



Qatar's Cloud Adoption Guidelines

Date: June 2026



◆ Disclaimer/Legal Rights

The Ministry of Communications and Information Technology (MCIT) has developed this publication, entitled Qatar's Cloud Adoption Guidelines, reference DIA-GUI-001 (hereinafter referred to as the "Work"), as a guidance resource for all organizations in the State of Qatar seeking to adopt cloud services.

The "Work" has been prepared in accordance with the laws of the State of Qatar and does not confer, and may not be used to support, any right on behalf of any person or entity against the State of Qatar or its agencies or officials. If a conflict arises between this document and the laws of Qatar, the latter should take precedence. Every effort has been made to ensure the "Work" is accurate, but no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the "Work". Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites or any associated organization, product or service.

Any reproduction of this "Work" either in part or full and irrespective of the means of reproduction, should acknowledge MCIT as the source and owner of the "Work". Any reproduction concerning the "Work" with intent of commercialization should seek a written authorization from MCIT. MCIT reserves the right to assess the functionality and applicability of all such reproductions developed for commercial intent. The authorization from MCIT should not be construed as an endorsement of the developed reproduction and the developer should in no way publicize or misinterpret this in any form of media or personal / social discussions.

◆ Legal Mandate

The guidelines have been issued pursuant to Amiri Decision No. (57) of 2021 regarding the specification of ministries' mandates, which includes the competencies of the Ministry of Communications and Information Technology. It is also issued under Ministerial Decision No. (17) of 2024, which established departments within the administrative units of the Ministry of Communications and Information Technology and defined their functions.



Strategic Alignment



Qatar National Vision 2030

- Foster innovation in a **knowledge-based economy**
- Leverage **advanced technologies** to support **sustainable development and economic growth**

2030 الأجنـدة الرقـمية
Digital Agenda

Digital Agenda 2030

- Cloud is mentioned as a driver for Hypercomputing, IoT and 5G connectivity
- Develop **cutting-edge infrastructure** which includes boosting localized cloud capabilities
- Develop **cutting edge data centers and cloud services** through strategic partnerships with leading technology companies
- Calls for **cloud-friendly policies and regulations**, supporting the expansion of cloud data centers



Document Summary

Name	Qatar's Cloud Adoption Guidelines
Version	1.0.0
Document Reference	DIA-GUI-001
Document Type	Guidelines
Summary	The document provides organizations with practical guidelines for secure, efficient, and interoperable cloud deployment through a comprehensive cloud adoption framework that outlines key considerations across each phase of the cloud adoption journey.
Publishing Date	June 2026
Applicable To	All organizations in the State of Qatar
Owner	Ministry of Communications and Information Technology (MCIT)



◆ Acronyms

AI	Artificial Intelligence
API	Application Programme Interface
AWS	Amazon Web Services
CRA	Communications Regulatory Authority
GCP	Google Cloud Platform
CSP	Cloud Service Provider
DevOps	Development and Operations
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
ICT	Information and Communication Technology
KPI	Key Performance Indicator
MCIT	Ministry of Communications and Information Technology
NCSA	National Cyber Security Agency
NIAS	National Information Assurance Standard
OECD	Organization for Economic Co-operation and Development
PaaS	Platform as a Service
QCB	Qatar Central Bank
SaaS	Software as a Service
SLA	Service Level Agreement
SMEs	Small and Medium-sized Enterprises



Glossary Of Terms And Definitions

Term	Definition
Cloud technologies	A model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction.
Infrastructure as a Service (IaaS)	A cloud service model that provides fundamental computing infrastructure such as virtual machines, storage, and networks. Users manage operating systems and applications, while the provider manages the underlying hardware.
Platform as a Service (PaaS)	A cloud service model that provides a platform for developers to build, deploy, and manage applications without managing the underlying infrastructure. It includes tools, libraries, and services for application development.
Software as a Service (SaaS)	A cloud service model that delivers software applications over the internet. Users access applications via web browsers or APIs, while the provider manages infrastructure, platforms, and the application itself.
Public Cloud	A deployment model where cloud infrastructure is owned and operated by third-party providers such as AWS, Azure, or GCP, and resources are shared among multiple tenants over the internet.
Private Cloud	A deployment model with cloud infrastructure dedicated to a single organization. It may be hosted on-premises or by a third party, offering enhanced control and privacy.
Sovereign Cloud	Cloud computing service designed to ensure that data, its processing, and the underlying infrastructure remain within a specific country's borders and are subject to its laws and regulations.
Shared-responsibility model	Framework that clearly defines which security and operational tasks are the responsibility of the cloud service provider (CSP) and which belong to the customer.
Landing zone	Pre-configured environment designed to host applications and workloads in the cloud.
Hybrid Cloud	A deployment model that integrates public and private clouds, allowing data and applications to move between environments for greater flexibility and optimization.



Table of Contents

01

Introduction	8
1.1 What is the purpose of this document?	8
1.2 What are cloud technologies?	8
1.3 What are the benefits of cloud adoption?	11
1.4 What are the risks and challenges of cloud adoption?	12
1.5 What is the current state of cloud adoption in Qatar?	13

02

Scope and Application	15
------------------------------	----

03

Phases of Cloud Adoption	16
Phase 1 - Plan	17
Phase 2 - Adopt	23
Phase 3 - Run	29

04

Roles and Responsibilities	30
-----------------------------------	----

05

Reporting Mechanisms	34
-----------------------------	----

06

Checklist	35
------------------	----

07

References	37
-------------------	----

08

Document Control	38
-------------------------	----



01 Introduction

1.1 | What is the purpose of this document?

The Qatar's Cloud Adoption Guidelines aim to provide **organizations in the State of Qatar** with clear and actionable guidelines on the secure, efficient and interoperable adoption of cloud in their organizations.

The document provides a **cloud adoption framework**, outlining considerations for organizations across each phase to drive consistent deployment of cloud.

The **purpose** of this document is to:

Outline the phases of cloud adoption and provide a set of considerations and guidelines for each phase of the cloud adoption framework.



Offer guidance on engaging with selected and endorsed Cloud Service Providers in line with Qatar's regulatory frameworks.



Support organizations in building the skills, processes, and governance needed for cloud adoption.



1.2 | What are cloud technologies?

Cloud computing refers to a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.¹ According to the Organization for Economic Co-operation and Development (OECD), **cloud plays a critical role in accelerating digital transformation**. Its adoption by organizations not only provides the foundations for data-driven decision making through greater technology scalability and resilience but also supports economic competitiveness by improving firm-level productivity.²

¹ <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>

² https://www.oecd.org/en/publications/digitalisation-and-productivity-in-search-of-the-holy-grail-firm-level-empirical-evidence-from-eu-countries_5080f4b6-en.html



Cloud computing is underpinned by **five core characteristics** that shape its scalability, efficiency, and flexibility³:

Role	Description
 Rapid Elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly up or down in line with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
 Resource Pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge of the exact location of the resources provided but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing capacity, memory, and network bandwidth.
 Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
 Measured Services	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
 On Demand Self Service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

³ https://www.oecd.org/en/publications/digitalisation-and-productivity-in-search-of-the-holy-grail-firm-level-empirical-evidence-from-eu-countries_5080f4b6-en.html

To fully realize its benefits, organizations must understand the different service models through which cloud computing is delivered. Cloud computing can be used under different service models offered by cloud computing providers (CSPs), including but not limited to:

Service models



Infrastructure as a Service (IaaS) which provides computing infrastructure



Platform as a Service (PaaS) which provides a platform for application development and management



Software as a Service (SaaS) which provides access to applications and software over the internet



Disaster Recovery as a Service (DRaaS) which provides cloud-based backup and disaster recovery capabilities



Function as a Service (FaaS) which provides serverless execution of code in response to events



AI as a Service (AIaaS) which provides pre-built AI capabilities over the cloud

What it provides

Provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications.

Deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

Enable the replication and hosting of physical or virtual servers by a third party to provide failover in the event of a disaster or service disruption.

Allow users to run individual functions in stateless containers that are triggered by specific events without managing servers or infrastructure.

Offer ready-to-use AI tools and APIs such as natural language processing, computer vision, predictive analytics, and machine learning model hosting.

Management

The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user specific application configuration settings.

The provider manages the recovery infrastructure, but the consumer may configure backup policies and recovery plans based on their needs.

The provider manages all aspects of infrastructure and scaling. The consumer is responsible for the logic and behavior of the functions.

The provider manages the AI infrastructure and models, while the consumer integrates and configures services based on application needs.

Service models are complemented by deployment models, which define how and where cloud services are hosted, such as:

- **Public cloud:** Owned and managed by third-party providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP); infrastructure is shared across organizations over the internet.
- **Private cloud:** Dedicated infrastructure for a single organization, either on-premises or hosted/managed by a third party; not shared with others.
- **Hybrid cloud:** Interoperable mix of private and public cloud environments, enabling portability of workloads and unified management.
- **Community cloud:** Shared by multiple organizations with common concerns (e.g. compliance, jurisdiction); hosted or managed internally or externally with shared governance.
- **Multi-cloud deployment:** Use of multiple public cloud providers to distribute workloads and avoid dependency on a single vendor: each cloud may be used for different services or geographies.

1.3 | What are the benefits of cloud adoption?

Cloud is a foundational enabler of Qatar's digital transformation and the modernization of public services. It provides the scalable computing, storage and integration capabilities required to operate data-intensive services, Artificial Intelligence, advanced analytics, Internet of Things solutions and smart digital platforms. For public-sector entities, cloud provides a more flexible foundation for renewing legacy systems, sharing data securely across government and developing common platforms and reusable capabilities. This can reduce duplication across entities and support more joined-up, reliable and responsive services for citizens and businesses. Initiatives such as Fanar, the Arabic Large Language Model, and the TASMU Smart Qatar Program demonstrate how cloud-enabled infrastructure can support innovation and digital service delivery across sectors.

At the **organizational level**, cloud adoption can improve how technology is accessed, operated and developed. Key benefits include:

- **Greater agility:** Technology resources can be provisioned and scaled more quickly, allowing organizations to respond to changing demand and introduce new services faster.
- **More efficient use of resources:** Organizations can replace some fixed infrastructure investments with consumption-based services, better align capacity and costs with actual demand, and redirect effort from routine infrastructure management towards innovation and service improvement.
- **Improved resilience & continuity:** Cloud-based backup, recovery and distributed infrastructure can help organizations maintain critical services, recover more quickly from disruptions and manage periods of peak demand more effectively.
- **Access to advanced capabilities:** Organizations, including SMEs, can access Artificial Intelligence, advanced analytics and other specialized technologies without having to build and maintain the full underlying infrastructure themselves.
- **Stronger collaboration & accessibility:** Secure access to applications and information across locations can facilitate remote work, strengthen collaboration between teams, and support more flexible service-delivery models.

1.4 | What are the risks and challenges of cloud adoption?

While cloud computing offers transformative benefits such as agility, scalability, and cost efficiency, its adoption also introduces a set of complex risks and challenges that organizations must carefully consider:

Security Risk

Migrating data and applications to third-party cloud environments can introduce security risks related to data confidentiality, integrity, availability, and secure access control. Without appropriate security architecture, configuration management, monitoring, and incident response capabilities, organizations may be exposed to misconfigurations, unauthorized access, data leakage, and service disruption.

Regulatory and Compliance Risk

Organizations must comply with applicable national and sector-specific regulatory requirements when adopting cloud services (e.g., data sovereignty, privacy, auditability, and contractual controls). Failure to interpret and implement these requirements appropriately (including establishing robust governance and assurance mechanisms) may result in compliance gaps, legal exposure, and operational restrictions.

Vendor Lock-In

Many cloud platforms utilize proprietary technologies, Application Programming Interface (APIs), and architectures that can limit interoperability and portability. This dependency may restrict an organization's ability to switch providers, increase long-term costs, and create challenges during migration or system integration.

Data Residency

Adhering to national and sector-specific regulations often requires sensitive or classified data to be stored within national borders. This presents challenges related to data residency, cross-border data transfer limitations, and the need to ensure that cloud providers comply with local legal and audit standards.

Lack of resources/expertise

As cloud technologies evolve rapidly, the success of cloud adoption depends heavily on having resources with the right skills and expertise. Managing cloud infrastructure, security, automation, and services requires specialized knowledge that traditional IT teams may lack. Without the right capabilities, organizations risk misconfigurations, security vulnerabilities, and underutilization of cloud benefits. Building cloud competency through training, hiring, and technology partnerships ensures that the firm can design, operate, and optimize cloud environments effectively.

Lack of governance

In the absence of a structured governance framework, cloud adoption can lead to uncontrolled resource provisioning, inconsistent security practices, and compliance violations. Further, shadow IT, misaligned roles, and a lack of accountability often result in operational inefficiencies.

Physical infrastructure

Cloud environments rely on physical facilities and supporting utilities. Disruptions such as data center incidents (e.g., fire, flooding, overheating, power outage), deliberate acts (e.g., theft, vandalism, sabotage), or geopolitical situations (e.g., war) can lead to service unavailability or degraded performance.

Operational resilience (backup & disaster recovery readiness)

Cloud adoption can create a false sense of resilience if backup, replication, and disaster recovery mechanisms are not correctly configured, activated, and regularly tested (e.g., failover/failback drills).

1.5 | What is the current state of cloud adoption in Qatar?

The State of Qatar recognizes cloud computing as a critical enabler of its long-term national development objectives, underpinning ambitions in smart city development, digital government modernization, and the advancement of a competitive technology-driven economy.

Aligned with Qatar National Vision 2030, the government has articulated a strategic ambition to establish Qatar as a regional hub for cloud and data center services, with the objective of doubling **national cloud data center capacity** and progressively evolve into a net exporter of digital services. By 2030, the Information and Communications Technology (ICT) sector which encompasses cloud is expected to generate QR 40 billion (USD 11 billion) in economic value and contribute to positioning Qatar among the top 10 countries globally in digital competitiveness indices.⁴

Over the past few years, Qatar has pursued a strategy encouraging the establishment of data centers and investing in ecosystem development which had led to significant growth of the cloud market. Notably, strategic alliances with global cloud providers have enabled the launch of hyperscale cloud regions in Qatar.

To ensure consistent deployment and adoption of cloud, Qatar has taken a policy and regulation led approach by issuing a series of national cloud policies, regulatory frameworks, and compliance standards to guide cloud adoption and provide structure to both the private and public sector:



Cloud Security Policy (2018)⁵

Applies to government entities using or planning to use cloud services and sets out security and privacy considerations, baseline controls and safeguards for the secure adoption of cloud computing.

⁴ <https://oxfordbusinessgroup.com/reports/qatar/2025-report/ict-innovation/early-adoption-public-and-private-actors-are-taking-key-steps-in-integrating-innovative-technologies-into-a-range-of-sectors-overview/>

⁵ https://qcert.ncsa.gov.qa/sites/default/files/public/documents/cs-csps_cloud_security_policy_eng_v1.3.pdf



	Cloud Policy Framework (2022)⁶	Establishes policy and regulatory principles to support a trusted and cloud-friendly environment in Qatar. Provides recommendations on topics like cloud-first policy, data residency, digital inclusion, Service Level Agreements (SLAs) etc.
	Cloud Computing Handbook for SMEs (2022)⁷	Explains what cloud computing is, the meaning of typical cloud contractual provisions and key points that SMEs should pay close attention to before subscribing to cloud services.
	Cloud First Policy (2024)⁸	Requires government agencies working on projects involving new IT systems or technology refreshes to firstly consider and evaluate cloud solutions from CSPs who have agreements with MCIT.
	Cloud Computing Regulation (QCB) (2024)⁹	Establishes the minimum regulatory requirements for QCB-regulated entities using cloud computing arrangements, including requirements for governance, risk management, service-provider due diligence, contractual safeguards, ongoing oversight and exit planning.
	Cloud Data Interoperability & Portability Regulation (2024)¹⁰	Ensures CSPs embed data portability and interoperability into their services. It mandates minimum contractual commitments, adoption of international standards, and API availability for government entities to facilitate seamless data exchange.

While Qatar has made remarkable strides in cloud infrastructure and policy development, there remains significant untapped potential, particularly within the private sector. This highlights a major opportunity for growth as awareness, infrastructure, and support continue to improve. Moreover, with 60% of organizations identifying business and technology skills as a top challenge, the demand for cloud professionals is rapidly growing.¹¹

Considering Qatar's cloud-related policies, strategic objectives, and varying adoption rates across organisations, there is a need to support organizations in their adoption of cloud computing not only for accelerating digital transformation but also for fulfilling Qatar's aspirations under the Digital Agenda 2030.

In this context, MCIT has developed **Qatar's Cloud Adoption Guidelines**, providing a structured, practical approach to cloud planning, deployment, and operations. This guidance should be used in conjunction with the policies and regulations outlined above.

⁶ <https://www.cra.gov.qa/en/document/cloud-policy-framework>

⁷ <https://www.cra.gov.qa/en/document/cloud-computing-a-handbook-for-smes>

⁸ <https://www.mcit.gov.qa/-/media/mcit/documents/policies/cloudfirstv100en0.pdf>

⁹ <https://www.qcb.gov.qa/Documents/InformationSecurity/Cloud%20Computing%20Regulation.pdf>

¹⁰ <https://www.cra.gov.qa/en/document/regulation-for-cloud-data-interoperability-and-data-portability>

¹¹ <https://www.pwc.com/m1/en/issues/upskilling/hopes-and-fears-2022>.

02 Scope and Application

Qatar's Cloud Adoption Guidelines apply to:



All organizations in the State of Qatar including public, private, semi-government, non-profit, academic and other entities.

While these guidelines are non-binding¹², MCIT encourages organizations to consider them as a practical reference for planning, adopting, and operating cloud services responsibly. The Guidelines have been intentionally developed to be sector-agnostic. Each organization remains responsible for identifying and complying with the laws, regulations and standards applicable to its own industry and operations.

Public-sector organizations may refer to these Guidelines as a practical reference for cloud adoption; however, they must continue to comply with all applicable government policies, regulations, standards and processes, including but not limited to¹³:

- **The Cloud First Policy**, which requires government entities to assess government-endorsed cloud solutions for new IT systems and major technology refreshes.
- **The National Data Classification Policy**, which requires data to be classified according to its sensitivity and handled using the appropriate controls.
- **The National Information Assurance Standard**, which establishes information-security and assurance requirements for government entities.
- **The Cloud Security Policy**, which sets out cloud-specific security, privacy and risk-management requirements.
- **The National Data Policy and related standards**, which establishes requirements for the governance, management, sharing and protection of data.
- **Any applicable guidance**, approvals and reporting requirements issued by MCIT, NCSA, NPC, CRA or other competent authorities.

Public sector entities are encouraged to consult **MCIT Cloud Computing & Networks Department** for guidance on cloud adoption.

To ensure these guidelines remain practical and effective over time, MCIT encourages organizations to provide feedback on their implementation of the Cloud Adoption Guidelines to (dipd@mcit.gov.qa). Given the rapid pace of change in cloud computing, MCIT may also conduct an annual review of the guidelines to maintain alignment with evolving global best practices, emerging industry standards, and regulatory updates.

¹² The Guidelines do not introduce new regulatory obligations for cloud services and organizations should continue to comply with applicable national laws and sector-specific regulations (e.g., cybersecurity, data classification, data protection, and sector-specific requirements where applicable).

¹³ This includes but is not limited to the [Cloud First Policy](#), [National Data Classification Policy](#), [National Information Assurance Standard](#), [Cloud Security Policy](#), [National Data Policy](#), [National Data Standards](#)



03 Phases of Cloud Adoption

Cloud adoption enables organizations to achieve agility, scalability, cost-efficiency, and digital service innovation. However, successful adoption requires a structured, secure, and compliant approach, which supports an organization's business objectives and digital transformation.

Therefore, Qatar's Cloud Adoption Guidelines outline a framework with a set of considerations across 3 phases (plan, adopt and run) and 7 underlying stages of cloud adoption/deployment:



In addition, **governance and assurance** should be treated as a continuous function that spans the entire Plan–Adopt–Run lifecycle and should be maintained and enforced throughout all phases to ensure ongoing alignment with national policies, regulatory requirements and risk management practices. Organizations should also consider **responsible, ethical, and sustainable** cloud practices as guiding principles. As cloud increasingly underpins advanced digital services, this includes responsible data practices, transparency in cloud-enabled systems, and awareness of environmental impact.

The following section defines each of the phases and provides a set of high-level guidelines. Organizations are encouraged to consider the following best practice guidelines across the various phases of adoption.





Plan

01

Adopt

02

Run

03

Phase 1 - Plan

In this phase, organizations should focus on gaining awareness of cloud concepts, opportunities, and challenges. A thorough capability assessment is performed to identify cloud suitability and areas of improvement. Business and IT goals should be aligned to ensure clarity of purpose. Strong governance frameworks should be introduced early to manage risks, compliance, and costs. This phase lays down the strategic vision structured around four key stages:

Stage 1.1 | Build a foundational understanding of cloud technologies

First and foremost, organizations must develop a clear understanding of cloud computing, its core concepts, advantages, and potential challenges. This foundational awareness is essential for informed decision-making and effective planning. To achieve this, organizations should:

- **Establish Executive Sponsorship for Cloud Adoption:** Establish sponsorship at executive level for cloud within the organization.
- **Build Organizational Cloud Literacy:** Educate organization's stakeholders on key cloud service models (IaaS, PaaS, SaaS), deployment options (public, private, hybrid, and multi-cloud), and the associated benefits such as scalability, cost efficiency, and operational agility. This can be done by leveraging Cloud Champions to drive literacy across the organization and offer foundational training and sensitization workshops.
- **Build Technical Cloud Literacy and AI:** Develop and enhance the technical cloud skills of existing staff, while augmenting teams with specialists where needed. In addition, organizations should understand the technical, operational, and capability requirements associated with AI workloads.
- **Articulate the Strategic Value of Cloud:** A critical focus area of the cloud literacy-building exercise should be to communicate the business value of cloud adoption in a clear and compelling way. Leadership plays a vital role in this effort by demonstrating how the cloud enables digital transformation, supports innovation, and improves the scalability and resiliency of services. This can be reinforced through live case studies that highlight practical examples of cloud-driven success.



Stage 1.2 | Assess your capabilities and define your goals

This stage focuses on defining a clear vision for cloud adoption in line with organizational goals and ensuring readiness across the organization. By clarifying motivations, assessing the current IT landscape, and setting measurable targets, organizations can develop a structured approach to cloud adoption that supports their business strategy and broader digital transformation.

Organizations should actively involve business unit leaders to ensure that cloud adoption is not solely IT-driven but instead reflects the broader business needs, ongoing initiatives and future strategic ambitions. The effort should be guided and endorsed by strong executive sponsorship to ensure alignment, accountability, and momentum.

The following components form the essential building blocks of this foundational stage:

- **Develop a Cloud Adoption Business Case:** Build a compelling business case to justify cloud adoption and secure organizational commitment. It should clearly articulate the strategic intent behind the adoption by outlining the following:
 - **Motivations:** Define the key drivers for cloud adoption, how it addresses current business-IT needs and pain areas and drives strategic ambition (i.e. reducing operational risk, accelerating innovation cycles, improving service agility, enhancing scalability, or achieving cost efficiencies).
 - **Mission Statement:** Clearly describe the purpose of the cloud adoption:
 1. Why cloud adoption is being pursued?
 2. What does the organization aim to achieve?
 3. How will cloud services be leveraged to enable that vision?
 - **Objectives:** Establish specific, measurable, and time-bound goals that align with broader organizational strategy. These should demonstrate how cloud adoption will deliver tangible value, such as enabling digital services, enhancing resilience, or unlocking new business capabilities.
- **Engage Business Stakeholders:** Engage business units at an early stage to build a cloud strategy that reflects operational realities and future requirements.





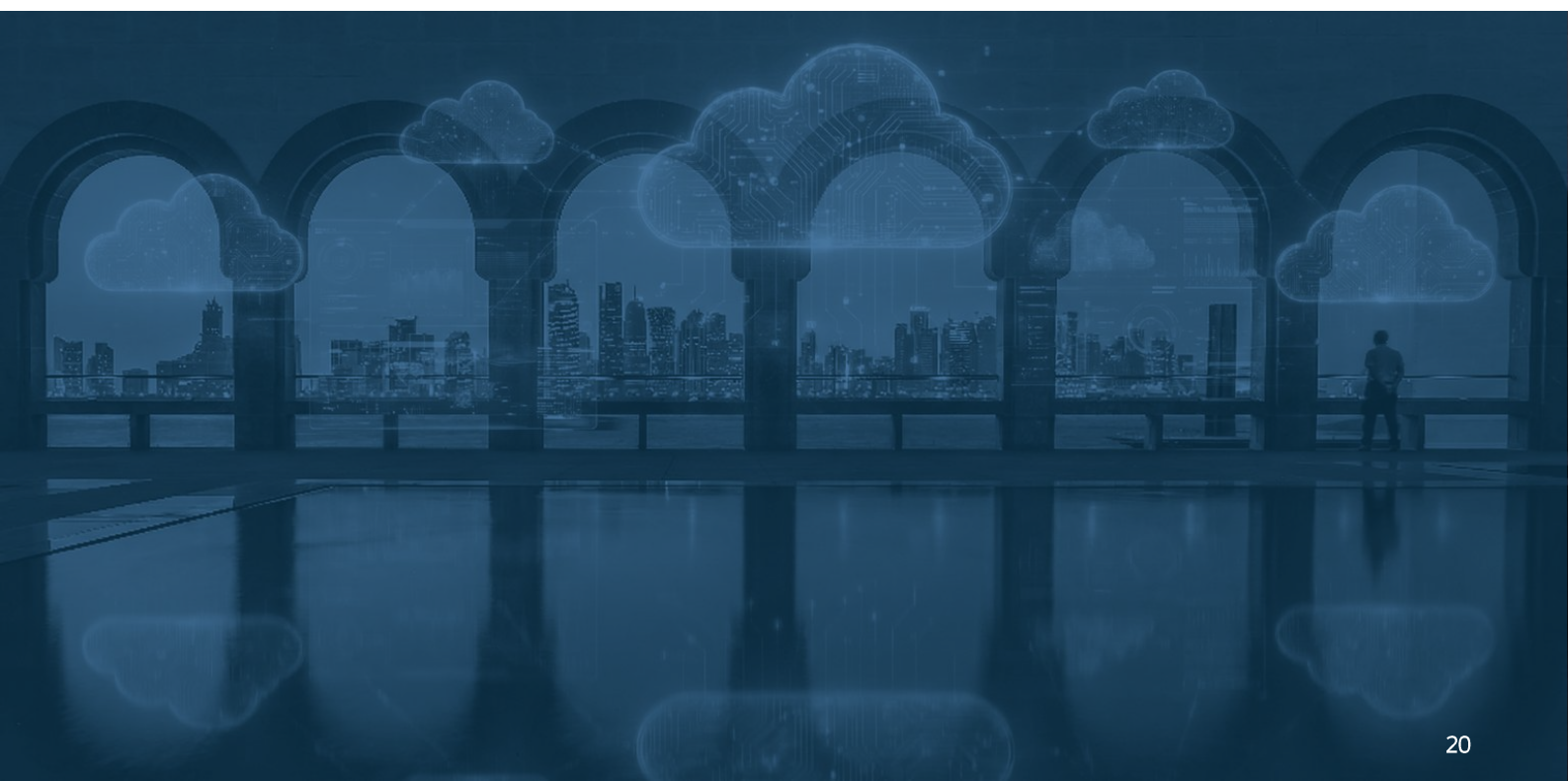
- **Assess Current State:** Conduct a Cloud Maturity Assessment, including infrastructure, application portfolio, data maturity, and technical debt. This baseline will help identify which applications, systems, workload, and data are best suited for cloud migration. Key guiding questions include:
 - Is IT aligned with the future business and strategic priorities?
 - What is the current data volume, growth rate, and retention policy?
 - What is the current IT spending? Are there any FinOps practices currently in place?
 - What hardware and network assets are currently in use?
 - Which applications are business-critical vs. non-essential?
 - What are the data governance, privacy, and classification practices?
 - Are there outdated systems or unsupported technologies in use?
 - What are the current licensing models (perpetual vs subscription) and renewal timelines?
 - What is the current risk assessment and cloud readiness?
 - Does the organization have cloud-related skills or certifications?
 - Is there a tested and updated disaster recovery and business continuity plan?
 - Is the organization legally and regulatory-compliant?
- **Define Target Outcomes:** Establish clear KPIs or metrics, along with targets and owners, aligned to each objective to track progress effectively. Regularly review these indicators to assess performance, identify gaps, and take corrective actions where needed to stay on course. Ensure metrics are specific, measurable such as cost reduction, customer satisfaction, or operational efficiency are directly tied to desired business outcomes.



Stage 1.3 | Perform a gap analysis and produce a roadmap

Once the capabilities are assessed, organisations should perform a gap analysis which will later help developing the roadmap.

- **Perform a Gap Analysis:** Compare the current versus desired capabilities across infrastructure inventory (servers, storage, network), application portfolio (criticality, dependencies, tech stack), data landscape (classification, governance, quality), IT operating model (processes, skills, org structure), security, compliance, risk posture and financials (IT spend, CapEx vs OpEx).
 - The current capability shortfall should be prioritized based on business impact, risk, regulatory compliance, and ease of resolution.
 - Organizations should consider the total cost of ownership based on their own accounting methods, to be able to really judge the cost savings provided by cloud infrastructure.
- **Develop a Cloud Adoption Roadmap:** Conduct a migration readiness assessment for each application and create a phased roadmap across pre-migration, migration execution and post migration stages that outlines the sequence of activities across business units and systems, prioritizing based on risk, impact, and readiness.
 - **Identify and classify the types of data handled by the organization** (i.e. operational, financial, customer, R&D, marketing, sales, compliance, and legal) and determine where each should be hosted based on its classification, for instance sensitivity, criticality, and applicable regulations.
 - **Apply a hosting strategy based on security controls and data sensitivity:** For example, R&D workloads are typically well-suited for cloud deployment.





Plan

01

Adopt

02

Run

03

Stage 1.4 | Establish clear governance for cloud usage

Before implementation, the organization must establish roles & responsibilities, robust governance structures & policies, structured processes and enabling technologies to manage cloud use in a secure and compliant manner. To achieve this, organizations should:

- **Design a Cloud Operating Model:** Define roles & responsibilities relevant to cloud deployment e.g. cloud architect, cloud service manager and cloud security lead. Refer to Section 5 (Roles & Responsibilities) for details related to roles, responsibilities and skills required. Additionally, a clear Shared Responsibility Model should be defined during vendor onboarding to delineate security, compliance, and operational accountabilities between the organization and the Cloud Service Provider.

On-Premises	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Figure 1: Example of Shared Responsibility Model

● You Manage

● Other Manages



Plan

01

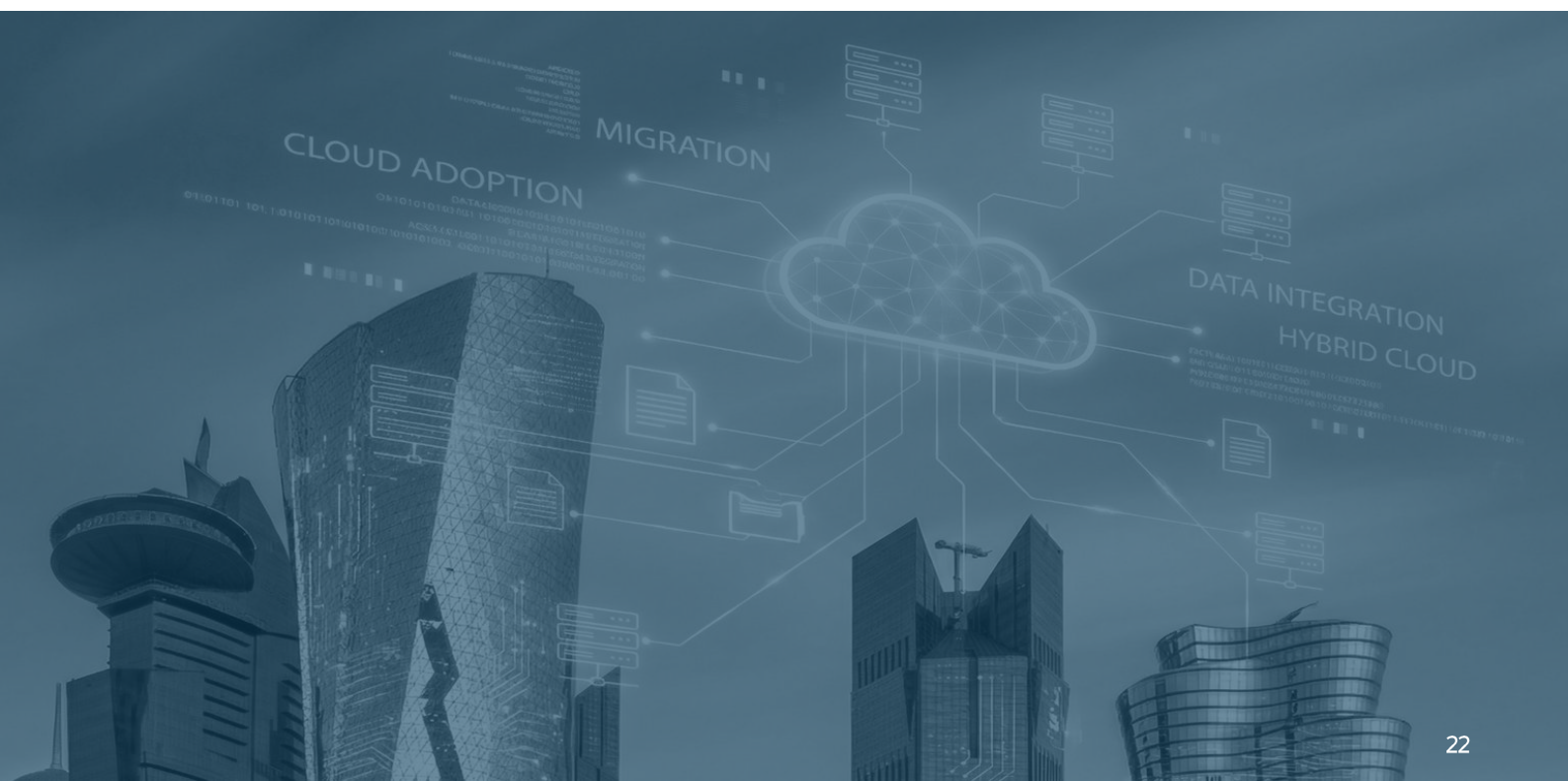
Adopt

02

Run

03

- **Develop Cloud-Specific Policies:** Create or update internal policies around cloud usage, including acceptable use, encryption, access management incident response, and backup. Organizations should consider setting up Identity and Access Management (IAM) policies to define roles, responsibilities, and access privileges across users, systems, and services within their cloud environment.
- **Establish Governance Boards or Committees:** Form steering committees or working groups to oversee adoption progress, address cross-cutting issues, and guide procurement and architecture decisions. Refer to Section 6 (Reporting Mechanism) for details.
- **Define Cloud Processes:** Define and document internal process workflows related to cloud planning, procurement, deployment and monitoring, change management, periodic compliance audit checks, cost optimization, vendor lock-in mitigation strategy, multi cloud strategy etc.





Plan

01

Adopt

02

Run

03

Phase 2 - Adopt

In this phase, the focus shifts from planning to execution. The right cloud provider is selected based on business, technical, and regulatory requirements. A scalable and secure architecture is designed to fit the organization's needs. Workloads and data are then migrated and deployed, transforming strategy into tangible outcomes.

Stage 2.1 | Select your cloud service provider

This stage involves the selection and procurement of CSPs as a strategic decision that should align with the organization's goals, regulatory requirements, and technical needs. To achieve this, organizations should:

- **Shortlist CSPs:** Identify potential CSPs, prioritizing approved providers¹⁴ such as Microsoft Azure, Google Cloud, and Oracle, while also considering other reputable options if regulatory conditions allow.
- **Evaluate CSPs Against Key Selection Criteria:** Assess each provider using a structured framework covering aspects such as regulatory compliance, security controls and certifications, technical capabilities and cost model. Weightage should be assigned to each of the parameters and all eligible CSPs should be evaluated against these parameters (not limited to):

Theme	Criteria	Key Considerations
 Regulatory compliance	Data residency and sovereignty alignment	CSPs should demonstrate compliance with applicable national data residency, sovereignty, and data protection requirements issued by the relevant authorities ¹⁵ . Legal review should ensure contractual clarity regarding where data is stored, processed, transferred, and backed up. Contract evaluations should verify that cloud service agreements clearly define data ownership, audit rights, data portability, secure data destruction, exit and transition arrangements, governance responsibilities, and the allocation of compliance obligations between the organization and the CSP.
	Regulatory Requirement	Organizations should ensure that the selected CSP enables compliance with all applicable legal, regulatory, and contractual obligations, including privacy, cybersecurity, records management, and any sector-specific requirements relevant to the organization's operations.
	Reputation and trustworthiness	Organizations should verify that CSPs have a strong track record of legal compliance and transparency. Where available, preference should be given to CSPs holding a valid National Information Assurance certification issued by NCSA ¹⁶ .

¹⁴ Non-exhaustive list of selected and endorsed Cloud Service Providers.

¹⁵ This includes: National Data Policy, Law No. (13) of 2016 on Protecting Personal Data Privacy

¹⁶ <https://www.ncsa.gov.qa/en/pages/certificationnia>



Plan			01	Adopt	02	Run	03
Theme	Criteria	Key Considerations					
 Security Controls and Certifications	Service model and product availability and certifications	Ensure that the CSP offers the appropriate cloud service models (IaaS, PaaS, SaaS) and a broad portfolio of platform and application services that meet current and future functional requirements. Product maturity, ecosystem richness, and regional service availability should also be considered. Confirm that the CSP holds relevant industry and regulatory certifications which demonstrate adherence to global best practices for security, privacy, and operational excellence.					
	Security certifications and IAM capabilities	CSPs must adhere to robust security standards.					
	Vendor lock-in and Data Disposal	Evaluate CSPs for portability, open standards support, and exit strategies, and ensure that contractual terms include data export options and mitigation for lock-in risks. Ensure how CSPs dispose data once the contract is stopped along with assurances provided in this aspect.					
 Technical capabilities	Service model and product availability and certifications	Ensure that the CSP offers the appropriate cloud service models (IaaS, PaaS, SaaS) and a broad portfolio of platform and application services that meet current and future functional requirements. Product maturity, ecosystem richness, and regional service availability should also be considered. Confirm that the CSP holds relevant industry and regulatory certifications which demonstrate adherence to global best practices for security, privacy, and operational excellence.					
	Uptime, latency, and service availability	CSP selection should factor in regional data center availability and network performance guarantees.					
	Disaster recovery and continuity capabilities	Assess whether the CSP offers built-in disaster recovery solutions, automated backups, cross-region failover, and guarantees on RTO and RPO. Include these capabilities in cloud services agreement negotiations to ensure they align with business risk tolerance.					
	Customer support, SLAs, and escalation mechanisms	Assess the CSPs customer support capabilities, ensuring that comprehensive SLAs are in place to cover availability, incident response times, and resolution protocols. The provider should also offer well-defined escalation mechanisms to address service disruptions or critical issues in a timely and accountable manner.					



Plan	01	Adopt	02	Run	03
------	----	-------	----	-----	----

Theme	Criteria	Key Considerations
 Cost model	Pricing models (on-demand, reserved, tiered)	Organizations should consider the different pricing models in line with their (future) business needs, such as: • Pay-as-you-go • Tiered / Volume-Based Pricing

- **Test Workload in a Pilot Environment:** Evaluate the performance, ease of integration, and operational alignment of the selected CSP in the pilot phase.
- **Conduct Procurement and Legal Review:** Engage legal and procurement teams to perform a thorough review of proposed contracts and finalize the commercial agreements. Ensure inclusion of SLAs and Key Performance Indicators (KPIs) covering uptime and availability guarantees, support response times and escalation paths, data handling, privacy, and sovereignty provisions and exit strategies (e.g., data portability, vendor lock-out clauses). Private organizations can refer to the **CRA Cloud Computing - Handbook for SMEs** for additional information on contractual matters.





Plan

01

Adopt

02

Run

03

Stage 2.2 | Develop and tailor your cloud architecture

Once the cloud service provider is selected, a secure, scalable, and interoperable cloud architecture suited to entity workloads and service models (IaaS, PaaS, SaaS) must be developed. To achieve this, organizations should:

- **Design Scalable and Resilient Architectures:**
 - Build fault-tolerant architecture with built-in redundancy, disaster recovery, and automated failover for mission-critical systems.
 - Establish data architecture by defining where and how data is stored, replicated, accessed, and governed by ensuring compliance with data residency, classification, and sovereignty requirements.
 - Incorporate network, security, and application design to ensure the architecture supports secure connectivity, identity and access controls, and integration with both legacy and modernized (cloud-native) applications.
- **Evaluate Cost Models Carefully:** Consider scalable options that match usage patterns, such as hourly or monthly pricing. Tailor access to align with business cycles, scaling up during peak demand and down during quieter periods to optimize spend, and application modernization and cloud native development.





Stage 2.3 | Migrate and deploy your data

The next stage involves a phased migration to the cloud, prioritizing business-critical applications and workloads, in a way that ensures minimal disruption to business processes and infrastructure operations. To achieve this, organizations should:

- **Adopt a Phased Migration Strategy:** Develop a clear and structured migration strategy that outlines the approach, guiding principles, and sequencing logic for moving applications, data, and systems to the cloud. The plan should consider technical dependencies, business priorities, risk appetite, and resource availability to ensure a smooth and coordinated transition.
- **Conduct Pre-Migration Testing:** Validate compatibility, performance, and security of workloads in a test environment before going live.
- **Enhance Cloud Infrastructure Foundation:** Expand the landing zone with multi-account/tenant structure, monitoring, and security.
- **Establish Rollback and Contingency Plans:** Prepare rollback options in case of failure and establish support arrangements with cloud vendors for post-migration issues.
- **Train Staff During Transition:** Provide technical and functional training to ensure IT teams and end users are confident in using new cloud-based services. Training should include:
 - Developing and delivering ongoing training programs on cloud technologies and best practices.
 - Regular awareness campaigns on cloud policies and compliance requirements.
 - Continuous learning and professional development.
- **Launch Pilot Phase:** For organizations with limited cloud capabilities, a pilot launch is critical to test resources, controls, and processes before full migration.
 - **Workload Selection:** Choose low-risk, non-critical applications with small data sizes and minimal dependencies. Keep sensitive data on-premises until governance and security are validated. Suitable workloads include:
 - i. Dev/Test environments
 - ii. Non-critical business apps (e.g., HR, ticketing)
 - iii. Collaboration tools (e.g., intranet, document management)
 - iv. Reporting apps with limited data



Plan

01

Adopt

02

Run

03

- **Testing in Pilot Environment:** Include testing of workload performance and operational challenges within the pilot to validate readiness and identify potential issues early.
- **Learning & Improvement:** Document challenges (e.g., performance, cost, compliance) and capture best practices. Use insights to refine the migration methodology and shape the cloud operating model.



Phase 3 - Run

This final phase ensures smooth operations and long-term value realization. Continuous monitoring safeguards performance, security, and compliance. Organizations focus on optimizing costs, automating operations, and enhancing resilience.

Stage 3.1 | Monitor the technology post-deployment

Post-deployment, organisations must operate, monitor, and manage their cloud environments to ensure security, efficiency, and continuous service quality. To achieve this, organizations should:

- **Establish Real-Time Monitoring:** Use dashboards and monitoring tools to track system performance, availability, and usage patterns.
- **Gather Stakeholder Feedback:** Regularly capture input from business and technical stakeholders on cloud performance, usability, and alignment with objectives, and feed these insights into continuous improvement and optimization efforts.
- **Enforce Security and Compliance:** Continuously scan for vulnerabilities, enforce security baselines, and maintain compliance with national and sector-specific regulations.
- **Monitor Recovery and Backup Effectiveness:** Regularly test disaster recovery plans and backup procedures to validate readiness. Ensure that recovery targets are being met, and that the organization remains compliant with internal continuity objectives and external regulatory requirements.
- **Implement Cost Management and FinOps Practices:** Adopt financial operations principles to monitor, analyze, and optimize cloud spending. Use cost dashboards, forecasting tools, and budgeting controls to improve financial accountability and prevent over-provisioning or waste.
- **Track CSP Service Updates and Announcements:** Monitor CSP communications for updates on maintenance windows, service deprecations, end-of-life notifications, and changes in the cloud services agreement or pricing. This ensures timely responses to service impacts and avoids disruption.
- **Explore and Evaluate New Cloud Services:** Continuously assess new CSP offerings (e.g., AI tools, advanced analytics, managed services) that could improve efficiency, performance, or enable new capabilities within the organization's digital services.
- **Conduct Regular Reviews and Audits:** Periodically review contracts, costs, and performance against cloud services agreements. The risk assessment and mitigation plan and exit strategy documentation should also be reviewed.
- **Foster a Culture of Innovation:** Encourage experimentation, agile development, and cross-functional collaboration to rapidly develop and deploy new services.



04 Roles and Responsibilities

The cloud ecosystem encompasses a vast network of various stakeholder types. When adopting and migrating to the cloud, an organization typically needs to assign clear roles and responsibilities to ensure a smooth and secure transition.

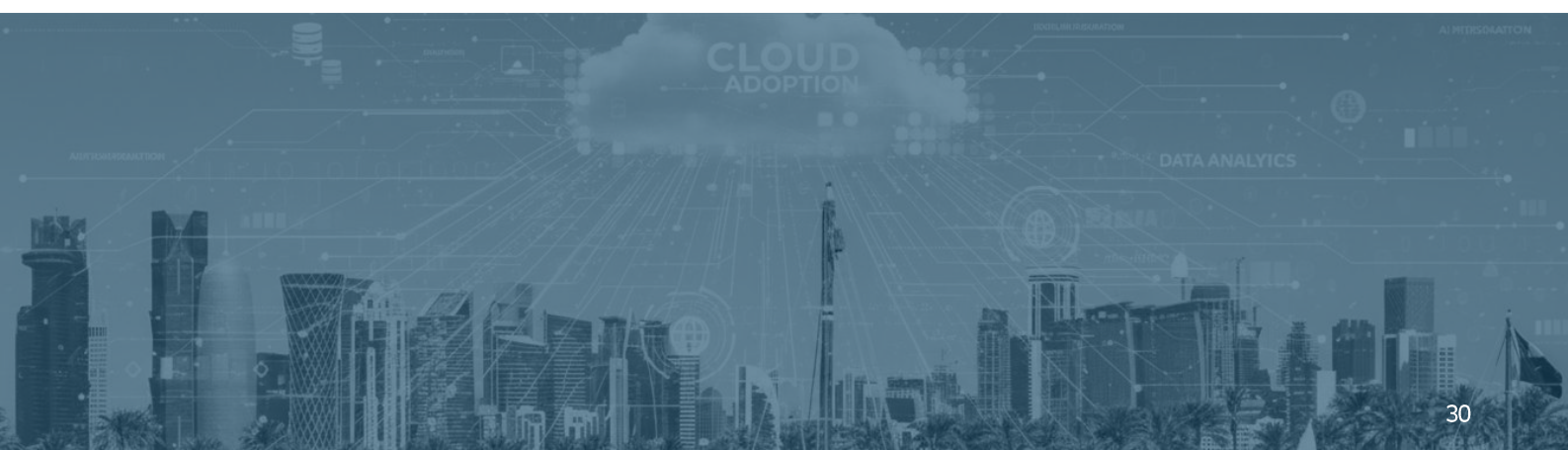
4.1 | What are the roles and skills that you need to adopt cloud technologies?

These **roles** span across strategic, technical, and operational domain. Successfully adopting cloud technologies requires a combination of **technical and soft skills**. It is important to keep in mind that these roles and skills may vary based on:

- The deployment model
- The type of workload
- The organization's structure

Therefore, the following are roles and core skills to consider, though not limited to:

Role 1: Executive Sponsor  Description: Sets strategic direction and secures budget for cloud adoption and monitors alignment with business goals. Technical Skills • Cloud service models • IT strategy and architecture basics • Budgeting, forecasting, financial governance • Risk, compliance, and security awareness Soft Skills • Strategic leadership • Stakeholder alignment • Executive communication	Role 2: Cloud Program Manager  Description: Oversees migration planning and execution. Manages timelines, risks, and stakeholder coordination. Technical Skills • Cloud models and cost tracking • Agile project management tools • Cloud KPIs and reporting • Cost allocation and Chargeback Soft Skills • Communication & coordination • Risk management • Adaptability and problem-solving	Role 3: Business Owner  Description: Represents the interests of a specific business unit and ensures that cloud adoption delivers measurable business value. Technical Skills • Understanding of cloud capabilities from a business perspective • Data classification awareness • Basic familiarity with cloud KPIs and SLAs Soft Skills • Business acumen • User-centric thinking • Communication and influence
---	--	--





Role 4: Cloud Architect



Description: Designs scalable, secure cloud architecture and define the migration approaches and selects technologies.

Technical Skills

- Cloud architecture
- Infrastructure as Code
- Cloud networking and identity (VPC, IAM)
- Cost optimization and system resilience

Soft Skills

- Cross-team collaboration
- System-level thinking
- Stakeholder engagement

Role 5: Enterprise Architect



Description: Ensures that cloud adoption plans align with the organization's current enterprise architecture and support the transition toward the desired future-state architecture.

Technical Skills

- Enterprise architecture frameworks
- Application and data integration
- EA modeling tools

Soft Skills

- Strategic planning
- Systems thinking
- Stakeholder engagement

Role 6: Security & Compliance Lead



Description: Ensures regulatory compliance and security standards and implements IAM, encryption, security assessment, incident response, and risk controls.

Technical Skills

- IAM, encryption, and authentication
- Compliance tools
- Cloud security monitoring
- Risk assessments and audits

Soft Skills

- Critical thinking and ethical judgment
- Collaboration and communication
- Decision-making under pressure

Role 7: Migration Engineer



Description: Executes technical migration tasks (apps, data, infra) while ensuring system stability and rollback readiness.

Technical Skills

- Migration tools
- Scripting tools
- Network and hybrid integration
- Testing and rollback planning

Soft Skills

- Attention to detail
- Coordination
- Risk awareness

Role 8: Application Engineer



Description: Supports application readiness and refactoring for the cloud environment. Works on modernizing legacy applications and ensuring compatibility with target cloud platforms.

Technical Skills

- Application modernization techniques
- API integration and containerization
- Cloud-native development

Soft Skills

- Problem-solving
- Collaboration with developers and architects

Role 9: FinOps Analyst



Description: Manages cloud costs and ensures financial accountability across teams. Helps balance innovation with cost efficiency.

Technical Skills

- Cloud cost tools
- Budgeting
- Forecasting

Soft Skills

- Communication
- Financial acumen

Additional roles may also include Compliance Lead, Cloud Infrastructure Engineer, Cloud Data Specialist, and SRE Manager.

More specifically, the roles can be mapped under the different phases of the Cloud Adoption framework.

Plan	1.1 Build a foundational understanding of cloud technologies	Executive Sponsor	Champion cloud awareness and alignment with business goals
		Business Owner	Define business needs and expected value from cloud
		Cloud Program Manager	Coordinate literacy and readiness activities
	1.2 Assess your capabilities and define your goals	Executive Sponsor	Approve strategy and funding
		Business Owner	Define measurable business KPIs
		Enterprise Architect	Assess current architecture and dependencies
		Security & Compliance Lead	Define initial compliance, RTO, and RPO requirements
	1.3 Perform a gap analysis and produce a roadmap	Cloud Program Manager	Lead the gap analysis workplan; consolidate findings into a prioritized cloud adoption roadmap
		Enterprise Architect	Assess application and infrastructure gaps
		Security & Compliance Lead	Identify security, regulatory, and data-classification gaps
		FinOps Practitioner	Assess cost and financial-management gaps
	1.4 Establish clear governance for cloud usage	Executive Sponsor	Provide governance mandate and oversight
		Cloud Program Manager	Establish governance processes and stakeholder coordination
		Security & Compliance Lead	Define compliance controls and risk frameworks
		FinOps Practitioner	Define financial accountability and cost management rules
Adopt	2.1 Select your cloud service provider	Cloud Architect	Evaluate cloud providers and technical fit
		Security & Compliance Lead	Assess provider compliance and security standards
		FinOps Practitioner	Evaluate cost models and ensure financial viability
	2.2 Develop and tailor your cloud architecture	Cloud Architect	Design target cloud architecture
		Enterprise Architect	Ensure alignment with enterprise IT landscape
		Application Engineer	Prepare applications for modernization/refactoring
		Security & Compliance Lead	Define IAM, encryption, and security controls
	2.3 Migrate and deploy your data	Migration Engineer	Execute data, app, and infra migration
		Application Engineer	Refactor and adapt applications for cloud
		Cloud Program Manager	Oversee migration timelines and risks
		Security & Compliance Lead	Ensure secure migration and compliance during deployment

Run	3.1 Monitor the technology post-deployment	FinOps Practitioner	Monitor cloud spend, optimize cost, implement chargeback/showback
		Security & Compliance Lead	Conduct compliance audits, manage risks, and ensure security monitoring
		Cloud Program Manager	Track KPIs, report to executives, manage ongoing improvements
		SRE Manager	Ensure system reliability, scalability, and performance
		Business Owner	Measure business value delivered against KPIs

4.2 | What is the role of government in supporting your adoption of cloud technologies?

The MCIT and CRA play crucial roles in regulating and driving cloud adoption in Qatar. The governance section outlines the key roles played by MCIT, CRA, other public sector entities and the private sector in driving cloud adoption across the country.

The Role of MCIT:

- Plays the role of cloud policy maker, setting the national direction for cloud development and deployment in alignment with Qatar's national aspirations and objectives
- Defines strategic initiatives, national frameworks, and national policies that guide the deployment/adoption of cloud across industries

The Role of CRA:

- Serves as the primary cloud regulator in Qatar, ensuring that cloud security and data interoperability align with national laws and international best practices
- Regulates the contractual commitments associated with cloud procurement, deployment and implementation

Role of other public sector entities:

- Develop cloud capabilities and skills across their organizations
- Deploy and implement cloud computing technologies in alignment with national policies, guidelines and standards including Qatar's Cloud First Policy and Qatar's Cloud Adoption Guidelines
- Contribute to improving the foundational enablers of cloud adoption and creating an environment that is conducive to cloud deployment and adoption
- Drive cloud adoption through strategic partnerships with CSPs that have established agreements with MCIT



05 Reporting Mechanisms

To support a successful transition to cloud, comprehensive and well-defined reporting structures should be established across the organization. These structures play a critical role in promoting accountability at all levels, fostering transparency in decision-making and execution, and ensuring alignment with the overall strategic objectives of the cloud adoption journey. Examples of reporting mechanisms include:

Role	Description	Composition	Frequency
Cloud Steering Committee	- Oversees the entire cloud program - Resolves escalated issues, and ensures strategic alignment	Senior leadership from IT, business units, security, finance, and legal	Monthly or quarterly meetings
Cloud Approval Panel	- Reviews and approves cloud project proposals, budgets, and risk assessments. - Ensures each project aligns with security, compliance, and value delivery goals.	Cloud Program Manager Cloud Architect Enterprise Architect Business Owner Security & Compliance Lead	Bi-weekly or Ad-hoc
Operational Review Boards	- Tracks implementation milestones - Manages resource allocation, and reviews operational risks	Project managers Cloud architects	Weekly or bi-weekly

Alongside reporting on activities and milestones, organizations should agree a small, standard set of KPIs to track both service outcomes and delivery performance. Where applicable, these may include deployment frequency, mean time to restore service (MTTR), and change fail rate, complemented by modernization progress indicators (e.g., percentage of workloads modernized vs. rehosted). These metrics are widely used to measure delivery performance and service resilience and can help ensure reporting remains consistent and decision-useful.

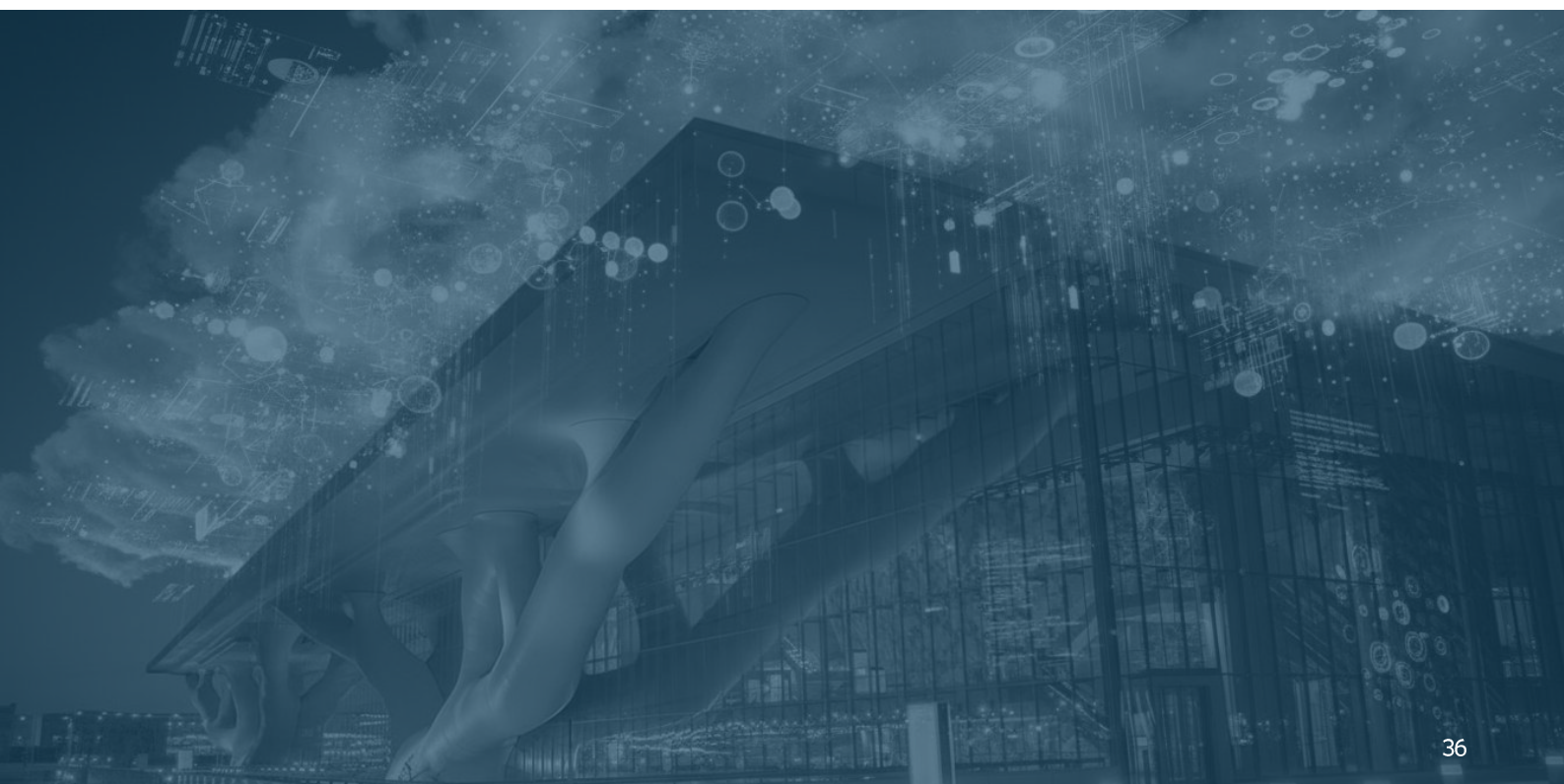


06 Checklist

This checklist serves as a practical tool to guide organizations through a structured and strategic cloud adoption journey, consolidating key guidelines and considerations across each stage of the process.

Phase	Stage	Checklist Item	
Plan	Build a foundational understanding of cloud technologies	Establish Executive Sponsorship for Cloud Adoption	☐
		Build Cloud Literacy	☐
		Build Technical Cloud Literacy and AI	☐
		Articulate the Strategic Value of Cloud	☐
	Assess your capabilities and define your goals	Develop a Cloud Adoption Business Case	☐
		Engage Business Stakeholders	☐
		Assess Current State	☐
		Define Target Outcomes	☐
	Perform a gap analysis and produce a roadmap	Perform a Gap Analysis	☐
		Develop a Cloud Adoption Roadmap	☐
	Establish clear governance for cloud usage	Design a Cloud Operating Model	☐
		Develop Cloud-Specific Policies	☐
		Establish Governance Boards or Committees	☐
		Define Cloud Processes	☐
Adopt	Select your cloud service provider	Shortlist CSPs	☐
		Evaluate CSPs Against Key Selection Criteria	☐
		Test workload in a Pilot Environment	☐
		Conduct Procurement and Legal Review	☐
	Develop and tailor your cloud architecture	Design Scalable and Resilient Architectures	☐
		Evaluate Cost Models Carefully	☐
	Migrate and deploy your data	Adopt a Phased Migration Strategy	☐
		Conduct Pre-Migration Testing	☐
		Enhance Cloud Infrastructure Foundation	☐
		Establish Rollback and Contingency Plans	☐
		Train Staff During Transition	☐
		Launch Pilot Phase	☐

Phase	Stage	Checklist Item	
Run	Monitor the technology post-deployment	Establish Real-Time Monitoring	☐
		Gather Stakeholder Feedback	☐
		Enforce Security and Compliance	☐
		Monitor Recovery and Backup Effectiveness	☐
		Implement Cost Management and FinOps Practices	☐
		Track CSP Service Updates and Announcements	☐
		Explore and Evaluate New Cloud Services	☐
		Conduct Regular Reviews and Audits	☐
		Foster a Culture of Innovation	☐





References

NCSA (2018) Cloud Security Policy. Available at:

https://qcert.ncsa.gov.qa/sites/default/files/public/documents/cs-csps_cloud_security_policy_eng_v1.3.pdf

CRA (2022) Cloud Computing: a Handbook for SMEs. Available at:

<https://www.cra.gov.qa/en/document/cloud-computing-a-handbook-for-smes>

CRA (2022) Cloud Policy Framework. Available at:

<https://www.cra.gov.qa/en/document/cloud-policy-framework>

CRA (2024) Regulation for Cloud Data Interoperability and Data Portability. Available at:

<https://www.cra.gov.qa/en/document/regulation-for-cloud-data-interoperability-and-data-portability>

Oxford Business Group (2025) Early adoption: public and private actors are taking key steps in integrating innovative technologies into a range of sectors. Available at:

<https://oxfordbusinessgroup.com/reports/qatar/2025-report/ict-innovation/early-adoption-public-and-private-actors-are-taking-key-steps-in-integrating-innovative-technologies-into-a-range-of-sectors-overview/>

MCIT (2024) Cloud First Policy. Available at:

<https://www.mcit.gov.qa/-/media/mcit/documents/policies/cloudfirstv100en0.pdf>

NIST (2011) The NIST definition of cloud computing. Available at:

<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>

OECD (2014) Cloud computing: the concept, impacts and the role of government policy. Available at:

https://www.oecd.org/en/publications/cloud-computing-the-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en.html

OECD (2025) Competition in the provision of cloud computing services. Available at:

https://www.oecd.org/en/publications/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad.html

PwC (2022) PwC Middle East workforce hopes and fears survey. Available at:

<https://www.pwc.com/m1/en/issues/upskilling/hopes-and-fears-2022.html>

QCB (2024) Cloud Computing Regulation. Available at:

<https://www.qcb.gov.qa/Documents/InformationSecurity/Cloud%20Computing%20Regulation.pdf>

08

Document Control

Version	Date	Amendments	Author
1.0.0	2026	Publication of the Guidelines	MCIT

وزارة الاتصالات وتكنولوجيا المعلومات
Ministry of Communications and Information Technology
دولة قطر • State of Qatar



Prepared by
Digital Industry Policies Department
Ministry of Communications & Information Technology
Version 1.0.0 2026

E-Mail: dipd@mcit.gov.qa
www.mcit.gov.qa