Deloitte.

# Key considerations for a cloud-enabled data center modernisation

2021

MAKING AN IMPACT THAT MATTERS since 1845

# Table of contents




**Authors**
Thomas Kessler
Peter Versmissen


Cloud-enabled data center modernisations are becoming mainstream as there is now strong consensus that the public cloud paradigm shift is rendering on-premise data centers obsolete.

However, to capture the cloud-promised value, a so-called ‘lift and shift’ of the on-premise estate to the cloud is not sufficient as it doesn’t address the broader imperatives.

In this paper we share our learnings for this journey and the 7 key success factors, ranging from Executive alignment to Security.

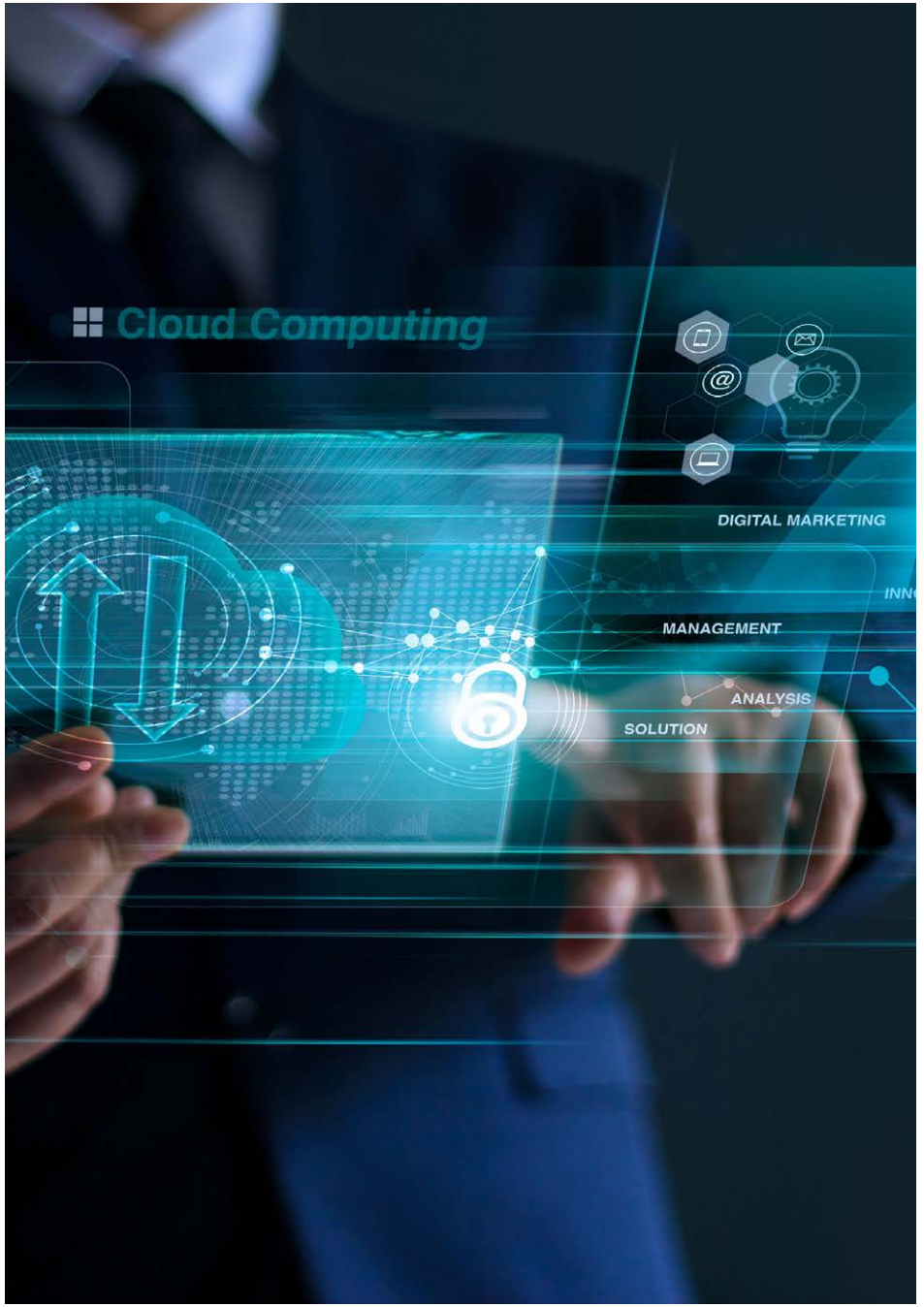
# I. Market trends and key drivers

For the past 15 years, cloud adoption has been primarily driven by SaaS and new workloads built natively in the cloud on IaaS and PaaS. But in recent years we have seen an acceleration of infrastructure modernisations whereby on-premise data center workloads are being 'lift and shifted' and modernised in the cloud.

Today, this shift from specific cloud solutions to cloud at scale is becoming mainstream. In 2019, cloud migration services reached $119bn and is expected to grow 29% per year until 2025[1]. Which is why CIOs are expecting the three hyperscale cloud providers (Amazon, Microsoft and Google) to gain most IT wallet share in the next three years[2].

This momentum is underpinned by three key drivers:

1. **Business innovation acceleration** and enabling 'try fast, fail fast', as applications and data hosted in the cloud can leverage 600+ platform services to increase development agility while having virtually infinite and immediate scalability worldwide across 20 to 60 regions per cloud provider. In addition, the cloud's pay-per-use model significantly reduces the entry cost for new initiatives (e.g., infrastructure investments, provisioning agility, etc.).
2. **IT infrastructure savings** as cloud-enabled cost optimisations, combined with increased internal cost transparency, provide on average 25-30% TCO savings. However, there are significant saving variances across companies as they depend on a number of factors such as data center capex investment cycle, server utilisation patterns, data center power usage effectiveness, bring-your-own-license to the cloud options, etc. Also, to achieve these savings, a simple migration to the cloud is often not sufficient and it has to be complemented by a modernisation approach.
3. **IT capabilities** as IT management delegates infrastructure commodity services to cloud providers while benefiting from their maturity to improve availability (e.g., SLA of 99.95% with two-hour disaster recovery), agility (e.g., provisioning of servers in minutes), security (as cloud providers invest billions every year in cloud security) and automation of IT operations (Infrastructure as Code).




1 Source: Mordor Intelligence (Cloud Migration Market - Growth, Trends, Forecasts 2020 - 2025)
2 Source: Morgan Stanley CIO Survey 2020 Q1

# II. Key success factors

While cloud-enabled data center modernisations are sometimes over-simplified as 'lift and shift', experience shows that a more comprehensive approach driven by seven key success factors is essential.

**The key success factors are:**

- Executive alignment
- Architecture design
- Migration approach
- Security
- Legal and contracting
- IT operating model
- Cost savings tracking

## Executive alignment

Executive alignment, beyond IT management, is key as it will shape the approach:

- What is the primary objective: prioritise business innovation acceleration or cost savings levers?
- What is the scope: full data center footprint or business area applications?
- What part of the organisation beyond IT should be mobilised (e.g., business for User Acceptance Testing)?
- How is this initiative prioritised compared to other IT initiatives?

Creating this alignment typically requires a dedicated prestudy (~two months) to define the cloud-enabled data center modernisation business case thereby providing the management with the required insights before deciding on the journey.

It is key that such a prestudy not only covers the cloud vision and financial business case (comparing cloud with on-premise TCO), but also the architecture feasibility (e.g. what will be the approach for more complex workloads such as Mainframe and AS/400), the operating model and the security considerations.

In addition, the prestudy needs to define a roadmap taking into account the level of change required and the organisation's capacity to absorb this.

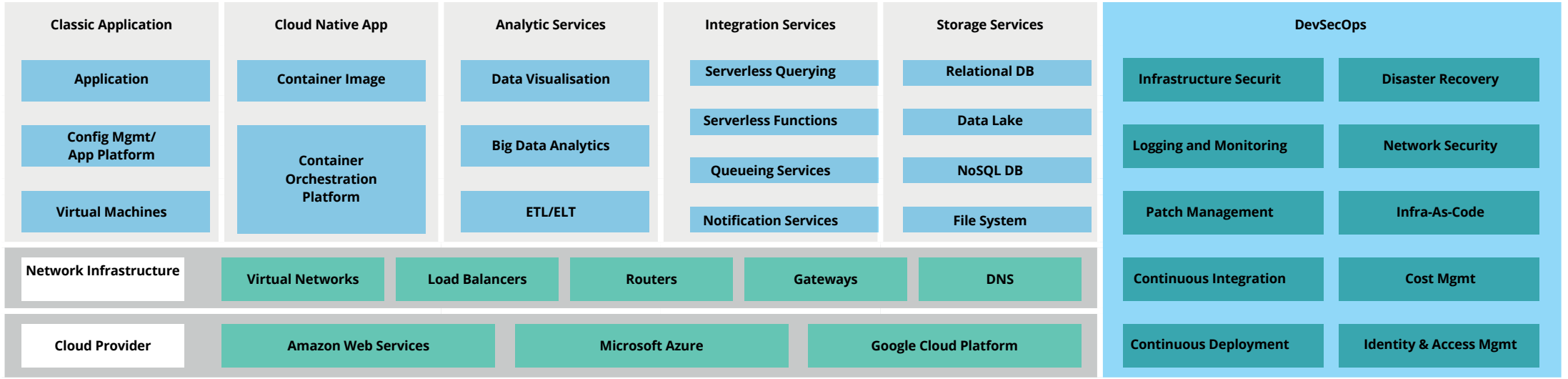
## Architecture design

Although general IT concepts for the cloud remain the same as on-premise, cloud solutions introduce a number of new architectural patterns. Therefore, architecture design should not be merely a replication of existing architecture choices, and should be driven by a number of key choices such as:

- Multi-cloud vs. single-cloud strategy, balancing cloud vendor negotiation power and best-in-class fit vs. operational complexity and skillset fragmentation (as a rule of thumb, multi-cloud strategy should be considered as of €20–30m cloud consumption per year)
- Tight platform integration with cloud native services vs. cross-platform solutions (e.g., infrastructure as code with Azure Resource Manager vs. Terraform)
- Level of automation (Infrastructure as Code), taking into account architecture modernisation ROI and IT staff skills ramp-up

These strategic choices then drive the design of a cloud reference architecture at infrastructure level (e.g. networking, security, IAM, etc.) but also at application level (e.g. applications landing zones patterns, DevSecOps, etc.).

**High-level cloud application reference architecture**

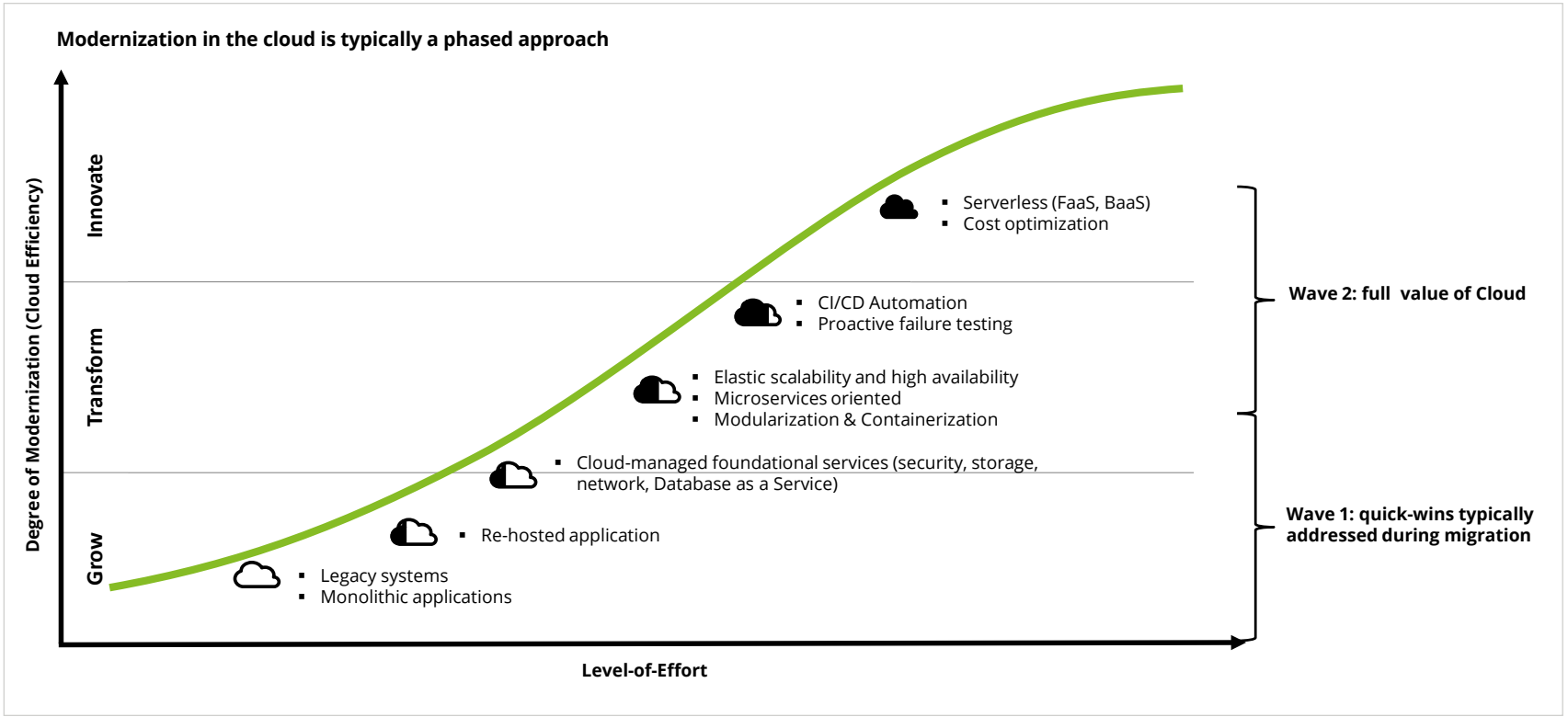


## Migration approach

While the scope of the initiative can encompass a migration of a full data center or all applications of a specific business unit, the migration is not a one-size-fits-all approach as applications have different business and technical requirements. It is key to assess the cloud suitability and business value of each application. Cloud suitability is measured through a set of criteria such as technology stack compatibility, integration needs or elasticity.

This provides a general view of the application landscape, allows to identify application clusters and enables the prioritisation of workloads when defining the migration roadmap. Once these application clusters have been identified, a migration strategy is defined using the 6 Rs model[3] (ranging from rehosting to retiring). While the bottom-up assessment is done at an application level, the migration roadmap should then be defined per application cluster, taking into account business dependencies and a technical roadmap such as the strategy on legacy platforms (e.g. Mainframe, AS400) and the integration or convergence with O.T. systems.

Finally, while modernisation is a key lever, it is typically phased and prioritised based on the ambitioned business case.




3 https://docs.aws.amazon.com/whitepapers/latest/aws-migration-whitepaper/the-6-rs-6-application-migration-strategies.html

## Security

When migrating to the cloud, the data center footprint becomes hybrid (on-premise and cloud) and a shared security responsibility model is introduced where the cloud consumer responsibilities differ depending on the acquired service model (IaaS, Paas or SaaS). While hyperscale cloud providers are investing billions in security every year, significant security responsibilities remain with the enterprise and require new IT skills to safeguard the new footprint.

In addition to this, the cloud-enabled modernisation of data centers often introduce technologies such as Software Defined Networks (SD-WAN), Zero Trust Networks (ZTN), Cloud Access Security Brokers (CASB), etc. that also require new security skills and governance.

This underpins Gartner's assessment that 99% of cloud security failures will be a customer's fault[4], which is also reflected in the key threats identified by the Cloud Security Alliance's Top Threats report[5] and where mitigations must be defined:

**1. Data breaches**
As data is more centralised and exposed, (un)intentional errors can now lead to easier data breaches. The key element is to have a sound data security governance strategy and policy which must be translated into technical controls to safeguard cloud-stored data at rest, in motion and—if applicable—in use. Examples include data lifecycle management, encryption key management, PII protection process, privacy by design, digital rights management, etc.

**2. Misconfiguration and inadequate change control**
To safeguard the (cloud) security posture of the enterprise, authorised changes in the cloud must be reflected in existing change management process(es) and must be tested in different deployment environments. These activities must be fully integrated with existing patch and vulnerability management processes. With Cloud Security Posture Management (CSPM) technologies (e.g., AWS's Security Hub, Microsoft's Azure Security Center, etc.) the cloud security configuration can be continuously monitored for (un)intentional configuration changes.

**3. Insufficient identity, credential, access and account hijacking**
A strong identity and access management capability is paramount. A centralised identity orchestration engine interlinked with current IAM policies ensures smooth and secure transitions between various cloud platforms and on premise solutions. A mature Privileged Access Management strategy and capability, which is capable of providing a single control plane in the hybrid IT landscape, is critical and must cover credential and API secret management. The capability must also be wired into the dev(sec)ops CI/CD pipelines.

**4. Insecure interfaces and APIs**
Cloud interconnections provide interfaces that allow consummation and publication of data flows. Many of these interfaces are publicly exposed, generating a larger attack surface and, when poorly designed, they can result in data breaches or allow for attack reconnaissance (i.e., using input response verification). They must be strictly controlled and well designed using security by design, thorough testing and continuous monitoring.

**5. Lack of cloud security architecture and strategy**
Security policies, standards and baselines must be available per service (and applicable deployment) model with the necessary attention for shadow cloud as it's never been so easy for staff to set up and test-drive new cloud capabilities. The new capabilities must be designed using a standard template, which incorporates enterprise standard security principles. A continuous monitoring and improvement model for enhancing security architecture must be established, preferably risk driven and standardising the security capabilities throughout the ecosystem.

4 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
5 https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

**Cyber security framework**

## Business objectives and risks

**Cyber threats - (Data breaches, misconfiguration, insufficient identity, insecure APIs, lack of security architecture, etc.)**

| | | |
|---|---|---|
| **Unauthorised access to data** | **Unwanted change of data** | **Unavailability of service** |
| **Loss of data ownership** | **Escalation of operative costs** | **Loss of organisational control** |

## Cloud Governance

### Provider Governance
- Data Ownership and Custodianship
- Contractual Controls
- Searchability and Legal Seizure
- Subscription Management

### Compliance and Audit
- Location and Jurisdiction Policies
- Regulations Management
- Audits and Certification

### Risk Management
- Risk Assessment
- Risk Mitigation
- Risk Monitoring and Reporting

### Security Governance
- Cloud Security Strategy
- Awareness and Training

| Data Protection | Devices, Identity and Access | Application Security | Network and Infrastructure | Cloud Security Monitoring | Cloud Resilience |
|---|---|---|---|---|---|
| **Data Governance**<br>• Data Classification<br>• Data Lifecycle Management<br>• Data Mapping and Discovery | **Devices**<br>• Device Management<br>• Device Authentication<br>• Health Checks and Telemetry<br>• Unknown Device Management | **Secure Design and Development**<br>• Security Requirements and Metrics<br>• Supply Chain Management<br>• Threat Modelling<br>• Technical Training | **Platform Protection**<br>• Hardening and Patching<br>• Malware Protection<br>• Resource Authorisation<br>• Vulnerability Scanning | **Logging and Monitoring**<br>• Log Collection and Correlation<br>• SOC integration | **Withstand**<br>• Resilient Design<br>• Resilient Operations<br>• Supplier Management |
| **Cryptography**<br>• Data at Rest<br>• Data in Transit<br>• Data in Use<br>• Key Management | **Identity and Access Management**<br>• Identity Lifecycle Management<br>• User Access Reviews and Audits<br>• Privileged Account Management<br>• Multi-Factor Authentication | **Secure Deployment**<br>• Deployment Lifecycle Security<br>• Application Security Testing | **Cloud Integration and SDN**<br>• Network Architecture<br>• Cloud Migration | **Security Configuration and Detection**<br>• Misconfiguration Scanning<br>• Intrusion Detection Measures | **Respond**<br>• Crisis Management<br>• Incident Management and Root Cause Analysis<br>• Communications |
| **Data Loss Prevention**<br>• Egress Monitoring<br>• Local Copies | | **Secure Operations**<br>• Administrative Oversight<br>• Web Applications Security<br>• Penetration Testing<br>• Red Teaming | **Network Protection**<br>• Advanced Network Defence<br>• Network Segmentation | **Security and Usage Analytics**<br>• Performance Monitoring<br>• Threat Intelligence | **Recover**<br>• Recovery and Continuity Planning<br>• Backup and Archival<br>• Assurance and Testing |

## Legal and contracting

Moving workloads to the cloud triggers questions about legal and contracting (L&C) requirements. Some are sector-specific, some are general. In essence, the need to focus on L&C is twofold: (i) enabling cloud transformation and (ii) identifying and preventing risk.

In order to meet these two objectives, "old" (offline grounded) laws must be translated into the new online situation and upcoming laws and regulations must be anticipated. Not doing so may lead to overlooked items and insufficient allocation of accountabilities, responsibilities and liabilities amongst the cloud (service) provider, the cloud user, its system integrator and the data owner.

Examples of L&C challenges include:

- Cloud contracts: identify and mitigate red flag risks in (often non-negotiable) contracts with cloud service providers (vendor lock-in, data portability, etc.) and have business continuity guaranteed.
- Data ownership: having access to data is not the same as owning data. In order to set up a business model around data (e.g., service model based on machine-generated data), make sure to have sufficient rights, either licensed or owned
- Data localisation and retention: operating in multiple jurisdictions may lead to different data transferability rules as data transfers from the EU to the US is complex under GDPR as certain countries' government bodies may access data (e.g., CLOUD Act). Choosing the right location for data is essential. Sector specific regulations may pose restrictions on the location of the data storage and retention period and should also be addressed.
- Confidentiality, intellectual property rights and trade secrets: when storing data in the cloud, some of the most valuable intangibles are moved to third-party controlled locations. Check contracts with partners to understand whether confidential information may be transferred and stored to the cloud.
- Sector regulation: depending on the sector, specific rules and requirements may apply (e.g., financial services with prudential control requirements, life science with GxP guidelines)

## IT operating model

As the hosting platform becomes hybrid (on-premise and cloud), the IT operating model needs to evolve, not only to mitigate the new risks and needs induced by the cloud, but also to fully leverage its new capabilities such as self-servicing, cost transparency and IT operations automation. In essence, the ambition should be to bring cloud to the operations, and not the other way around.

Before designing the future operating model, a number of key principles need to be defined, such as:

- Centralisation vs federation: how do we ensure central oversight to mitigate issues like shadow IT while using a federated model to deliver business focus?
- Security vs agility: how do we balance the need for robust security processes and the need for quick approvals?
- Cost control: how do we empower lines of business and enable self-servicing while keeping costs under control?
- Skills: how do we close the gap in cloud skill level in the central IT team and across the organisation?
- Service management: which IT processes will require changes to encompass the cloud?

This is where a model based on a Cloud Center of Excellence (CCoE) is key to centralise the expertise of the new platform while playing three pivotal roles:

- Act as platform broker (commercial negotiation, subscription management, internal cost transparency or chargeback, etc.)
- Define and enforce reference architecture (including security policies) for shared services and application landing zones
- Support business projects with cloud expertise, accelerating the organisation's maturity

The CCoE is composed of multidisciplinary teams combining infrastructure and application development expertise.

**Example of Cloud Center of Excellence operating model**

**Customers -** Customers of technology services expect straightforward and timely access to approved services as per their business needs

| | | | | | | |
|---|---|---|---|---|---|---|
| **Cloud Business Office**<br>**Offer cloud as a service** | **Client Engagement** | **Strategy and Communications** | **Learning and Development** | **Financial Mgmt.** | **Third Party Mgmt.** | **Portfolio Management** |
| **Business Product Teams** - Responsible for delivery and operations of business products, pulling from a resource pool comprised of multiple competencies | | | | | | |
| **Common Business Services/Common Transactions** | | | | | | |
| **Technology Office**<br>Maintain product and platform standards | **Platform Services Team** - Execute shared service capabilities and frameworks that are used across the organisation | | | | | |
| **Enterprise Architecture** | PaaS | Data Science | CI/CD Tooling | IaaS Offerings | | |
| | API Management | Automation | ServiceNow | ... | | |
| **Governance, Risk, Compliance** | **Foundational Services Team** - Build and operate core foundational infrastructure capabilities to support the successful delivery of business products | | | | | |
| **Security** | **Hardware/Cloud** | | **Network** | | **Orchestration** | |

| |
|---|
| **Site Reliability**<br>**Engineering Support day-to-day operations of applications and platforms** |
| **Application SRE** |
| **Platform SRE** |
| **Infrastructure SRE** |
| **Call Centre** |

## Cost savings tracking

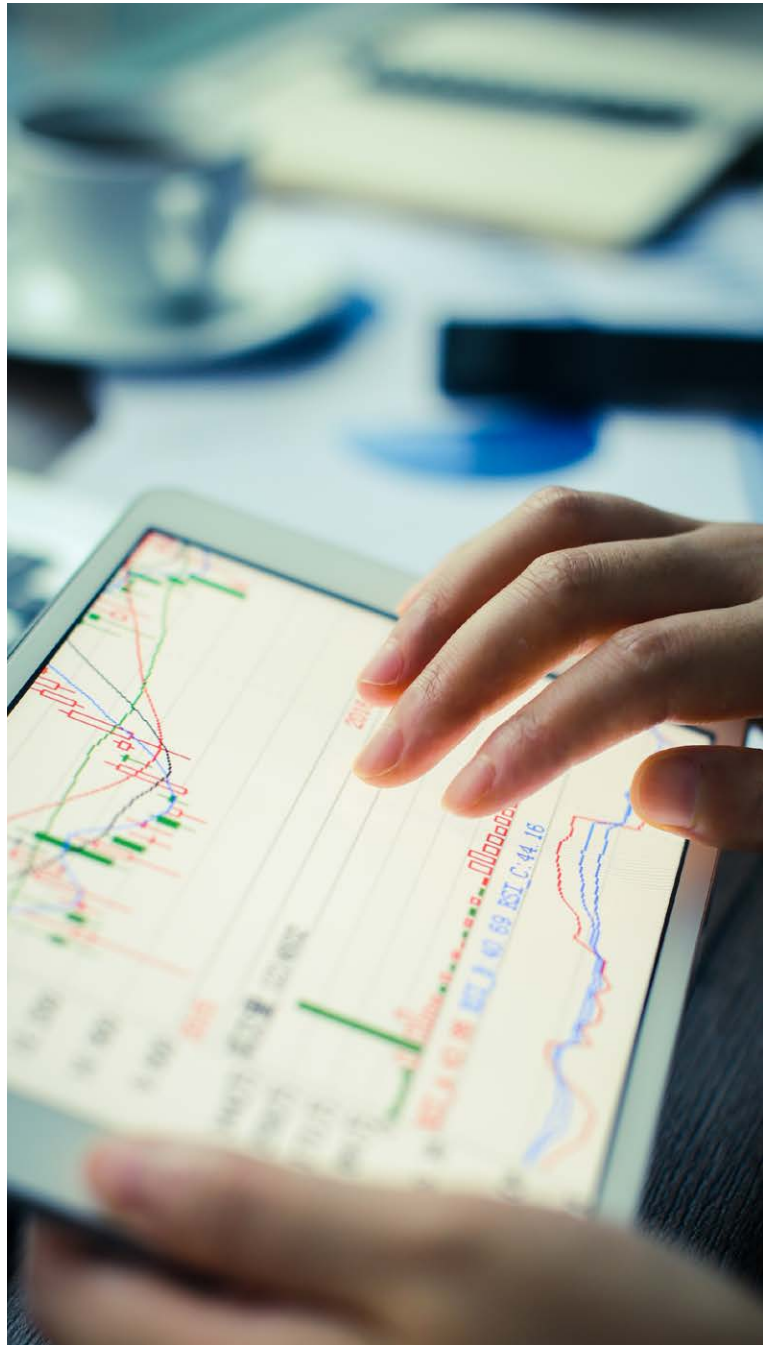
While the main reason to move to the cloud is often the acceleration of business innovation and the improvement of IT capabilities, it also has the potential to generate cost savings in three areas: infrastructure cost savings (servers, facilities, maintenance), application development productivity gains (DevOps and the use of PaaS) and business processes automation. While the latter two address the largest cost base, infrastructure cost savings are often the most immediate and tangible.
However, to realise the ambitioned infrastructure cost savings, a strong cost management approach is required to ensure a disciplined assessment and implementation of relevant levers. Examples when defining the target architecture include:

- Rightsizing: while on-premise overprovisioning is frequent (due to longer provisioning delays and anticipating future capacity needs), cloud instantaneous provisioning and pay-per-use models eliminate overprovisioning needs. It is thus key to not blindly replicate on-premise infrastructure sizing
- Snoozing: shutting down unused virtual machines such as development environments outside business hours
- Leveraging PaaS: some platform services provide automated cost optimisations such as storage auto-tiering (from hot to cold) or virtual desktop (VDI) auto-scaling
- Optimising stable workloads: production workloads can benefit by moving from a pay-per-use to a reserved instance billing model (typically 40%-60% discount)
- Policies for costs: defining acceptable boundaries (VM sizing, availability requirements, etc.) and cascading them through automated cloud policies
- Automating operations: leveraging infrastructure as code (including containerisation) to automate operations such as provisioning, deployment and patching
- Optimising commercials: maximising cloud vendor discounts thanks to a well-prepared negotiation (prior to selecting a target platform and with a clear view on potential consumption commitments) and by assessing bring-your-own-license options

After migrating to the cloud, a number of additional cost savings levers are key:

- Showback or chargeback: tagging of cloud resources (e.g., per business unit or project) to provide internal cost transparency and enable businesses to adopt a consumption-based behaviour
- Continuously optimise: leveraging built-in advisors (Azure, AWS, GCP) as they provide customised recommendations based on usage to resize or shutdown under-utilised resources
- Modernise application layer: identifying applications where platform services (DBaaS, serverless compute, etc.) would have most impact

Finally, when cost savings is a key driver for the business case, the optimal scenario to consider is a full data center migration to the cloud as decommissioning a data center significantly improves the TCO (facilities, on-site operations staff, etc.).



# III. It is a journey

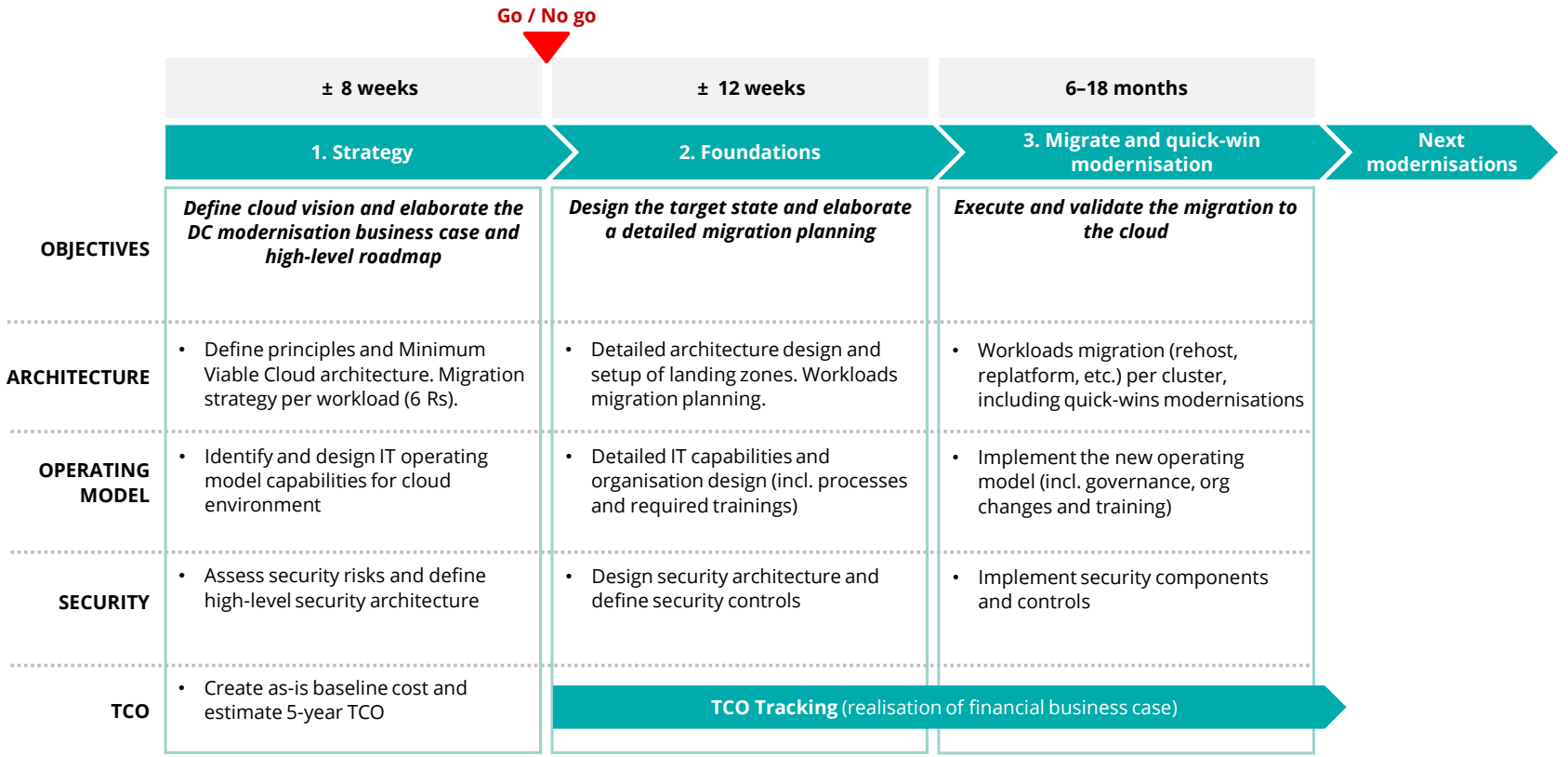
Modernising a data center to the cloud is a 12 to 24-month journey. Defining the appropriate migration pace is key as it depends on:

- Current cloud maturity (architecture, operating model, skills, etc.)
- Organisation capacity to absorb the change (e.g., start small and scale fast)
- Mobilisation of resources (what are the other IT priorities?)
- Activities insourced vs. outsourced

Before such a programme is launched, a strong stage-gating process is paramount, based on a strategic prestudy that provides a tangible business case enabling a well-informed go/no-go decision.

Once the data center has been migrated with a first set of quick-win modernisations, the continuous improvement cycle begins and the next wave of modernisations can be addressed as most of the applications refactoring modernisations (e.g., serverless compute, integration of PaaS services, etc.) take more time and should be considered when there is a new business need which justifies the investment.

**Cloud-enabled data center modernization journey**



# Contacts in Belgium


**Patrick Callewaert**
Cloud Transformation
+32 2 749 57 43
pacallewaert@deloitte.com

**Thomas Kessler**
Cloud Eminence
+ 32 2 301 83 37
thkessler@deloitte.com

**Yves Rombauts**
CIO and Cloud
+32 600 69 20
yrombauts@deloitte.com

**Wesley Bille**
Cloud in Public Sector
+ 32 2 301 82 58
wbille@deloitte.com

**Nicolas Georlette**
Cloud in Financial Services
+ 32 2 600 60 68
ngeorlette@deloitte.com

**Vincent Debusschere**
Cloud in Telco, Media & Technology
+32 2 301 84 03
vdebusschere @deloitte.com

**Bruno Peelaers**
Cloud in Private Market
+32 2 800 23 19
bpeelaers@deloitte.com

**Vincent Fosty**
Subscription Economy
+32 2 749 56 56
vfosty@deloitte.com

**Geert Hallemeesch**
Machine Learning
+32 2 749 53 50
ghallemeesch@deloitte.com

**Annelies Dieusaert**
Tax  Technology and Cloud
+ 32 2 301 82 81
andieusaert@deloitte.com

**Annelies Stragier**
Business Tax and Cloud
+32 2 600 67 98
astragier@deloitte.com

**Charlotte Degadt**
Transactional Tax and Cloud
+32 2 301 81 88
cdegadt@deloitte.com

**Peter Versmissen**
Security and Cloud
+ 32 2 301 81 22
pversmissen@deloitte.com

**Johan Van Grieken**
Risk and Cloud
+32 2 800 24 53
jovangrieken@deloitte.com

**Natalia Khamraeva**
Internal control and Cloud
+32 2 800 26 05
nkhamraeva@deloitte.com

**Bram De Schouwer**
Cloud Engineering
+ 32 27 49 56 29
bradeschouwer@deloitte.com

**Gaëtan Vernaeve**
Cloud Architect
+ 32 2 749 52 49
gvernaeve@deloitte.com

**Matthias Vierstraete**
Legal and Cloud
+ 32 2 800 70 37
mvierstraete@deloitte.com

**Pieter Sauwens**
Cloud Innovation
+32 2 800 24 13
psauwens@deloitte.com

**Yves Van Durme**
Cloud Operating Model
+ 32 2 749 59 97
yvandurme@deloitte.com

**Tim Paridaens**
Internet of Things and Cloud
+ 32 2 749 57 03
tparidaens@deloitte.com

**Kris Bornauw**
SAP on Cloud
+ 32 2 749 57 47
kbornauw@deloitte.com

**Peter Van Horebeek**
Data on cloud
+ 32 2 749 57 77
pvanhorebeek@deloitte.com

**Herwig Thyssens**
Mainframe on Cloud
+ 32 2 301 84 19
herthyssens@deloitte.com

Deloitte.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 332,000 professionals, all committed to becoming the standard of excellence.