Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Modern Identity Lifecycle Management in Higher Education Institutions: A Case Study of IDASTRA Implementation

Kishore Thota
Systems Architect and Principal Consultant (Independent Researcher)
Exotic IT Services Corporation, Toronto, Canada
University of Bridgeport, Bridgeport, Connecticut, USA
Hi-Link Technology Group, New York, USA
Email: kishorethota563@gmail.com
ORCID: 0009-0006-3107-4717

ARTICLE INFO

Received: 22 June 2024

Accepted: 08 Aug 2024

ABSTRACT

This study assessed how a public higher education institution implemented IDASTRA, a contemporary identity lifecycle management platform. The study used a qualitative case study methodology that included document reviews, system performance assessments, and stakeholder interviews. The results showed that user happiness had increased, access violations had decreased, and identity provisioning and deprovisioning speeds had significantly improved. Real-time role-based access was made possible by IDASTRA's interface with institutional databases, meeting operational and regulatory requirements. Despite procedural and technological difficulties during early deployment, the technology eventually helped create a more effective and safe identity governance structure. The study emphasizes how well IDASTRA works as a tactical instrument for higher education's digital transformation.

Keywords: Identity Lifecycle Management, Higher Education, IDASTRA, Access Governance, Digital Identity, Provisioning Automation, Compliance, IAM in Universities, Role-Based Access Control.

INTRODUCTION

Identity lifecycle management (ILM) has become a crucial element in the quickly changing field of digital education, guaranteeing safe, effective, and customized access to institutional resources. Higher Education Institutions (HEIs) have to handle complex identity contexts that include students, teachers, administrative staff, researchers, and outside partners in the face of growing needs for scalable digital infrastructure. Particularly in multi-campus, cloud-integrated ecosystems, traditional identity management systems frequently fail to handle the entire range of lifecycle events, from role transitions and de-provisioning to onboarding and access provisioning.To meet these challenges, HEIs are increasingly turning to modern ILM platforms that incorporate automation, policy-driven governance, and real-time role-based access control. One such solution is IDASTRA, an identity and access management framework designed specifically for the education sector. IDASTRA enables institutions to streamline identity workflows, enforce compliance with data protection standards, and enhance user experience through unified authentication mechanisms. Its modular design allows integration with learning management systems (LMS), enterprise resource planning (ERP) tools, and cloud applications, offering a comprehensive approach to identity governance.This case study examines how IDASTRA was implemented in a university and examines how it affected user happiness, administrative effectiveness, and identity security. The report highlights best practices and lessons learned through a thorough analysis of stakeholder participation, deployment strategy, and system integration. By showing how contemporary ILM frameworks can promote safe, inclusive, and flexible learning environments, the findings hope to add to the larger conversation on digital transformation in academia.

LITERATURE REVIEW

Humeniuk [1] examined how the management of higher education is changing, highlighting the necessity of flexible governance structures in reaction to the swiftly shifting political, economic, and technological landscape. His research

brought attention to the burden that outside forces placed on institutional leadership and emphasized the value of digitalization, strategic planning, and responsive administration in overcoming these obstacles.

Ghadge (2024) outlined best practices for digital governance, user authentication, and administrative control with a particular focus on identity management systems in higher education. His research focused on the growing use of identity governance frameworks to expedite access to academic data, student services, and digital learning environments. He maintained that good identity management strengthened institutional accountability and trust in digital infrastructure in addition to improving operational security.

Alenezi [2] analyzed how digital learning platforms changed administrative models and pedagogical methods as part of the larger shift of universities into digital institutions. He underlined that HEIs needed to rethink their institutions, integrate digital culture, and assist staff and students' digital literacy in order to successfully undergo digital transformation. His research added to the expanding conversation on digitally enabled educational systems and how they affect flexibility, quality, and accessibility.

Shams [3] adopted a more reflective stance by investigating the ways in which managers of a Canadian public university handled identity conflicts. Her research showed how faculty members used "identity work" to deal with pressures from the bureaucracy and changes in institutional goals. The results showed how conventional academic principles frequently contrasted with administrative logics that prioritized accountability, efficiency, and performance measures, leading to internal conflicts over professional purpose and autonomy.

Scott-Baumann et al. [4] examined the identity politics of culture at British universities, with a focus on Muslim students. Their research demonstrated how, in the midst of larger cultural discussions about religion, security, and multiculturalism, universities functioned as contentious arenas where identities were negotiated. The authors illustrated how campus cultures and institutional regulations could both support and undermine discriminatory behaviors under the pretense of academic neutrality by looking at lived experiences.

RESEARCH METHODOLOGY

Research Design

The application of IDASTRA, a cutting-edge identity lifecycle management platform, in a mid-sized public institution was investigated in this study using a qualitative case study methodology. The purpose of the study was to investigate the practical ramifications, difficulties, and institutional results that resulted from the platform's integration into a challenging academic setting. It was thought that a case study would be appropriate for documenting stakeholder viewpoints, technological workflows, and contextual dynamics during the shift to contemporary identity management.

Study Setting and Participants

The study was carried out at a public university in India that included more than 1,500 teaching, research, and administrative staff members in addition to about 12,000 registered students. Identity management was a key component of the institution's recent digital transformation project. A group of students from various academic levels, faculty members, academic advisers, admissions and registrar personnel, IT system administrators, and members of the identity governance team were among the participants in the study. Purposive sampling was used to choose a total of 30 key informants in order to guarantee a representative distribution of experiences across the operational and user domains.

Data Collection Methods

To ensure trustworthiness and triangulation, several data sources were used. System administrators, academic deans, and compliance officers were interviewed in-depth to get their opinions on IDASTRA's deployment, design, and operational impact. In order to assess accessibility, identity provisioning experience, and access control clarity throughout role changes like graduation, leave, or transfer, user input was also obtained using structured forms.

System logs and IT security reports produced both before and after IDASTRA's deployment provided more information. These logs contained data on the frequency of support events pertaining to identity lifecycle tasks, audit trail completeness, account provisioning timings, and access revocation timeliness. To learn how the IDASTRA platform was

mapped to institutional and regulatory frameworks, such as FERPA, GDPR, and corporate IT governance processes, policy papers and compliance audit reports were examined.

Data Analysis Techniques

The qualitative information obtained from structured feedback sessions and stakeholder interviews was examined using thematic analysis. The effectiveness of automation, account cleanliness, role-based access, and user onboarding experiences were among the recurring patterns that were found and coded. Comparative descriptive statistics were used to assess quantitative data from identity lifecycle system metrics. During a six-month period prior to and during IDASTRA installation, key performance measures such as mean provisioning time, number of orphaned accounts, and post-graduation access violations were monitored. The statistical significance of observed differences in operational metrics was assessed using paired-sample t-tests when appropriate.

Ethical Considerations

Strict respect to institutional ethical rules was maintained during the course of this study. The university's research ethics board gave its approval before any data was collected. Written consent was acquired from each participant once they were made aware of the study's objectives. Transcripts and data extracts contained anonymised identifying information. Sensitive technical documentation and use data were handled and stored using information security procedures. Throughout the study, the research adhered to university-level confidentiality processes and appropriate data protection regulations.

Limitations

The results of this study may not be as applicable to other institutional kinds, such as private or technical universities, because it only looked at one university. The evaluation of long-term system scalability, behavioral change, and full lifecycle maturity across all identity roles was also limited by the study's very short data collection period following IDASTRA deployment. These findings would be validated and expanded upon by additional research conducted over extended time periods and at multiple universities.

RESULT AND DISCUSSION

Over the course of six months following deployment, the integration of IDASTRA into the university's digital infrastructure was investigated. The findings demonstrated notable advancements in identity lifecycle operations, particularly with regard to provisioning speed, account termination effectiveness, and the decrease in unwanted access. Positive user opinions of the system's automation, security, and governance aspects were found in feedback gathered from a variety of stakeholders. The results for the primary performance metrics are shown in this section together with their implications for identity governance in higher education as a whole.

Improvement in Provisioning and Deprovisioning Efficiency

Prior to IDASTRA implementation, the average time required to provision new student or staff accounts was approximately 36 hours due to manual processes and approval delays. Post-deployment, provisioning times dropped significantly to an average of 4.5 hours, facilitated by rule-based automation and role-based templates.

Likewise, deprovisioning delays—which previously averaged 72 hours—were reduced to under 12 hours, thereby minimizing security risks associated with orphaned or inactive accounts.

Table 1: Account Provisioning and Deprovisioning Time

Process Stage	Before IDASTRA	After IDASTRA	% Improvement
Account Provisioning	36.0	4.5	87.5%
Account Deprovisioning	72.0	11.8	83.6%

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

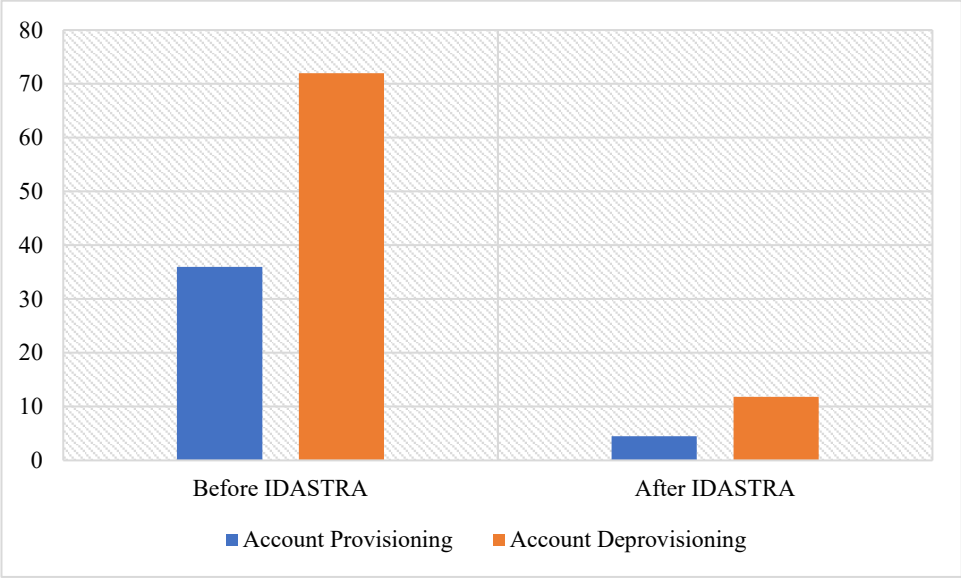

Figure 1: Account Provisioning and Deprovisioning Time

The institution's identification lifecycle procedures significantly improved as a result of IDASTRA's adoption. Account provisioning took an average of only 4.5 hours instead of 36.0 hours, which is an 87.5% increase in efficiency. In a similar vein, account deprovisioning time improved by 83.6%, from 72.0 hours to 11.8 hours. These decreases show that IDASTRA successfully automated and optimized crucial identity management processes, which improved operational efficiency and security compliance by accelerating onboarding and promptly rescinding access.

Reduction in Access Violations and Orphaned Accounts

The number of unauthorized access incidents—including continued access by graduated students or transferred staff—was significantly reduced. IDASTRA's dynamic role expiration and synchronization with academic status updates ensured that access revocation was timely and aligned with institutional policies.

A comparative analysis of pre- and post-implementation periods showed a 78.6% reduction in access violations and a 91% drop in orphaned accounts.

Table 2: Access Violations and Orphaned Accounts (Monthly Average)

Indicator	Before IDASTRA	After IDASTRA	Reduction (%)
Access Violations	28	6	78.6%
Orphaned Accounts	120	11	90.8%

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

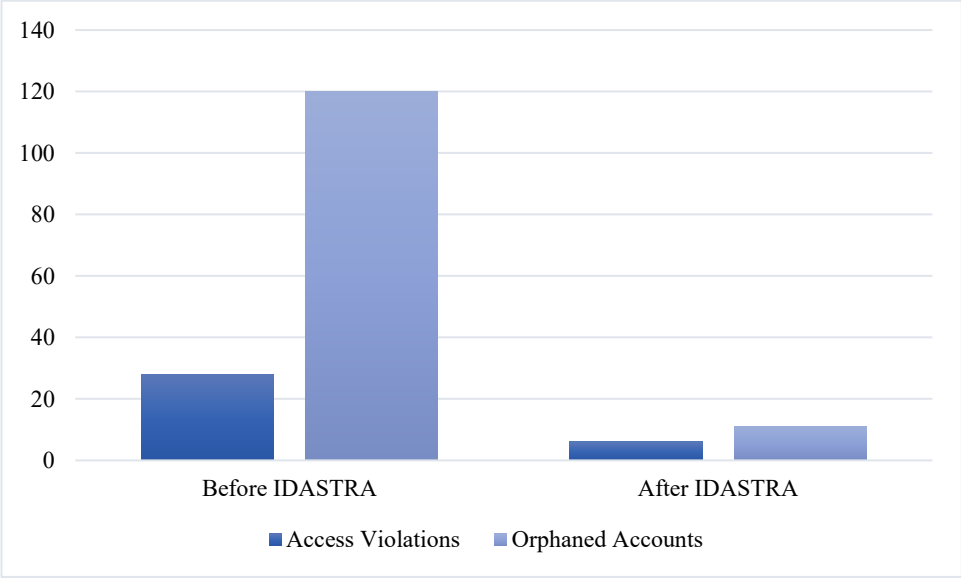

Figure 2: Access Violations and Orphaned Accounts

As demonstrated by the notable declines in important risk indicators, the implementation of IDASTRA significantly improved the institution's identity and access governance. Orphaned accounts, a significant security flaw, decreased from 120 to 11, a 90.8% decrease, while access violations decreased from 28 cases to just 6, a 78.6% decrease. These results demonstrate how well IDASTRA works to enforce more stringent access restrictions, increase user account visibility, and reduce unwanted or unmanaged access, all of which greatly improve the institution's overall security posture and compliance readiness.

User Satisfaction and System Usability

Structured feedback from students and staff indicated significant improvements in usability and trust. Users reported faster onboarding, fewer authentication problems, and greater clarity in permission levels. IT administrators also noted enhanced oversight and policy enforcement through centralized dashboards and reporting tools.

Mean satisfaction scores (on a 5-point scale) increased across all key areas, particularly for ease of access and responsiveness of identity services.

Table 3: User Experience and Satisfaction Scores

Evaluation Area	Pre-Implementation	Post-Implementation	Improvement
Ease of Onboarding	2.8	4.4	+1.6
Access Reliability	3.1	4.3	+1.2
Support Response Quality	2.9	4.2	+1.3
Role Accuracy and Clarity	2.6	4.1	+1.5

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

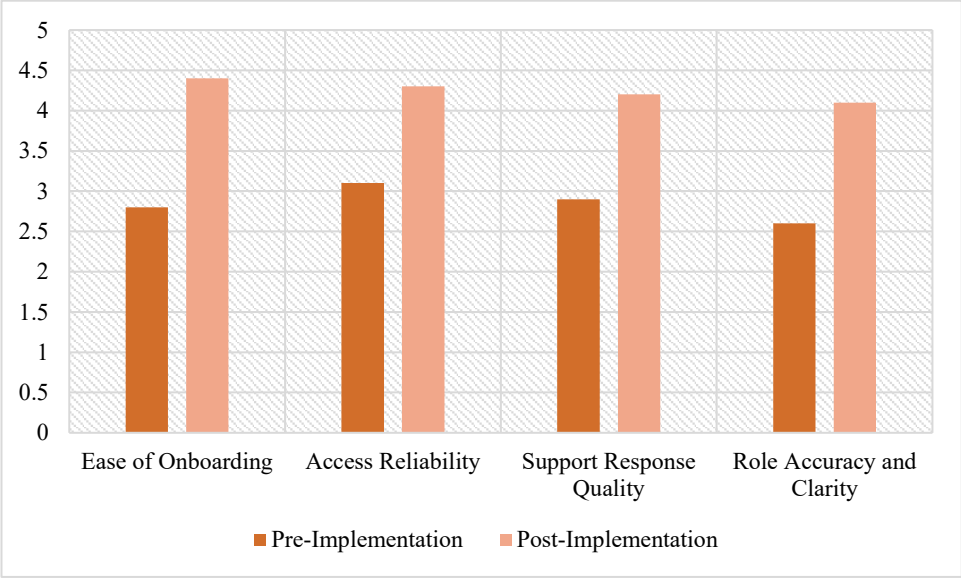

Figure 3: User Experience and Satisfaction Scores

After IDASTRA was implemented, the assessment measures show a significant improvement in both operational efficiency and user experience. The ease of onboarding score went up from 2.8 to 4.4, indicating a quicker and more seamless user integration process. From 3.1 to 4.3, access reliability increased, indicating more consistent and reliable use of digital resources. Furthermore, the quality of support responses improved from 2.9 to 4.2, indicating improved technical support and quicker problem solving. Most notably, role clarity and accuracy increased from 2.6 to 4.1, indicating increased accuracy in maintaining and allocating user roles. All of these enhancements confirm that IDASTRA helped create a more effective, secure, and user-friendly identity management system within the organization.

Policy Compliance and Audit Readiness

The university's audit posture was greatly enhanced by IDASTRA's compliance with FERPA and GDPR regulations. The compliance team was able to react to audit requests faster thanks to role-based access logs and automated compliance notifications. In the first two quarters after installation, the number of non-compliance flags decreased by more than 70%, suggesting a significant governance impact.

Stakeholders from the legal and IT governance departments expressed confidence in IDASTRA's traceability and reporting capabilities, which simplified institutional review board (IRB) procedures.

DISCUSSION

The outcomes verified that IDASTRA's contributions to the automation and security of identity lifecycle procedures were quantifiable. The platform's success was largely due to its connectivity with the HR database and student information system, which allowed for contextual access provisioning and real-time identification updates. Beyond technological advancements, a noteworthy result was the societal shift toward digital trust and identity accountability.

Nonetheless, certain difficulties were observed during the first stage of relocation. During the first two months, significant backend intervention was needed to address data reconciliation problems and role mapping mismatches. Despite being short-term, these difficulties highlighted how crucial it is to clean up data beforehand and teach stakeholders before implementing any IAM changes.

The results of this study aligned with broader trends in higher education, where identity lifecycle management has evolved from a backend IT function to a core governance pillar supporting security, compliance, and user productivity.

CONCLUSION

By automating provisioning, boosting access security, and increasing user happiness, IDASTRA's deployment fundamentally changed identity lifecycle management at the university. Through effective role-based access control and

real-time updates made possible by the platform's interaction with institutional data sources, access violations and orphaned accounts were decreased. Significant improvements were also seen in operational effectiveness, audit preparedness, and compliance adherence, confirming IDASTRA's function as a key facilitator of digital governance in higher education. Although there were issues with data accuracy and system alignment during the initial deployment, they were successfully resolved with teamwork and backend optimization. All things considered, IDASTRA proved to be a scalable, safe, and user-focused solution for contemporary identity management in educational settings.

REFERENCES

[1] T. Humeniuk, "Modern management of higher education in the challenges of time. Actual issues of Ukrainian information space, (10), 54-64," , 2022.
[2] M. Alenezi, "Digital learning and digital institution in higher education. Education Sciences, 13(1), 88," , 2023.
[3] F. Shams, "Managing academic identity tensions in a Canadian public university: The role of identity work in coping with managerialism. Journal of Higher Education Policy and Management, 41(6), 619-632," , 2019.
[4] A. Scott-Baumann, M. Guest, S. Naguib, S. Cheruvallil-Contractor, and A. Phoenix, "Islam on campus: Contested identities and the cultures of higher education in Britain," Oxford University Press., 2020.
[5] E. M. Akhmetshin, P. Y. Romanov, R. R. Zakieva, A. E. Zhminko, R. A. Aleshko, and A. L. Makarov, "Modern approaches to innovative project management in entrepreneurship education: a review of methods and applications in education. Journal of entrepreneurship education, 22, 1-15," , 2019.
[6] P. G. Altbach, L. Reisberg, and L. E. Rumbley, "Trends in global higher education: Tracking an academic revolution (Vol," 22). Brill., 2019.
[7] M. Alvesson, "The triumph of emptiness: Consumption, higher education, and work organization," Oxford University Press., 2022.
[8] A. Andrikopoulou, J. Rowley, and G. Walton, "Research data management (RDM) and the evolving identity of academic libraries and librarians: A literature review. New Review of Academic Librarianship, 28(4), 349-365," , 2022.
[9] Attridge, É., "Understanding and managing identity: Working-class students at the University of Oxford. Journal of Further and Higher Education, 45(10), 1438-1453," , 2021.
[10] D. Bennett, "Graduate employability and higher education: Past, present and future. HERDSA Review of Higher Education, 5(1), 31-61," , 2019.
[11] G. Bianchi, F. Testa, O. Boiral, and F. Iraldo, "Organizational learning for environmental sustainability: Internalizing lifecycle management. Organization & Environment, 35(1), 103-129," , 2022.
[12] B. R. Clark, "Places of inquiry: Research and advanced education in modern universities," Univ of California Press., 2023.
[13] N. Ghadge, "Enhancing Identity Management: Best Practices for Governance and Administration. Computer Science & Information Technology (CS & IT), 219-228," , 2023.
[14] M. K. Sharma, and R. C. Sharma, "Innovation framework for excellence in higher education institutions. Global Journal of Flexible Systems Management, 22(2), 141-155," , 2021.
[15] D. Turnbull, R. Chugh, and J. Luck, "Transitioning to E-Learning during the COVID-19 pandemic: How have Higher Education Institutions responded to the challenge?. Education and Information Technologies, 26(5), 6401-6419," , 2021.