Deloitte.

Cloud Migration
Maximize with Architecture, Services & Security Orchestration?

Jan Seffinga, Partner, Deloitte | 27.08.2019

Why go into the cloud? Key drivers and characteristics

Drivers

Increased Business Agility

Gain greater flexibility on architecture and sourcing, scale up and down as needed, maximize efficiency, **accelerate time to value**, reduce time to start up and complete projects

Reduce IT capital spending

Use of **"pay-as-you-go"** model instead purchase/lease
Move IT costs from CAPEX to OPEX

Innovation

Shift from asset ownership to service consumption
Tap into private sector innovation
Encourages entrepreneurial culture
Better **linked to emerging technologies**

Reallocation of resources

As routine processes are automated through Cloud, **resources can be re-positioned to higher value-add activities**

Characteristics

Scalable

React quickly to increased business demand, acquisitions, or new business models without large CapEx expenditures and increased long run-off periods

Self-Service

Creating environments, enhancing capabilities, adding capacity with less labor and reduced lead times

Multi-Business

Cloud computing delivers shared capacity across business lines, reducing duplicate environments

Security

Platform security, tenant segregation and security-aware maintenance processes as key principles

Dynamic

On-Demand Provisioning. The ability to add capability and capacity as rapidly as business requires

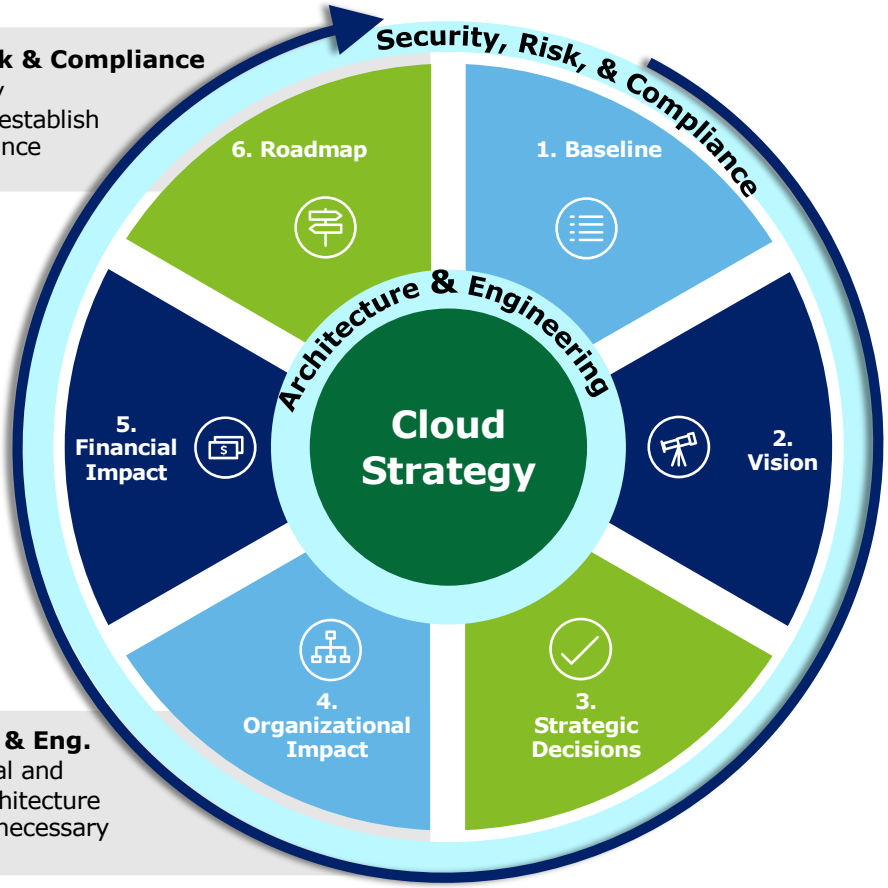
Flexible Pricing

Recapture capacity and spend for use in other areas as business demands fluctuates

Digital-Based Architecture

Cloud architectures are based on virtualized environments defined by their use not by hardware

Cloud Strategy - Serve as the initial entry point helping you set the tone, pace, and direction for your Cloud transformation journey



Security, Risk & Compliance
Assess security requirements, establish Risk & Compliance controls

Architecture & Eng.
Define technical and integration architecture as well as the necessary tooling

Baseline
Assess the current state IT footprint incl. in-flight projects and constraints. Capture issues and opportunities

Vision
Get business alignment, define guiding principles and set the pace of the Journey to the Cloud

Strategic Decisions
Find the right mix of Public / Private / Hybrid Cloud. Evaluate key platforms and decide on the transformation approach

Organisational Impact
Define the future governance and organisation incl. processes. Highlight impact on talent acquisition

Financial Impact
Calculate the value case. Show costs, potential savings and the impact on CAPEX and OPEX

Roadmap
Wrap up decisions of previous phases into a bought-in plan incl. dependencies and key milestones

Success factors for a secure and compliant cloud environment

Protecting and monitoring data in a manner that complies with security and applicable regulatory mandates without specific requirements and implementing effective security controls remain top challenges for many organizations

Data Protection

- Securing data as it is moved, processed and stored in cloud is critical for organizations reputation and financial as well as compliance requirements
- Identifying applicable data protection mechanism (encryption, tokenization, masking data loss prevention (DLP), etc.) and understanding specific management aspects will be critical to implement data security
- Organizations should evaluate data residency issues

Regulatory Compliance

- Determining compliance requirements and factoring impacts as part of the solution delivery plan
- Adhere to the principles of cyber risk management for public cloud as with other forms of outsourcing arrangements

Security Monitoring in the cloud

- Address new visibility and detection requirements and implement security monitoring that is "cloud aware"
- Decide whether to use on-premise enterprise Security Information and Event Monitoring (SIEM) o host in the cloud
- Enhanced procedures and SOC (Security Operations Center) for cloud monitoring are needed to provide the organization with visibility to cloud activity

Clear asset ownership

- Organizations should have defined asset owners and consistent tagging within their cloud implementations

Automating Security in the cloud

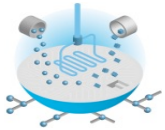
- Leverage the DevSecOps model to automate security in cloud (security as code) and enhancing the security posture
- Organizations need to consider the target model for a cloud security team (DevSecOps) and what are the roles and outputs of this group

In the digital age, the Technology Operating Model will be affected by nine big shifts

Ways of working

Agility and speed become the new norm. Organisations learn and adapt by experimenting and **fast deployment**.

The **boundaries between business and IT blur**, business-led IT increases and tech fluency is vital for all.



The rise of **innovation ecosystems** with joint risk taking, and value creation among quickly engaging and disengaging partners.

What is a Target Operating Model?

What

- Personas
- Services
- Mission

How

- Capabilities & Skills
- Processes
- Metrics & KPI's
- Funding & Charging
- Functions & Interactions
- Tooling

Where

- Sourcing & Ecosystems
- Collaboration & Location
- Culture / work style

Who

- Organization Structure
- Governance & Decision rights
- Roles & Responsibilities
- Incentives & Rewards

Technology

Cloud becomes the dominant IT delivery model, with **highly automated IT processes**.

Competitive advantage shifts in favour of **data and algorithms** fuelling algorithmic business.

Information technology (IT) and operational technology (OT) **converge.**

Resources

The **workforce transitions** as digital, data, AI and robotics create **new jobs** and cause existing jobs to disappear.

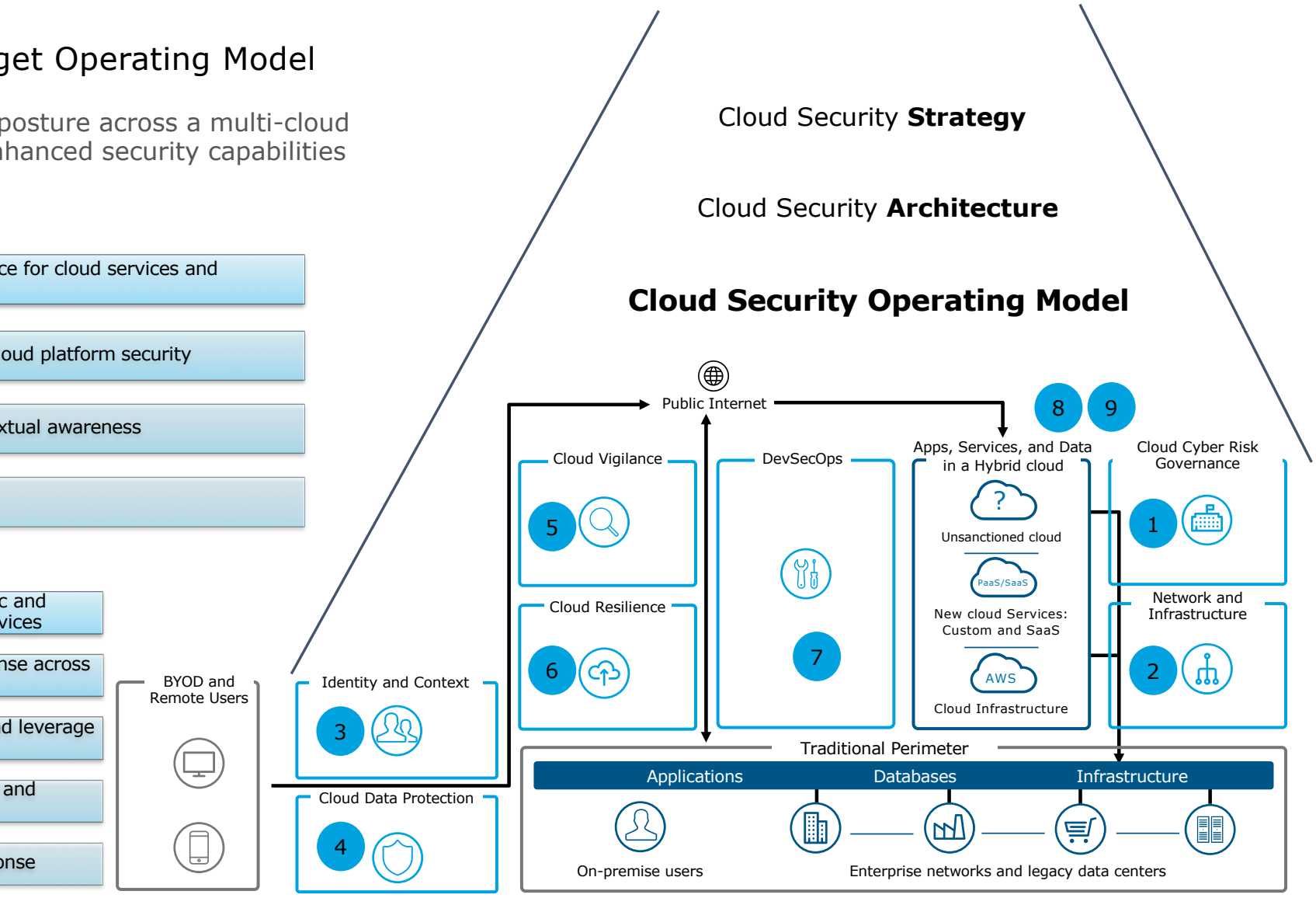
Organisations adopt the vision, values, culture and leadership required **to build digital DNA.**

Innovation and experimentation require a **larger share of resources**, with fit-for-purpose **funding mechanisms and governance**.

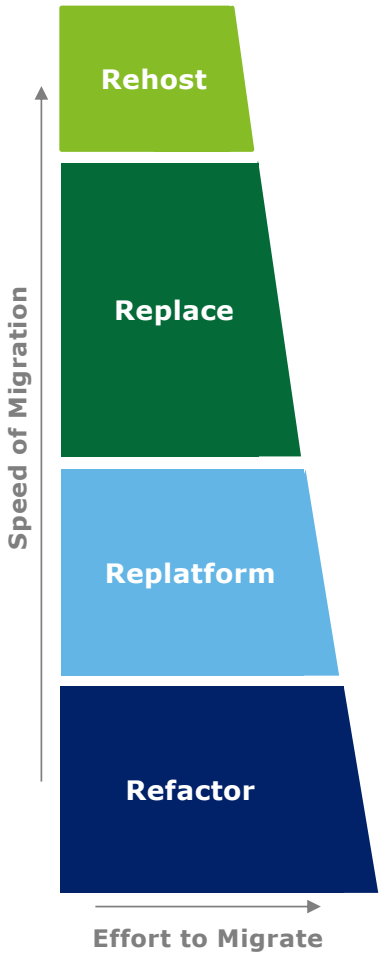
Cloud Security Target Operating Model

A comprehensive cyber posture across a multi-cloud environment requires enhanced security capabilities

1. Governance risk and compliance for cloud services and providers
2. Virtual infrastructure and cloud platform security
3. Identity, access, and contextual awareness
4. Data protection and privacy
5. Monitoring of risks of cloud traffic and integrations with other cloud services
6. Resilience and incident response across the cloud
7. Secure cloud applications and leverage automation for controls
8. Continuous cloud compliance and security monitoring
9. Cloud forensic and incident response



Cloud Migration Considerations



Migrate only suitable workload to cloud solutions, and assess via business and technical questions

Challenge the scope that needs to migrate, and consider alternative Software-as-a-Service solutions

Prepare BaU teams to manage the new hosting environment from day one (e.g. cutover / rollback)

Mitigate risk when migrating data externally via the use of third party secure data shipping services

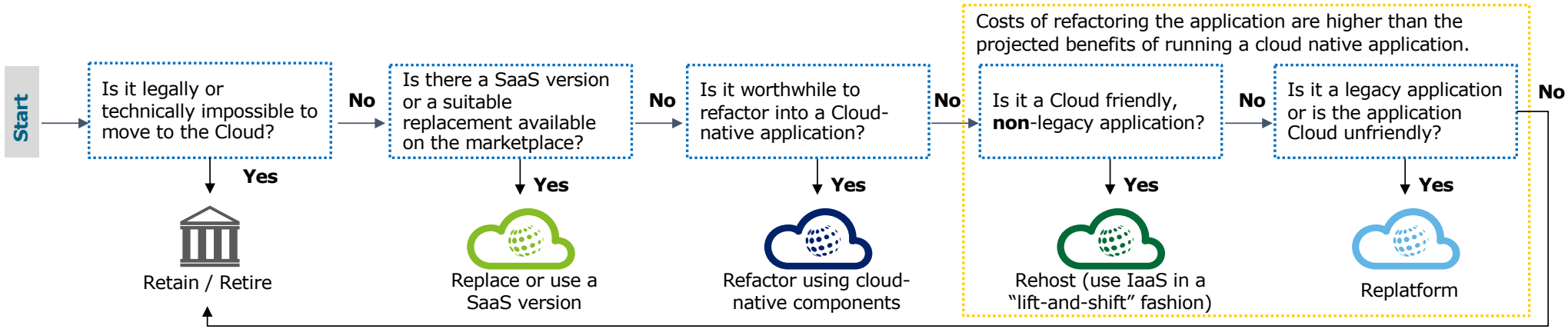
Acknowledge the services which require close and regular proximity to core IT and manage effectively

Cut build team resource cost due to the automated, pre-configured nature of cloud infrastructure builds

Carefully manage the integration of old and new tooling and software, preventing duplication or contradiction

Reduce infrastructure wastage and cut capacity management headcount in the use of cloud Just-in-Time provisioning

The most suitable migration approach is defined by a comprehensible, transparent decision framework



Retire

Application that is to be retired / end of life, possibly with users migrated to another application

Retain

Leave application as part of on premise legacy non-cloud infrastructure

Replace

Application that is to be replaced by another application (or set of applications) and use commercial software delivered as a service

Refactor

Application component is not cloud suitable and/or business demands requires targeted changes to the application to be more Cloud Native

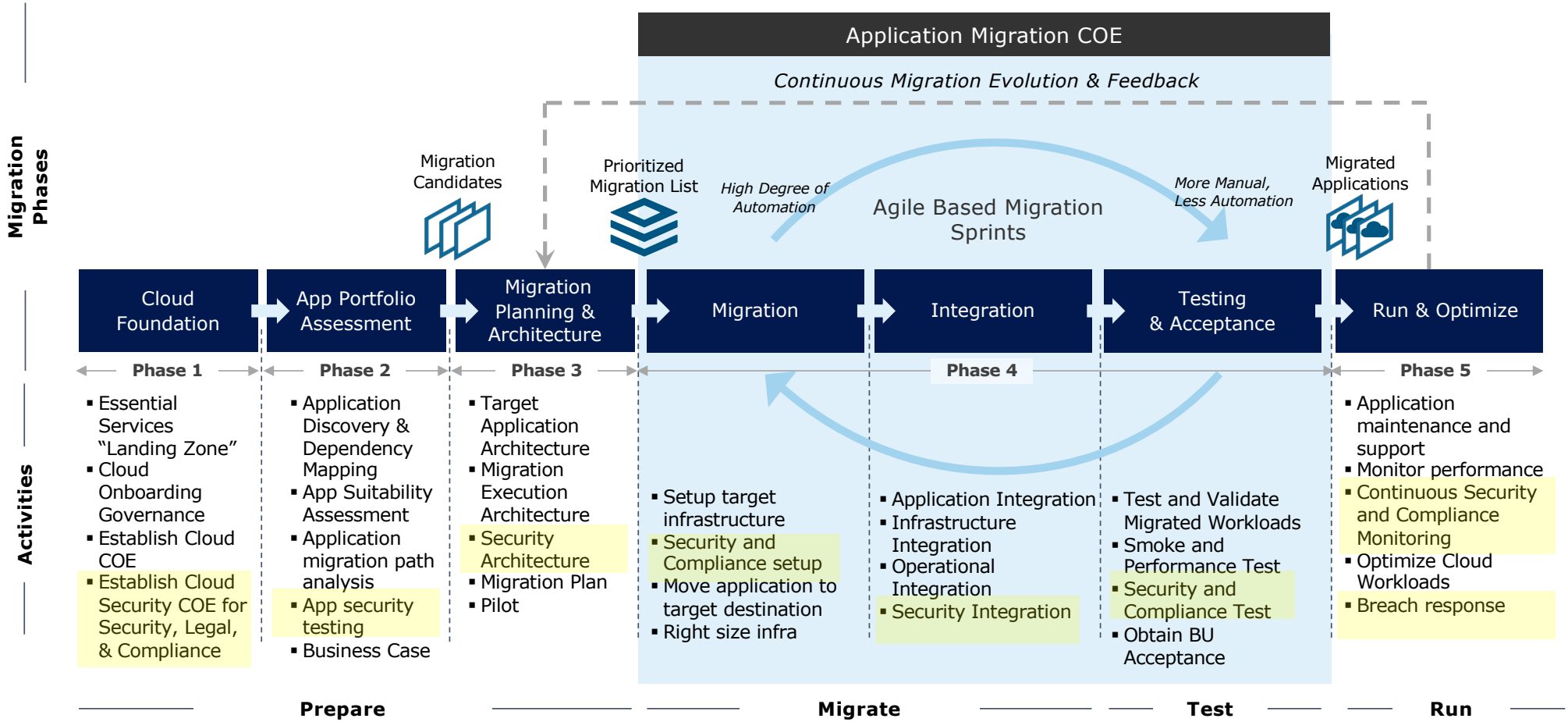
Rehost

Application component is cloud friendly and requires few changes post virtualization. This is a lift and shift of the application onto a Cloud IaaS stack

Replatform

Application components are not available on the cloud or not cost-effective and therefore need to be adjusted

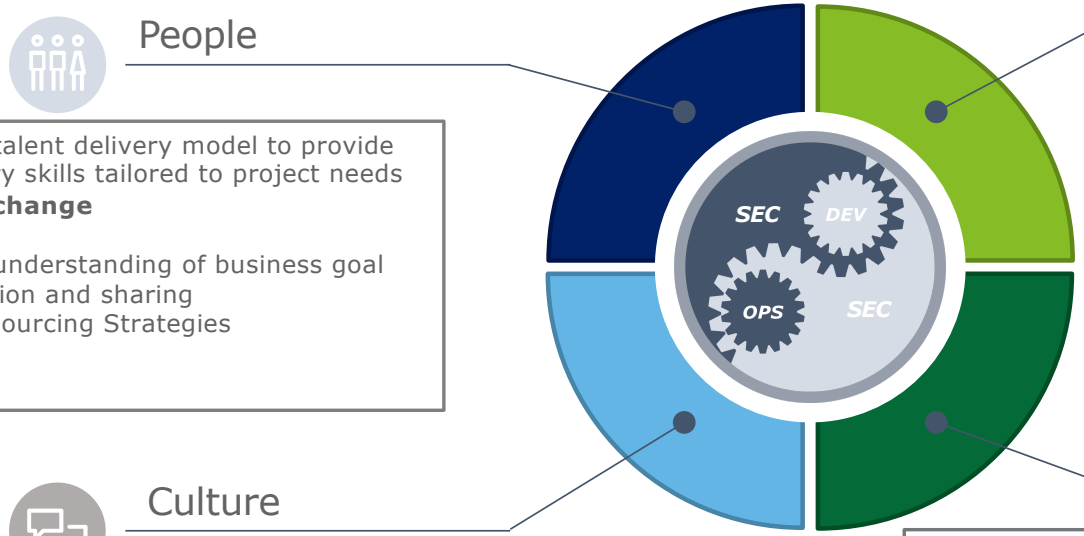
A suitable Cloud Migration Methodology helps running a successful cloud migration*



For mass migrations, Deloitte recommends setting up an Application Migration COE to benefit from economies of scale and efficiencies

* Deloitte Methodology

To become "Cloud Native" and release better quality in less time, business, development and operations need to be closely aligned throughout the service lifecycle



People

Established talent delivery model to provide the necessary skills tailored to project needs

- **Cultural change**
- Training
- Common understanding of business goal
- Collaboration and sharing
- Modified Sourcing Strategies

Process

Improve toolset to support the delivery and automation of the process specifically to accelerate software delivery activities

- One integrated platform
- **Automate process to increase agility and visibility across teams**
- Configure and integrate tools across teams
- Automate using **workflow to minimize user intervention**

Culture

Establish a Trust and Autonomy Culture

- Replacing an organizational culture that "fears bad news" with a trust culture that supports collaboration, collective ownership, shifting left, and failing early
- Aligning HR incentive and recognition programs to encourage a culture of collaboration

Technology

Establish **standardized interconnected process to software practices**

- Adopting industry best practices around operating process designs, tooling, testing, and configuration
- Achieve Continuous Integration and Continuous Delivery for applications to enable quicker time to market
- Shifting from monolithic, tightly coupled applications to loosely coupled microservices
- Release planning
- Continuous monitoring and feedback

Driven by Cloud Culture & Mindset

Driven by Cloud Technologies

Deloitte.

Contact:

Jan Seffinga
Partner Cloud
jseffinga@deloitte.ch

Reto Häni
Partner Cyber
rhaeni@deloitte.ch