

CLOUD COMPLIANCE CHALLENGES IN HIGHER EDUCATION: NAVIGATING FERPA, GDPR, AND LOCAL REGULATIONS

Rajesh PAVADI,

PhD., School of Computer and Information Sciences, University of the Cumberlands, USA

rajeshpavadi@gmail.com

Editor's Summary

The present paper is aimed at discussing cloud compliance peculiarities higher education institutions have to face when moving to cloud technologies to store information, learn, and manage administrative systems. It refers to the complexities of being in compliance with the most relevant laws such as FERPA in the United States, GDPR in Europe, and local data protection regulations. Some of the major approaches to attaining compliance that are used and discussed in the paper are the employment of compliance frameworks, technology solutions, and models of governance. There are case studies in successful cloud adaptations with a consideration of compliance. Finally, the paper highlights the practicability of striking the balance between innovation and compliance of institutions implementing the usage of cloud solution.

Abstract

Higher education is moving toward increased use of cloud technologies to revolutionize data storage, learning management, and administrative systems with benefits including their high levels of scalability, flexibility, and cost-efficiency. Nevertheless, the regulatory obstacles, such as FERPA, GDPR, and local data protection regulations are a complicating factor in adopting cloud-based solutions. This paper describes the challenge that institutions are facing which they can overcome by good compliance frameworks, technology solutions and important governance models. Although compliance is associated with advantages like greater data protection and augmented stakeholder confidence, it has various impediments to do with expenses and intricacy. The paper foretells the use of successful case studies of compliance-oriented cloud adoption and the discussion of new trends in cloud compliance which accentuate the necessity of proactive planning and continuous adjustment to the change in compliance rules.

Keywords: Compliance, FERPA, GDPR, Cloud Adoption, Data Privacy.

DOI: 10.31039/bjir.v2i7.57

IT systems to a level that suits their students, faculty, and employees. It is the power of the adaptation to new technologies and efficiency of the work that enables the institutions to remain competitive and answer the new requirementsⁱⁱⁱ.

An essential aspect of the practice in the education sector is compliance with data protection regulations such as FERPA, GDPR, and local regulations when the cloud technology is introduced. To save themselves against the threat of breaching their sensitive data and legal and financial implications, institutions should assure that their cloud vendors have these standards. The ability to address regulatory requirements, act proactively in planning the compliance and selecting vendors with well-developed compliance programs is bound to help meet the demands of the regulatory framework, and ensure accountability on the part of the institution.

2. THE PROMISE OF CLOUD IN HIGHER EDUCATION

Benefits of Cloud Computing for Educational Institutions

The benefits of cloud computing in higher education schools run deep as it provides great cost-effectiveness, flexibility of operations, and improved accessibility. Universities can now scale their IT-related resources based on their needs through Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) models and make massive hardware capital-purchasing investments unnecessary. Adopting the cloud helps institutions to make learning tools and administrative systems readily available to students, faculty, and staff so that they could collaborate easier and create conditions of remote learning^{iv}. Moreover, educational institutions are able to enhance service delivery by reducing the maintenance and upgraded costs of continuously running educational institutions since cloud providers assume the costs of maintaining infrastructure as well as upgrading the infrastructure. Being dexterous with the possibility to shift resources on-demand and in a municipal way, cloud computing in enablement universities to attend to altering necessities of the digital learning condition.

Cloud as a Solution to Traditional IT Challenges

Cloud computing resolves various difficulties related to conventional IT infrastructure issues in higher education including outdated systems and scalability. Most institutions have invested in and continue to use legacy systems that cannot stand up to the current requirements in regard to speed, capacity and flexibility^v. Cloud technologies do not have these limitations

because they involve flexible resources and the absence of bulky investments in on-site infrastructure^{vi}. By means of cloud-based solutions, universities will be able to expand and shrink with the requirements, which exhibit varying changes, more efficiently distribute resources, and stop straining internal information technology departments.

3. UNDERSTANDING THE COMPLIANCE LANDSCAPE

FERPA: Protecting Student Privacy in the Cloud

FERPA is an essential higher education regulation, and it helps higher learning institutions to keep education records of their students confidential. The institutions should implement a system and streamlined manner of data storage and access, taking into consideration the standards of FERPA, when they adopt cloud services. The essential factors to consider are the access control to sensitive student information, secure information sharing, and secure clouds^{vii}. When it comes to FERPA compliance, cloud vendors can support by providing encryption, access controls, and audit trails to make sure that the institutions have the needed privacy up to the requirement.

GDPR: The Global Data Privacy Standard

The General Data Protection Regulation (GDPR) places a rigid workload on the processing of personal data on the institutions located on the EU territory or the practices on data of EU origin. The topics covered by compliance with GDPR are issued related to obtaining consent when it comes to data processing, enforcing secure transfer of the data, and preserving the right of erasure^{viii}. Institutions should deal with cross-border transfers of data and must ensure that cloud providers meet the standards under GDPR, and this should include provision of adequate protection of personal data to the courts.

Local Regulations: Variations Across Jurisdictions

Universities and colleges also have to avoid local data protection laws like PIPEDA in Canada that puts in place certain privacy laws in how schools manage personal data. The issue emerges when institutions cross two or more jurisdiction with different rules and regulations^{ix}. Institutions need to make sure that cloud providers comply with those regulations and keep in mind all the challenges of dealing with the data on the international students and establish compliance related to various data protection laws.

4. CLOUD SECURITY AND DATA PRIVACY CHALLENGES

General Cloud Security Risks

Higher education institutions face considerable threats in terms of what cloud security can bring in terms of misconfigurations, information steals, and third-party access. Institutions have to have confidence in the cloud service providers so that sensitive information is safeguarded. It is important to have Clear Service Level Agreements (SLA), in order to agree responsibilities between the institution and the vendor^x. Confidentiality, integrity, and availability of data should be provided by institutions with rigorous security practices such as encryption, identity, and security policies.

Balancing Security with Accessibility

Accessibility is the key aspect needed to incorporate cloud security and ultimately cloud adoption in higher education. Putting into practice strong access controls and identity management processes like multi-factor authentication (MFA) is something that organisations have to do. This will make sure that unauthorized users access sensitive data and still provide flawless access to students and staff^{xxi}. Said security features are to be instated in secure platforms of remote learning to protect educational resources and personal information. The encryption is important to make data secure at any platform.



Figure 2 Balancing Security and Accessibility

5. COMPLIANCE MANAGEMENT STRATEGIES FOR CLOUD ADOPTION

Choosing the Right Cloud Providers

The institutions of higher learning should judge cloud providers based on compliance capacities like certifications such as ISO 27001 and SOC 2 and therefore see to it that suppliers comply with global and domestic standards. Pertinent is the fact that the data centres provided by the provider must be in line with the regulation particularly as far as protection of student data is concerned^{xii}. Due to regulatory changes and the need to minimize associated risks, institutions should consider employing vendors with strong compliance documentation, transparency, and data residency and security guidelines as their prime consideration^{xiii}.

Contractual and Operational Measures

Compliance clauses the institutions will have to insert compliance clauses in the cloud contracts such as data residency, access controls, and audit rights. Preliminary interaction with legal and compliance office is important so as to discuss the issues that may jeopardize service-level agreements (SLAs) and so as to see that the cloud services meet the institutions policies^{xiv}. Availability of clear contractual terms also serves to reduce the risks by indicating the obligations of both parties thus introducing accountability and additionally indicating methods of auditing the compliance of contract.

Building a Compliance-First Culture

Institutions should enhance a compliance-first culture by education of staff on the details and application of the applicable data privacy laws such as FERPA and GDPR to maintain compliance. This entails the frequent data security and compliance training. Also, institutions should conduct incessant monitoring and auditing, with the aid of automated tools to monitor compliance on-time and make changes in policies against any alterations in regulations. Compliance is proactive and this means that institutions will be responsible and minimize such exposure to legal risks^{xv}.

6. CASE STUDIES AND PRACTICAL INSIGHTS

University Adoption of Cloud with Compliance Focus

A number of higher education organizations have managed to traverse the cloudification complexities and still comply with data protection requirements like FERPA and GDPR. An example is the University of California, Berkeley, which changed to cloud delivery to improve the collaboration and bandwidth expansion^{xvi}. They had put in place effective data governance policies such as data encryption capabilities and data access restriction so as to safeguard student data and so as to be able to comply with FERPA regulations. European universities are also exploiting cloud solutions that make use of data centres in the EU giving it a data residency and protection as required by GDPR^{xvii}. Other activities by these institutions include regular data protection impact assessments and training of staff to ensure that they are compliant to these assessments.

Lessons from Cloud Failures in Education

Regardless of the advantages, there have been cases of institutions struggling to embrace cloud and this has resulted in non-compliance challenges. The most prominent is the 2017 information leak of a U.S. university where revelation of the records of private student data was witnessed since the settings of cloud storage were misconfigured. This episode demonstrated that it is essential to have appropriate cloud setup and access control. The institution changed its cloud security rules, introduced more rigid access to all data, and carried out extensive training of the staff regarding data protection procedures^{xviii}. They also contributed to the process of regular auditing to be certain that they adhere to FERPA and other rules regularly.

These case studies promote the importance of having a proactive higher education institution adopt cloud adoption and the need to be compliant, secure, and continuously monitoring sensitive student information.

7. THE FUTURE OF CLOUD AND COMPLIANCE IN HIGHER EDUCATION

Emerging Trends in Cloud Computing and Compliance

Machine learning and Artificial Intelligence (AI) are transforming the automatization of compliance in the higher education. The use of AI-based tools offers improved real-time threat detection, compliant reporting automation, and compliance with the changes in the regulations (GDPR, FERPA, etc.)^{xix}. As an example, ML algorithms allow you to deal with large volumes of data and discover their anomalies, enhancing data protection level and compliance checks. Amidst rising cloud adoption, institutions have to be ready to face issues to do with data jurisdiction, the shifting legality environment, and the necessity to be continuously monitored and thus in compliance.

Ongoing Adaptation to Regulatory Changes

Data protection is an area that is getting more and more complicated by regulation. Laws Institutions need to be aware of new laws and the upcoming law in 2023, the Digital Operational Resilience Act (DORA) and Consumer Privacy Protection Act (CPPA) so they can comply^{xx}. Cloud technologies are therefore critical in ensuring a fit in such changes to include having scalable solutions that are immensely updateable in real-time in a bid to comply with the law. The use of standards, such as the EU Cloud Code of Conduct would help the institutions in harmonizing their cloud services with data protection regulations.

8. CONCLUSION

Conclusively, Key issues institutions of higher learning encounter when implementing cloud technologies are issues of abidance by regulations such as FERPA, GDPR, and local data protection rules. The niceties of maintaining data privacy, access control measures, and regulatory frameworks have to be planned well and continuously monitored. Although the flexibility, scalability, and operational efficiency of cloud adoption are bigger advantages, they should strike the right balance with the strong compliance frameworks, so as to safeguard student and institutional data that is considered sensitive.

Such difficulties need to be overcome with proactive compliance planning as the primary concern of the institutions. It is important to involve legal and IT staff in the cloud

adoption process early enough, vet the vendors to ensure they comply with the regulations and consider the use of continuous monitoring. In this way, higher learning institutions will be able to utilize the cloud technologies competently at the same time having the required adherence to shifting regulations.

REFERENCES

- ⁱHewardMills. (2025). Preparing for data protection and privacy laws coming into force in 2025 | HewardMills. Hewardmills.com. https://www.hewardmills.com/preparing-for-data-protection-and-privacy-laws-coming-into-force-in-2025/?utm_source=chatgpt.com
- ⁱⁱ Helaimia, R. (2023). Cloud computing in higher education institutions: pros and cons. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(ISSN: 2980-0811).
- ⁱⁱⁱ Al Hadwer, A., Tavana, M., Gillis, D., & Rezanian, D. (2021). A systematic review of organizational factors impacting cloud-based technology adoption using technology-organization-environment framework. *Internet of Things*, 15, 100407.
- ^{iv} Azem Qashou, A. M., Bahar, N., & Mohamed, H. (2025). Qualitative Exploration of Data Security Risks in Mobile Cloud Computing for Higher Education. *Security and Privacy*, 8(2), e70001.
- ^v Alam, A. (2021, December). Cloud-based e-learning: development of conceptual model for adaptive e-learning ecosystem based on cloud computing infrastructure. In *International Conference on Artificial Intelligence and Data Science* (pp. 377-391). Cham: Springer Nature Switzerland.
- ^{vi} Renjith, E. J. An Effective Method for Ensuring Data Privacy and Security in Digital Education using Cloud Computing. *Eureka Publications*, 109.

- ^{vii} Thavi, R., Jhaveri, R., Narwane, V., Gardas, B., & Jafari Navimipour, N. (2024). Role of cloud computing technology in the education sector. *Journal of Engineering, Design and Technology*, 22(1), 182-213.
- ^{viii} Al-Malah, D. K. A. R., Aljazaery, I. A., Alrikabi, H. T. S., & Mutar, H. A. (2021, February). Cloud computing and its impact on online education. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1094, No. 1, p. 012024). IOP Publishing.
- ^{ix} Sharma, D. K., Boddu, R. S. K., Bhasin, N. K., Nisha, S. S., Jain, V., & Mohiddin, M. K. (2021, October). Cloud computing in medicine: Current trends and possibilities. In *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)* (pp. 1-5). IEEE.
- ^x Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, 14(1), 11.
- ^{xi} Yanamala, A. K. Y. (2024). Emerging challenges in cloud computing security: A comprehensive review. *International Journal of Advanced Engineering Technologies and Innovations*, 1(4), 448-479.
- ^{xii} Babalola, O., Adedoyin, A., Ogundipe, F., Folorunso, A., & Nwatu, C. E. (2024). Policy framework for Cloud Computing: AI, governance, compliance and management. *Glob J Eng Technol Adv*, 21(02), 114-26.
- ^{xiii} Yusuf, N. (2024, March). Cloud management for maximizing security and compliance in business. In *AIP Conference Proceedings* (Vol. 2816, No. 1, p. 110005). AIP Publishing LLC.
- ^{xiv} Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2025). Cloud security challenges and solutions: A review of current best practices. *Int J Multidiscip Res Growth Eval*, 6(1), 26-35.
- ^{xv} Islam, R., Patamsetti, V., Gadhi, A., Gondu, R. M., Bandaru, C. M., Kesani, S. C., & Abiona, O. (2023). The future of cloud computing: benefits and challenges. *International Journal of Communications, Network and System Sciences*, 16(4), 53-65.

- ^{xvi} Yusuf, N. (2024, March). Cloud management for maximizing security and compliance in business. In AIP Conference Proceedings (Vol. 2816, No. 1, p. 110005). AIP Publishing LLC.
- ^{xvii} Folorunso, A., Adewa, A., Babalola, O., & Nwatu, C. E. (2024). A governance framework model for cloud computing: Role of AI, security, compliance, and management. *World Journal of Advanced Research and Reviews*, 24(2), 1969-1982.
- ^{xviii} Babalola, O., Adedoyin, A., Ogundipe, F., Folorunso, A., & Nwatu, C. E. (2024). Policy framework for Cloud Computing: AI, governance, compliance and management. *Glob J Eng Technol Adv*, 21(02), 114-26.
- ^{xix} Islam, R., Patamsetti, V., Gadhi, A., Gondu, R. M., Bandaru, C. M., Kesani, S. C., & Abiona, O. (2023). The future of cloud computing: benefits and challenges. *International Journal of Communications, Network and System Sciences*, 16(4), 53-65.
- ^{xx} Scott, H. S. (2021). The EU's Digital Operational Resilience Act: Cloud Services & Financial Companies. Available at SSRN 3904113.