Coursework Report

Module: Cloud Operations and Management

Title: Evaluating Microsoft Azure Resource Manager (ARM) for Cloud Infrastructure Design

Team Submission (Weeks 1-6)

Group A - Akaffou, N., Abiodun, D., Collins, M and Hamberger, G

Word Count: 1,083

Date: August 2025

Table of Contents

Evaluating Microsoft Azure Resource Manager (ARM) for Cloud Infrastructure Design

1. Overview

Microsoft Azure Resource Manager (ARM) is the native deployment and management framework within Azure, enabling users to provision, configure, and manage cloud resources through declarative templates, scripting, or GUI-based tools (Borra, 2024). ARM ensures consistency by applying governance policies, access controls, and resource tagging across deployments, making it a cornerstone for cloud automation and compliance (Varian Medical Systems, 2025). Buyya et al. (2009) conceptualise cloud computing as the “5th utility”, emphasising elasticity, on-demand self-service, and broad network access. ARM builds on this by enabling declarative provisioning of compute, storage, and networking resources.

Modern practice increasingly uses Bicep, a domain-specific language that compiles into ARM JSON, thereby improving readability and modularity. Furthermore, research shows that embedding Zero trust principles into ARM templates strengthens governance and reduces risk of misconfiguration (Dakić et al., 2024; Manolov et al., 2025).

2. Service Model Analysis

ARM supports multiple cloud service models:

- Infrastructure as a Service (IaaS): ARM provisions compute (VMs), storage, and networking. For example, enterprises can automate DR strategies with templates and scale compute nodes without manual intervention (Borra, 2024).

- Platform as a Service (PaaS): ARM enables seamless deployment of managed services like Azure App Service and Kubernetes Service (AKS). This supports modernisation of applications by reducing administrative overhead (Varian Medical Systems, 2025).

- Software as a Service (SaaS): ARM integrates SaaS platforms, such as Microsoft 365 or marketplace solutions, into enterprise ecosystems with centralised security and compliance policies (Kleinman, 2024).

This versatility ensures ARM supports both infrastructure-heavy workloads and

cloud-native applications.
Armbrust et al. (2010) highlight that while IaaS, PaaS, and SaaS are distinct, they increasingly converge into unified ecosystems. ARM functions at the critical provisioning boundary between IaaS and PaaS. However, Zhang et al. (2010) note challenges of portability and interoperability across vendors, which makes Azure-specific ARM templates potentially restrictive in multi-cloud settings.

Comparative studies further contextualise ARM: AWS is often seen as more mature and feature-rich, Azure excels in enterprise integration and hybrid cloud capabilities, while GCP is strong in analytics and machine learning (Mufti, 2021; Alhassan & Adjei, 2017). These positions ARM competitively but also underscore vendor lock-in risks.

3. Deployment Types

ARM is flexible across deployment environments:

- Public Cloud: Its primary deployment is via Azure’s global public cloud, where organisations access services at scale (Borra, 2024).
- Private Cloud: Through Azure Stack Hub, ARM extends into private data centres, allowing sovereignty over sensitive workloads while retaining ARM’s management consistency (Varian Medical Systems, 2025).
- Hybrid Cloud: With Azure Arc and ExpressRoute, ARM unifies management of on-premises and cloud-based resources, enabling compliance with region-specific laws such as GDPR and HIPAA (Borra, 2024). Notably, Azure regions explicitly follow national borders and geopolitical boundaries, meaning that data remains in the jurisdiction of the originating country (Borra, 2024). This is a significant consideration for Information Governance departments.

These deployment options enable gradual cloud adoption journeys while ensuring continuity and governance. Krishnan (2020) stresses that hybrid and multi-cloud deployments introduce interoperability and governance challenges, despite Azure’s strong support through Stack Hub and Arc. These features improve hybrid consistency but also add cost and operational complexity. Hauser (2015) provides historical context, showing how Azure’s hybrid approach evolved to address sovereignty and compliance needs.

4. Infrastructure Design

Designing infrastructure in ARM typically involves:

1. Define Requirements: Establish compute, storage, networking, and compliance needs.
2. Resource Group Creation: Logical grouping of all related resources.

3. Template Development: JSON templates capture specifications (location, VM size, dependencies), ensuring repeatability (Borra, 2024).
4. Networking: Deploy Virtual Networks, Subnets, Network Security Groups, and configure ExpressRoute or VPN connections.
5. Compute & Storage: Provision VMs and attach managed disks, configure replication and backups.
6. Security & Compliance: Apply Role-Based Access Control (RBAC) and enforce policies through ARM (Varian Medical Systems, 2025).
7. Monitoring: Integrate Azure Monitor and Log Analytics for observability.

The declarative and idempotent approach ensures reliable redeployment, critical in disaster recovery scenarios (Iveson, 2024).

While ARM and Bicep accelerate delivery and ensure repeatability, empirical studies show that Infrastructure as Code (IaC) can introduce configuration “smells” if not carefully managed. Best practices include running “what-if” deployments, integrating Azure Policy and Blueprints into CI/CD pipelines, and monitoring drift via Resource Graph queries (Rittinghouse & Ransome, 2017).

Security-by-design is also strengthened when Zero Trust principles, least privilege, segmentation, and continuous verification are codified directly into ARM/Bicep templates (Dakić et al., 2024; Manolov et al., 2025).

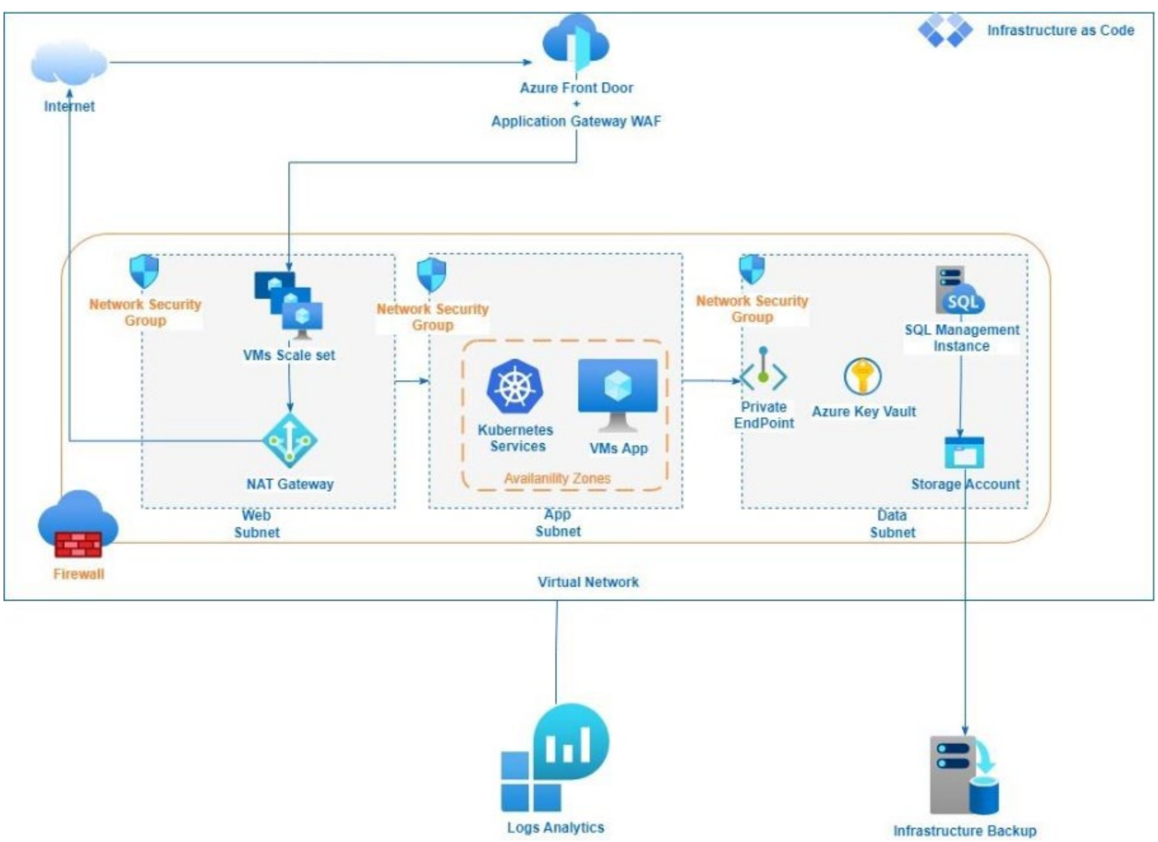

Figure 1: Infrastructure Diagram (Akaffou et.al., 2025)

5. Case Study: Varian Medical Systems

Varian Medical Systems developed its FullScale Infinity Cloud (FSIC) using Azure Resource Manager (Varian Medical Systems, 2025). FSIC primarily operates as an IaaS environment, providing oncology treatment solutions while isolating sensitive PHI/PII through segregation of duties and Azure RBAC.

Security Measures:
- Contractors have restricted, task-specific access.
- VIPER password management enforces rotation and protects access credentials.
- Azure ExpressRoute ensures private, secure connections for data transfer, avoiding exposure to the open internet (Borra, 2024).

Business Continuity:
By leveraging ARM within Azure, Varian avoids costly downtime seen in on-premises environments. A six-hour outage in an on-premises data centre would have been mitigated under Azure's high availability (Iveson, 2024).

Limitations:
- ExpressRoute as a single point of failure: outages, such as at Royal Surrey Hospital in 2024, disrupted services (Iveson, 2024).
- Third-party dependencies: global disruption from the CrowdStrike update in 2024 showed risks in cloud reliance (Kleinman, 2024).

This example illustrates ARM's strengths in resilience, compliance, and automation, but also highlights cost and dependency trade-offs.
This aligns with Qarkaxhija (2020), who documented Azure adoption in another enterprise setting. The study found clear benefits in scalability and availability, but also emphasised cost and complexity as barriers to full realisation of cloud potential. This comparison shows that while Varian successfully leveraged ARM for compliance and resilience, such adoption is rarely without trade-offs.

6. Conclusion

Microsoft Azure Resource Manager delivers a comprehensive cloud framework supporting all service models and deployment types. Its template-driven and policy-enforced approach ensures secure, scalable, and repeatable infrastructure deployment.

The Varian Medical Systems case demonstrates real-world benefits in compliance, security, and resilience. However, challenges such as ExpressRoute dependency and cloud-wide vulnerabilities show that balancing cost with resilience remains critical for organisations.

Overall, the literature reinforces ARM's strengths in automation, policy enforcement, and hybrid integration, while cautioning against vendor lock-in, IaC misconfigurations, and the operational burden of hybrid strategies (Armbrust et al., 2010; Zhang et al., 2010; Krishnan, 2020). This balanced perspective suggests that successful ARM adoption requires not only technical design but also governance, testing, and cost management disciplines.

References

Akaffou, N., Abiodun, D., Collins, M and Hamberger, G. (2025) Evaluating Microsoft Azure Resource Manager (ARM) for Cloud Infrastructure Design. Cloud Operations. September 2025. Essay submitted to the University of Essex Online.

Alhassan, I. and Adjei, J. (2017) *Microsoft Azure vs Amazon AWS cloud services: a comparative study*. Available at: https://d1wqtxts1xzle7.cloudfront.net/53932691/Microsoft_Azure_vs_Amazon_AWS_Cloud-libre.pdf (Accessed 16 August 2025).

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R. et al. (2010) 'A view of cloud computing', Communications of the ACM, 53(4), pp. 50–58. Available at: https://doi.org/10.1145/1721654.1721672

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009) 'Cloud computing and emerging IT platforms', *Future Generation Computer Systems*, 25(6), pp. 599–616. Available at: https://doi.org/10.1016/j.future.2008.12.001.

Borra, P. (2024) 'Comparison and Analysis of Leading Cloud Service Providers (AWS, Azure and GCP)', International Journal of Advanced Research in Engineering and Technology (IJARET), 15(3), pp. 266–278. Available at: https://doi.org/10.2139/ssrn.4914145.

Dakić, V., Kajganić, A. and Šećerov, N. (2024) 'Analysis of Azure Zero Trust Architecture Implementation', *Computers*, 5(1), p. 2. Available at: https://doi.org/10.3390/jcp5010002

Hauser, H. (2015) *Microsoft Azure: planning, deploying, and managing your data center in the cloud*. New York: Springer. Available at: https://books.google.de/books?id=EfFxBgAAQBAJ (Accessed 16 August 2025).

Iveson, H. (2024) Radiotherapy service update | News. Royal Surrey NHS Foundation Trust. Available at: https://www.royalsurrey.nhs.uk/news/radiotherapy-service-update-12715 (Accessed: 24 August 2025).

Kleinman, Z. (2024) How a single IT update caused global havoc. BBC News. Available at: https://www.bbc.com/news/articles/cpwdyxx0v64o (Accessed: 24 August 2025).

Krishnan, S. (2020) *Practical guide to hybrid cloud and multi-cloud*. Berkeley, CA: Apress. Available at: https://link.springer.com/book/10.1007/978-1-4842-5958-0 (Accessed 16 August 2025).

Manolov, D., Milev, B. and Staneva, B. (2025) 'Creating Automated Microsoft Bicep Application Environments with Zero Trust Principles for Azure', *Electronics*, 14(3), 520. Available at: https://doi.org/10.3390/fi17080359

Mufti, T. (2021) *A review on Amazon Web Service (AWS), Microsoft Azure, Google Cloud Platform (GCP) services*. Available at: https://www.researchgate.net/publication/350126601_A_Review_on_Amazon_Web_Service_AWS_Microsoft_Azure_Google_Cloud_Platform_GCP_Services(Accessed 16 August 2025).

Qarkaxhija, J. (2020) *Using cloud computing as an infrastructure case study: Microsoft Azure*. Available at: https://www.researchgate.net/publication/344713632_Using_Cloud_Computing_as_an_Infrastructure_Case_Study-_Microsoft_Azure(Accessed 16 August 2025)

Rittinghouse, J.W. and Ransome, J.F. (2017) 'Cloud computing: implementation, management, and security', in *Cloud computing: implementation, management, and security*. Berkeley, CA: Apress, pp. 1–36. Available at:https://doi.org/10.1007/978-1-4842-1043-7_1.

Varian Medical Systems (2025) FullScale Infinity Cloud 1.8 Security White Paper. Available at: https://www.varian.com/resources-support/cybersecurity-varian (Accessed: 15 August 2025).

Zhang, Q., Cheng, L. and Boutaba, R. (2010) 'Cloud computing: state-of-the-art and research challenges', Journal of Internet Services and Applications, 1, pp. 7–18. Available at: https://doi.org/10.1007/s13174-010-0007-6

Appendix A – List of Acronyms

AKS: Azure Kubernetes Service

ARM: Azure Resource Manager

AWS: Amazon Web Services

CI/CD: Continuous Integration/Continuous Delivery or Deployment

DR: Disaster Recovery

FSIC: FulScale Infinity Cloud

GCP: Google Cloud Platform

GDPR: General Data Protection Regulations

GUI: Graphical User Interface

HIPAA: Health Insurance Portability and Accountability Act

IaaS: Infrastructure as a Service

IaC: Infrastructure as Code

JSON: JavaScript Object Notation

PaaS: Platform as a Service

PHI/PII: Protected Health Information / Personally Identifiable Information

RBAC: Role Based Access Control

SaaS: Software as a Service

VIPER: Varian Infrastructure Password with Enforced Rotation

VM: Virtual Machine

VPN: Virtual Private Network