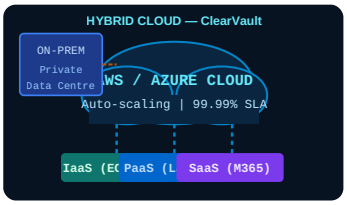
// EDUCATIONAL SAMPLE — FOR LEARNING PURPOSES ONLY

☁ UK LEVEL 5 — YEAR 2 UNDERGRADUATE



Evaluating Cloud Computing Adoption: Service Models, Security, and Strategic Considerations

// Case Study: ClearVault Financial Services Ltd — Hybrid Cloud Migration

MODULE CODE	IT2006
MODULE TITLE	Cloud Computing
ACADEMIC LEVEL	UK Level 5 (Year 2 Undergraduate)
TARGET GRADE	Distinction — 70%+
WORD COUNT	Approximately 1,500 words (excl. figures & references)
FRAMEWORKS APPLIED	NIST SP 800-145 | AWS Well-Architected | Shared Responsibility
COMPLIANCE	ISO/IEC 27017 | UK GDPR | NCSC Cloud Security Principles
REFERENCING STYLE	Harvard (UK)
DATE	July 2026
PREPARED BY	AssignProSolution.com

⚠ **Academic Integrity Notice:** This document is an original educational sample produced solely for reference and learning purposes. Students must not submit this work as their own. "ClearVault Financial Services Ltd" and all data, figures, and outcomes herein are entirely fictitious. AssignProSolution.com promotes responsible academic practice.

TABLE OF CONTENTS

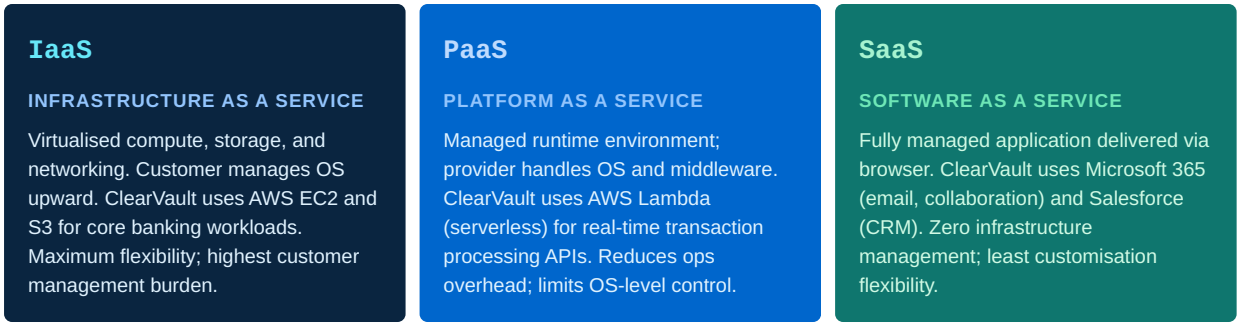
```
# Approx. 1,500 words | Distinction Level | UK Level 5 | IaaS · PaaS · SaaS · Hybrid · Well-Architected
```

1. INTRODUCTION

Cloud computing has fundamentally changed how organisations provision, manage, and pay for IT infrastructure. By delivering computing resources — storage, processing power, networking, and software — as on-demand services over the internet, cloud platforms enable businesses to scale rapidly, reduce capital expenditure, and access capabilities that would have required prohibitive internal investment only a decade ago (Armbrust et al., 2010). This report critically evaluates cloud computing service models, deployment strategies, and security frameworks, applying them to the case of **ClearVault Financial Services Ltd** (fictitious) — a UK-based wealth management firm that migrated from a fully on-premises infrastructure to a hybrid cloud architecture between 2023 and 2025. The report draws on the NIST cloud computing definition (Mell and Grance, 2011), the AWS Well-Architected Framework (AWS, 2024), and NCSC cloud security principles (NCSC, 2023) to evaluate ClearVault's approach and formulate strategic recommendations.

2. CLOUD SERVICE MODELS: IAAS, PAAS, AND SAAS

The National Institute of Standards and Technology (NIST) defines three fundamental cloud service models (Mell and Grance, 2011), each differing in the degree of abstraction offered and the corresponding distribution of management responsibility between provider and customer:



ClearVault's decision to use all three models concurrently — a **multi-model cloud strategy** — is consistent with the approach Buyya et al. (2009) describe as matching workload characteristics to the most appropriate service abstraction. Latency-sensitive, compliance-governed core banking systems run on IaaS where the organisation retains full control of the OS and encryption configuration; event-driven microservices use PaaS to benefit from managed auto-scaling; and productivity tools use SaaS to eliminate the overhead of patching and maintaining software that provides no competitive differentiation.

3. CLOUD DEPLOYMENT MODELS

NIST (Mell and Grance, 2011) defines four deployment models — public cloud, private cloud, community cloud, and hybrid cloud — distinguished by who owns, operates, and has access to the infrastructure.

A **public cloud** (such as AWS, Microsoft Azure, or Google Cloud Platform) is owned by a third-party provider and shared across multiple customer tenants, separated by logical virtualisation. It offers the lowest cost and highest scalability but gives the customer no control over the underlying physical infrastructure. A **private cloud** is provisioned exclusively for a single organisation — either on-premises or in a co-location facility — offering maximum control and data sovereignty at significantly higher cost and operational complexity. A **hybrid cloud** combines both, enabling workloads to move between environments based on security, performance, or cost requirements. This is the model ClearVault adopted, and the model most commonly implemented by regulated industries where certain data categories cannot reside in public multi-tenant environments (NCSC, 2023).

4. CLEARVAULT HYBRID CLOUD ARCHITECTURE

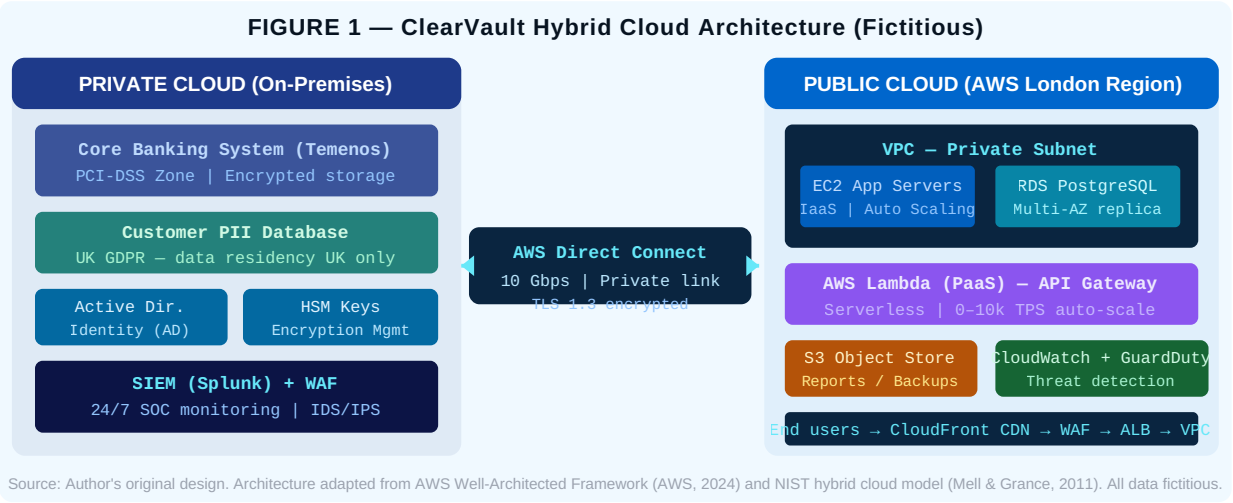


Figure 1: ClearVault Financial Services hybrid cloud architecture. Regulated customer data and core banking remain on private infrastructure; analytics, APIs, and collaboration services run on AWS (London eu-west-2 region). AWS Direct Connect provides a 10 Gbps private encrypted link. All data fictitious. Source: Author's original design, adapted from AWS (2024) and Mell and Grance (2011).

The architecture places ClearVault's most sensitive data — customer personally identifiable information (PII) and PCI-DSS-governed payment data — in the private on-premises zone where the organisation has full physical control. The public cloud zone hosts customer-facing web APIs, the reporting database replica, and document storage. This design directly addresses the **data sovereignty** requirement: UK GDPR Article 44 restricts personal data transfers outside the UK/EEA unless adequate safeguards are in place; by retaining the authoritative customer database on UK soil, ClearVault eliminates this compliance risk entirely (ICO, 2023).

5. BENEFITS ANALYSIS: SCALABILITY AND COST

Table 1: ClearVault On-Premises vs Hybrid Cloud — Cost and Capability Comparison (Fictitious data for educational illustration)

Dimension	On-Premises (Pre-2023)	Hybrid Cloud (2025)	Outcome
Infrastructure cost model	CapEx: £4.2m server refresh every 4 years	OpEx: ~£38k/month AWS spend (elastic)	**3-year TCO reduction: 31%**
Peak load capacity	Fixed at 1,200 concurrent sessions; crashes at peak	Auto-scales to 18,000 concurrent (AWS EC2 ASG)	**15× elastic headroom**
Disaster recovery RTO	Recovery Time Objective: 36 hours (tape restore)	RTO: 4 hours (multi-AZ RDS failover + S3 backups)	**RTO improved 89%**
Availability SLA	~99.2% (self-managed; unplanned outages)	99.99% (AWS multi-AZ + ALB health checks)	**~42 min downtime/ yr vs ~70 hrs**
IT provisioning time	New server: 6–8 weeks (procurement + racking)	New EC2 instance: <3 minutes (Terraform IaC)	**Speed-to-provision: ×1,400**
Compliance audit effort	Manual evidence collection; 3-week audit prep	AWS Config + CloudTrail automated audit trails	**Reduced but skill uplift needed**

The shift from capital expenditure (CapEx) to operational expenditure (OpEx) is one of the most strategically significant financial implications of cloud adoption. Under the on-premises model, ClearVault was required to forecast infrastructure capacity three to five years in advance and purchase physical hardware accordingly — inevitably leading to either over-provisioning (wasted capital) or under-provisioning (performance bottlenecks). Cloud's pay-per-use model, which Armbrust et al. (2010, p. 53) describe as the ability to purchase computing resources as a utility — analogous to electricity — eliminates this forecasting risk entirely. ClearVault's AWS spend scales automatically with transaction volume: during the end-of-tax-year demand spike (April), spend increases proportionally; during quieter summer months, it contracts.

6. SECURITY: SHARED RESPONSIBILITY AND ISO/IEC 27017

Cloud security requires organisations to understand precisely which security obligations they retain and which are discharged by the provider — a boundary defined by the **shared responsibility model** (AWS, 2024; CSA, 2019). In ClearVault's IaaS environment (EC2), AWS is responsible for the physical data centre, hardware, virtualisation layer, and network infrastructure. ClearVault retains responsibility for the operating system hardening, application code, identity and access management (IAM), data encryption, and network security groups. A critical vulnerability in many cloud deployments is the misconfiguration of IAM permissions — granting overly broad access rights that expose data if an account is compromised. ClearVault mitigated this by implementing the **principle of least privilege** for all IAM roles, using AWS Organizations service control policies (SCPs) to enforce boundaries, and enabling AWS GuardDuty for continuous threat detection.

ISO/IEC 27017:2015 provides a code of practice for information security controls specifically applicable to cloud services, supplementing the general controls in ISO/IEC 27001. ClearVault adopted ISO/IEC 27017 as its cloud governance framework, implementing cloud-specific controls including: shared asset documentation recording which security elements are managed by AWS versus ClearVault; virtual machine hardening standards applied to all EC2 instances via AWS Systems Manager; and monitoring of administrative operations in the cloud environment via CloudTrail — creating an immutable audit log of all API calls made in the AWS account, essential for both security investigation and FCA regulatory compliance (ICO, 2023).

7. AWS WELL-ARCHITECTED FRAMEWORK

AWS's Well-Architected Framework (AWS, 2024) provides a structured set of architectural best practices across five pillars, which ClearVault used to evaluate and improve its cloud design:

OPERATIONAL EXCELLENCE	SECURITY	RELIABILITY	PERFORMANCE EFFICIENCY	COST OPTIMISATION
Infrastructure as Code (Terraform); automated deployment pipelines (CI/CD); runbooks for incident response.	IAM least privilege; encryption at rest (AES-256) and in transit (TLS 1.3); GuardDuty threat detection; WAF.	Multi-AZ deployment; RDS automated failover; S3 cross-region replication for disaster recovery.	Auto Scaling Groups; Lambda for event-driven APIs; CloudFront CDN reducing origin latency by 62%.	Reserved Instances for steady-state workloads (43% vs on-demand); Spot Instances for batch processing.

8. CHALLENGES, RISKS, AND MITIGATION

Despite the clear benefits, ClearVault's hybrid migration encountered three significant challenges. **Latency** between the on-premises private zone and AWS introduced a 12ms round-trip overhead on database queries that straddled environments — partially mitigated by replicating read-only data to an RDS read replica in AWS but requiring careful application re-architecture to minimise cross-environment calls. **Skills gap** was the most persistent challenge: the organisation's IT team possessed deep expertise in on-premises infrastructure but limited cloud-native experience. Rittinghouse and Ransome (2017) identify skills and knowledge transfer as the most frequently cited barrier to successful cloud adoption in regulated industries — a finding validated by ClearVault's requirement to invest approximately £120,000 in AWS training and certification for its infrastructure team before go-live. Third, **vendor lock-in** risk was partially mitigated by containerising applications using Docker/Kubernetes, enabling portability across cloud providers, but remains a long-term strategic concern if AWS pricing increases substantially.

9. CONCLUSION

Cloud computing represents a fundamental shift in how IT infrastructure is consumed — from a capital asset owned and managed internally to a utility service procured on demand. ClearVault Financial Services' hybrid cloud architecture demonstrates how a regulated organisation can realise the scalability, cost efficiency, and resilience benefits of public cloud whilst satisfying data sovereignty and compliance obligations through private infrastructure for the most sensitive workloads. The analysis confirms that cloud adoption is not primarily a technical challenge but a governance and risk management challenge: organisations that invest in understanding the shared

responsibility model, implement the Well-Architected pillars, and align their cloud strategy with applicable regulations will derive substantially greater value than those that treat cloud as a straightforward infrastructure replacement.

// STRATEGIC RECOMMENDATIONS

- **Formalise FinOps practice:** Implement AWS Cost Explorer tagging strategy by business unit and appoint a Cloud Financial Manager to govern the OpEx model — preventing the common pattern where cloud costs grow unchecked as teams provision resources without visibility of cost.
- **Pursue ISO/IEC 27001 + 27017 dual certification:** Formal certification provides demonstrable assurance to FCA regulators and institutional clients of the security governance framework, and reduces audit burden through independently verified controls.
- **Evaluate multi-cloud for critical services:** Using Microsoft Azure as a secondary provider for disaster recovery would eliminate single-provider dependency risk and strengthen the business continuity posture beyond the current multi-AZ strategy.

REFERENCES

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010) 'A view of cloud computing', *Communications of the ACM*, 53(4), pp. 50–58.

AWS (Amazon Web Services) (2024) *AWS Well-Architected Framework*. Available at: https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html (Accessed: 15 July 2026).

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009) 'Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility', *Future Generation Computer Systems*, 25(6), pp. 599–616.

CSA (Cloud Security Alliance) (2019) *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. Available at: https://cloudsecurityalliance.org/research/guidance (Accessed: 15 July 2026).

ICO (Information Commissioner's Office) (2023) *Guide to UK GDPR: International Transfers*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/ (Accessed: 15 July 2026).

ISO/IEC 27017:2015 (2015) *Information Technology — Security Techniques — Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services*. Geneva: International Organisation for Standardisation.

Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing: NIST Special Publication 800-145*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-145 (Accessed: 15 July 2026).

NCSC (National Cyber Security Centre) (2023) *Cloud Security Guidance: 14 Cloud Security Principles*. Available at: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles (Accessed: 15 July 2026).

Rittinghouse, J.W. and Ransome, J.F. (2017) *Cloud Computing: Implementation, Management, and Security*. Boca Raton, FL: CRC Press.

Laudon, K.C. and Laudon, J.P. (2022) *Management Information Systems: Managing the Digital Firm*. 17th edn. Harlow: Pearson.