Building Resilience in Online and Distance Learning: A Risk Management Perspective

Raziana Che Aziz[1*], Mohd Tajudin Md Ninggal[2], Ahmad Izanee Awang[3]

[1,2,3]Open University Malaysia

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90300101

Received: 10 February 2025; Revised: 25 February 2025; Accepted: 28 February 2025; Published: 02 April 2025

ABSTRACT

The implementation of an Enterprise Risk Management (ERM) framework at an open and distance learning (ODL) institution has played a key role in identifying, managing, and mitigating risks specific to the ODL environment. This study examines the effectiveness of the institution's ERM practices in addressing critical risk areas, including technology infrastructure, academic integrity, regulatory compliance, and student engagement. Findings indicate that the institution's overall risk rating is low-to-moderate, reflecting the presence of well-established controls to manage uncertainties and support strategic objectives. Despite the institution's overall low-to-moderate risk rating, four areas—accreditation, partner performance, human capital, and geopolitical factors—pose significant risks requiring immediate intervention. The study offers practical recommendations to refine risk management practices, benefiting ODL institutions striving for sustainability and operational excellence.

Keywords: Online Distance Learning, Enterprise Risk Management, Academic Integrity, Technology Risks, Educational Sustainability

INTRODUCTION

Online and Distance Learning (ODL) has transitioned from a specialised educational option to a widely accepted delivery method, driven by technological advancements and evolving academic needs. An ODL institution is at the forefront of this transformation, integrating digital platforms into its educational model. While this approach provides flexibility and accessibility, it also introduces unique risks that could affect the benefits of online education.

For the ODL institution, these risks span multiple areas: technological vulnerabilities, maintaining academic integrity, ensuring regulatory compliance, and fostering consistent student engagement. Dependence on digital platforms heightens exposure to cybersecurity threats, system disruptions, and data breaches, which can interrupt learning and jeopardise sensitive information. Furthermore, the remote nature of ODL poses challenges in upholding academic integrity, with increased opportunities for dishonesty and plagiarism due to the lack of physical supervision.

Regulatory compliance adds complexity to the institution's operations, requiring continuous adaptation to evolving educational standards and policies. These efforts must balance compliance with the delivery of high-quality academic programmes that meet national and international expectations.

Student engagement in an online setting can also be challenging, as the absence of in-person interaction may lead to disengagement or isolation. Sustaining high levels of engagement necessitates innovative technological solutions and ongoing refinement of teaching methods.

This study aims to evaluate the effectiveness of the ERM framework in mitigating risks within an ODLinstitution, with a focus on technology, academic integrity, regulatory compliance, and student engagement.

To address these challenges, the institution has developed an Enterprise Risk Profile, as illustrated in Figure 1.

This framework systematically integrates risk management into its overall strategy, helping to identify, assess, and mitigate risks specific to the ODL environment.

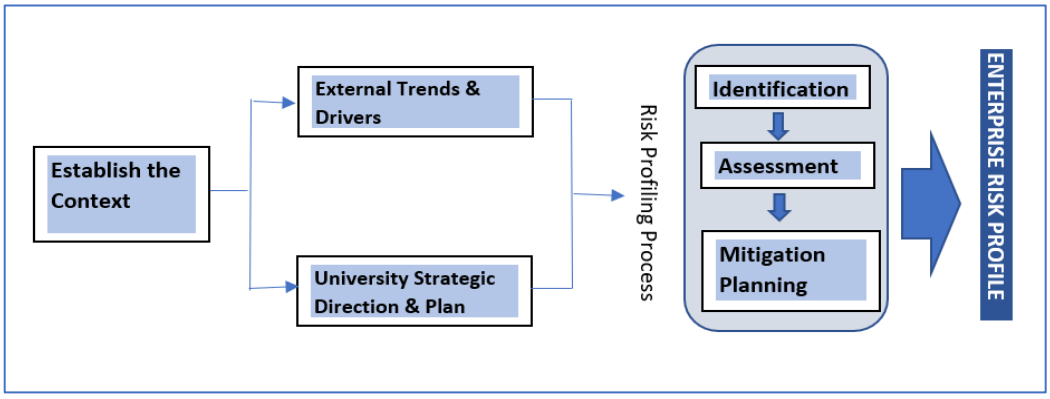

Figure 1: Enterprise Risk Profile in ODL Institution

LITERATURE REVIEW

Enterprise Risk Management (ERM) in higher education has evolved to include strategic, reputational, and compliance risks alongside traditional financial and operational concerns. A robust ERM framework facilitates strategic decision-making by integrating risk awareness into the institutional culture (Kaplan & Mikes, 2012). Research shows that higher education institutions must adapt their ERM strategies to address rapid technological changes, which impact teaching methods and increase vulnerability to cyber threats (Attain Partners, 2021). With the reliance on digital platforms, unique challenges arise, such as data privacy issues and increased susceptibility to cyberattacks, underscoring the need for adaptive and comprehensive ERM approaches (Adams & Bell, 2021; Roberts & Thomas, 2020).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has developed a framework (shown in Figure 1) that is instrumental in enhancing Enterprise Risk Management (ERM) across various organizational contexts, including higher education. This framework emphasizes the importance of integrating risk management into the organizational culture, thereby facilitating strategic decision-making and reinforcing the institution's ability to manage a broad spectrum of risks—from operational to strategic and reputational (Kaplan & Mikes, 2012). In academic settings, the COSO framework supports ODL institutions in strategically managing risks associated with financial operations, compliance obligations, and academic integrity, thereby enhancing overall institutional governance. The COSO framework's comprehensive approach ensures that risk management processes are standardized yet flexible enough to adapt to the unique challenges and evolving dynamics of higher education institutions (COSO, 2017).

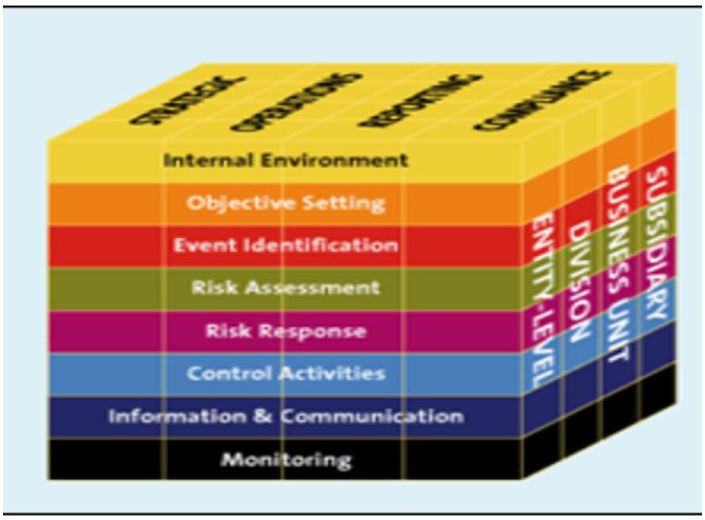

Figure 2: The COSO Framework
source: https://www.coso.org

Similarly, the ISO 31000 ERM framework (shown in Figure 2) provides a structured and comprehensive method for managing risks, which is crucial for educational institutions that increasingly rely on digital platforms and face various internal and external threats. ISO 31000 advocates for a systematic approach to risk management that includes the identification, analysis, and mitigation of risks, ensuring that all potential threats are addressed effectively. This framework's flexibility allows it to be customized to fit the specific needs and risk profiles of ODL institutions, aligning with strategic objectives and enhancing resilience against disruptions (ISO, 2018). Implementing the ISO 31000 framework can help the university strengthen its risk management capabilities by providing clear guidelines and practices that support the identification of risks, the assessment of their potential impacts, and the development of robust mitigation strategies.

Regulatory compliance is a growing concern as ODL providers must navigate a complex web of international, national, and regional regulations. King and Boyatt (2015) stress that institutions must remain agile to adapt to evolving policies and accreditation standards. This complexity requires a proactive approach to compliance within an ERM framework, ensuring the institutions to maintain accreditation while addressing new educational technologies.

Technological risks in Online and Distance Learning (ODL) are increasingly significant as institutions rely on digital platforms to deliver educational content. This dependence introduces a variety of cybersecurity threats, including system failures, data breaches, and cyberattacks, all of which can disrupt educational services and compromise sensitive information. Higher education institutions are particularly vulnerable due to the vast amounts of personal and academic data they store, making comprehensive cybersecurity measures essential for effective Enterprise Risk Management (ERM) in these settings (Ulven & Wangen, 2021). Implementing strategic cybersecurity protocols—such as real-time monitoring, regular system audits, and data encryption—is critical to safeguarding educational operations and building trust among stakeholders, including students and faculty (Alwi et al., 2022; Saravanan et al., 2021). Proactive measures not only enhance institutional resilience but also support the continuity and security of online educational environments.

Another key area of concern is academic integrity. McCabe, Butterfield, and Trevino (2012) suggest that theperceived anonymity in ODL environments increases the temptation for dishonest behaviours, such as plagiarism and cheating. Without physical supervision, maintaining the credibility of assessments becomes a significant challenge. Watson and Sottile (2010) argue that institutions must adopt technology-based solutions, including plagiarism detection tools and secure online exam platforms, to ensure academic standards are upheld.

Student engagement is another critical risk factor in ODL settings. According to Dixson (2015), engagement levels are influenced by course design, the responsiveness of instructors, and the availability of interactive tools. In a digital learning environment, the risk of disengagement is higher due to the lack of physical presence and traditional social cues. Martin and Bolliger (2018) suggest that fostering an interactive and inclusive learning experience through innovative pedagogical techniques is essential for improving student engagement in ODL.

Despite the growing importance of ERM in higher education, there is limited empirical research on its application in ODL environments. While theoretical discussions on risk management frameworks are common (Adams & Bell, 2021), more research is needed to examine how these frameworks are implemented in practice, particularly in digitally-driven learning institutions.

Economic downturns often force institutions to reassess financial risk management, particularly in student enrolment and funding models (Adams & Bell, 2021). Similarly, shifts in government policies on digital education can alter compliance requirements, necessitating dynamic ERM strategies (King & Boyatt, 2015).

This review of literature underscores the critical need for a comprehensive ERM framework in ODL institutions. The next sections will explore how ODL institution implements ERM in its operations and examine the key risks identified in the literature, particularly in the areas of technology, academic integrity, regulatory compliance, and student engagement.

METHODOLOGY

This study employs a qualitative case study approach to analyse ERM at an ODL institution. The methodology

involves a comprehensive review of internal documents, including risk management policies and incident reports, as well as semi-structured interviews with key personnel. The interviews focused on high-risk areas to gain a deeper understanding of the institution's risk management strategies and their effectiveness. Participants included 15 department heads, IT security officers, compliance managers, the examination manager, admission and records staff, and academic staff, selected based on their roles in institutional risk management.

This study is limited to a single ODL institution, as it is the only known institution with a structured Risk Management Committee. Other ODL universities either lack formal ERM frameworks or were unable to provide access for research. Despite this limitation, the findings offer valuable insights into ERM implementation in ODL settings. Future research could explore how other institutions approach risk management as ERM frameworks become more widely adopted.

Data Collection

Document Review:

The first phase of data collection involves a comprehensive review of the university's internal documents related to risk management. This includes risk management policies, compliance reports, internal audit records, and documented incidents related to technology failures, cybersecurity breaches, and academic misconduct. The document review provides a baseline understanding of how risks are identified, mitigated, and managed at the institutional level. By analysing these documents, we can evaluate both the scope and effectiveness of current risk management practices.

Semi-Structured Interviews:

The second phase involved conducting semi-structured interviews with key personnel from various departments within the university. Participants included department heads, IT security officers, compliance managers, examination officers, admission and records staff, LMS administrators, accreditation officers, student affairs representatives, international unit staff, facilities managers, academic staff, and library personnel. These individuals were selected based on their direct involvement in risk management within the institution. The semi-structured format provided flexibility, allowing interviewees to share their experiences and insights while ensuring consistency across key topics. The interviews explored daily risk management practices, the perceived effectiveness of the ERM framework, and challenges in implementing risk mitigation strategies. Additionally, they aimed to identify discrepancies between formal policies and actual practices, as well as uncover innovative solutions that may not be formally documented. To enhance the reliability of findings, data triangulation was applied by cross-referencing interview responses with internal reports, policy documents, and compliance records. This approach ensured a comprehensive and validated assessment of the institution's risk management framework.

Data Analysis

Data from the document review and interviews were analysed using thematic analysis. This approach enabled the identification of recurring themes, particularly in relation to technology risks, academic integrity, regulatory compliance, and student engagement. By cross-referencing findings from internal documents and interview responses, the analysis highlighted gaps in the current risk management framework and areas for improvement. Additionally, the study examined how well the institution's ERM strategies align with international standards, such as ISO 31000 for risk management and ISO 22301 for business continuity. This ensured a structured evaluation of the effectiveness and adaptability of existing risk management practices

Ethical Considerations

All participants in the interviews were provided with information about the study and gave informed consent before participating. Confidentiality was maintained by anonymising the interview data, and no sensitive institutional information has been disclosed. This methodology provides a robust framework for exploring the intricacies of risk management within ODL environment. By combining document analysis with qualitative

insights from key personnel, the study aims to deliver a comprehensive understanding of how ERM is applied in practice and highlight areas for improvement.

RESULTS AND DISCUSSION

This study's analysis of risk management at a selected ODL institution in Malaysia delineates a comprehensive risk landscape across multiple dimensions of its Online and Distance Learning (ODL) operations. Based on the Table 1, the risks are categorized into 5 main areas, reflecting diverse challenges that are intrinsic to the complex environment in which the university operates. Each category's risks have been rated from low to very high, enabling a prioritized approach towards risk mitigation (ISO 31000, 2018).

Table 1: Rating and Key Risk Events

	Category	Rating	Risk Event
1	Academic	Very High (VH)	Failure to meet regulatory and ranking requirement
		Low (L)	Failure to maintain the quality of assessment and evaluation
2	Human Capital	High (H)	Failure to maintain and acquire academic experts, specialisation and critical capabilities
		Medium (M)	Drop in staff productivity
3	Operation and Technological	Medium (M)	Information system failure/ service outrage
		Low (L)	Loss or leakage of critical data
4	Market	Medium (M)	Failure to maintain and expand international market share
		Low (L)	Loss of ODL market share
5	Geopolitical	High (H)	Unable to operate and/or repatriate revenue
		Medium (M)	Failure to comply international regulations
6	Student Management	High (H)	Increase in student attrition and drop-out rates
		Medium (M)	Ineffective student support services impacting engagement and retention

Academic Risks is the most pressing concern highlighted is the very high risk associated with failing to meet the regulatory bodies' standard and ranking requirements. Such shortcomings can critically undermine the university's reputation and its ability to attract and retain students (King and Boyatt, 2015). Additionally, the low risk tied to the quality of assessment and evaluation points to potential vulnerabilities in maintaining academic excellence and integrity, a fundamental aspect underscored by McCabe, Butterfield, and Treviño (2012).

Operational and Technological Risks are linked to information systems failures and data security, are identified as medium to low risks but could have severe repercussions on the university's operational continuity and integrity. The frequency of system failures and data breaches calls for an enhancement of the existing IT infrastructure and cybersecurity measures to safeguard sensitive information and ensure stability during critical academic activities (EdTech Magazine, 2024; Ed Scoop, 2024).

ODL institutions face difficulty retaining expert faculty due to limited career progression opportunities and the demand for digital teaching skills. Human capital risks manifest significantly in the challenges of acquiring and

retaining qualified academic staff and a noticeable drop in staff productivity. These risks directly impact the quality of education and institutional effectiveness, necessitating robust strategies for talent management and development (Lee & Hammer, 2020). Market-related risks, including the failure to expand international markets and loss of ODL market share, suggest a need for aggressive marketing strategies and innovative program offerings to sustain and grow the university's market presence.

Geopolitical risk is rated as high due to increasing international regulatory constraints and potential restrictions on cross-border online education. Geopolitical conflicts and failures in compliance with international regulations present medium risks, impacting institution's international operations and collaborations. These risks require proactive management to navigate the complex regulatory environments and maintain compliance with international standards (Adams & Bell, 2021). The dynamic nature of regulatory compliance in education further exacerbates these challenges, necessitating a more structured and anticipatory compliance strategy to keep pace with evolving standards (King and Boyatt, 2015).

Student management is a critical aspect of risk in Online and Distance Learning (ODL) institutions, as it directly affects retention, engagement, and overall institutional success. High student attrition rates pose a significant challenge, particularly in ODL settings where students often face barriers such as limited interaction with peers and instructors, difficulties in self-directed learning, and inadequate academic or administrative support (Simpson, 2013). Research indicates that online students are more likely to disengage and withdraw compared to traditional on-campus learners due to feelings of isolation and a lack of immediate academic guidance (Dixson, 2015).

One of the key risks in student management is the increase in student attrition and drop-out rates**,** which has been rated as a high-risk factor in this study. Attrition in ODL institutions is often linked to external factors such as work and family commitments, financial constraints, and technological barriers (Lee & Choi, 2011). Unlike conventional universities, ODL institutions cater to a diverse group of learners, many of whom are working professionals balancing multiple responsibilities. Without structured student engagement strategies and timely interventions, dropout rates may continue to rise, affecting institutional credibility and financial sustainability (Hart, 2012).

Another medium-risk factor is the ineffectiveness of student support services, which can impact student engagement and retention. Effective student support mechanisms, including academic advising, mental health counselling, and proactive communication, are crucial in ensuring student success in ODL environments (Tinto, 2017). Studies have shown that institutions implementing personalised learning support, frequent instructor feedback, and interactive online communities have lower dropout rates and higher student satisfaction levels (Martin & Bolliger, 2018). Without these support structures, students may struggle with academic and administrative issues, leading to frustration and eventual withdrawal from their programmes.

To mitigate these risks, ODL institutions must adopt targeted retention strategies, including early warning systems for at-risk students, enhanced tutor-student interaction, and student engagement analytics (Boyle et al., 2010). By leveraging technology such as artificial intelligence-driven learning analytics, institutions can track student participation patterns and intervene before disengagement escalates (Gašević et al., 2016). Additionally, fostering a strong sense of community through virtual networking events and discussion forums can help reduce the feeling of isolation among students (Kember, 1995).

RECOMMENDATIONS FOR ODL INSTITUTIONS.

Based on the findings, there are recommendations are proposed for ODL Institutions. to enhance its ERM practices and mitigate key risks: To enhance the accreditation processes, Open University Malaysia should develop a proactive accreditation task force dedicated to continuously updating and aligning academic programs with the latest accreditation standards. This could be complemented by regular training sessions for faculty and administrative staff to ensure a thorough understanding and compliance with accreditation requirements.

Investing in human capital development is vital for maintaining competitive edge and innovation. The university should introduce advanced training programs focused on leadership and risk management, and implement a talent acquisition strategy that prioritizes diversity and adaptability, aligning with the university's long-term

goals.

The findings highlight that geopolitical uncertainties and economic shifts impact regulatory compliance risks, necessitating adaptive accreditation strategies to maintain institutional stability. To mitigate geopolitical risks, forming a dedicated geopolitical risk assessment team would enable the university to stay informed about international events that could impact the university. Developing and regularly updating a geopolitical risk management plan, including strategies for rapid response to international crises, is essential.

Enhancing cybersecurity measures by upgrading cybersecurity infrastructure with the latest technology will protect sensitive data and prevent breaches. Regular cybersecurity training for all staff will ensure awareness of potential cyber threats and effective response strategies.

Broadening risk management training across all levels of the organization is also recommended to foster a culture of risk awareness and proactive management. Including risk management as a critical component of both the induction process for new employees and ongoing training for current staff will reinforce its importance.

Lastly, ODL institution should conduct annual reviews of the ERM framework to adapt to new risks and operational changes. Engaging external consultants to provide an independent assessment of the university's risk management practices can offer new perspectives and suggest areas for improvement.

Implementing these measures will significantly enhance the university's ability to manage high-risk areas, support its strategic objectives, and maintain its reputation as a leading institution in online and distance learning.

CONCLUSION

The study concludes that ODL institution's ERM framework effectively addresses many of the institution's risks, maintaining a low-to-moderate overall risk rating. However, the high-risk areas of Accreditation, Human Capital, and Geopolitical Conflicts require urgent and focused improvements. Recommendations include enhancing partner management protocols, strengthening human capital policies, and developing more robust strategies for geopolitical awareness and compliance

Future research could explore how emerging AI-driven risk management tools can further strengthen ODL institutions' resilience. As the digital education sector continues to expand, the development of more sophisticated risk management practices will be essential for maintaining the integrity and effectiveness of educational offerings.

REFERENCES:

1. Adams, R., & Bell, L. (2021). Enterprise risk management in higher education: A study of online learning institutions. Online Journal of Distance Learning Administration, 24(2), 34–45.
2. Bishop, M. (2020). Cybersecurity challenges in education: Protecting data in higher ed. Journal of Information Security Education, 15(3), 198–210.
3. Boyle, F., Kwon, J., Ross, C., & Simpson, O. (2010). Student retention in distance education: Are we failing our students? Open Learning: The Journal of Open, Distance and e-Learning, 25(2), 147-160. https://doi.org/10.1080/02680511003787313
4. Cyber Defense Magazine. (2024). Why higher education is so vulnerable to cyber-attacks — and what to do about it. Cyber Defense Magazine. Retrieved from https://www.cyberdefensemagazine.com/why-higher-education-is-so-vulnerable-to-cyber-attacks-and-what-to-do/
5. Dixson, M. D. (2015). Creating effective online courses: Engaging students through course design and facilitation. Journal of Educational Technology Systems, 43(4), 363-371. https://doi.org/10.2190/ET.43.4.b
6. Ed Scoop. (2024). Rising cybersecurity threats target U.S. higher education institutions. EdScoop. Retrieved from https://edscoop.com/rising-cybersecurity-threats-target-u-s-higher-education-institutions/
7. EdTech Magazine. (2024, March). Cyberattacks on higher ed rose dramatically last year, report shows. EdTech Magazine. Retrieved from https://edtechmagazine.com/higher/article/2024/03/cyberattacks-

higher-ed-rose-dramatically-last-year-report-shows
8. Gašević, D., Dawson, S., Rogers, T., & Gašević, D. (2016). Learning analytics should not promote one-size-fits-all: The effects of instructional conditions in predicting academic success. The Internet and Higher Education, 28, 68-84. https://doi.org/10.1016/j.iheduc.2015.10.002
9. Hart, C. (2012). Factors associated with student persistence in online programs: A review of the literature. Journal of Interactive Online Learning, 11(1), 19-42.
10. International Organization for Standardization. (2018). ISO 31000: Risk management – Guidelines. Geneva, Switzerland: ISO.
11. International Organization for Standardization. (2018). ISO 22301: Security and resilience – Business continuity management systems – Requirements. Geneva, Switzerland: ISO.
12. Kaplan, R. S., & Mikes, A. (2012). Risk management – The revealing hand. Harvard Business Review, 90(6), 48–60. Retrieved from https://hbswk.hbs.edu/item/risk-management-the-revealing-hand
13. Kember, D. (1995). Open learning courses for adults: A model of student progress. Educational Technology Publications.
14. King, M., & Boyatt, R. (2015). The impact of regulations on higher education: Ensuring compliance in online distance learning. Journal of Higher Education Policy and Management, 37(2), 123–134.
15. Lee, C., & Hammer, J. (2020). Engagement in online learning: Strategies for fostering student success. Educational Technology Research and Development, 68, 2031–2050.
16. Lee, Y., & Choi, J. (2011). A review of online course dropout research: Implications for practice and future research. Educational Technology Research and Development, 59(5), 593-618. https://doi.org/10.1007/s11423-010-9177-y
17. Malaysian Qualifications Agency. (2021). Quality assurance practices for higher education institutions in Malaysia. Kuala Lumpur, Malaysia: MQA.
18. Martin, F., & Bolliger, D. U. (2018). Engagement matters: Student perceptions on the importance of engagement strategies in the online learning environment. Online Learning, 22(1), 205-222. https://doi.org/10.24059/olj.v22i1.1092
19. McCabe, D. L., Butterfield, K. D., & Trevino, L. K. (2012). Cheating in academic institutions: A decade of research. Ethics & Behaviour, 11(3), 219–232.
20. McGetrick, J., & Gordon, M. (2019). Cybersecurity threats in higher education. Journal of Information Security, 12(1), 102-117.
21. Sevnarayan, K., & Maphoto, K. B. (2024). Exploring the dark side of online distance learning: Cheating behaviours, contributing factors, and strategies to enhance the integrity of online assessment. Journal of Academic Ethics, 22, 51–70. https://doi.org/10.1007/s10805-023-09501-8
22. Simpson, O. (2013). Supporting students in online, open, and distance learning (3rd ed.). Routledge. https://doi.org/10.4324/9780203070519
23. Tinto, V. (2017). Through the eyes of students. Journal of College Student Retention: Research, Theory & Practice, 19(3), 254-269. https://doi.org/10.1177/1521025115621917
24. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(39). https://doi.org/10.3390/fi13020039
25. Watson, G., & Sottile, J. (2010). Cheating in the digital age: Do students cheat more in online courses? Online Journal of Distance Learning Administration, 13(1).