Critical Evaluation of Cloud Operations and Management

Adaptation within the Regulated Swiss Financial Sector

Tobias Zeier, 12696372, the 20th of October 2025
University of Essex Online

---

1. Introduction

This report reflects on my journey through the cloud operations and management module and its adaptation to the Swiss finance industry, where I am currently employed. My e-Portfolio, containing all formative and summative assignments as well as key concepts of each unit, can be found here: https://tobizeier.github.io/posts/COM/.

2. Personal Reflections

Engaging with this module, while fascinating and highly relevant, required significant management of competing demands. My role as an IT team lead in the Swiss banking sector, a highly pressured environment currently undergoing transformation and facing job cuts, imposed a heavy workload that challenged my ability to fully engage (Cohen and Illien, 2025; Mucklejohn, 2025; McGachey, 2025).

This period was a crucible for developing strategic prioritisation. Faced with constrained time, I necessarily shifted my focus from completing all exercises to the strategic identification and mastery of high-value learning outcomes. I prioritised core concepts like Kubernetes and security frameworks, which helped to understand the foundation of cloud concepts, over supplementary discussion posts on the student forum. This selective engagement forced a higher degree of metacognitive reflection: continuously assessing the minimum viable learning artifact needed to demonstrate critical understanding. This approach directly mirrors the resource allocation decisions essential for an IT leader in a time-constrained environment.

The stress of balancing professional project execution with academic rigor ultimately fostered a crucial leadership capability: the management of resource trade-offs. I learned that intellectual ambition must be tempered by practical constraints, forcing a

clear articulation of priorities to achieve acceptable outcomes across all domains. Successfully navigating this demanding period demonstrated the application of theoretical project management concepts, equal to critical path analysis and resource levelling, not just to work, but to my personal academic plan. The key personal learning outcome was the realisation that successful academic and professional work relies on the ability to scope ambition to available resources. Moving forward, I must refine my time management to pre-allocate protected time for high-value critical analysis, ensuring a sustainable balance between professional, academic, and social commitments.

3. Cloud Operations and Management Reflections

The module provided a robust conceptual foundation, progressing from service models IaaS, PaaS, SaaS and core principles to crucial theoretical frameworks like TOGAF, SDLC, and Infrastructure as Code (IaC) (Pahl, Jamshidi and Zimmermann, 2018). These methodologies provided the lens through which I could critically examine our existing deployment strategies.

A key practical advance was the deep dive into cloud-native technologies, specifically Python/Bash scripting (Unit 4) and Kubernetes container orchestration (Unit 5). This marked my first experience deploying applications using Docker and Kubernetes, and despite the time-consuming nature of the formative assignments, the resulting skill set is directly applicable to automating and managing modern banking environments. Critical reflection on this practical work highlighted the significant chasm between successful lab deployment and the requirements for a production-grade banking system. Achieving production readiness requires careful attention to networking, persistent storage, and strict security context constraints. These concepts are introduced only at a conceptual level but demand expert implementation in my professional environment. The module provided the theoretical permission to explore these tools, but the transfer to my high-stakes workplace demands a far greater mastery of operational resilience.

The unit on AI in cloud design (Unit 3) proved insightful, demonstrating how machine learning could optimise resource provisioning and costs. However, a critical reflection

emerged when applying this to a restrictive banking context: while AI offers immense potential, its adoption in regulated finance is fundamentally constrained by the need for governance and auditability. Implementing AI-driven resource optimisation, for instance, means trading potential cost agility for the non-negotiable requirement of maintaining transparent audit trails (i.e., proving why a resource scaled in a certain way). This demands that the implementation must be iterative and heavily validated against regulatory frameworks, requiring a human-in-the-loop architectural decision process rather than relying solely on algorithmic output. The learning here is that the ethical application of AI in the cloud context requires rigorous scrutiny of the inherent trade-off between agility and control. Furthermore, control of data flow and storage must be prioritised since a data leak could have hefty consequences.

Security and disaster recovery (Unit 7 and 8) were the most critically important sections. The material stressed compliance with general standards like ISO/IEC 27001 (Hegde *et al.*, 2023). However, the banking context demands critical scrutiny of the shared responsibility model. While a CSP secures the cloud infrastructure, the client organisation secures resources in the cloud. Given stringent FINMA (Swiss Financial Market Supervisory Authority) regulations, this boundary often extends deeper into the provider's domain from a regulatory standpoint, necessitating tailored security protocols, advanced encryption, and rigorous audit trails that must critically exceed general industry benchmarks. Regulatory adherence requires satisfying the supervisory authority's expectations for data protection and financial stability beyond the letter of ISO/IEC 27001. A key takeaway is that true compliance in finance is not achieved by simple adherence to a checklist, but by a continuous, critical assessment of regulatory risk against technical implementation details.

Unit 9 on cloud migration and integration strategies provided the 6Rs (rehost, replatform, refactor, repurchase, retire and retain) taxonomy, which immediately served as a critical framework for evaluating internal modernisation proposals. I realised that defaulting to 'Rehost' (lift and shift), often driven by perceived speed, risks migrating technical debt and vendor lock-in. For complex banking applications, the analysis reinforced that a carefully managed 'Replatform' strategy, focusing on containerisation and IaC integration with minimal application code changes, is the critical decision point to achieve long-term agility and return on investment while

mitigating risk. This is because it enables infrastructure modernisation with minimal disruption, while enhancing scalability, compliance, and operational efficiency. The financial implications are stark: 'Rehost' offers a quick capital expenditure (CapEx) to operational expenditure (OpEx) shift but perpetuates long-term high OpEx due to lack of cloud-native optimisation. 'Replatform' incurs a higher initial engineering cost but guarantees a lower, optimised long-term OpEx and significantly reduced regulatory risk, making it the preferred strategic approach in financial services (Singiri, Jain and Gopalakrishna Pandian, 2024).

Finally, the exploration of serverless computing (FaaS) in unit 10 provided a counterpoint to our current VM-centric architecture. FaaS offers unprecedented cost efficiency and zero-downtime scaling for specific, low-volume, event-driven banking tasks like API triggers for payment confirmations or calculation requests for mortgages. The key insight is that serverless is a critical tool for targeted cost optimisation in high-variability workflows, not an all-or-nothing solution. The module's final forward-looking units on Blockchain and Quantum Computing (Unit 12) were instrumental in aligning my professional focus with future financial technology disruptions.

4. Application to Industry

In my role as an IT team lead, cloud principles are critical to operational efficiency, constantly requiring us to evaluate applications for deployment on-premises or via SaaS. Factors like FINMA and FDPA (Federal Data Protection Act) compliance, security, and data residency dominate every architectural discussion, especially regarding services like M365/Microsoft Teams, where provider assurance on data location is a non-negotiable roadblock. This regulatory strictness elevates cloud governance from a technical choice to a core legal requirement.

A major internal project is the automation of infrastructure deployment using IaC. The module informed my critical comparison between declarative IaC (e.g., Terraform) and imperative approaches (e.g., Ansible). Declarative tools offer superior state management and auditability, aligning perfectly with financial governance requirements. However, our reliance on bespoke, legacy Windows configurations

makes a purely declarative paradigm difficult. My reflection, grounded in unit 2, is that a hybrid IaC approach, using Terraform for provisioning greenfield public cloud infrastructure, and leveraging Ansible for complex configuration management of legacy on-premises systems, is the most pragmatically effective strategy for our hybrid architecture. This critical realisation ensures that automation efforts are tailored to the reality of the existing estate, rather than being forced into a theoretically pure but impractical model (Byzov, 2025).

Furthermore, the principles of hybrid cloud in unit 6 are highly relevant for balancing the security of our on-premises legacy systems with public cloud agility (Meduri, 2024). The primary challenge is achieving true operational parity. This requires the consistent application of the TOGAF framework to ensure a unified operating model, security policy, and CI/CD pipeline across both environments. This parity extends to core services: unified identity and access management (IAM) is required to ensure that a banking user's permissions are consistently applied regardless of whether the resource is on-premises or in the cloud. Similarly, consistent network security policies (e.g., firewalls, logging) must be enforced across both domains. The module provided the critical insight that this rigorous, consistent application of framework is necessary to prevent the hybrid cloud from becoming merely two incompatible data centres. Our fundamental objective is to use standardised concepts like Kubernetes and shared pipelines to abstract the underlying infrastructure, creating a truly portable solution, thereby reducing management complexity and increasing regulatory confidence.

5. Ethical, Social, and Professional Impact

The module compelled a reflection on the wider responsibilities of cloud practitioners within a global institution. Professionally, the rapid pace of cloud adoption creates a significant skills gap. The ethical mandate is for leadership to implement training programs that prioritise re-skilling and mentorship for long-serving employees. The cloud transition must enhance equality and inclusion by valuing existing institutional knowledge, not discarding it in favour of external talent. The transition from managing physical assets to abstract cloud services requires a cultural shift that must be carefully managed to avoid marginalisation.

The convergence of AI and cloud in unit 11 also presents an acute ethical challenge regarding algorithmic fairness and operational transparency. As AI automates security and resource allocation, the potential for bias, and the lack of human interpretability in decision-making, becomes a tangible risk. For a bank, a biased AI model could have serious legal or financial consequences. Therefore, my professional practice must now integrate principles of explainable AI (XAI) and rigorous adversarial testing for any AI-driven cloud management tool before deployment. This critical examination of wider impact elevates technical execution to necessary ethical and social governance, ensuring that technology serves the bank's fiduciary and societal obligations.

6. Future Learning Goals

The module has provided a clear roadmap for my continued professional development. My primary goal is to deepen my knowledge of AI and machine learning as they apply to cloud security, specifically moving beyond conceptual understanding to hands-on exploration of models that can analyse security logs (Unit 7) for predictive threat intelligence. This is crucial for shifting the bank's security posture from reactive defence to proactive, anomaly-based detection.

Secondly, I plan to gain deeper knowledge in Fog and Edge Computing. While seemingly distant from a centralised Swiss bank, the inevitable proliferation of IoT and localised data processing mandates means decentralised architectures will become a necessity for low-latency operations like real-time trading and faster processing of branch data. My goal is to proactively build a pilot program demonstrating low-latency data aggregation at network perimeters. Finally, I will focus on developing expertise in serverless monitoring and cost governance, recognising that the critical challenge of FaaS is not deployment, but managing thousands of ephemeral functions and preventing runaway costs. This requires mastering detailed cost tracking mechanisms and setting up budget alerting policies, which are new necessities for cloud finance management. My long-term goal is to climb the corporate ladder; therefore, it is crucial for me to have a profound understanding in cloud technology since I will part of the strategy decision process as a higher manager.

Word Count: 1,880

References:

Byzov, I. (2025) ‘Terraform vs Ansible: When and how to use infrastructure tools as code’, *Technologies and Engineering*, 25(6), pp. 11–17. Available at: https://doi.org/10.30857/2786-5371.2024.6.1

Cohen, C. and Illien, I. (2025) *UBS Cuts France Jobs Amid Credit Suisse Integration*. Available at: https://www.bloomberg.com/news/articles/2025-05-06/ubs-cuts-france-jobs-amid-credit-suisse-integration (Accessed: 14 October 2025).

Hegde, T., Gangl, J., Babenko, S. and Coffman, J. (2023) ‘Cloud Security Frameworks’, Proceedings of the IEEE/ACM 16th International Conference on Utility and Cloud Computing (UCC ’23). Available at: https://doi.org/10.1145/3603166.3632553

Matyja, M. (2020) ‘Swiss Direct Democracy and Regulation of Banking Sector’, *Technium Social Sciences Journal*, 3(1), pp. 1–10. Available at: https://doi.org/10.47577/tssj.v3i1.72

McGachey, K. (2025) *Julius Baer CEO says no new job cuts planned, despite savings drive*. Available at: https://www.fnlondon.com/articles/julius-baer-ceo-says-no-new-job-cuts-planned-despite-savings-drive-85c3312e (Accessed: 14 October 2025).

Meduri, V. (2024) ‘Hybrid Cloud Architectures for Scalable and Cost-Effective AI in Banking’, *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 10(6), pp. 1840–1849. Available at: https://doi.org/10.32628/CSEIT241061226

Mucklejohn, L. (2025) *SIX set to cut 150 jobs in bid to boost margins*. Available at: https://www.fnlondon.com/articles/six-set-to-cut-150-jobs-e2051845 (Accessed: 14 September 2025).

Pahl, C., Jamshidi, P. and Zimmermann, O. (2018) ‘Architectural Principles for Cloud Software’, *ACM Transactions on Internet Technology*, 18(2), pp. 1–23. Available at: https://doi.org/10.1145/3104028

Singiri, S., Jain, S. and Gopalakrishna Pandian, P.K. (2024) ‘Modernizing Legacy Data Architectures with Cloud Solutions: Approaches and Benefits’, *International Research Journal of Modernization in Engineering Technology and Science*, 6(8), pp. 2608–2616. Available at: https://doi.org/10.56726/irjmets61252