define responsibilities related to information security behaviour and data handling practices.	Improved consistency in user understanding of role expectations and security-related responsibilities.
Information Security Awareness, Education, and Training	Conduct periodic awareness sessions focusing on data accuracy, secure data handling, and user responsibilities within academic scheduling activities.	Increased user awareness and more consistent execution of operational activities related to information security.
Disciplinary Process	Formalize the disciplinary process by defining structured procedures that link user actions with policy compliance, including clear behavioural expectations and corrective measures.	User behaviour becomes more accountable and aligned with organizational policies through consistent enforcement mechanisms.
Responsibilities After Termination or Change of Employment	Implement a formal, role-based access transition procedure supported by an approval workflow to ensure controlled transfer and revocation of access rights.	User behaviour related to access management becomes more controlled, reducing informal practices and improving accountability in access handling.
Confidentiality or Non-Disclosure Agreements	Establish formal confidentiality agreements and reinforce them through user awareness initiatives emphasizing behavioural responsibility in protecting information.	Strengthened user commitment to confidentiality and more consistent behaviour in preventing unauthorized information disclosure.
Remote Working	Define and communicate secure access requirements for remote or non-standard working conditions, including expected user behaviour in accessing and handling information securely.	Users demonstrate consistent secure behaviour regardless of working location, ensuring alignment with information security practices.
Information Security Event Reporting	Develop a formal and standardized incident reporting mechanism accompanied by clear behavioural guidelines for users in identifying and reporting incidents.	Improved consistency in user reporting behaviour, enabling more structured and reliable incident handling practices.

Table 5 outlines operational recommendations intended to address observed implementation gaps in daily academic scheduling activities, particularly those related to procedural consistency, access handling, and user reporting practices.

Table 6. Long-Term Recommendations for ISO/IEC 27001:2022 Annex A.6

Annex A.6	Recommendation	Expected Impact
Screening	Integrate information security-related considerations, including awareness of data accuracy, information availability, and the impact of inaccurate data handling on system reliability, into personnel selection and role allocation procedures.	Improved alignment between personnel assignment practices and information security objectives, resulting in greater awareness of data handling responsibilities and reduced risk of scheduling data inaccuracies.
Terms and Conditions of Employment	Incorporate information security responsibilities into institutional governance policies and long-term human resource management practices.	Sustainable implementation of standardized security-related responsibilities across organizational roles.
Information Security Awareness, Education, and Training	Develop continuous information security education and behavioural awareness programs integrated into organizational culture.	Strengthened long-term security awareness and behavioural consistency in information management practices.
Disciplinary Process	Integrate disciplinary procedures into institutional governance frameworks supported by continuous monitoring and evaluation mechanisms.	Improved organizational accountability and reinforcement of standardized behavioural practices.
Responsibilities After Termination or Change of Employment	Establish integrated access governance mechanisms supported by periodic review and formal authorization controls.	Sustainable and accountable management of access rights throughout personnel lifecycle changes.
Confidentiality or Non-Disclosure Agreements	Institutionalize confidentiality protection practices through continuous policy reinforcement and behavioural awareness initiatives.	Increased organizational commitment to information confidentiality and reduced risk of unauthorized disclosure.
Remote Working	Develop institutional policies and long-term governance mechanisms for secure remote access and distributed working practices.	Consistent implementation of secure information handling practices across evolving work environments.
Information Security Event Reporting	Establish an integrated organizational incident reporting culture supported by continuous evaluation and behavioural reinforcement mechanisms.	Improved organizational responsiveness and sustainability of information security incident management practices.

Table 6 outlines strategic recommendations intended to support institutional integration of People Controls through policy development, governance mechanisms, and continuous behavioural reinforcement.

IV. CONCLUSION

This study indicates that the implementation of People Controls based on ISO/IEC 27001:2022 Annex A.6 in academic scheduling management is at Level 2 (Managed) with an achievement percentage of 40%. At this stage, user behaviour reflects the execution of basic control activities but is not yet consistently aligned with standardized organizational practices.

The findings highlight that issues related to data accuracy and timeliness are closely associated with variations in user behaviour, particularly in how responsibilities are performed and how data is managed during operational processes. This demonstrates that the reliability and availability of information are influenced not only by system capabilities but also by the consistency of user actions.

Strengthening information security therefore requires greater emphasis on shaping consistent user behaviour, reinforcing role-based accountability, and embedding structured practices to support

accurate and timely information management. From a managerial perspective, university leadership plays a critical role in establishing formal policies, disciplinary procedures, and clear operational guidelines to ensure consistent compliance with information security practices. Institutional commitment through policy enforcement, regular monitoring, and accountability mechanisms is essential to support sustainable improvements in academic scheduling governance and information security management.

ACKNOWLEDGMENT

The author expresses sincere gratitude to all interview participants who provided valuable insights for this study. Their willingness to share experiences, explain operational practices, and provide detailed information regarding course scheduling activities played a crucial role in the completion of this research. The author greatly appreciates their time, cooperation, and openness throughout the data collection process.

REFERENCES

[1] Saniyah, M. Arsyad, and A. S. Arlan, "Pengaruh Efektivitas Sistem Informasi Akademik (SIAKAD) terhadap Kualitas Pelayanan Akademik di Sekolah Tinggi Ilmu Administrasi Amuntai," *Pelayanan Publik*, vol. 2, no. 1, pp. 122–131, 2025.

[2] M. Rofi'i, "Analisis Manfaat dan Tantangan Sistem Informasi Akademik dalam Manajemen Perguruan Tinggi: Pendekatan Systematic Literature Review," *J. Islam. Manag. Educ.*, vol. 1, no. 01, pp. 1–13, 2024, [Online]. Available: https://journal.iaisyaichona.ac.id/index.php/imej/article/view/135

[3] B. Kholifah, I. Thoib, N. Sururi, and D. S. Nugraha, "Efektivitas Sistem Informasi Akademik dalam Meningkatkan Komunikasi dan Informasi Akademik di Institut Teknologi Mojosari," *Komun. Islam*, vol. 5, no. 1, pp. 89–100, 2024.

[4] & A. Romdoniyah, Dedih, "Dampak Implementasi Sistem Informasi Manajemen terhadap Kualitas Layanan Administrasi Pendidikan," *EPISTEMIC J. Ilm. Pendidik.*, vol. 4, no. 2, pp. 131–152, 2025.

[5] J. T. T. Thiodora, R. Iskandar, "Pengaruh Kualitas Pelayanan Sistem Informasi Akademik Pengguna Di Universitas Panca Sakti Bekasi," *Econ. Digit. Bus. Rev.*, vol. 7, no. 1, 2025.

[6] S. Damayanti, Y. G. Elysia, O. Amanatillah, P. Purba, I. Farida, and A. Prawira, "Pengaruh Penggunaan Sistem Informasi Akademik di Lingkungan Pendidikan Tinggi," *J. MANAJERIAL*, vol. 20, no. 1, pp. 43–53, 2021.

[7] R. Budi Setiadi and D. Meliana, "Optimasi Proses Penjadwalan Mata Kuliah di Perguruan Tinggi : A Literature Review," *Proceeding Mercu Buana Conf. Ind. Eng.*, vol. 6, no. July, p. 303, 2024.

[8] J. Cerah, A. Sujjada, K. Kamdan, and G. P. Insany, "Implementasi Metode Kanban pada Penjadwalan Mata Kuliah Berbasis Web," *J. Ekon. Manaj. Sist. Inf.*, vol. 6, no. 5, pp. 3435–3445, 2025.

[9] F. Rahman, T. B. Bun, and E. L. Tatuhey, "Sistem Penjadwalan Matakuliah Menggunakan Metode Pewarnaan Graph Pada PRODI TI USN Papua," *J. TEKNO KOMPAK*, vol. 20, no. 1, pp. 103–113, 2025.

[10] M. C. Utami, Y. Sugiarti, M. S. Akbar, and M. Q. Huda, "Assessing

Technology Acceptance for SIAKAD Usage among Scholarly Community," *J-INTECH (Journal Inf. Technol.*, no. 10, 2025.

[11] A. Khair, D. Ishmatul, and Y. Amrozi, "A Problem of Information System Integration At a University in Indonesia," *SAINTEKBU J. Sci. Technol.*, vol. 14, no. August, pp. 9–15, 2022.

[12] K. D. Setyowati, T. Chamidy, and M. Faisal, "Analysis of Academic Information System Using Information System Success Model and System Quality Model Case Study of Institut Teknologi Nasional Malang," *Trans. Informatics Data Sci.*, vol. 1, no. 1, pp. 33–44, 2024, doi: 10.24090/tids.v1i1.12234.

[13] Wahyu Triono, Kirana Lesmi, and Iim Khotimah, "Optimization and Challenges of Implementing Academic Service Management Information Systems in Muhammadiyah Higher Education: A Multiple-Case Study," *J. Pendidik. Islam*, vol. 12, no. 2, pp. 155–162, 2023, doi: 10.14421/jpi.2023.122.155-162.

[14] A. M. F. Wahyudi, D. Saputra, "Strategi Implementasi Kebijakan Keamanan Informasi Di Era Transformasi Digital," *Sist. Inf.*, vol. 5, no. 2, pp. 344–350, 2025.

[15] A. Mita Baqis, M. Irwan, and P. Nasution, "Pentingnya Perlindungan dan Keamanan Data Privasi di Era Digital," *J. Manaj. dan Pendidik. Agama Islam*, vol. 3, no. 3, p. 2025, 2025, [Online]. Available: https://journal.aripafi.or.id/index.php/jmpai

[16] E. S. A. Susilo, S. Mukaromah, "Pengukuran Tingkat Kapabilitas Manajemen Keamanan Informasi Menggunakan Cobit 5," *Pros. Semin. Nas. Teknol. dan Sist. Inf.*, vol. 1, no. September, pp. 6–7, 2023.

[17] A. A. Mike and A. P. R. Ntwari, "Human Factors Shaping Cybersecurity Behavior in Work from Home Environment in Ugandan Universities," *Int. J. Res. Innov. Appl. Sci.*, vol. XI, no. 2454, pp. 1487–1500, 2026, doi: 10.51584/IJRIAS.

[18] P. H. M. Shah, F. Iqbal, U. Rahman, "A comparative assessment of human factors in cybersecurity: Implications for cyber governance," *IEEE Access*, vol. 1, no. 1, 2023, doi: 10.1109/ACCESS.2023.3296580.

[19] A. R. Tanaamah and F. J. Indira, "Analysis of Information Technology Security Management UKSW SIASAT Using ISO/IEC 27001:2013," *IJITEE (International J. Inf. Technol. Electr. Eng.*, vol. 5, no. 2, p. 68, 2021, doi: 10.22146/ijitee.65670.

[20] A. F. Rebitasari, D. Yuniarto, and D. Setiadi, "Implementation of Iso 31000:2018 for Risk Management in Sistem Informasi Akademik (Siakad) At Sebelas April University," *J. Ris. Tek. Inform. V*, vol. x, no. y, pp. x-y, 2024.

[21] S. n, Y. Andriyani, E. MahdiyahMeitarice, M. Nababan, Y. Andriyani, and E. Mahdiyah, "Security Risk Management Analysis Of Siam At Poltekes Kemenkes Riau Using Fmea And ISO 27001:2013 Controls," *IJIRSE Indones. J. Inform. Res. Softw. Eng.*, vol. 5, no. 1, pp. 40–50, 2025.

[22] Nakita Sisilia and Rayyan Firdaus, "Analisis Faktor-Faktor yang Mempengaruhi Kinerja System Informasi Akuntansi," *Anggar. J. Publ. Ekon. dan Akunt.*, vol. 2, no. 4,

pp. 337–343, 2024, doi: 10.61132/anggaran.v2i4.1012.

[23] R. Ali, "Operationalising Information Security Management: A Procedural Framework Analysis of ISO/IEC 27001:2022 Implementation in a Financial-Technology Organisation," *arXiv Prepr.*, pp. 1–9, 2026, [Online]. Available: http://arxiv.org/abs/2604.23230

[24] C. Arumdiya, F. C., Rudianto, "Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi," *J. PETISI (Pendidikan Teknol. Inf.*, vol. 06, no. 02, pp. 167–186, 2025.

[25] S. S. H. Basuki, A. Hafiz, "Implementasi Sistem Manajemen Keamanan Informasi Iso / Iec 27001 : 2022 pada Unit Teknologi Informasi Perguruan Tinggi," *Remik Ris. dan E-Jurnal Manaj. Inform. Komput.*, vol. 10, no. 1, pp. 396–406, 2026.

[26] R. Sinaga and F. Taan, "Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala," *NUANSA Inform.*, 2024, doi: 10.25134/ilkom.v18i2.205.

[27] "ISO/IEC 27001:2022 - Information security management systems." https://www.iso.org/standard/27001 (accessed Apr. 26, 2026).

[28] Luis Gorgona, "Building a Maturity Model for COBIT 2019 Based on CMMI," *ISACA J.*, vol. 6, pp. 1–3, 2021, [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi%0Ahttps://www.isaca.org/resources/cobit

[29] D. Ria, Y. Tb, M. B. Wibawa, M. Dwi, Z. Musliyana, and G. D. Akumba, "Sistem Informasi Penjadwalan Kuliah Berbasis Web Studi Kasus Fakultas Ilmu Kesehatan Universitas Ubudiyah Indonesia," *J. Informatics Comput. Sci.*, vol. 11, no. 1, pp. 137–142, 2025.