Alpine Digital Bank: Cloud Strategy Assessment Report

Advanced Cloud Concept

Tobias Zeier, 12696372, the 13th of October 2025
University of Essex Online

---

1 Executive Summary

Alpine Digital Bank (ADB), a high-growth neo-bank operating within the competitive, highly regulated Swiss financial market, currently operates with an unsustainable IT landscape. This hybrid solution includes inflexible legacy on-premises infrastructure for core operations and a basic public cloud tenancy for front-end services. This fragmented approach inherently creates severe bottlenecks in new product delivery, significantly impedes the effective adoption of advanced analytics, and presents escalating challenges in maintaining stringent FINMA (Swiss Financial Market Supervisory Authority) compliance and the FADP (Federal Data Protection Act).

This report proposes a comprehensive Switzerland-centric hybrid cloud strategy built on governance, automation, and innovation. The strategic design leverages a multi-region public cloud hyperscaler, based on Microsoft Azure, for maximum agility and feature access, tightly coupled with a secure Swiss private cloud environment. The private cloud is strictly reserved for sensitive client identifying data (CID) and the core ledger system (CLS). The entire solution will be defined and managed through Infrastructure as Code (IaC), using Terraform, and supported by a robust continuous integration, continuous deployment (CI/CD) pipeline.

Expected Outcomes: The strategy is projected to optimise IT operational costs, whilst simultaneously accelerating product deployment cycles by 40%. Crucially, it establishes an immutable, auditable, and compliant infrastructure that sustains FINMA requirements and positions ADB to capitalise strategically on advanced technologies, such as AI-driven security and intelligent automation.

2 Strategic Rationale and Business Needs Analysis

The transition to an advanced cloud model is driven by critical business imperatives specific to the Swiss financial sector, necessitating a paradigm shift in IT governance and operations.

2.1 The Competitive Landscape and Growth Imperative

ADB's reliance on on-premises infrastructure imposes significant capital expenditure (CapEx) burdens and lengthy procurement cycles, undermining its core neo-bank advantages of speed and low operating costs (Shwetha, 2025). Transitioning to a sophisticated cloud model is essential to shift spending to a flexible operational expenditure (OpEx) structure, enabling the financial agility needed for sustained growth. However, this shift carries risks: without strong financial governance, known as FinOps, cloud costs can become unpredictable and undermine the agility sought. Thus, cloud adoption must be paired with a robust cost management culture. Technically, hyper-scalability is key, requiring seamless handling of exponential user growth and transaction spikes, with a target system reliability of 99.999%.

2.2 Regulatory Environment (FINMA and FADP)

Swiss financial regulation is among the world's strictest. FINMA Circular 2018/3 requires thorough due diligence, control, and audit rights over outsourced IT services(FINMA, 2017). Additionally, the FADP indirectly mandates data residency for critical client data within Switzerland (Schneider, Vasella and Reeves, 2025). ADB must demonstrate full operational control, auditability, and a documented exit strategy for outsourced environments. A generic public cloud solution without a sovereign component would be inadequate, exposing the bank to serious regulatory risks and potential sanctions.

2.3 Technical Debt and Legacy Constraints

The current infrastructure is highly susceptible to configuration drift and manual deployment errors, leading to inherent and non-auditable security vulnerabilities (Rahman and Parnin, 2023). This technical debt directly compromises the bank's

capacity for low-risk innovation and prevents the rapid iteration required in modern FinTech. The new strategy must explicitly challenge this legacy paralysis by enforcing immutability and fully automating infrastructure management, a core prerequisite for achieving operational stability and compliance.

3 Cloud Solution Design: A Switzerland-Centric Hybrid Model

The proposed architecture is a sophisticated hybrid cloud model, a cloud sovereign approach, tailored specifically for highly regulated Swiss entities (Katari, Muthsyala and Allam, 2024). This complex interplay of public and private environments is best visualised in figure 1 on the next page, which clearly illustrates data segregation based on criticality and compliance requirements.

3.1 Architecture Overview and Workload Segmentation

Workload placement is fundamentally dictated by the principle of least privilege and regulatory segregation, summarised below and visually detailed later in figure 1.

Workload Type	Cloud Environment	Key Rationale
Core Banking System (CLS) & CID	Swiss private cloud	Guaranteed Swiss data residency, legal jurisdiction, and FINMA compliance.
Mobile Front-End & Analytics	public cloud (Swiss region)	Superior scalability, immediate access to PaaS services (e.g., ML tools).
Development, Testing, Sandbox	public cloud (global/secondary region)	Cost-effective, disposable environments for rapid CI/CD cycles.
Disaster Recovery (DR)	public cloud (geographically separate EU region)	Geo-redundancy for resilience, using encrypted, tokenised data.

Table 1: Assigning Workload Type to Cloud Environment (Zeier, 2025)

A secure, high bandwidth dedicated interconnect, based on Azure ExpressRoute, will form the network spine, establishing a single, logical hybrid environment with extremely low latency.

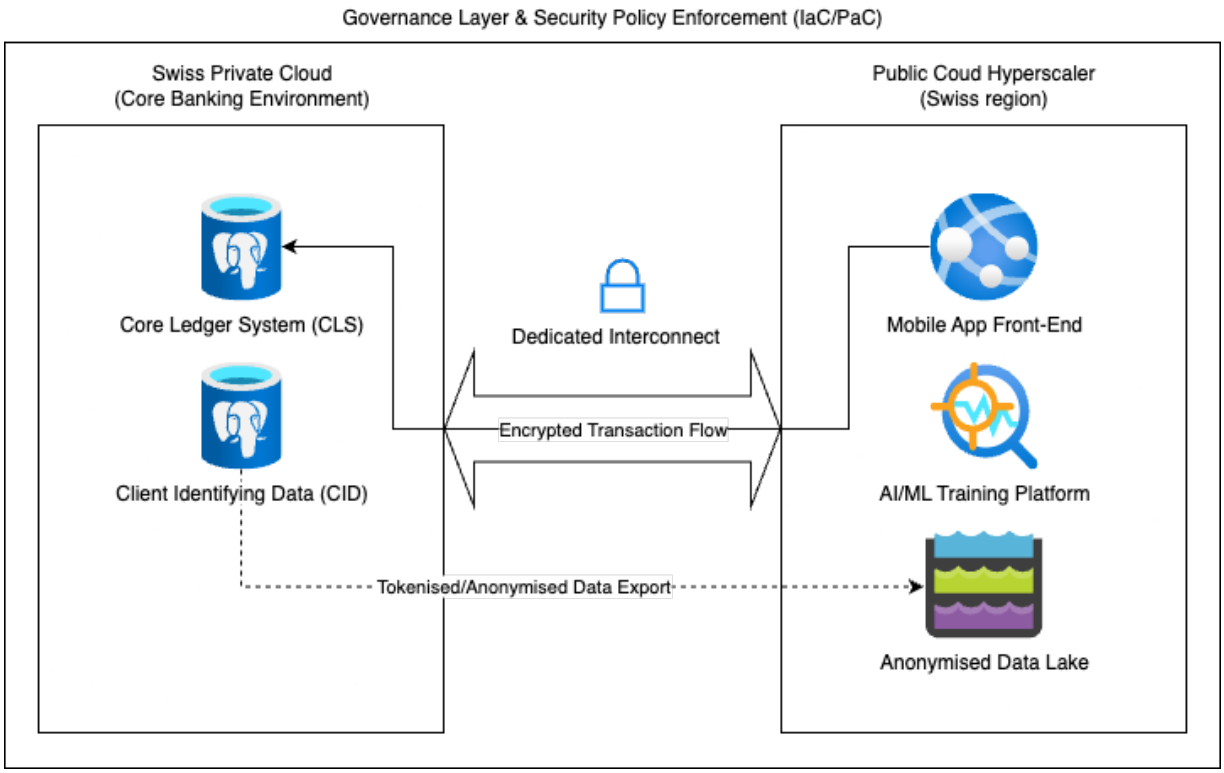

Figure 1: Switzerland-Centric Hybrid Cloud Architecture for Alpine Digital Bank (Zeier, 2025)

3.2 Infrastructure as Code (IaC) with Terraform

The cloud infrastructure is defined entirely through code, enabling a DevOps-centric, GitOps-aligned model where the code repository serves as the single source of truth. HashiCorp Terraform is selected for its declarative syntax and essential multi-cloud capabilities. Its ability to manage both public and private cloud resources via bespoke APIs offers a key advantage over single-cloud tools, reducing long-term vendor lock-in (Gudelli, 2023). While provider-native tools like Azure Bicep may offer quicker access to new features, this is outweighed by the strategic need to avoid vendor dependency. Terraform's platform-agnostic nature is central to ADB's mandatory exit strategy, a core requirement for FINMA compliance.

Use of IaC for Security and Compliance:

1. **Immutability:** Resources are strictly version-controlled in a Git repository. All infrastructure changes must be rigorously reviewed via a pull request and applied solely by the CI/CD pipeline, guaranteeing that production environments exactly match the approved code state. This fundamentally addresses FINMA's need for strict change control and auditability.
2. **Policy as Code, PaC:** Tools like Open Policy Agent (OPA) will be integrated into the Terraform workflow and deployment gates. This critically prevents deployment if the IaC configuration violates pre-defined rules, for example prohibiting public IP addresses on CLS servers, ensuring compliance is proactively enforced at deployment time, rather than relying on costly, post-facto security checks (Gorle, Muthusamy and Inampudi, 2025).

3.3 Network and Security Design

The architecture will enforce a stringent Zero Trust security model. Network segmentation is achieved using isolated virtual private clouds (VPCs) and fine-grained network micro segmentation. Identity and Access Management (IAM) is centralised across all environments, requiring multi-factor authentication (MFA) for all administrative and privileged access (Sheikh, Pawar and Lawrence, 2021).

4 Integration of Advanced Cloud Technologies

ADB's strategy centres on the integration of Automation and AI, leveraging cloud features to deliver a significant competitive advantage in security and customer experience.

4.1 Cloud Automation and CI/CD Pipeline

The automation approach focuses on deployment and operational tasks, significantly reducing human error and boosting deployment frequency.

- **Continuous Delivery:** The CI/CD pipeline automates the entire software lifecycle. After testing, Terraform is executed to provision necessary

infrastructure, for example a new Kubernetes cluster for a microservice, and the application is deployed automatically. This ensures releases are frequent, reliable, and fundamentally decoupled from the underlying infrastructure complexity, a key driver of organisational agility.

- **Serverless for Operational Efficiency:** Serverless Functions (FaaS) are utilised to replace traditional batch scripts and scheduled jobs. This includes automated cost control, where FaaS automatically shuts down non-production VMs after business hours based on resource tags. Additionally, real-time event processing, where FaaS instantly processes new transaction records, routes them to the CLS, and triggers initial fraud checks, significantly reducing processing latency (Peri, Tsenos and Kalogeraki, 2023).

4.2 AI and Machine Learning (ML) Integration

AI is a key differentiator for modern banking, demanding the scalable computational power provided by the public cloud.

- **Advanced Fraud Detection:** ADB will employ a supervised ML model for predictive fraud detection. The training data, which is sanitised and stored in the public cloud data lake, will be processed using high-performance PaaS ML services, such as Databricks or SageMaker. The resulting ML model is deployed as a low-latency API endpoint which the core transaction processing system calls in real-time. This approach provides a significantly higher fraud catch rate than static rule sets (Khalid *et al.*, 2024).
- **Personalised Customer Experience:** Natural Language Processing (NLP) models, accessible via PaaS, will be deployed for advanced sentiment analysis within customer service transcripts and chat logs. This detailed information is used to personalise banking advice and offers, providing the hyper-tailored service expected by neo-bank clients, thereby increasing customer engagement and retention (Ghobakhloo and Ghobakhloo, 2022).

4.3 Hybrid Integration and Abstraction

The success of the hybrid approach hinges on abstraction from proprietary cloud interfaces. Containerisation, using Kubernetes (K8s), abstracts applications from the underlying cloud environment. A unified K8s management layer can span both the Swiss private cloud and the public cloud, allowing ADB to deploy the same application container to either environment, facilitating easier migration, load balancing, and resilience. This strategy is an essential strategic defence against vendor lock-in, enhancing application portability (Huda and Kusumawardani, 2022).

5 Risk and Compliance Assessment

An effective cloud strategy demands rigorous risk assessment, particularly in a regulated market. Figure 2 provides a visual risk assessment heatmap, plotting the identified key risks against their likelihood and potential business impact. This mapping strategically prioritises mitigation resources, ensuring governance is risk aware.

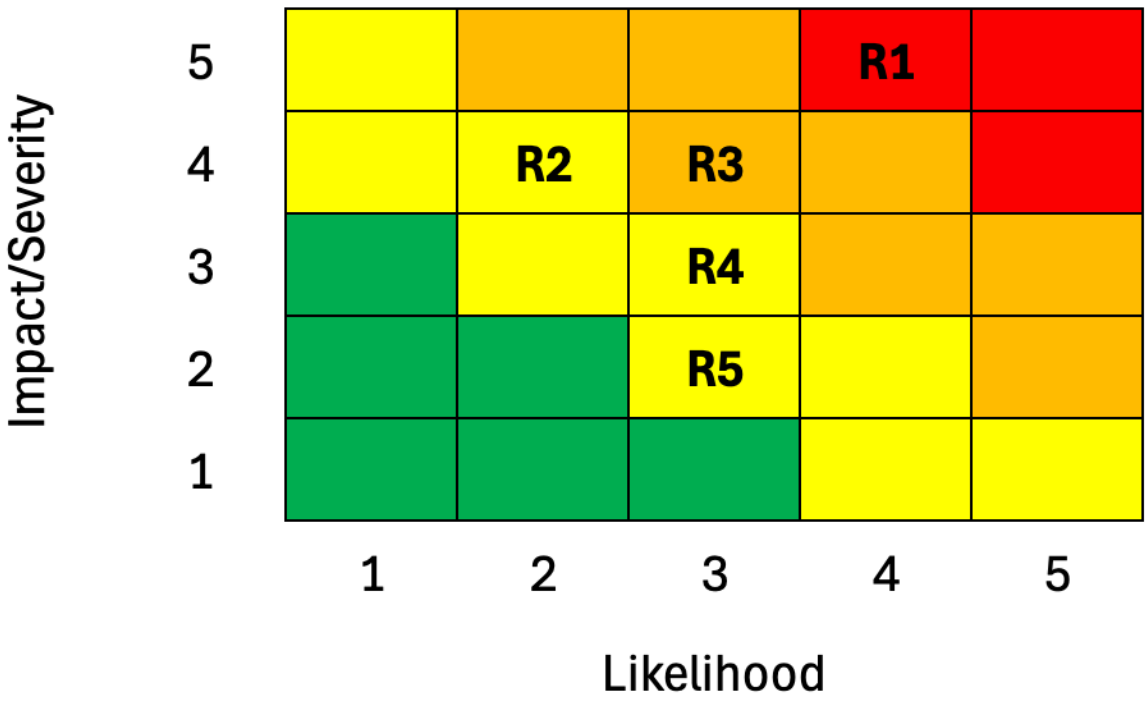

Figure 2: Alpine Digital Bank Cloud Strategy Risk Heatmap (Zeier, 2025)

5.1 Regulatory and Legal Risks

- **R1: FINMA Outsourcing Compliance:** Failure to maintain auditability and a clear exit strategy is a core regulatory risk.
    - **Mitigation:** The IaC approach ensures all changes are inherently auditable. Contractually, ADB must include FINMA-mandated audit clauses and maintain a fully tested reverse-migration strategy and data portability agreement, demonstrating clear, non-negotiable control over data egress and vendor relationship management.

- **R2: The CLOUD Act Risk:** The US CLOUD Act allows US legal authorities potential access to data held by US-based cloud providers globally, despite Swiss hosting, raising concerns over data sovereignty (Rojszczak, 2020).
    - **Mitigation:** Strict enforcement of the workload segmentation rule is mandatory. All CID and regulatory-sensitive records must exclusively reside in the Swiss Private Cloud. Furthermore, all public cloud data, including backups, must be encrypted using keys managed exclusively by ADB (bring your own key, BYOK). This renders the data unintelligible to the provider, thereby ensuring a necessary technical control against unwarranted access.

5.2 Security and Resilience Risks

- **R3: Data Exfiltration:** Unauthorised movement of data outside the secure perimeter represents a catastrophic security failure.
    - **Mitigation:** Implementation of a robust data loss prevention (DLP) policy enforced at the network edge and within data storage services. This will automatically block sensitive data patterns, for example social security numbers or banking codes, from being transferred to unauthorised external endpoints or unencrypted storage, acting as a critical final defence layer.

- **R4: Configuration Drift:** The manual, unmanaged introduction of errors or policy violations into the production environment is a significant operational failing.
    - **Mitigation:** The CI/CD pipeline must be the only entity with credentials capable of modifying infrastructure through IaC. Any manual intervention must be automatically flagged and reverted by the IaC deployment mechanism, thereby reinforcing the system's immutability and state integrity. Furthermore, vulnerability scanning based on OpenVAS will be implemented. These automated scans run weekly to identify and catalogue security weaknesses, such as missing patches or misconfigurations. These are then resolved according to a mandatory, risk-ranked patching schedule, acting as an important detective control against drift (Sharma *et al.*, 2024).

5.3 Operational and Financial Risks

- **R5: Cloud Sprawl and Cost Overruns:** Unmanaged resources lead to unpredictable OpEx, critically undermining the financial rationale for cloud migration.
    - **Mitigation:** Adoption of a dedicated FinOps (Financial Operations) culture is essential. This involves mandatory, granular resource tagging for cost allocation, leveraging reserved instances for steady-state workloads, and integrating real-time cloud cost monitoring dashboards for immediate budgetary control and accountability (Bhardwaj, 2025).

6 Future Recommendations and Innovation Readiness

ADB must look beyond immediate deployment to secure future readiness, demonstrating Innovation and Future Readiness.

6.1 Edge Computing for Front-Office Operations

Leveraging edge computing is necessary to minimise latency in high-stakes, consumer-facing transactions. Deploying containerised security microservices to

regional, low-latency edge nodes would allow for near-instantaneous fraud and credit checks for physical card transactions, enhancing customer satisfaction and system resilience against typical network latency issues (Ren *et al.*, 2019). However, the adoption of edge computing must be carefully managed, as it inherently expands the bank's security perimeter. Deploying services outside the centralised cloud introduces new security challenges that require investment in distributed monitoring and threat detection capabilities.

6.2 Quantum-Safe Cryptography (QSC) Strategy

The long-term security of cryptographic assets is profoundly threatened by the theoretical capabilities of quantum computers. ADB must treat this as a mandatory strategic imperative, initiating a multi-year QSC migration roadmap. This involves inventory of all cryptographic assets, research into NIST-approved post-quantum algorithms, for example CRYSTALS-Kyber, and investment in cloud provider QSC services, a critical investment in digital resilience against a potentially catastrophic technological shift (Sahu and Mazumdar, 2024).

6.3 Responsible AI Governance and Ethical Cloud Use

Given the integration of AI for automated decision-making, ADB requires a stringent responsible AI framework. This must be enforced via cloud governance tools, ensuring the ML models are explainable (XAI), free from systemic bias, and fully compliant with forthcoming European and Swiss AI regulations.

7 Conclusion

The proposed cloud strategy is a necessary and critical undertaking that moves Alpine Digital Bank from a legacy-constrained model to a resilient, innovation-driven platform. The Switzerland-centric hybrid cloud approach provides the essential regulatory shield for core data whilst strategically unlocking public cloud scalability and feature access. By embedding IaC, automation, and advanced AI into the operational fabric, ADB not only achieves exemplary compliance but also establishes a significant competitive advantage. Success ultimately relies on the

ongoing commitment to a FinOps culture and proactive engagement with the emergent technologies of Edge Computing and Quantum-Safe Cryptography.

Word Count: 2,188

References:

Bhardwaj, P. (2025) 'The Role of FinOps in Large-Scale Cloud Cost Optimization', *International Journal of Scientific Research in Engineering and Management*, 09(01), pp. 1–5. Available at: https://doi.org/10.55041/IJSREM28086

FINMA (2017) *Circular 2018/3 - Outsourcing – banks, insurance companies and selected financial institutions under FinIA*. Bern: FINMA. Available at: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf (Accessed: 30 September 2025).

Ghobakhloo, Mehregan and Ghobakhloo, Melika (2022) 'Design of a personalized recommender system using sentiment analysis in social media (case study: banking system)', *Social Network Analysis and Mining*, 12(1), p. 84. Available at: https://doi.org/10.1007/s13278-022-00900-0

Gorle, S., Muthusamy, P. and Inampudi, R.K. (2025) 'Consent-Driven Continuous Delivery with Open Policy Agent and Spinnaker', *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, 4(2), pp. 102–112. Available at: https://doi.org/10.60087/jklst.v4.n2.009

Gudelli, V.R.G. (2023) 'Cloud Formation and Terraform: Advancing Multi-Cloud Automation Strategies', *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences*, 11(2). Available at: https://doi.org/10.37082/IJIRMPS.v11.i2.232164

Huda, A.N. and Kusumawardani, S.S. (2022) ‘Kubernetes Cluster Management for Cloud Computing Platform: A Systematic Literature Review’, *JUTI: Jurnal Ilmiah Teknologi Informasi*, 20(2), pp. 75–83. Available at: https://doi.org/10.12962/j24068535.v20i2.a1103

Katari, A., Muthsyala, A. and Allam, H. (2024) ‘Hybrid Cloud Architectures for Financial Data Lakes: Design Patterns and Use Cases’, *International Research Journal of Modernization in Engineering Technology and Science*, 3(1), pp. 1421–1430. Available at: https://doi.org/10.56726/IRJMETS5966

Khalid, A.R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J. and Adejoh, J. (2024) ‘Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach’, *Big Data and Cognitive Computing*, 8(1), p. 6. Available at: https://doi.org/10.3390/bdcc8010006

Peri, A., Tsenos, M. and Kalogeraki, V. (2023) ‘Orchestrating the Execution of Serverless Functions in Hybrid Clouds’, in *2023 IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS)*. IEEE, pp. 139–144. Available at: https://doi.org/10.1109/ACSOS58161.2023.00032

Rahman, A. and Parnin, C. (2023) ‘Detecting and Characterizing Propagation of Security Weaknesses in Puppet-based infrastructure Management’, *IEEE Transactions on Software Engineering*, 49(6), pp. 1–18. Available at: https://doi.org/10.1109/TSE.2023.3265962

Ren, J., Yu, G., He, Y. and Li, G.Y. (2019) ‘Collaborative Cloud and Edge Computing for Latency Minimization’, *IEEE Transactions on Vehicular Technology*, 68(5), pp. 5031–5044. Available at: https://doi.org/10.1109/TVT.2019.2904244

Rojszczak, M. (2020) ‘CLOUD act agreements from an EU perspective’, *Computer Law & Security Review*, 38, p. 105442. Available at: https://doi.org/10.1016/j.clsr.2020.105442

Sahu, S.K. and Mazumdar, K. (2024) ‘State-of-the-art analysis of quantum cryptography: applications and future prospects’, *Frontiers in Physics*, 12. Available at: https://doi.org/10.3389/fphy.2024.1456491

Schneider, J., Vasella, D. and Reeves, H. (2025) *Data Protection & Privacy 2025*. Available at: https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/switzerland/trends-and-developments (Accessed: 12 October 2025).

Sharma, M., Desai, D., Arun, A.R., Lakshmanan, P. and Rajagopalan, N. (2024) ‘OpenVAS vs the Rest: Unveiling the Competitive Edge in Vulnerability Scanners’, in *2024 3rd International Conference for Innovation in Technology (INOCON)*. Bangalore, India: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/INOCON60754.2024.10511864

Sheikh, N., Pawar, M. and Lawrence, V. (2021) ‘Zero trust using Network Micro Segmentation’, in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, pp. 1–6. Available at: https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645

Shwetha, S. (2025) ‘Study on neo bank’, *International Journal For Multidisciplinary Research*, 7(2). Available at: https://doi.org/10.36948/ijfmr.2025.v07i02.39582

Zeier, T. (2025) ‘Alpine Digital Bank: Cloud Strategy Assessment Report’, *COM: Cloud Operations and Management July 2025*. Essay submitted to the University of Essex Online.