ORIGINAL RESEARCH

Adoption of Best Practices in Running and Maintaining IT-Based Information Systems in Higher Learning Institutions

Chiza M. Christophe[1] · Bua Anthony[2] · Cirhuza Cibangu[1] · Abdi T. Abdalla[2]

Abstract

The transition from paper-based to information-technology-based (IT-based) systems has warranted a significant impact on how commercial, administrative, and academic processes are carried out today. This is due to the deployment of numerous Information Systems (IS) that support essential business and institutional activities by facilitating data collection, processing, and dissemination. The deployed IT-based systems are mostly susceptible to processing errors, unacknowledged data modification, data loss, system failures, cyber-attacks, and other potentially detrimental risks. It is, therefore, argued that to ensure trustful and high-quality service delivery through the use of IT-based IS and virtual resources in Higher Learning Institutions (HLIs), IT engineers and managers should have a thorough understanding of IT best practices. Thus, this study develops an IT best practices adoption theoretical framework based on the daily routines of HLIs' IT engineers and managers. According to the framework, IT system utilization and dependability, knowledge of the sensitivity of information and IT systems, and the budget allotted to IT infrastructure upkeep are the primary drivers of the adoption of IT best practices.

Introduction

In classical paper-based systems, data are manually gathered, archived, and processed. This method presents a number of physical challenges and risks, including document loss during archive location changes, unauthorized access

This article is part of the topical collection "Computer Supported Education" guest edited by James Uhomoibhi and Beno Csapó.

✉ Chiza M. Christophe
   chizamwaka@gmail.com

   Bua Anthony
   antwonyb@gmail.com

   Cirhuza Cibangu
   cirhuza.cibangu@ucbukavu.ac.cd

   Abdi T. Abdalla
   abdit@udsm.ac.tz

[1] Département d'informatique, Faculté des Sciences, Université Catholique de Bukavu, Bukavu, Democratic Republic of Congo

[2] Department of Electronics and Telecommunications Engineering, College of Information and Communication Technologies, University of Dar es Salaam, Dar es Salaam, Tanzania

to the archive that may reveal confidential information, theft and document destruction [1]. Paper aging, document classification error, document duplication, prolonged document retrieval and limited physical space for documents storage are also reported among major limitations of classical paper-based systems [1, 2]. To alleviate the abovementioned challenges, the paper-based business processes were digitized using computer-based Information Systems (ISs) [2, 3].

ISs are now owned by organizations for data acquisition, segmentation and dissemination in order to facilitate management processes [4–6]. Apart from the common sense that organizations value data or information, in terms of governance decision enablers, some organizations and institutions consider information as influential assets for development, growth and market competition [4, 7, 8]. In the first consideration case, an IS is regarded as a system of strategic information, while in the second, it is regarded as a strategic information system [7].

With recent significant advancements in digital transformation, current IT-based ISs integrate not only the previously mentioned functionalities but also data analysis and processing capabilities. Indeed, the introduction of artificial intelligence (AI) and machine learning (ML) has given the possibility of patterns and irregularities

identification, and prediction of future outcomes from the data sets [1, 7, 9, 10]. AI and ML give further considerations to strategic ISs or intelligent decision support systems by giving the ability to learn, collect and automatically process huge amounts of data from real-time user behavior or experience [9]. In that regard, IT-enabled systems become drivers for improving services management capabilities in organizations, as mentioned in ITIL V4. Depending on the given consideration by institutions, outlooks on the matter concerning service quality, data value, protection and privacy, huge financial resources and well-trained staff are assigned to upgrade, maintain, or develop IT-based ISs.

Motivated by the revolution of IT, sizable numbers of countries, agencies and universities launched projects to support institutions with IT solutions and infrastructures which contributed to the migration from paper-based to IT-based ISs and modernization of management procedures in higher learning institutions [11–14]. These IT infrastructures are hardware or software facilities that are provided to enable institutions avoid responses such as this is an illegible handwriting; no time to produce all those documents; we have lost them; the volume was difficult to store; we could not make them timely; we were too distant, just to mention a few [2]. The use of IT-based ISs improves consistency, collaboration, accountability, timeliness, accessibility, effectiveness, efficiency, accuracy and other aspects of business processes or institutional activities [3, 15–17]. Beside these advantages, IT infrastructures subject higher learning institutions to different physical and logical challenges undermining computer systems. These include but are not limited to data leakage, incorrect data processing, cyber-attacks, data loss, and expensive IT infrastructures and systems that are not offset by optimal usage [18–21].

The goal of this study was to determine the extent to which best practices are implemented by IT engineers and managers who manage ISs in higher learning institutions. The main concern is that, despite the efforts made to provide error free, high speed, stand-alone or interoperable higher learning information systems, the performance, reliability, resilience, and recovery of the deployed systems depend on different practices in running and maintaining the systems, managing, and preventing possible threats and attacks. The study explicitly considered the fact that scholars focused on the adoption of IT-based systems without championing IT best practices, which should also be championed in accordance with current state of service quality and business continuity requirements, IT risks, and cyber-attacks.

The remainder of the paper is organized as follows: Sect. "Related Works" highlights previously published related works. The authors present the research methodology in Sect. "Methods", and the research findings in Sect. "Findings". Finally, Sect. "Conclusion" concludes with closing remarks.

Related Works

IT management and governance aim to align IT systems with business processes in order to achieve value creation through the use of a specific IT system or interaction between several IT systems in the organization [22, 23]. IT service management (ITSM) refers to the practices of IT departments in developing or acquiring, deploying, running, and maintaining the IT infrastructure, whereas IT governance (ITG) refers to leadership alignment of IT goals with organization's goals [24, 25]. This alignment of IT systems and business processes, regarding the design and implementation of agile information systems, has been thoroughly discussed in the literature [22, 26].

Tools such as ISO/IEC 20000 and ISO/IEC 38500, ITIL (IT Infrastructure Library), COBIT (Control Objectives for Information and Related Technologies), and DevOPs (Development and Operations), to name a few, have gained attraction in enterprises, agencies, and industries that rely heavily on IT-enabled systems [27–31]. The general context of these tools is that appropriate precautions, nontechnical and technical controls are used in developing or acquiring, implementing, running, and maintaining IT infrastructures and hosted information systems [32, 33]. These are strategies, guidelines, or frameworks that provide methods for mitigating physical and logical threats that may impair the performance and reliability of IT systems or infrastructures [27, 33, 34].

Academics frequently question the adoption of the management and governance practices promoted by these tools, because it is difficult for different organizations to achieve long-term and high-quality service delivery through IT-enabled systems [29]. Most frequently, they suggest that the quality of service provided by information systems, information technology infrastructures, and the IT department, should be measured or audited in order to ensure that IT organization goals or targets are met and risks are accepted or transferred [35].

ISO/IEC 20000 and ISO/IEC 38500, ITIL, and COBIT are commonly used by researchers and IT practitioners in developing models, extracting, conceptualizing, and testing items that should be considered by IT managers and

stakeholders in measuring and improving the quality of IT service delivery, and identifying constraints that often undermine the evaluation of IT service delivery [29, 34]. Researchers focused on ITSM and ITG strategies as recognized by IT service organizations or providers, as well as E-marketplaces providing customer-centric services [27, 28, 36]. It has been pointed out that IT service organizations capitalize on ITSM strategies to gain competitive advantages, appreciation, and trust from their customers through IT process and capability improvement [23, 24], but this is not the case for HLIs.

Higher learning institutions have committed significant financial resources to adopting and developing IT systems that allow the transition from paper-based to IT systems, improving accountability, efficiency, and effectiveness in delivering various services to the community. Additionally, the COVID-19 pandemic has accelerated this adoption by pushing universities to use remote services, e-libraries, and online teaching platforms [25, 30]. However, allocating financial resources to IT-based ISs in HLIs will not ensure accountability, efficiency, performance, and other quality of service dimensions if ITSM and ITG practices are not implemented properly [25]. Therefore, the adoption of IT best practices in HLIs continues to be a crucial research area, which is the key focus of this article.

Methods

This study was carried out using a mixed research approach; various factors and indices have been identified through interviews and content analysis. Interviews were used to identify various factors viewed as potential influencers of IT best practices adoption in HLIs, and content analysis was used to compile a list of best practices from the ITIL 4 (IT Infrastructure Library release 4) manual. Following that, the list of best practices compiled from ITIL 4 was rated using a questionnaire completed by responsible IT engineers and managers in HLIs. ITIL 4 is the most recent release of the IT infrastructure library, and it provides best practices for enabling organizations to efficiently integrate digital transformation and IT service management into their life cycles [37]. The framework aims to ensure that value creation, business continuity and service delivery are at acceptable levels, even after disruption or failure of IT enabled systems or in cyberattacks, through risk assessment, mitigation, acceptance as well as the adoption of best practices in operating IT-enabled systems. IT teams from 15 universities in 7 countries were targeted, but only 10 were willing to disclose their information and thus completed the questionnaire. The findings section highlights identified factors, IT best practices and finally causal relationships and correlations analysis based on the collected data.

Findings

IT Best Practices

IT best practices are collections of actions, measures and ethics that have been recognized for their effectiveness in ensuring proper and reliable development, deployment, use and management of IT-based systems. They are typically gathered from work routines in various firms, industries and expert enterprises and are verified through case studies, criticized, and reviewed by scholars, auditors and other trailblazers. They are attested to and documented in the form of IT system guidelines, norms, standards, and regulations. The level of compliance, by an institution, to one or more standards predicts the precaution or safety in the course of the supported business processes.

The reported findings emphasize the adoption of best practices presented in ITIL 4 for the use and maintenance of IT infrastructures or systems. Table 1 lists the best practices that have been identified in order to create a clear and stand-alone reading flow. They have been divided into four domains in order to guide analysis in a comparative manner. These domains are specifically capacity and performance management, security control, service availability and business continuity, and change control.

Factors Influencing the Adoption of IT Best Practices

Interviews were conducted to identify various factors that may significantly influence adoption of IT best practices. The identified factors include IT team competency, IT systems use and dependability, awareness on the sensitivity of information and IT systems, IT infrastructure complexity, and sufficiency of budget assigned to maintaining IT infrastructure. IT department or team competency refers to IT team members' ability to handle IT-related problems and duties as well as adopt and implement cutting-edge systems and solutions. Years of experience, education level, number of workshops and certifications on IT equipment and systems, and segregation of duties among members of the IT team were identified as substitutes for this factor, as shown in Table 2.

Interviewees also mentioned the IT systems use and dependability, which is a factor that characterizes the integration of IT-based systems in various functions or business processes of the organization. As per the collected data, this factor is built up on the number of services or business processes supported by IT systems, the total number of employees accessing the IT-enabled services, usage rate of virtual resource or datasets, financial and reputational losses in case of IT infrastructure outage. In the context of the collected

Table 1 IT best practices

Capacity and performance management	1. Performance metrics and measurements are established 2. The organization's performance goals are well known 3. Performance evaluation of services and components is done on a regular basis to ensure that the organization's performance targets are met 4. Analysis of capacity requirements; determines whether current capacity meets current and future demand; capacity is reconsidered when adding or supporting new services, customers, or users 5. Plan for Resource allocation; conditions and procedures for resource allocation exist and followed 6. Performance improvement plan; upgrade plan and replacement of old, obsolete or deficient equipment 7. Engage or consult customers and users in capacity and performance planning so as to ensure their expectation is met and proper satisfaction is achieved
Security control	1. Information security being part of the practical security plan of the organization 2. Existence of a team or individual dedicated to assessing security risks and developing physical and logical access policies and procedures 3. IT vulnerabilities are assessed and countermeasures are established based on likelihood and consequences 4. Particularly, procedures for penetration tests or cybersecurity vulnerability assessment exist 5. Identity and access policies are established 6. Security controls are reviewed and audited 7. Measuring the level of security risk awareness at user level 8. Measuring user compliance with information security policies and other controls 9. Measuring user consideration and value of data and information 10. Security configuration, update, change and patch deployment procedures exist and are followed 11. Security updates and patches are applied on a regular basis 12. Consideration of new security methods in newly developed platforms, services and practices 13. Security plan and policy are documented and communicated effectively, 14. Having a culture of providing information on new security measures and policies 15. Having a system that records user activities (log files) and auditing these logs on a regular basis
Service availability and Business Continuity	1. Plans and mechanisms for measuring availability (mean availability time: mean time between failures MTBF, mean time to restore services, logs can be archived and an improvement plan can be established) exist and are effective 2. Availability targets exist and appropriately known for different services taking into account user and customer experience 3. Monitoring, analyzing and reporting the availability of IT infrastructure and services 4. IT infrastructure is designed and updated to ensure that the desired level of availability is met. Alternatively, the actual availability level is accepted 5. The availability requirements for new services are documented and compared to the current level of IT infrastructure availability 6. The source of failures is identified and managed 7. Adequate redundant options exist for different services and suppliers; these options are tested or verified to ensure that they can properly deliver in the event of interruption or fault 8. Availability is considered when outsourcing services and the service level agreement is verified 9. A business impact analysis is carried out and the organization defines a disaster based on its business impact, this is updated continually 10. Disaster recovery plan in place and is updated, monitored and audited to ensure that business can resume in the agreed upon timeframe following the disaster 11. Recovery time objective (RTO) and recovery point objective RPO are established 12. An appropriate disaster recovery site is deployed based on the agreed RTO and RPO. (Regular data and configurations Backup as per RTO and RPO, backup files are regularly tested) 13. The deployment of services, equipment, or components is determined by the organization's business continuity requirements 14. The ongoing processes and practices are carried out in accordance with the organization's business continuity requirements and policies 15. Documentation that is effective for core activities and routines
Change control	1. Existence of change policies and procedures 2. Change classification, timetable and authorizations level 3. Known change request procedures 4. Proper change risk assessment by people who understand the risks involved and the benefits of the change 5. Measuring the IT infrastructure's ability to support new functionalities so that it can deliver proper performance after the change 6. Impact of change must be communicated to users and personnel who carry out processes, before change is deployed 7. Change authorization by a correct change authority

Table 2 IT team competency sub-factors

Sub factors	Years of experience	Number of workshops and certifications	Education level	Segregation of duties
Contribution (%)	34.46	25.15	20.44	19.94

Table 3 IT systems use and dependability

Sub factors	Number of services or business processes supported by IT systems	Total number of employees accessing the IT enabled services	Usage of virtual resources or datasets	Financial losses in case of IT infrastructure outage	Reputational losses in case of IT infrastructure outage
Contribution (%)	27.57	17.31	17.23	20.74	17.13

Table 4 Complexity of IT infrastructure

Sub factors	Number of information systems	Number of physical servers and virtual environments	Number of routers and other network layer equipment	Number of interconnected LANs or sites
Contribution (%)	24.36	26.92	26.34	22.35

data, contributions of these sub-factors are summarized as in Table 3.

The complexity of IT infrastructure has mostly been defined as the heterogeneity of the IT infrastructure and difficulties in maintaining it, which includes the number of information systems, physical servers and virtual environments, routers and other network layer equipment, and the number of interconnected local area networks (LANs) or sites. Contributions of sub-factors for the complexity of IT infrastructure are also presented as in Table 4.

Results and Discussion

Overview

The questionnaire, which was completed by IT engineers and managers who maintain ISs in the concerned higher education institutions, yielded adoption rates for the various best practices. The rates were added for each respondent, assuming the same contribution weight in their respective domains. Figure 1 shows a summary of the collected data.

This graph depicts the extent to which best practices are implemented; it shows that IT best practices are being given little consideration in HLIs. The graph also shows that best practices in capacity and performance management are more widely adopted than others. This implies that more efforts or intentions are being allocated to the use of calibrated and robust IT infrastructures in order to ensure optimal user experience while maintaining a cost-effective resource usage. In other language, the figure alludes that, best practices for capacity and performance management

Fig. 1 Adoption of IT best practices in in higher learning institutions
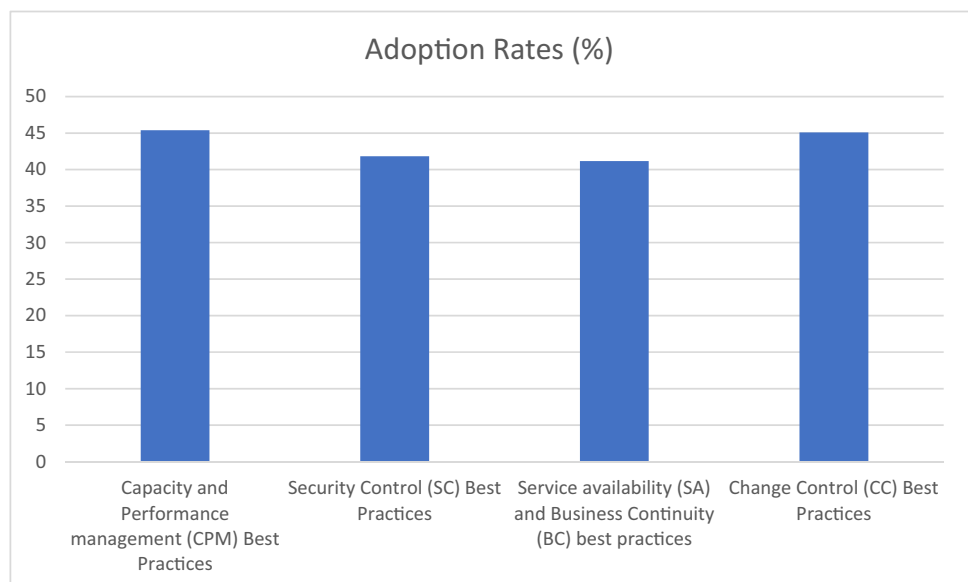
are less difficult to implement or adopt when compared to other practices.

To validate this observation, paired sample t tests were used to compare means and the results revealed that the differences were not significant at the 95 percent confidence level of the interval. Considering the security control domain with the lowest mean value, $t(10) = 0.604$ revealed that the means 45.39 ± 4.81 and 41.83 ± 7.46 do not differ significantly for a p-value of $0.565 > 0.05$.

Proposed Framework for IT Best Practices Adoption

The aforementioned factors resulted in a theoretical framework as per causal relationships analysis between factors and best practices, as well as correlation between domains of best practices, as shown in Fig. 2.

The hypothesis underlying the causal relationships investigation is that each independent variable positively impacts the adoption of IT best practices. Both regression and correlation analyses were conducted with a 95 percent confidence level of interval.

The linear regression revealed that awareness on the sensitivity of information and IT systems (*ASITS*) and the IT systems use and dependability (*ITSUD*) factors explain the observed variations in the adoption of capacity and performance management best practices as presented in Table 5 below.

For a p-values of 0.004 and 0.019, both less than 0.05, the regression equation is such as:

$$CPM\ (IDV) = 1.18 + 0.51 \times ASITS + 0.404 \times ITSUD \quad (1)$$

Table 5 Regression results for capacity and performance management

Predictors	Coefficient	T value	P value	correlation
Constant	1.18			
Sensitivity of information and IT systems (ASITS)	0.51	5.181	0.004	0.865
IT systems use and dependability (ITSUD)	0.404	3.403	0.019	0.718

For convenience purposes, *IDV* stands for Independent Variables throughout the paper.

According to Eq. (1), the need for deploying and maintaining reliable IT infrastructures is influenced first and foremost by the awareness on the sensibility of deployed IT systems and the number of services or academic processes that rely heavily on IT infrastructure in their course. Analysis also showed that IT systems use and dependability (*ITSUD*), awareness on the sensitivity of information and IT systems (*ASITS*), and Sufficiency of Budget assigned to maintaining IT infrastructure (*SITBudget*) justify the variations observed in adoption of service availability (*SA*) and business continuity (*BC*) best practices, as in Table 6 below.

For p-values of 0.001, 0.002 and 0.018 relating to *ITSUD*, *ASITS* and *SITBudget* independent variables, respectively, the regression equation is written as:
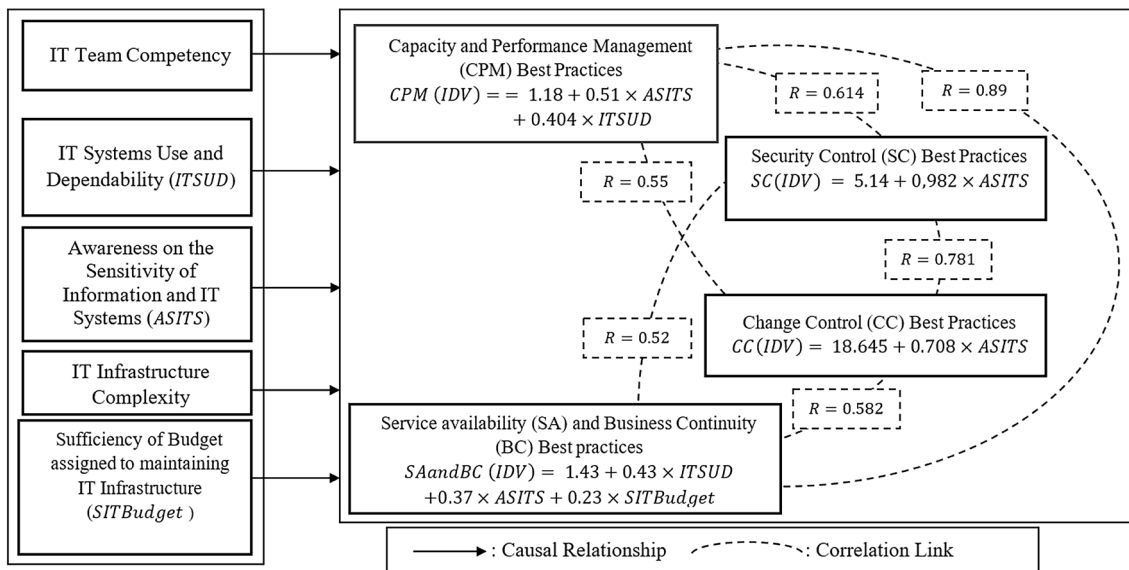
Fig. 2 IT best practices adoption framework

Table 6 Regression results for availability (*SA*) and business continuity (*BC*)

Predictors	Coefficient	T value	P value	Correlation
Constant	1.43			
IT systems use and dependability (*ITSUD*)	0.43	13.38	0.001	0.803
Awareness on the sensitivity of information and IT systems (*ASITS*), and Sufficiency of	0.37	14.23	0.002	0.832
Budget assigned to maintaining IT infrastructure (*SITBudget*)	0.23	3.85	0.018	0.095

Table 7 Regression results for security control (*SC*)

Predictors	Coefficient	T value	P value	Correlation
Constant	5.14			
Awareness of the sensitivity of information and IT systems (*ASITS*)	0.982	4.098	0.006	0.858

$$SA \text{ and } BC\,(IDV) = 1.43 + 0.43 \times ITSUD + 0.37 \times ASITS + 0.23 \times SITBudget \qquad (2)$$

Equation (2) demonstrates that IT infrastructure availability and business continuity measures that are implemented in HLIs depend on the extent to which people use and depend on IT infrastructure, the understanding of the sensitivity of information and the deployed systems, as well as the budget that they allocate to maintaining this IT infrastructure.

The linear regression showed that only the awareness of the sensitivity of information and IT systems (*ASITS*) factor justifies the variations that have been observed in the adoption of security control (*SC*) best practices as shown in Table 7.

For a *p*-values of 0.006, the regression equation is

$$SC\,(IDV) = 5.14 + 0.982 \times ASITS \qquad (3)$$

Equation (3) states that the extent to which people understand the sensitivity of the deployed systems, the risk associated with their use, and the value that people assign to their data and information determines the security measures and precautions taken in using IT-enabled systems in HLIs.

Indeed, the linear regression results in Table 8 revealed that the *ASITS* is the factor that explains the variations or changes in the adoption of change control (CC) best practices.

For a *p*-value of 0.035, the regression equation is

$$CC\,(IDV) = 18.645 + 0.708 \times ASITS. \qquad (4)$$

According to Eq. (4), the degree to which people understand the sensitivity of the system that will accommodate changes is the primary factor that drives precaution considerations when implementing new changes. A concluding observation is that, as shown in Fig. 2 and Table 9, correlation coefficients (*R*) reveal that adoption rates for different domains of IT best practices are highly correlated.

Conclusion

The performance, reliability, resilience, and recovery of IT-enabled systems are critical parameters in ensuring long-term quality service delivery in areas where IT infrastructures play a significant role. Adoption of IT best practices is strongly advised in order to avoid potential IT-related threats, achieve maximum precaution, and achieve satisfactory levels of service delivery, value creation and business continuity. According to the findings of this study, the use of and dependability on IT systems, awareness on the sensitivity of information and IT systems, and the budget allocated to IT infrastructure maintenance have acknowledgeable impact in improving the adoption of IT best practices.

Despite the fact that the adoption of IT-based IS and the spread of digital transformation in HLIs is being seen on a global scale, data collected revealed that the adoption of

Table 9 Correlation between IT best practices

	CPM	SC	SA and BC	CC
CPM	1			
SC	0.614	1		
SA and BC	0.89	0.52	1	
CC	0.55	0.781	0.582	1

Table 8 Regression results for change control (CC)

Predictors	Coefficient	T value	P value	Correlation
Constant	18.645			
Awareness of the sensitivity of information and IT systems (*ASITS*)	0.708	2.703	0.035	0.741

IT best practices is being given little consideration. As a result, significant efforts, stringency, and resources are still required to enforce the adoption of best practices in the operation and maintenance of IT-based IS in HLIs. Principally, the security control and business continuity best practices should be taken seriously, high caution and maturity should be achieved because ISs are being maintained in areas where suspicious data modification and system failure generate considerable damage. Another concerning situation is that some educational institutions offer IT and cyber security classes that include substantive penetration tests or cyber-attacks for learning purposes resulting into an increased threats level.

Our future research agenda includes an audit-based assessment that will provide a practical view of the extent to which IT best practices are used in higher education institutions. Furthermore, identifying specific constraints impeding the adoption of best practices in higher education institutions remains undrafted research thematic.

Declarations

Conflict of interest All authors have given their consent for this manuscript to be published. Prior to the submission of this manuscript, all authors declared that they had no conflicts of interest.

References

1. Romanenko EV, Kravets AG. Development and implementation of multi-agent approach to support the process of requests execution in a distributed information system "Toureast: CRM AI". World Appl Sci J. 2013;24:145–50.
2. Ayatollahi H, Bath PA, Goodacre S. Paper-based versus computer-based records in the emergency department: Staff preferences, expectations, and concerns. Health Informatics J. 2009;15(3):199–211.
3. S. Otamiri and V. A. Zeb-Obipi, "Automated Hospital Information Systems and Service Delivery of Teaching Hospitals," *Int. J. Innov. Econ. Manag. Sci. Account. Res.*, vol. 9, no. 1, 2021.
4. Ujunju MO, Wanyembi G. Evaluating the role of information and communication technology (ICT) support towards processes of management in institutions of higher learning. Int J Adv Comput Sci Appl. 2012;3(7):55–8.
5. S. K. Boell and D. Cecez-Kecmanovic, "What is an Information System ?," *IEEE Comput. Soc.*, 2015.
6. Indrayani E. Management of academic information system (AIS) at higher education in the city of Bandung. Procedia Soc Behav Sci. 2013;103:628–36.
7. O. Thiery and A. A. David, "Modélisation de l'utilisateur , systèmes d'informations stratégiques et Intelligence Economique," *Res. Gate*, 2002.
8. A. Ragowsky, N. Ahituv, and S. Neumann, "The Benefits of Using Information Systems," *Commun. ACM Res. Gate*, 2000.
9. J. Merkert, M. Mueller, and M. Hubl, "A Survey of the Application of Machine Learning in Decision Support Systems," *ECIS*, pp. 0–15, 2015.
10. Sarker IH. AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN Comput Sci. 2022;3(2):1–20.
11. Rafidah S, Dawam M. The use of ICT in public and private institutions of higher. CCSE. 2009;2(4):122–8.
12. Sife AS, Lwoga ET, Sanga C. New technologies for teaching and learning: Challenges for higher learning institutions in developing countries. Int J Educ Dev Inf Commun Technol. 2007;3(2):57–67.
13. John SP. The integration of information technology in higher education: a study of faculty's attitude towards IT adoption in the teaching process. Contaduría y Adm. 2015;60:230–52.
14. A. E. Kalinga, R. B. B. Bagile, and L. Trojer, "An Interactive e-Learning Management System (e-LMS): A Solution to Tanzanian Secondary Schools ' Education," vol. 1, no. 4, pp. 250–253, 2007.
15. Köylüoğlu AS, Duman L, Bedük A. Information systems in globalization process and their reflections in education. Procedia - Soc Behav Sci. 2015;191:1349–54.
16. B. Bygstad, E. Øvrelid, S. Ludvigsen, and M. Dæhlen, "From dual digitalization to digital learning space: Exploring the digital transformation of higher education," *Comput. Educ.*, vol. 182, no. February, 2022.
17. Alkhalaf S, Drew S, AlGhamdi R, Alfarraj O. E-learning system on higher education institutions in KSA: attitudes and perceptions of faculty members. Procedia - Soc Behav Sci. 2012;47:1199–205.
18. J. S. Suroso and J. J. Halim, "Information System Audit Using Framework Cobit 4 . 1 on PT Klikfix Asia International," *2018 Int. Conf. Inf. Manag. Technol.*, pp. 1–9, 2018.
19. D. M. Walker and R. L. E. al Jones, "Management Planning Guide for Information Systems Security Auditing," *Natl. State Audit. Assoc. U. S. Gen. Account. Off. Jt.*, 2001.
20. J. T. Force, "Control Baselines for Information Systems and Organizations Control Baselines for Information Systems and Organizations," *Natl. Inst. Stand. Technol.*, 2020.
21. K. Lyytinen and K. Lyytinen, "Different Perspectives on Information Problems and Solutions Systems," *ACM Comput. Surv.*, vol. 19, no. 1, 1987.
22. Bent S, Guetat A, Ben S, Dakhli D. The four spaces model: a framework for services governance in urbanized information systems. Procedia - Procedia Comput Sci. 2016;100:1208–19.
23. A. Shrestha, A. Cater-steel, M. Toleman, S. Behari, and R. M. Mehdi, "Development and evaluation of a software-mediated process assessment method for IT service management," no. September, 2019.
24. Salomonson SCN. Measures that matters : service quality in IT service management. Int J Qual Serv Sci. 2014;6:60–76.
25. H. Sofyani, A. Tahar, and I. Ulum, "The Role of IT Capabilities and IT Governance on Accountability and Performance of Higher Education Institutions During the COVID-19 Pandemic," *Management and Accounting Review*, Volume 21 No 2, 2022.
26. B. Johansson and H. Jaadla, "Designing a Tool for Measuring IT Process Maturity in an Agile Development Context." *30th International Conference On Information Systems Development*, Cluj-Napoca, Romania, 2022
27. A. Luís *et al.*, "Assessing the quality of information technology infrastructure services," *Industrial Management and Data Systems,* 2018.
28. Informasi MS, Kristen U, Wacana S. Information Technology governance design in DevOps-based E-marketplace companies using COBIT 2019 framework. INTENSIF. 2022;6(2):233–52.

29. Widianto A, Subriadi AP, Widianto A, Subriadi AP. IT service management evaluation method based on content, context, and process approach : A literature review context, and process approach. Procedia Comput Sci. 2022;197(2021):410–9.

30. F. R. V. Santos, F. M. V. Santos, and V. C. P. Chalen, "Governance Trend Of Information Technologies In Public Sector Higher Education Institutions." Journal of positive school psychology, vol. 6, pp. 689–700.

31. Altunel H, Say B. Software product system model : a customer - value oriented, adaptable, DevOps - based product model. SN Comput Sci. 2022;3(1):1–11.

32. M. I. Javed and M. I. Javed, "Widely practiced Information Technology Service management Frameworks." *International Journal of Latest Trends in Engineering and Technology (IJLTET),* Vol. 3, Issue 3, 2014.

33. Assobarry H. Analysis of information technology services management using ITIL V3 domain service operation (Case Study: Hotel Sinar Sidoarjo). Int J Comp Netw Secur Inform Syst. 2022;3(2):30–3.

34. Production EBN, Suryani E. Risk assessment on integrated information smart service using COBIT 5 framework related papers. Int J Comp Appl. 2021;183:14.

35. Fasihuddin H, Alharbi S, Alshehri A, Alzahrani A, Fatani H. Measuring the maturity of information technology governance based on COBIT. Romanian J Inform Technol Autom Control. 2022;32(2):65–78.

36. Herdiyanti A, Listyawati NR, Astuti HM. Understanding the total value of information technology services from the perspective of students and academic staffs. Procedia Comput Sci. 2018;124:429–36.

37. M. Basham, *Itil Foundation*, Itil 4th E. TSO (The Stationery Office), part of Williams Lea, 2019.