e-ISSN:2582 - 7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 4, Issue 9, September 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 5.928

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

Enterprise Multi-Cloud Transformation and Managed Services Modernization

Samiuddin Mohammed, Venkata Kalyan Polamarasetty

Managing Solution Architect, Fujitsu North America, Inc., USA

Independent Researcher, USA

ABSTRACT: The rapid evolution of digital technologies has compelled enterprises to rethink traditional information technology (IT) infrastructures and operational models. Multi-cloud transformation has emerged as a strategic approach that enables organizations to leverage services from multiple cloud providers, improving flexibility, scalability, resilience, and innovation capabilities. By distributing workloads across diverse cloud environments, enterprises can reduce vendor dependency, optimize performance, and align cloud services with specific business requirements. However, the adoption of multi-cloud architectures introduces challenges related to governance, security, compliance, interoperability, cost management, and operational complexity.

Managed services modernization plays a critical role in addressing these challenges by transforming conventional IT support models into intelligent, automated, and cloud-centric service frameworks. Modern managed services incorporate advanced technologies such as automation, artificial intelligence for IT operations (AIOps), infrastructure as code (IaC), observability platforms, and continuous monitoring to enhance operational efficiency and service reliability. These capabilities enable organizations to streamline cloud operations, improve resource utilization, accelerate application deployment, and strengthen security postures.

This article explores the concepts, drivers, architecture, benefits, challenges, and best practices associated with enterprise multi-cloud transformation and managed services modernization. It examines the role of cloud-native technologies, governance frameworks, automation strategies, and service management approaches in supporting successful digital transformation initiatives. Furthermore, the paper highlights emerging trends and future directions that are shaping the next generation of enterprise cloud ecosystems. The findings demonstrate that a well-structured multi-cloud strategy combined with modernized managed services can significantly enhance business agility, operational resilience, and long-term digital competitiveness.

KEYWORDS: Multi-Cloud Computing, Cloud Transformation, Managed Services Modernization, Digital Transformation, Cloud Governance, Cloud Security, Cloud-Native Architecture, Infrastructure as Code (IaC), DevOps, AIOps, IT Service Management (ITSM), Automation, Hybrid Cloud, Enterprise Architecture, Operational Resilience, Cloud Cost Optimization, Observability, Platform Engineering.

I. INTRODUCTION

The digital transformation era has significantly reshaped the way organizations design, deploy, and manage information technology (IT) infrastructures. Increasing demands for business agility, scalability, innovation, and operational efficiency have encouraged enterprises to move beyond traditional on-premises data centers toward cloud-based computing environments. Cloud computing has evolved from a cost-saving technology into a strategic business enabler that supports rapid application development, data-driven decision-making, and global service delivery.

As organizations continue their cloud adoption journeys, many enterprises are choosing multi-cloud strategies rather than relying on a single cloud provider. A multi-cloud environment involves the use of services from multiple public and private cloud platforms to meet diverse business, technical, regulatory, and operational requirements. This approach allows organizations to leverage the strengths of different cloud providers while minimizing risks associated with vendor lock-in, service outages, and geographic limitations. By distributing workloads across multiple cloud environments, enterprises can achieve greater flexibility, resilience, and performance optimization.

The growing complexity of enterprise applications has further accelerated the adoption of multi-cloud architectures. Modern organizations operate a combination of legacy systems, cloud-native applications, microservices, and data-

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

intensive workloads that require diverse infrastructure capabilities. Different cloud providers often offer specialized services in areas such as artificial intelligence, machine learning, analytics, database management, networking, and security. Consequently, enterprises increasingly select cloud services based on workload requirements rather than committing to a single technology ecosystem.

Despite its advantages, multi-cloud transformation presents several challenges. Managing multiple cloud platforms introduces operational complexity, requiring organizations to address issues related to governance, security, compliance, interoperability, monitoring, and cost control. The lack of standardized management frameworks across cloud providers can result in fragmented operations and reduced visibility into enterprise-wide cloud resources. Organizations must therefore establish effective governance models and operational strategies to ensure consistency, security, and efficiency across diverse cloud environments.

In parallel with cloud transformation initiatives, enterprises are modernizing their managed services models to support increasingly dynamic and distributed IT ecosystems. Traditional managed services were primarily focused on infrastructure maintenance, incident management, and reactive support processes. However, modern digital enterprises require proactive, automated, and intelligent service management capabilities that align with cloud-native operating models. Managed services modernization integrates automation, artificial intelligence for IT operations (AIOps), Infrastructure as Code (IaC), continuous monitoring, observability platforms, and predictive analytics to enhance service delivery and operational performance.

The modernization of managed services enables organizations to streamline cloud operations, reduce manual intervention, improve system reliability, and accelerate innovation cycles. Automated provisioning, self-healing infrastructure, centralized governance, and advanced analytics contribute to improved operational efficiency and enhanced user experiences. Furthermore, modern managed services help enterprises address security and compliance requirements through continuous monitoring, automated policy enforcement, and real-time threat detection.

The convergence of multi-cloud transformation and managed services modernization represents a significant shift in enterprise IT strategy. Organizations are increasingly adopting integrated approaches that combine cloud technologies, automation frameworks, and intelligent service management practices to achieve sustainable business outcomes. This transformation is not solely a technological initiative but also involves changes in organizational culture, operational processes, workforce skills, and governance structures.

This article examines the key concepts, architectures, benefits, challenges, and implementation strategies associated with Enterprise Multi-Cloud Transformation and Managed Services Modernization. The discussion explores how organizations can leverage cloud-native technologies, automation frameworks, and modern service management practices to build resilient, scalable, and secure digital ecosystems. Additionally, the article highlights emerging trends and future developments that are expected to shape the next generation of enterprise cloud operations and managed service delivery.

II. ENTERPRISE MULTI-CLOUD TRANSFORMATION: CONCEPTS AND BUSINESS DRIVERS

Enterprise multi-cloud transformation represents a strategic evolution in information technology infrastructure where organizations deploy and manage workloads across multiple cloud service providers rather than relying on a single vendor. This approach enables enterprises to combine the strengths of different cloud platforms while optimizing performance, availability, compliance, and operational flexibility. Unlike traditional cloud migration initiatives that primarily focus on relocating workloads from on-premises environments to a single public cloud, multi-cloud transformation emphasizes the creation of an integrated ecosystem capable of supporting diverse business objectives and rapidly evolving digital services.

The widespread adoption of digital business models has significantly increased the demand for scalable computing resources, intelligent analytics, and globally distributed applications. Enterprises are now expected to deliver uninterrupted services while responding quickly to changing customer expectations and market conditions. Multi-cloud architectures provide the flexibility required to dynamically allocate workloads, optimize resource utilization, and reduce dependency on any single cloud provider.

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

Organizations increasingly recognize that different cloud vendors excel in different technology domains. Some providers offer superior artificial intelligence and machine learning services, while others specialize in large-scale analytics, enterprise application hosting, edge computing, or global networking capabilities. By leveraging multiple providers, enterprises can select the most suitable platform for each workload instead of forcing every application into a single cloud ecosystem.

In addition to technology diversification, regulatory compliance has become a significant driver of multi-cloud adoption. Many industries including healthcare, banking, government, telecommunications, and manufacturing must comply with stringent regulations governing data privacy, residency, security, and operational continuity. Multi-cloud deployment enables organizations to host sensitive workloads within specific geographic regions while utilizing other cloud platforms for analytics, disaster recovery, development, and customer-facing services.

Business continuity and disaster recovery have also become central considerations in enterprise cloud strategy. Service disruptions caused by infrastructure failures, cyberattacks, or regional outages can significantly affect business operations. Multi-cloud environments improve resilience by enabling workload replication, geographic redundancy, automated failover, and cross-cloud backup mechanisms that minimize downtime and ensure service availability.

Another important factor driving enterprise transformation is cost optimization. Cloud pricing models vary considerably among providers based on compute resources, storage, networking, licensing, and managed services. Organizations increasingly distribute workloads across providers to achieve better financial efficiency while avoiding unnecessary operational expenditures. Advanced cloud financial management (FinOps) practices further enable enterprises to monitor consumption patterns, optimize resource allocation, and improve return on cloud investments.

The modernization of application development practices has further accelerated multi-cloud adoption. Cloud-native applications built using microservices, containers, Kubernetes orchestration, and serverless computing are designed to operate across heterogeneous infrastructure environments. These technologies reduce platform dependency and simplify workload portability, allowing enterprises to deploy applications wherever operational or business requirements dictate.

Digital transformation initiatives also require greater integration between legacy enterprise systems and modern cloud services. Most organizations continue to operate mission-critical applications within private data centers while simultaneously expanding cloud-native services. Multi-cloud strategies provide a practical framework for integrating hybrid infrastructures, enabling gradual modernization without disrupting existing business operations.

Beyond infrastructure considerations, organizational agility has become a major business objective. Enterprises seek technology platforms that support rapid experimentation, continuous innovation, and faster time-to-market for new products and services. Multi-cloud environments provide development teams with access to specialized cloud capabilities that accelerate software delivery while supporting DevOps, continuous integration/continuous deployment (CI/CD), and agile development methodologies.

The adoption of artificial intelligence, advanced analytics, Internet of Things (IoT), and real-time data processing further strengthens the value of multi-cloud architectures. Different cloud providers offer unique AI models, streaming platforms, database technologies, and edge computing services that organizations can selectively integrate to maximize innovation while maintaining operational flexibility.

Although the benefits are substantial, successful multi-cloud transformation requires comprehensive planning, governance, and operational discipline. Organizations must establish standardized security policies, identity management frameworks, workload placement strategies, cost management processes, and monitoring capabilities to effectively coordinate services across multiple cloud environments. Without proper governance, operational complexity can offset many of the anticipated advantages.

Ultimately, enterprise multi-cloud transformation is not merely a technology migration initiative but a long-term business strategy that aligns cloud capabilities with organizational goals. By combining flexible infrastructure, cloud-native development practices, intelligent automation, and integrated governance, enterprises can create resilient digital ecosystems capable of supporting continuous innovation and sustainable growth.

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

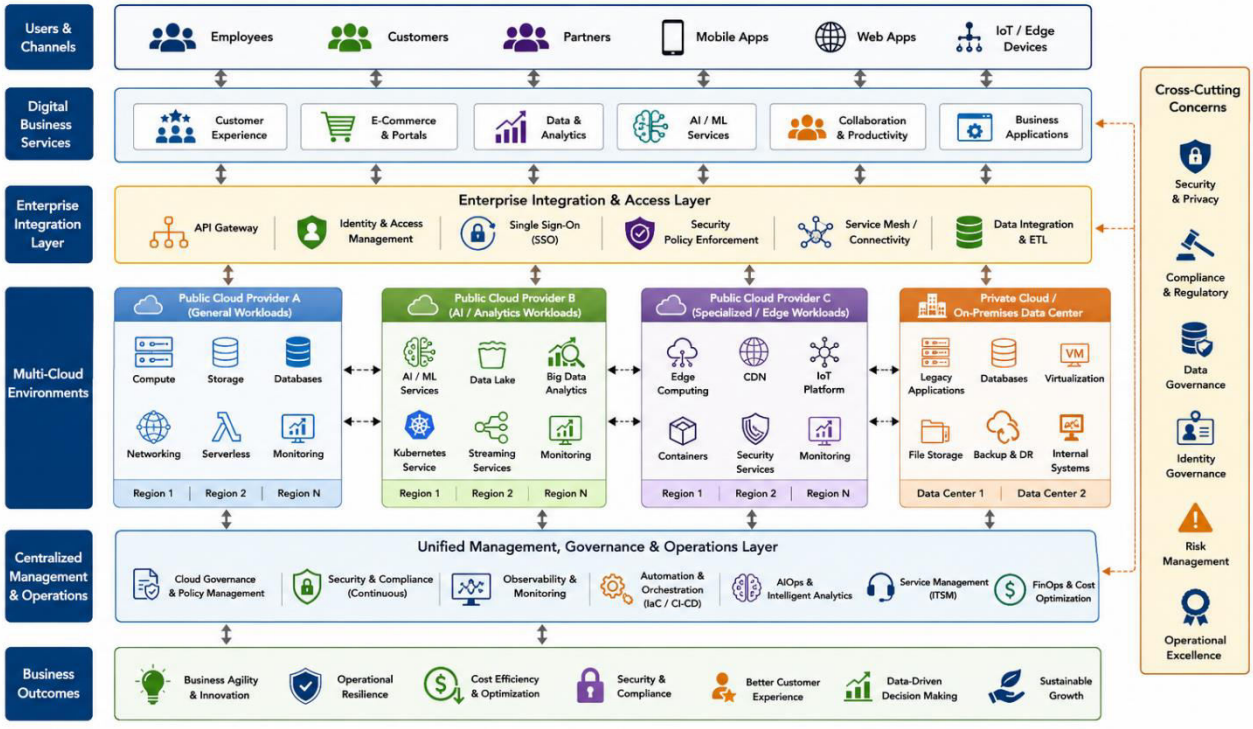
| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

Table 1. Major Business Drivers for Enterprise Multi-Cloud Transformation

Business Driver	Description	Enterprise Benefit
Business Agility	Rapid deployment of digital services	Faster innovation
Vendor Independence	Utilize multiple cloud providers	Reduced vendor lock-in
Disaster Recovery	Cross-cloud redundancy and failover	High availability
Regulatory Compliance	Regional data hosting	Improved compliance
Cost Optimization	Provider-specific pricing optimization	Reduced operational costs
Cloud Innovation	Access to specialized cloud services	Enhanced competitiveness
Scalability	Elastic infrastructure expansion	Better workload performance
Global Operations	Multi-region deployment	Improved customer experience

Fig. 1. High-Level Enterprise Multi-Cloud Transformation Ecosystem.



III. MULTI-CLOUD REFERENCE ARCHITECTURE AND CORE COMPONENTS

Enterprise multi-cloud transformation requires a comprehensive architectural framework capable of integrating heterogeneous cloud platforms, on-premises infrastructure, enterprise applications, security controls, and operational services into a unified ecosystem. Unlike single-cloud deployments, multi-cloud architectures must support interoperability across multiple service providers while maintaining consistent governance, security, performance, and operational visibility.

A modern enterprise multi-cloud architecture is typically organized into several logical layers, each responsible for a specific set of business and technical functions. These layers collectively enable organizations to build scalable, resilient, and cloud-agnostic digital platforms capable of supporting mission-critical workloads.

The uppermost layer consists of business applications and digital service consumers. Enterprise users access services through multiple channels, including web applications, mobile applications, APIs, partner portals, IoT devices, and

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

enterprise collaboration platforms. These applications generate requests that are securely routed through the enterprise integration layer before reaching the underlying cloud platforms.

The enterprise integration layer serves as the communication backbone of the architecture. It incorporates Application Programming Interfaces (APIs), API gateways, identity and access management (IAM), Single Sign-On (SSO), service mesh technologies, enterprise messaging platforms, and data integration services. This layer ensures standardized communication between distributed applications while enforcing authentication, authorization, traffic management, and policy-based security controls.

Beneath the integration layer lies the multi-cloud infrastructure layer, which consists of multiple public cloud providers, private cloud environments, and existing enterprise data centers. Each cloud environment is selected according to workload characteristics, business priorities, compliance requirements, and service capabilities. Mission-critical databases may remain within private cloud environments, while analytics, artificial intelligence, and customer-facing applications are distributed across specialized public cloud platforms.

Cloud-native technologies play an essential role in enabling workload portability across multiple cloud providers. Containerization platforms such as Docker, Kubernetes orchestration, serverless computing, and microservices architectures allow applications to remain largely independent of underlying infrastructure implementations. This portability significantly reduces vendor dependency while simplifying migration, scaling, and disaster recovery processes.

A unified management and operations layer provides centralized governance across all cloud environments. Rather than managing each cloud independently, enterprises establish centralized platforms for monitoring, logging, automation, orchestration, security management, configuration control, and financial governance. This layer improves operational consistency while reducing administrative overhead.

Automation forms the foundation of modern multi-cloud operations. Infrastructure as Code (IaC) enables infrastructure provisioning using declarative templates, eliminating manual configuration errors while ensuring consistent deployments across cloud providers. Continuous Integration and Continuous Deployment (CI/CD) pipelines automate application delivery, enabling organizations to release software updates more frequently with improved reliability.

Artificial Intelligence for IT Operations (AIOps) has become a critical architectural capability within multi-cloud environments. By analyzing telemetry, logs, performance metrics, and infrastructure events, AIOps platforms automatically identify anomalies, predict failures, recommend corrective actions, and initiate self-healing workflows. These intelligent capabilities significantly reduce operational complexity while improving system availability.

Observability platforms provide comprehensive visibility across distributed cloud infrastructures. Modern observability extends beyond traditional monitoring by collecting logs, metrics, traces, events, and application telemetry from multiple cloud providers. Unified observability enables IT teams to rapidly identify performance bottlenecks, diagnose application failures, optimize resource utilization, and improve user experience.

Security is integrated throughout every architectural layer rather than implemented as a standalone component. Zero Trust security principles, identity-centric access control, encryption, multi-factor authentication, network segmentation, cloud workload protection, security information and event management (SIEM), and continuous compliance monitoring collectively establish a secure operating environment. Security policies are consistently enforced regardless of workload location or cloud provider.

Cloud governance frameworks ensure that enterprise standards are uniformly applied across all cloud environments. Governance encompasses policy management, resource provisioning standards, tagging strategies, financial accountability, regulatory compliance, operational auditing, and lifecycle management. Well-defined governance enables organizations to maintain control while supporting decentralized innovation across business units.

Data management represents another fundamental architectural element. Enterprise data frequently spans multiple cloud platforms, requiring robust mechanisms for data integration, synchronization, replication, backup, disaster recovery, and lifecycle management. Modern data architectures incorporate distributed databases, object storage, data lakes, streaming

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

platforms, and metadata management systems that facilitate secure and efficient information exchange across cloud environments.

Platform engineering has recently emerged as a key architectural discipline supporting enterprise multi-cloud operations. Internal developer platforms provide standardized infrastructure services, deployment pipelines, security controls, monitoring capabilities, and reusable templates that accelerate application development while maintaining governance consistency. These platforms improve developer productivity and simplify enterprise-wide cloud adoption.

As enterprises continue expanding digital operations, reference architectures increasingly emphasize modularity, interoperability, automation, and resilience. Rather than focusing solely on infrastructure deployment, modern multi-cloud architectures integrate operational intelligence, governance, security, and service management into a unified enterprise platform capable of supporting continuous digital transformation.

Table 2. Core Components of Enterprise Multi-Cloud Architecture

Architectural Layer	Major Components	Primary Functions
Business Services Layer	Web Applications, Mobile Apps, APIs, IoT	Digital service delivery
Integration Layer	API Gateway, IAM, SSO, Service Mesh	Secure communication and interoperability
Multi-Cloud Infrastructure	Public Cloud, Private Cloud, Hybrid Cloud	Compute, storage, networking
Container Platform	Kubernetes, Docker, OpenShift	Workload portability and orchestration
Automation Layer	IaC, CI/CD, Configuration Management	Automated deployment and provisioning
Observability Layer	Logs, Metrics, Traces, Dashboards	Performance monitoring
AIOps Platform	Predictive Analytics, Event Correlation	Intelligent operations
Governance Layer	Policy Management, Compliance, FinOps	Cloud governance and optimization
Security Layer	Zero Trust, IAM, SIEM, Encryption	Enterprise security and compliance

Key Characteristics of Modern Multi-Cloud Architecture

Characteristic	Enterprise Value
Scalability	Dynamic resource allocation
High Availability	Cross-cloud redundancy
Portability	Vendor-independent deployments
Automation	Reduced operational effort
Security	Consistent policy enforcement
Governance	Enterprise-wide compliance
Observability	End-to-end operational visibility
Cost Optimization	Improved cloud financial management

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

Fig. 2. Reference Architecture for Enterprise Multi-Cloud and Managed Services Modernization

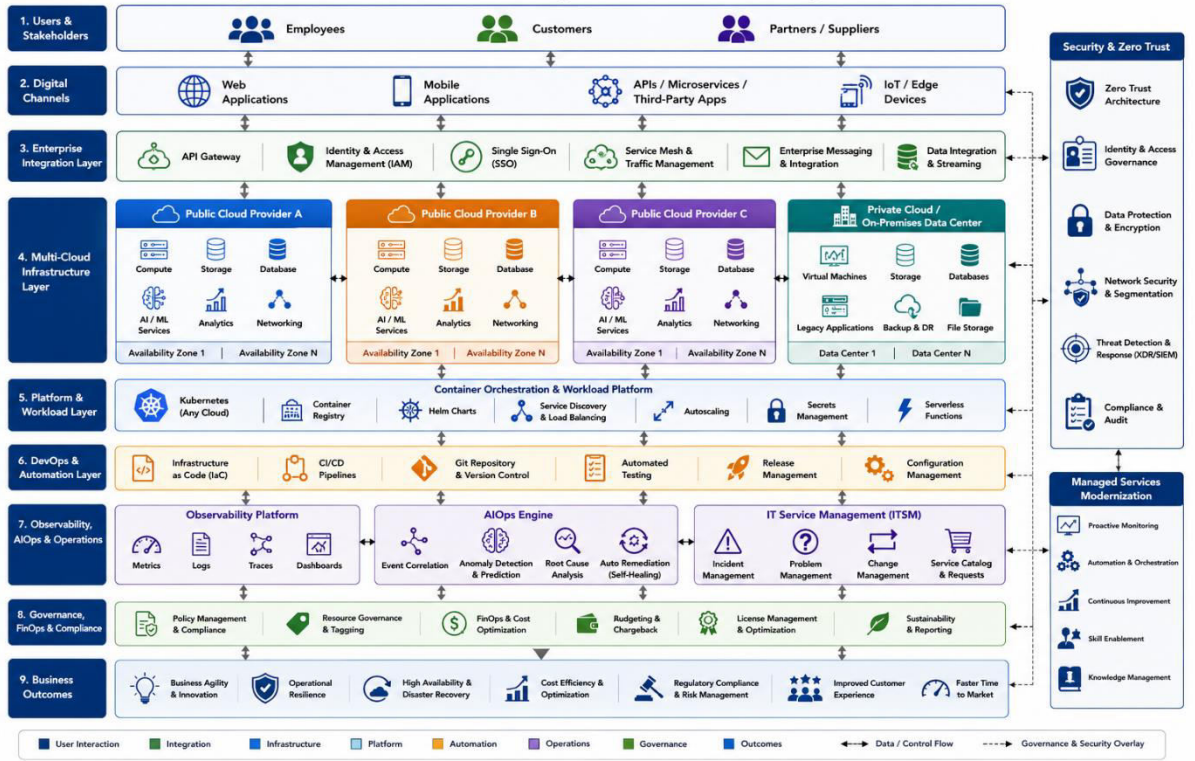


Figure 2. Reference Architecture for Enterprise Multi-Cloud and Managed Services Modernization

IV. MANAGED SERVICES MODERNIZATION FRAMEWORK

The rapid expansion of multi-cloud environments has fundamentally transformed enterprise IT operations. Traditional managed services, which primarily focused on infrastructure maintenance, reactive incident management, and periodic system administration, are no longer sufficient to support today's highly distributed digital ecosystems. Enterprises now require modern managed service models that are proactive, intelligent, automated, and capable of managing dynamic cloud-native workloads across multiple cloud platforms.

Managed Services Modernization (MSM) refers to the evolution of conventional IT operational support into an integrated service delivery framework that combines cloud technologies, automation, artificial intelligence, advanced analytics, and continuous service improvement. Rather than simply maintaining infrastructure, modern managed services continuously optimize performance, improve security, reduce operational risks, and accelerate digital innovation.

One of the primary objectives of managed services modernization is to shift operational activities from reactive problem resolution to proactive service management. Traditional IT operations typically respond after failures occur, resulting in increased downtime, service disruptions, and higher operational costs. Modern operational models continuously monitor infrastructure, applications, and business services to identify anomalies before they affect end users. Predictive analytics and intelligent automation enable organizations to detect potential issues early and initiate preventive actions without human intervention.

Automation serves as the cornerstone of managed services modernization. Routine operational activities such as infrastructure provisioning, software deployment, patch management, backup scheduling, configuration updates, compliance validation, and system recovery are increasingly executed through automated workflows. Infrastructure as Code (IaC) allows infrastructure resources to be provisioned using reusable templates, ensuring consistency, repeatability, and faster deployment across cloud environments. Configuration management platforms further reduce operational errors by enforcing standardized system configurations.

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

Cloud-native operations introduce Continuous Integration and Continuous Deployment (CI/CD) pipelines into managed service delivery. Software releases, infrastructure updates, and security patches are validated through automated testing before deployment into production environments. This approach significantly shortens release cycles while improving software quality and reducing deployment risks.

Artificial Intelligence for IT Operations (AIOps) has emerged as a transformative capability within modern managed services. AIOps platforms analyze massive volumes of operational data including system logs, performance metrics, application traces, infrastructure events, and user activity to identify abnormal behavior and predict service degradation. Advanced machine learning algorithms correlate events from multiple systems, reducing alert fatigue and enabling faster root cause identification.

Self-healing infrastructure represents another significant advancement in managed service modernization. Automated remediation engines can restart failed services, provision replacement infrastructure, scale workloads, recover databases, or reroute network traffic without requiring manual intervention. These capabilities significantly improve service availability while minimizing operational disruptions.

Observability extends beyond traditional monitoring by providing end-to-end visibility across distributed enterprise environments. Modern observability platforms collect metrics, logs, traces, events, and business transaction data from applications deployed across multiple cloud providers. Unified dashboards enable operations teams to monitor application health, infrastructure performance, user experience, and service dependencies through a centralized operational interface.

Security operations have become deeply integrated within managed service frameworks. Modern Security Operations Centers (SOC) leverage Security Information and Event Management (SIEM), Extended Detection and Response (XDR), Security Orchestration Automation and Response (SOAR), vulnerability assessment platforms, and continuous compliance monitoring to protect enterprise assets. Automated security policies ensure consistent enforcement across hybrid and multi-cloud infrastructures while supporting regulatory compliance requirements.

Information Technology Service Management (ITSM) remains a foundational element of managed services but has evolved considerably through automation and intelligent workflows. Modern ITSM platforms integrate incident management, problem management, change management, asset management, configuration management databases (CMDB), service request fulfillment, and knowledge management into unified digital workflows. Intelligent ticket routing, chatbot-based service desks, automated approvals, and predictive maintenance significantly improve service efficiency and user satisfaction.

Platform Engineering has recently emerged as a strategic discipline supporting enterprise managed services. Internal Developer Platforms (IDPs) provide standardized infrastructure services, deployment pipelines, security policies, monitoring capabilities, and reusable application templates. By abstracting infrastructure complexity, platform engineering enables development teams to focus on application innovation while maintaining operational consistency and governance.

Cloud Financial Operations (FinOps) has also become an essential component of modern managed services. As organizations increasingly consume cloud resources across multiple providers, financial governance becomes critical for controlling operational expenditures. FinOps platforms continuously monitor cloud usage, identify idle resources, recommend workload optimization strategies, and allocate costs across business units. These capabilities improve financial transparency and maximize return on cloud investments.

Modern managed services additionally emphasize Site Reliability Engineering (SRE) principles that combine software engineering practices with operational excellence. Service Level Objectives (SLOs), Service Level Indicators (SLIs), error budgets, automated testing, and reliability engineering enable organizations to improve application stability while supporting continuous software delivery.

Successful modernization requires organizational transformation alongside technology adoption. Enterprises must establish cloud operating models, cross-functional collaboration, DevSecOps practices, continuous workforce development, governance frameworks, and standardized operational procedures. Organizations that successfully integrate people, processes, and technology achieve higher operational maturity and greater business agility.

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

As digital transformation accelerates, managed services are evolving from traditional support organizations into intelligent business enablement platforms. The convergence of automation, cloud-native technologies, artificial intelligence, observability, security, and platform engineering creates resilient operational ecosystems capable of supporting enterprise innovation at scale.

Table 3. Evolution of Traditional and Modern Managed Services

Operational Area	Traditional Managed Services	Modern Managed Services
Monitoring	Reactive monitoring	Predictive observability
Infrastructure	Manual provisioning	Infrastructure as Code (IaC)
Incident Response	Human intervention	Automated remediation
Deployment	Manual release process	CI/CD automation
Security	Periodic assessment	Continuous monitoring & Zero Trust
IT Operations	Infrastructure-centric	Cloud-native operations
Analytics	Historical reporting	AI-driven predictive analytics
Cost Management	Manual budgeting	FinOps optimization
Service Desk	Ticket-based support	Intelligent ITSM with automation
Governance	Manual compliance	Continuous policy enforcement

Table 4. Key Technologies Supporting Managed Services Modernization

Technology	Enterprise Function	Business Benefit
Infrastructure as Code (IaC)	Automated provisioning	Faster deployment
Kubernetes	Container orchestration	Workload portability
AIOps	Intelligent operations	Reduced downtime
Observability	Unified monitoring	Faster troubleshooting
DevSecOps	Secure software delivery	Improved security
FinOps	Cloud cost optimization	Financial efficiency
SIEM & SOAR	Security automation	Faster threat response
Platform Engineering	Developer enablement	Increased productivity
ITSM	Service management	Improved service quality

V. CLOUD GOVERNANCE, SECURITY, AND COMPLIANCE IN MULTI-CLOUD ENVIRONMENTS

The successful adoption of enterprise multi-cloud environments depends not only on scalable infrastructure and modernized managed services but also on robust governance, comprehensive security, and continuous regulatory compliance. As organizations distribute applications and data across multiple cloud providers, maintaining consistent operational policies becomes increasingly challenging. Differences in cloud-native services, security controls, identity models, and management interfaces often create fragmented environments that increase operational risk. Consequently, enterprises must establish unified governance frameworks that provide centralized visibility, standardized policies, and automated control mechanisms across heterogeneous cloud platforms.

Cloud governance defines the policies, processes, standards, and accountability models that ensure cloud resources are deployed and managed in accordance with organizational objectives. Effective governance enables enterprises to balance innovation with operational control by standardizing resource provisioning, workload placement, financial accountability, service ownership, and lifecycle management. Governance frameworks also facilitate collaboration between cloud architects, security teams, developers, operations personnel, and business stakeholders, ensuring that cloud adoption aligns with strategic business goals.

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

One of the primary objectives of governance is maintaining operational consistency across diverse cloud environments. Standardized tagging policies, naming conventions, resource classification, configuration baselines, and infrastructure templates enable organizations to manage cloud assets efficiently while simplifying automation and reporting. Centralized governance platforms further provide enterprise-wide visibility into cloud resource utilization, performance metrics, security posture, and compliance status.

Security remains one of the most significant considerations in multi-cloud transformation. Traditional perimeter-based security models are no longer adequate for protecting highly distributed cloud-native environments. Modern enterprises increasingly adopt the **Zero Trust Security** model, which operates on the principle of "never trust, always verify." Every user, application, device, and workload must be continuously authenticated, authorized, and validated regardless of network location. This approach significantly reduces the attack surface while strengthening enterprise cyber resilience.

Identity and Access Management (IAM) serves as the foundation of Zero Trust architecture. Unified identity platforms centralize user authentication, authorization, and access control across multiple cloud providers. Technologies such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Privileged Access Management (PAM) ensure that users receive only the permissions necessary to perform their assigned responsibilities. Automated identity lifecycle management further enhances security by promptly provisioning, modifying, and revoking access privileges.

Data protection is another critical component of enterprise multi-cloud security. Organizations frequently store structured and unstructured data across public clouds, private clouds, and hybrid infrastructures. Comprehensive data protection strategies include encryption of data at rest and in transit, centralized key management, tokenization, data masking, immutable backups, and secure data replication. Data Loss Prevention (DLP) technologies continuously monitor sensitive information and prevent unauthorized disclosure or transfer.

Network security architectures have also evolved considerably within multi-cloud ecosystems. Software-Defined Networking (SDN), micro-segmentation, cloud-native firewalls, Web Application Firewalls (WAF), Secure Access Service Edge (SASE), and Cloud Access Security Brokers (CASB) enable organizations to establish secure communication channels between distributed workloads. Network segmentation minimizes lateral movement during cyberattacks while improving workload isolation and regulatory compliance.

Continuous security monitoring has become essential for detecting emerging cyber threats. Modern Security Operations Centers (SOCs) leverage Security Information and Event Management (SIEM), Extended Detection and Response (XDR), Endpoint Detection and Response (EDR), User and Entity Behavior Analytics (UEBA), and Security Orchestration, Automation, and Response (SOAR) platforms to analyze security events across multiple cloud environments. Artificial intelligence further enhances threat detection by identifying anomalous behavior patterns and automating incident response workflows.

Compliance management represents another major challenge within multi-cloud environments. Enterprises operating in regulated industries must comply with international standards and regulatory frameworks such as **ISO/IEC 27001**, **NIST Cybersecurity Framework**, **SOC 2**, **PCI DSS**, **HIPAA**, and the **General Data Protection Regulation (GDPR)**. Compliance requirements often vary across geographic regions, making centralized governance essential for maintaining consistent regulatory adherence.

Modern compliance frameworks increasingly rely on automation rather than periodic manual assessments. Policy-as-Code enables organizations to define compliance requirements as executable policies that are automatically evaluated during infrastructure provisioning and application deployment. Continuous compliance monitoring identifies policy violations in real time, allowing organizations to remediate issues before they impact business operations or regulatory audits.

Cloud governance also incorporates financial management through **Cloud Financial Operations (FinOps)**. As organizations expand cloud adoption across multiple providers, controlling operational expenditure becomes increasingly complex. FinOps frameworks provide visibility into cloud spending, optimize resource utilization, implement budgeting controls, allocate costs to business units, and recommend rightsizing strategies. Automated cost governance prevents resource overprovisioning while maximizing return on cloud investments.

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

Risk management remains an integral component of enterprise governance. Organizations perform continuous risk assessments to evaluate operational, cybersecurity, financial, and compliance risks associated with cloud services. Enterprise Risk Management (ERM) frameworks integrate cloud risk analysis with business continuity planning, disaster recovery strategies, third-party vendor assessments, and cybersecurity resilience programs. These practices ensure that organizations maintain acceptable risk levels while supporting ongoing digital transformation initiatives.

Governance maturity extends beyond technology implementation and requires clearly defined organizational responsibilities. Cloud Centers of Excellence (CCoEs), governance committees, security review boards, and cross-functional cloud operating teams establish enterprise-wide accountability for cloud adoption, architecture decisions, policy enforcement, and continuous improvement. Well-defined governance structures enable organizations to accelerate cloud innovation while maintaining security, compliance, and operational excellence.

As enterprise cloud ecosystems continue to expand, governance, security, and compliance increasingly become strategic enablers rather than operational constraints. Organizations that successfully integrate automated governance, Zero Trust security principles, continuous compliance monitoring, and intelligent risk management establish secure digital foundations capable of supporting long-term business growth, regulatory confidence, and operational resilience.

Table 5. Enterprise Cloud Governance Domains

Governance Domain	Primary Responsibilities	Business Benefits
Resource Governance	Resource provisioning, tagging, lifecycle management	Operational consistency
Security Governance	IAM, Zero Trust, encryption, access policies	Enhanced security
Compliance Governance	Regulatory controls, auditing, Policy-as-Code	Continuous compliance
Financial Governance (FinOps)	Budgeting, chargeback, cost optimization	Reduced cloud expenditure
Operational Governance	Monitoring, ITSM, automation	Improved service reliability
Risk Governance	Risk assessment, disaster recovery, business continuity	Business resilience

Table 6. Security Technologies in Enterprise Multi-Cloud

Technology	Function	Enterprise Advantage
Zero Trust Architecture	Continuous authentication and authorization	Reduced cyber risk
IAM with SSO & MFA	Centralized identity management	Secure user access
SIEM	Centralized security monitoring	Real-time threat detection
SOAR	Automated incident response	Faster remediation
CASB	Secure cloud application access	Improved cloud visibility
SASE	Secure networking for distributed users	Consistent security
DLP	Sensitive data protection	Regulatory compliance
Policy-as-Code	Automated compliance enforcement	Continuous governance

Key Benefits of Governance and Security

- Consistent governance across multiple cloud providers
- Reduced security vulnerabilities through Zero Trust principles
- Automated regulatory compliance and audit readiness
- Improved cloud cost visibility through FinOps
- Enhanced operational transparency and accountability
- Faster incident detection and automated response
- Better data protection and privacy controls
- Stronger business continuity and disaster recovery capabilities

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

VI. AUTOMATION, AIOPS, AND OBSERVABILITY FOR INTELLIGENT CLOUD OPERATIONS

The increasing complexity of enterprise multi-cloud environments has significantly transformed IT operations. Modern enterprises manage thousands of virtual machines, containers, databases, applications, APIs, and cloud services distributed across multiple cloud providers. Manual operational processes are no longer capable of supporting the scalability, speed, and reliability required by digital businesses. Consequently, organizations increasingly adopt automation, Artificial Intelligence for IT Operations (AIOps), and observability platforms to create intelligent, self-managing cloud ecosystems.

Automation has become the cornerstone of cloud operations modernization. It eliminates repetitive manual tasks while improving consistency, deployment speed, operational efficiency, and service reliability. Automation enables enterprises to provision infrastructure, deploy applications, configure networks, enforce security policies, perform backups, and recover systems through predefined workflows rather than manual intervention. This approach minimizes human error while accelerating the delivery of digital services.

Infrastructure as Code (IaC) is one of the most influential automation technologies supporting enterprise cloud transformation. Instead of manually configuring infrastructure components, IaC allows cloud resources to be defined using machine-readable templates and version-controlled code repositories. Infrastructure provisioning becomes repeatable, auditable, and consistent across multiple cloud providers. Organizations can rapidly deploy identical environments for development, testing, disaster recovery, and production while ensuring configuration consistency throughout the application lifecycle.

Continuous Integration and Continuous Deployment (CI/CD) pipelines further enhance automation by streamlining software delivery processes. Source code changes automatically trigger compilation, testing, security validation, artifact generation, and deployment across cloud environments. Automated testing frameworks reduce software defects, while deployment automation accelerates release cycles and minimizes operational risks. CI/CD enables enterprises to achieve faster time-to-market while maintaining software quality and operational stability.

GitOps has emerged as an extension of Infrastructure as Code by using Git repositories as the single source of truth for infrastructure configurations and application deployments. Every infrastructure modification is version-controlled, peer-reviewed, and automatically synchronized with production environments. GitOps enhances governance, simplifies rollback procedures, and strengthens operational transparency by maintaining a complete audit trail of infrastructure changes.

As cloud environments continue to expand, automation alone is insufficient for managing operational complexity. Enterprises increasingly rely on Artificial Intelligence for IT Operations (AIOps) to analyze operational data and provide intelligent decision support. AIOps platforms ingest large volumes of metrics, logs, traces, events, and telemetry from distributed infrastructure components. Machine learning algorithms identify hidden patterns, detect anomalies, correlate events, and predict system failures before they impact business operations.

Predictive analytics enables operations teams to anticipate infrastructure failures, application degradation, resource exhaustion, and capacity limitations. Instead of responding after incidents occur, organizations can proactively allocate additional resources, optimize workload placement, or initiate preventive maintenance activities. Predictive maintenance significantly reduces unplanned downtime while improving overall service availability.

One of the most valuable capabilities of AIOps is intelligent event correlation. Enterprise environments generate thousands of operational alerts every day from servers, applications, databases, networking devices, security tools, and cloud platforms. Traditional monitoring systems often produce duplicate or unrelated alerts, overwhelming operations teams. AIOps consolidates related events, identifies root causes, suppresses redundant notifications, and prioritizes critical incidents requiring immediate attention. This reduces alert fatigue and accelerates incident resolution.

Self-healing infrastructure represents another major advancement in intelligent cloud operations. Automated remediation workflows respond immediately to predefined operational conditions without requiring manual intervention. Common self-healing actions include restarting failed services, reallocating compute resources, replacing unhealthy containers, scaling applications, restoring failed databases, and rerouting network traffic. These capabilities significantly improve service resilience while reducing Mean Time to Recovery (MTTR).

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

Observability extends beyond conventional monitoring by providing comprehensive insight into the internal state of distributed cloud-native systems. Traditional monitoring focuses primarily on predefined performance metrics, whereas observability integrates metrics, logs, traces, events, and application telemetry to provide a holistic understanding of system behavior. This comprehensive visibility enables engineers to investigate complex performance issues across highly distributed microservices architectures.

Modern observability platforms collect telemetry from infrastructure components, container orchestration platforms, cloud-native applications, databases, messaging systems, APIs, and end-user devices. Distributed tracing follows individual transactions across multiple services, allowing engineers to identify latency bottlenecks, service dependencies, and application failures with greater accuracy. Centralized dashboards provide real-time operational visibility across multiple cloud providers, improving decision-making and incident response.

Automation and observability are increasingly integrated through closed-loop operational models. Observability platforms continuously monitor application performance and infrastructure health, while automation engines execute predefined remediation workflows based on operational policies. For example, abnormal CPU utilization may automatically trigger horizontal scaling, application failures may initiate container replacement, and security events may activate incident response procedures. These feedback mechanisms establish autonomous operational environments capable of adapting dynamically to changing workloads.

Site Reliability Engineering (SRE) principles complement automation by emphasizing reliability, service availability, and operational excellence. SRE practices define measurable Service Level Indicators (SLIs), Service Level Objectives (SLOs), and error budgets that guide operational decision-making. Automation enables SRE teams to focus on engineering improvements rather than repetitive maintenance activities, thereby enhancing long-term system reliability.

Operational intelligence also incorporates business-level analytics. Modern cloud management platforms integrate technical telemetry with business metrics such as customer transactions, application response times, revenue impact, and user experience indicators. This integrated perspective enables organizations to align operational decisions with strategic business objectives rather than focusing exclusively on infrastructure performance.

The convergence of automation, AIOps, observability, and reliability engineering is transforming enterprise IT operations from reactive support organizations into intelligent digital operations centers. By leveraging cloud-native automation, machine learning, predictive analytics, and real-time observability, enterprises establish resilient operational ecosystems capable of supporting continuous innovation, superior customer experiences, and sustainable digital transformation.

Table 7. Automation Technologies in Enterprise Multi-Cloud Operations

Technology	Primary Function	Enterprise Benefit
Infrastructure as Code (IaC)	Automated infrastructure provisioning	Faster deployment and consistency
CI/CD Pipelines	Continuous software delivery	Accelerated release cycles
GitOps	Version-controlled infrastructure management	Improved governance and rollback
Configuration Management	Automated system configuration	Reduced configuration drift
Workflow Automation	Automated operational processes	Higher operational efficiency
Container Orchestration	Workload scheduling and scaling	Improved resource utilization

VII. ENTERPRISE MIGRATION STRATEGY, IMPLEMENTATION ROADMAP, AND BEST PRACTICES

Enterprise multi-cloud transformation is a strategic initiative that extends beyond technology migration. Successful implementation requires a structured roadmap that aligns cloud adoption with business objectives, operational readiness, governance policies, workforce capabilities, and long-term digital transformation goals. Organizations that adopt phased migration strategies are better positioned to minimize risks, control costs, and achieve sustainable business outcomes while maintaining uninterrupted service delivery.

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

The first phase of a multi-cloud transformation initiative involves a comprehensive assessment of the existing IT landscape. Organizations evaluate application portfolios, infrastructure dependencies, business processes, data assets, security requirements, and regulatory obligations to determine cloud readiness. Workloads are classified according to criticality, performance requirements, technical complexity, and migration feasibility. This assessment enables enterprises to identify suitable migration candidates while establishing realistic project timelines and resource requirements.

Following the assessment phase, organizations define a target enterprise architecture that incorporates cloud-native design principles, standardized governance frameworks, security models, networking strategies, and operational processes. Reference architectures provide consistent design patterns for integrating multiple cloud providers, private cloud environments, and legacy systems. Standardization during this phase simplifies future expansion while reducing operational complexity.

Application modernization is often executed using the widely adopted **"6Rs" migration strategy**, allowing organizations to select the most appropriate migration approach based on workload characteristics.

- **Rehost:** Lift-and-shift migration with minimal application changes.
- **Replatform:** Limited application optimization for cloud environments.
- **Refactor:** Application redesign using cloud-native architectures.
- **Repurchase:** Replace legacy applications with Software-as-a-Service (SaaS) solutions.
- **Retire:** Decommission obsolete applications.
- **Retain:** Preserve applications that remain suitable for existing infrastructure.

Selecting the appropriate migration strategy for each application reduces migration risks while maximizing business value.

Data migration represents another critical component of enterprise transformation. Organizations implement secure migration pipelines that support database replication, data synchronization, validation, backup, and rollback capabilities. Incremental migration techniques reduce business disruption while maintaining data consistency throughout the transition process. Modern data integration platforms facilitate seamless movement of structured, semi-structured, and unstructured data across heterogeneous cloud environments.

Security must be embedded throughout the migration lifecycle rather than introduced after deployment. Security-by-Design principles ensure that identity management, encryption, access controls, compliance validation, vulnerability assessments, and security monitoring are incorporated into every migration activity. Automated security testing within CI/CD pipelines further strengthens application resilience by identifying vulnerabilities before production deployment.

DevSecOps practices play an increasingly important role in modern cloud transformation. Development, security, and operations teams collaborate throughout the software lifecycle to automate code validation, security scanning, compliance verification, infrastructure deployment, and operational monitoring. This integrated approach reduces deployment risks while accelerating software delivery.

Change management is equally important for organizational success. Cloud transformation often requires new operational models, revised governance structures, workforce reskilling, and cross-functional collaboration. Organizations invest in cloud competency programs, certification initiatives, and continuous learning to ensure employees possess the technical expertise required for cloud-native operations.

Pilot implementations are frequently used to validate architecture decisions before large-scale deployment. Initial migration projects typically focus on low-risk applications to evaluate performance, operational procedures, security controls, and governance effectiveness. Lessons learned from pilot deployments are incorporated into subsequent migration phases, reducing enterprise-wide implementation risks.

Continuous monitoring and performance optimization remain essential after migration completion. Organizations establish Key Performance Indicators (KPIs) to evaluate cloud performance, service availability, operational efficiency, security posture, customer satisfaction, and financial performance. Regular optimization activities include workload rightsizing, storage optimization, application tuning, cloud cost management, and capacity planning.

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

Business continuity planning must also be integrated into enterprise migration strategies. Disaster recovery architectures leverage geographically distributed cloud regions, automated failover mechanisms, cross-cloud replication, immutable backups, and recovery testing to ensure service continuity during infrastructure failures or cyber incidents.

Finally, cloud transformation should be viewed as an ongoing journey rather than a one-time migration project. Emerging technologies including artificial intelligence, edge computing, confidential computing, quantum-safe security, sustainable cloud computing, and autonomous operations will continue reshaping enterprise cloud strategies. Organizations that embrace continuous innovation and operational improvement will be better positioned to maintain competitive advantage within rapidly evolving digital ecosystems.

Table 8. Enterprise Multi-Cloud Migration Roadmap

Migration Phase	Key Activities	Expected Deliverables
Assessment	Application discovery, dependency mapping, cloud readiness assessment	Migration strategy
Planning	Architecture design, governance framework, security planning	Cloud roadmap
Pilot Migration	Low-risk workload migration	Validated architecture
Enterprise Migration	Large-scale workload migration	Multi-cloud deployment
Modernization	Automation, AIOps, observability, DevSecOps	Intelligent operations
Optimization	FinOps, performance tuning, continuous improvement	Operational excellence

Table 9. Best Practices for Enterprise Multi-Cloud Transformation

Best Practice	Organizational Benefit
Establish Cloud Center of Excellence (CCoE)	Improved governance
Adopt Infrastructure as Code	Consistent deployments
Implement Zero Trust Security	Strong cybersecurity
Standardize Cloud Architecture	Simplified operations
Utilize AIOps and Observability	Proactive operations
Implement FinOps	Optimized cloud spending
Enable DevSecOps	Secure software delivery
Continuously Measure KPIs	Ongoing operational improvement

VIII. CONCLUSION

Enterprise multi-cloud transformation has become a foundational strategy for organizations seeking to enhance business agility, operational resilience, scalability, and innovation in an increasingly digital economy. By leveraging services from multiple cloud providers, enterprises can optimize workload placement, reduce vendor dependency, improve disaster recovery capabilities, and utilize specialized cloud services that best align with business and technical requirements. However, the benefits of multi-cloud adoption can only be fully realized through comprehensive governance, standardized security controls, intelligent automation, and modernized managed services.

This article examined the key architectural principles, business drivers, operational frameworks, and implementation strategies associated with enterprise multi-cloud transformation and managed services modernization. The discussion demonstrated that cloud-native technologies, Infrastructure as Code, DevSecOps, AIOps, observability platforms, and FinOps collectively establish intelligent operational ecosystems capable of supporting continuous digital innovation. Modern managed services have evolved beyond traditional infrastructure support to become proactive, data-driven, and

| ISSN: 2582-7219 | www.ijmrset.com| Impact Factor: 5.928|Monthly, Peer Reviewed & Referred Journal |

| Volume 4, Issue 9, September 2021 |

|DOI:10.15680/IJMRSET.2021.0409023 |

automation-centric operational platforms that significantly improve service quality, operational efficiency, and customer experience.

Cloud governance, Zero Trust security, regulatory compliance, and policy-driven automation were identified as essential components for maintaining consistency across heterogeneous cloud environments. Organizations that integrate these capabilities with standardized operating models and continuous monitoring achieve greater operational visibility, improved cybersecurity, and enhanced regulatory compliance while effectively controlling cloud expenditure.

Furthermore, structured migration strategies, phased implementation roadmaps, workforce development, and continuous optimization enable enterprises to successfully navigate the complexities of large-scale cloud transformation initiatives. As emerging technologies such as artificial intelligence, edge computing, autonomous operations, confidential computing, and sustainable cloud architectures continue to mature, enterprise cloud ecosystems will become increasingly intelligent, adaptive, and business-centric.

Ultimately, enterprise multi-cloud transformation should be viewed as an ongoing strategic capability rather than a one-time infrastructure migration project. Organizations that combine modern managed services, intelligent automation, strong governance, and cloud-native innovation will be well positioned to achieve long-term operational excellence, business resilience, and sustainable competitive advantage in the evolving digital landscape.

REFERENCES

[1] NIST, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Rev. 5, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020.
[2] NIST, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020.
[3] Amazon Web Services, AWS Well-Architected Framework, Amazon Web Services, Seattle, WA, USA, 2020.
[4] Microsoft Corporation, Cloud Adoption Framework for Azure, Microsoft Azure Documentation, Redmond, WA, USA, 2020.
[5] Google Cloud, Google Cloud Architecture Framework, Google LLC, Mountain View, CA, USA, 2020.
[6] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Cloud Security Alliance, 2020.
[7] Flexera, 2021 State of the Cloud Report, Flexera Software, Itasca, IL, USA, 2021.
[8] HashiCorp, 2021 State of Cloud Strategy Survey, HashiCorp Inc., San Francisco, CA, USA, 2021.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 5.928

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

9710 583 466 9710 583 466 ijmrset@gmail.com

www.ijmrset.com