FINAL PROJECT: Cloud Computing

Devansh Naimish Patel

Ottawa University, Brookfield, WI

CLOUD-COMPUTING-IT-8003-FA2-2024

Dr. Cyndi Lambach

December 13th, 2024

Introduction

A.IX Capital, a small fintech startup, seeks to innovate rapidly in the provision of algorithm-based robo-advisory services. Cloud computing offers the scalability, flexibility, and cost-efficiency needed to support its technical requirements. However, adopting cloud computing involves making informed decisions on deployment and service models, governance, security, integration, and continuous management. This case study provides a structured methodology—based on a ten-step prescriptive series—to guide A.IX Capital's leadership and IT team from initial strategy through ongoing management. Integrating insights from previous analyses and newly added steps, this comprehensive report details the rationale behind each decision and explains how the chosen solutions align with the company's mission and constraints.

Assemble Your Team

The first step in cloud adoption is assembling a cross-functional team composed of senior management, IT specialists, business representatives, finance officers, legal counsel, and administrative personnel. A.IX Capital has fewer than ten employees, enabling rapid decision-making and collaboration. The founder and CEO provides strategic direction, while a lead developer and systems architect handle technical assessments. Business and marketing professionals ensure alignment with customer needs, and finance and legal counsel guide cost optimization and regulatory compliance.

This lean, integrated team fosters open communication and ensures each decision is made with both business objectives and technical realities in mind. Having all stakeholders engaged early prevents misalignments, accelerates decision-making, and ensures that cloud-related initiatives are well-understood and supported across the organization.

Develop a Business Case and an Enterprise Cloud Strategy

A.IX Capital's cloud strategy aims to deliver secure, scalable services efficiently. The business case highlights cost reduction opportunities, accelerated time-to-market for new robo-advisor features, and the ability to handle fluctuating workloads without over-provisioning on-premises infrastructure. The strategy aligns with the company's goals: focus on algorithm development rather than infrastructure management, ensure compliance with financial regulations, and maintain agility in an increasingly competitive fintech market (Marston et al., 2011; El-Gazzar, 2014).

Adopting a cloud environment enables the company to leverage pay-as-you-go pricing, minimize capital expenditures, and access advanced services—such as automated scaling and integrated analytics—faster than would be possible with traditional data centers.

Select Cloud Deployment Model(s)

After evaluating private, public, and hybrid models, A.IX Capital decided on a hybrid cloud deployment. The hybrid model combines a secure, outsourced private cloud environment for mission-critical applications and sensitive data with the scalability and cost advantages of public cloud services for non-critical workloads (Khajeh-Hosseini et al., 2010). This approach ensures compliance with regulatory requirements and data security standards, while still allowing the company to dynamically expand resources.

The hybrid deployment aligns with A.IX Capital's needs by placing sensitive financial data and core algorithms in a controlled environment and offloading development, testing, and high-demand workloads to a public cloud, optimizing cost and performance.

Select Cloud Service Model(s)

Platform as a Service (PaaS) emerged as the primary cloud service model. PaaS simplifies the development, testing, and deployment processes by managing underlying infrastructure. By choosing a PaaS like Red Hat OpenShift Online, which supports Python and Django (the languages of the robo-advisor's algorithms), the team can focus on core competencies rather than maintenance (Red Hat, 2016).

While PaaS is central, A.IX Capital remains open to leveraging Infrastructure as a Service (IaaS) for specific scenarios requiring deeper control and Software as a Service (SaaS) for ancillary services like CRM or accounting tools. This combination ensures flexibility without increasing operational overhead.

Determine Who Will Develop, Test, and Deploy the Cloud Services

In-house development and deployment was chosen to maintain control, ensure customization, and leverage existing technical expertise. The in-house team's familiarity with the algorithms and regulatory environment reduces integration complexity and aligns development timelines with business goals. While external providers could accelerate certain aspects, in-house development ensures tighter integration with legacy systems and retains intellectual property internally.

This decision is supported by Agile and DevOps methodologies to streamline development cycles, enhance collaboration between developers and operations staff, and facilitate continuous integration and deployment (Beck et al., 2001; Fitzgerald & Stol, 2017).

Develop Governance Policies and Service Agreements

Robust governance and well-defined service agreements ensure that cloud adoption aligns with security, compliance, and performance requirements. A.IX Capital's governance framework addresses data residency, regulatory compliance (e.g., GDPR), and internal audit

trails. Service Level Agreements (SLAs), Acceptable Use Policies (AUPs), and vendor contracts are reviewed carefully to clarify responsibilities, escalation paths, and remediation procedures (CSCC, 2015; NIST, 2012).

Transparency and accountability are paramount. Regular reviews of metrics and periodic audits build confidence among stakeholders and reduce the risk of disputes or misunderstandings with cloud providers.

Assess and Resolve Security and Privacy Issues

Security and privacy remain top concerns for any fintech enterprise. A.IX Capital adopts a risk-based approach, classifying data, applying appropriate encryption, and enforcing strict access controls. Compliance with standards like ISO/IEC 27001(International Organization for Standardization/International Electrotechnical Commission) and adherence to OWASP (Open Worldwide Application Security Project) guidelines ensure robust security baselines (ISO/IEC, 2013; OWASP, 2021).

Risk assessments guide decisions on where data resides and who can access it. Continuous monitoring and incident response planning mitigate threats without causing decision-making paralysis. By framing security as a manageable business enabler rather than an insurmountable challenge, the company avoids overreaction that could hinder innovation.

Integrate with Existing Enterprise Services

Integration with existing enterprise services is essential to maintaining operational continuity. The hybrid model facilitates seamless communication between on-premises systems (or outsourced private infrastructure) and public cloud environments. Well-defined APIs (Application Programming Interface), standardized data formats, and consistent authentication and authorization mechanisms ensure interoperability (Armbrust et al., 2010).

A.IX Capital invests in middleware and integration tools to synchronize data, enable secure file transfers, and maintain transactional integrity. Thorough integration testing ensures that legacy systems, such as on-premises databases or internal analytics tools, work seamlessly with cloud-based components.

Develop a Proof-of-Concept (POC) Before Moving to Production

Before fully deploying mission-critical applications, A.IX Capital implements a proof-of-concept environment. The POC tests the chosen PaaS platform's scalability, evaluates latency, and verifies security controls and compliance in a controlled setting. By simulating load conditions, testing failover procedures, and measuring performance against defined SLAs (Service Level Agreements), the POC reveals issues early, preventing costly rework later.

The POC also helps refine best practices in CI/CD (Continuous Inegration/Deployment) pipelines, infrastructure-as-code management, and containerization strategies. Stakeholders gain confidence that the chosen solutions will support production workloads reliably (Li et al., 2010).

Manage the Cloud Environment

Long-term success depends on effective cloud environment management. A.IX Capital establishes continuous monitoring for system performance, resource utilization, and security events. Using tools such as AWS CloudWatch, integrated logging, and analytics ensures that performance bottlenecks, anomalies, or security incidents are promptly addressed (Amazon Web Services, 2021).

Regular reviews of policies, SLAs, and emerging regulations keep governance frameworks current. Employee training ensures ongoing competence in secure coding, data handling, and incident response. Continuous improvement loops incorporate feedback from stakeholders, allowing the environment to evolve as business requirements change, new features are introduced, or market conditions shift (Fitzgerald & Stol, 2017).

Conclusion

The comprehensive approach outlined in this case study enables A.IX Capital to confidently adopt cloud computing, from assembling a cross-functional team through managing the environment over time. Decisions such as choosing a hybrid cloud model, focusing on PaaS for rapid development, and maintaining in-house deployment capabilities ensure the company's innovations remain agile, secure, and aligned with regulatory obligations. Robust governance frameworks, clear service agreements, and a balanced view of security and privacy transform potential roadblocks into manageable challenges. Integration with existing services, a carefully executed proof-of-concept, and continuous management practices support sustained adaptability and growth.

By embracing a structured, step-by-step methodology, A.IX Capital navigates the complexities of cloud adoption while preserving strategic focus. The result is a cloud-enabled infrastructure that empowers the organization to deliver advanced, compliant, and competitive robo-advisory services to its clients.

References

Amazon Web Services. (2021). *AWS Service Level Agreements*. Retrieved from https://aws.amazon.com/legal/service-level-agreements/

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58. https://doi.org/10.1145/1721654.1721672

Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., … & Thomas, D. (2001). *Manifesto for Agile Software Development*. Agile Alliance. https://agilemanifesto.org/

Cloud Standards Customer Council (CSCC). (2015). *Practical Guide to Cloud Service Agreements V2.0*. Retrieved from https://www.omg.org/cloud/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf

El-Gazzar, R. F. (2014). A literature review on cloud computing adoption issues in enterprises. *International Journal of Business and Management*, 9(1), 151–165. https://doi.org/10.5539/ijbm.v9n1p151

Fitzgerald, B., & Stol, K.-J. (2017). Continuous software engineering: A roadmap and agenda. *Journal of Systems and Software*, 123, 176–189. https://doi.org/10.1016/j.jss.2015.06.063

ISO/IEC. (2013). *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements*. International Organization for Standardization.

Khajeh-Hosseini, A., Sommerville, I., & Sriram, I. (2010). Research challenges for enterprise

cloud computing. *arXiv preprint arXiv:1001.3257*. https://arxiv.org/abs/1001.3257

Li, A., Yang, X., Kandula, S., & Zhang, M. (2010). CloudCmp: Comparing public cloud providers. In *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement* (pp. 1–14). ACM. https://doi.org/10.1145/1879141.1879143

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, 51(1), 176–189. https://doi.org/10.1016/j.dss.2010.12.006

NIST. (2012). *NIST Cloud Computing Synopsis and Recommendations* (Special Publication 800-146). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-146

OWASP. (2021). *OWASP Top Ten Web Application Security Risks*. OWASP Foundation. https://owasp.org/www-project-top-ten/