Politecnico di Torino

POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Gestionale (Engineering and Management)

Tesi di Laurea Magistrale

Organizational consequences of the adoption of cloud computing in a complex enterprise context

Relatore
Prof. Giulia Bruno

Candidato
Vincenzo LAMANNA

ANNO ACCADEMICO 2021-2022

Contents

1. Introduction

Today, most business problems and needs are likely to be addressed with technology. Cloud computing is the technological solution that represents one of the most powerful opportunity for organizations.
A Harvard Business Review survey has shown as for the vast majority of the companies, cloud is very or extremely important for their future strategy and growth. These organizations consider the cloud as enabler of a greater business agility, cost reduction, data analytics capabilities, and accelerated innovation.
However, according to the survey, 62% of IT executives agree that their companies are having difficulty keeping up with the rapidly evolving technology roles and responsibilities required to manage its increased cloud adoption. Executives also criticized the enterprise's difficulty to quickly realign the business to accept the necessary new capabilities and skills, as well as the increasing complexity that cloud computing brings.
Indeed, failed cloud adoption projects are hardly related to technological issues. Most problems happen when culture and abilities don't change quickly enough to use new technologies, like cloud computing, successfully [14].
At this purpose, the work aims to argue that cloud computing adoption by companies must be always based on an organizational transformation. Moreover, along with the implementation of the technology, the process should also involve new operating models, skills and cultural transformations.
In order to fully understand the reason why companies are increasingly adopting this technology, in the section 2, the cloud computing is introduced. In particular, it has been presented the advantages this technology brings in for organizations describing the types of cloud computing, the deployment models and the cloud global infrastructure.
In the section 3, the main differences with respect to traditional on-premises technologies has been illustrated by describing the cloud dynamics infrastructure. Furthermore, it has been important to illustrate the pillars for designing a cloud-based architecture and the widely used Infrastructure as Code approach.
Since cloud-based resources are run on a third-party physical infrastructure, responsibilities changes following a new paradigm, namely the Shared Responsibility Model which has been presented in the section 4.
However, to successful leverage the advantages of the above-mentioned technology, new skills and competences are needed to finally reach an organizational transformation. Therefore, building a Cloud Center of Excellence (CCOE), which is not just a team of experts to be consulted for their knowledge, is essential and it is a process described in the section 5.
The CCOE must introduce new models and new approaches for leveraging cloud-based resources for business needs. At this scope, DevOps and FinOps models for making more efficient and streamlined processes and managing cloud costs respectively, have been illustrated in the section 5.
The new skills and competencies that the company embraces thanks to the CCOE must lead to the definition of a new target operating models based on the new approaches, practices and organizational mindset to truly leverage cloud-based resources. The main cloud target operating models have been fully described in the section 7. Furthermore, in order to better illustrate how

a company should organized around product teams, which are widely adopted in the target operating models described in the previous section, the Spotify Organizational Framework has been presented in the section 8.
The section 9 describes the real case study, personally followed during a six months internship in Storm Reply in Turin to realize this final thesis work.
Conclusions with results and considerations are reported in the section 10.

2. The Cloud Computing

2.1 Description of the technology

Cloud Computing is one of the technologies leading the digital transformation of different industries following the paradigm of Industry 4.0.
This technology gets its name from a metaphor for the Internet. Usually, the Internet is represented as a cloud in a network diagram meaning it is someone else's concern. Probably, this is the best notion applicable to the cloud computing notions.
There are several definitions of Cloud Computing, the most comprehensive one has been given by the National Institute for Standard and Technology (NIST), a Technology Agent being part of the US Department of Commerce. The definition is:
"Cloud computing is 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."[16] [23]
Another insightful definition has been gives by Amazon Web Services (AWS), one of the largest Cloud Services Providers in the world. AWS has defined this technology as:
"Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing".
Today, Cloud Computing has been already implemented by a huge number of companies all around the globe, from different industries such as Automotive, Utilities, Manufacturing, Public Sector & Healthcare, Retail, Financial Services, Telco & Media, for different use cases such as data backup, disaster recovery, e-mail, virtual desktop, software development and test, Big Data analysis and web application for customer.
In fact, if we observe how the revenues of the major Cloud Service Providers have grown over the past few years, we can notice an increasingly exponential growth. In the Figure 2.1, it has been reported the annual revenue of Amazon Web Services from 2013 to 2021 in million U.S. dollars [27].

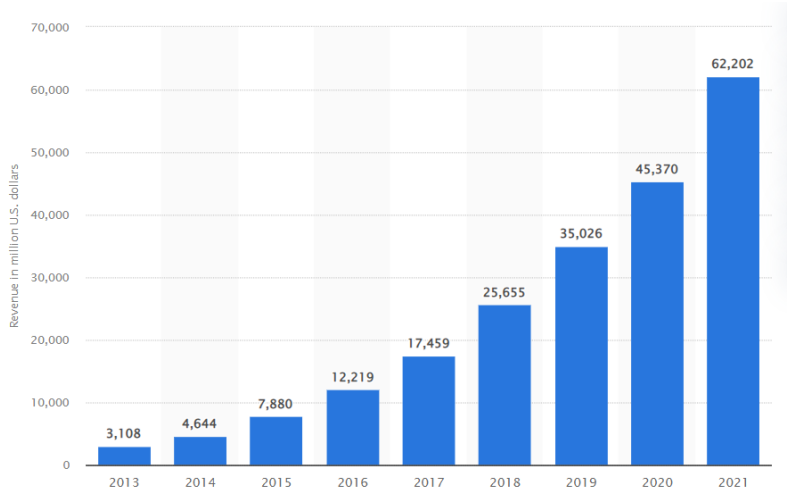

Figure 2.1. Annual revenue of Amazon Web Services (AWS) from 2013 to 2021 (in million U.S. dollars).

In April 2022, Gartner forecasted worldwide end-user spending on public cloud services to grow by 20.4% in 2022 to total $494.7 billion, up from $410.9 billion in 2021. In 2023, end-user spending is expected to reach nearly $600 billion [12].
The exponential increase in cloud adoption by many companies over time can be traced back to the advantages that this technology brings over traditional on-premises technologies. The most important advantages of the cloud computing are the following [2]:

1. *Trade fixed expense for variable expense.*
   Traditional datacenters must be acquired by company to satisfy the business needs. This solution implies huge Capital Expenses (CAPEX). Cloud based solutions turn these capital expenses into variable costs (OPEX). The customer will be charged periodically based on the actual quantity of resources (such as computing, network, storage resources) consumed. This innovative price model, that consists into a periodic bill charged to the customer, is usually called “pay as you go”.
2. *Benefit from massive economies of scale.*
   By using cloud computing, customer can achieve lower unit costs than he would achieve using traditional data centers on premises to provide IT services to the whole organization. The usages from hundreds of thousands of customers are aggregated. Therefore, the Cloud Services Provider can achieve higher economies of scale, which will turn out into lower operative costs.
3. *Stop guessing capacity.*
   Traditional data center must be purchased in advance. This brings the need for estimating the demand of IT infrastructure capacity that the company will face in the future. The customer is likely to end up either sitting on expensive idle resources or dealing with limited capacity. Cloud computing allows customer to obtain the exact capacity just in time or scale down if some resources are no longer needed.
4. *Increase speed and agility.*
   In a cloud computing environment, customers can obtain new IT resources with a click, which means that they can reduce the time to make those resources available to developers to satisfy the business. This results in a dramatic increase in agility for the organization since the cost and time to experiment and develop are significantly lower.
5. *Focus on what really matters.*
   Cloud computing avoid the need for running and maintaining data centers on premises. As a consequence, the organization can concentrate on projects that really bring value to the company, not on the IT infrastructure.
6. *Go global in minutes.*
   Organizations might exploit the possibility to deploy applications for their customers in multiple regions around the world. Cloud based infrastructure provides lower latency and a better experience for customers at minimal costs.

Almost every advantage mentioned above are based on the concept of *elastic infrastructure*. This idea is based on the issue of the demand for IT capacities over time. Especially the computing capacity is widely fluctuating making impossible for organization to exactly follow it (Figure 2.2) [28].

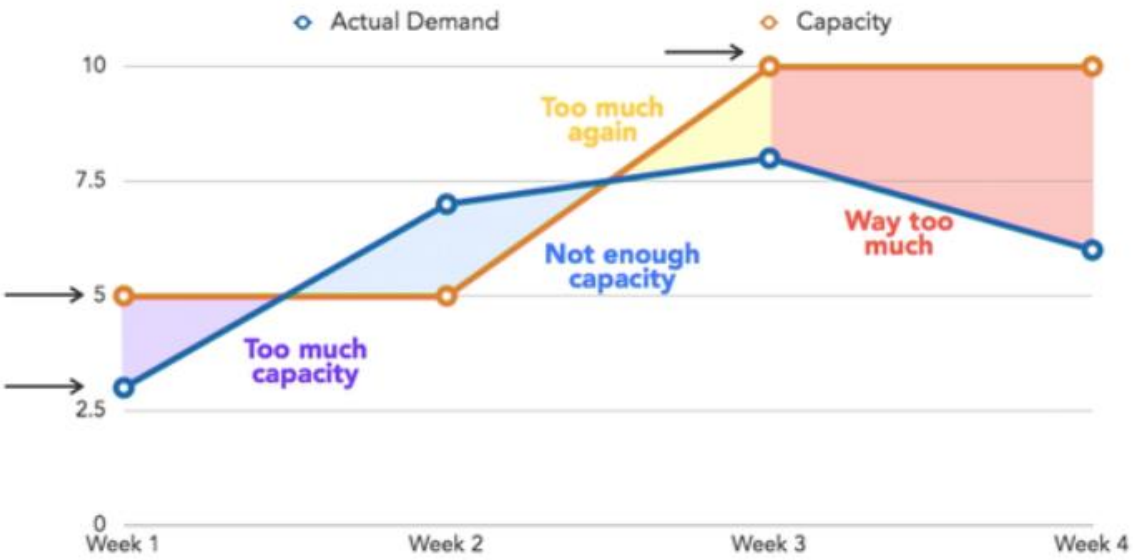

Figure 2.2. Example of comparison between the Actual Demand for IT Capacity and Actual IT Capacity

With an inelastic infrastructure, the company must purchase servers in advance while hoping the capacity will be enough to satisfy the demand. Companies can study the demand trend and try to apply methods of forecasting. While these methods might work, they are still an estimation that would turn out to be completely incorrect. Moreover, even if their estimations are correct, then they usually choose either (1) purchasing servers that can satisfy the average value of the fluctuating curve representing the demand or (2) purchasing servers that are able to satisfy the estimated peak in the demand.
However, none of these solutions are the optimal one. With the first solution (1), the company will not have enough computing capacity to satisfy the demand during peak periods. Meanwhile, with latter solutions (2), the company can provide computing capacity to always satisfy the demand. However, the purchased servers providing these capacities to the company will be underused for most of the time, thus, this solution can represent a huge waste of capital.
Cloud computing enable an *elastic infrastructure* to satisfy the business needs, such as developing a brand-new web-based application to serve customers. Cloud elasticity is the ability to grow and shrink the capacity for CPU, storage and network resources to exactly follow the changing demands of an organization. The elasticity can be even automatic setting up an automation, which can add and remove resources based on monitoring tools.
For instance, if the application used to serve the market is currently facing an increase in incoming traffic due to an unexpected number of requests made by clients, the organization can add more resources to increase the computing capacity and eventually elaborate all the requests simultaneously without losing any customer [25].

2.2 Types of Cloud Computing

Cloud Computing allows the company to focus on what really matters and avoid undifferentiated works such as procurement, maintenance, and capacity planning. Different

types of cloud service and deployment methods provide the company with different levels of control, flexibility and management. As a result, it is useful to define three different Cloud Service Models (Figure 2.3) as different services provided by the cloud service provider to the customers:

Infrastructure as a Service (IaaS)

The model typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides the customer with the highest level of flexibility and management control over IT resources to meet the business needs.
This service can be compared to existing IT resources currently known to IT departments and developers [2].

Platform as a Service (PaaS)

This model removes the needs for managing the underlying infrastructure, usually meaning hardware and operating systems, allowing the customer to use a cloud platform and to be only involved in the development, deployment and management of applications.
Therefore, there will not be concerns of the customer about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running the application [2].

Software as a Service (SaaS)

The latter model provides the customer with a completed product run and managed by the Cloud Service Provider. Most of the time, this model refers to end-user cloud-based applications.
With this model, the customer is never involved in making, managing or maintaining neither the infrastructure nor the application.
The most common example is the web-based email, in which the customer uses the service sending and receiving mails without being involved in making and managing servers, operating systems or any other component that the program is running on [2].

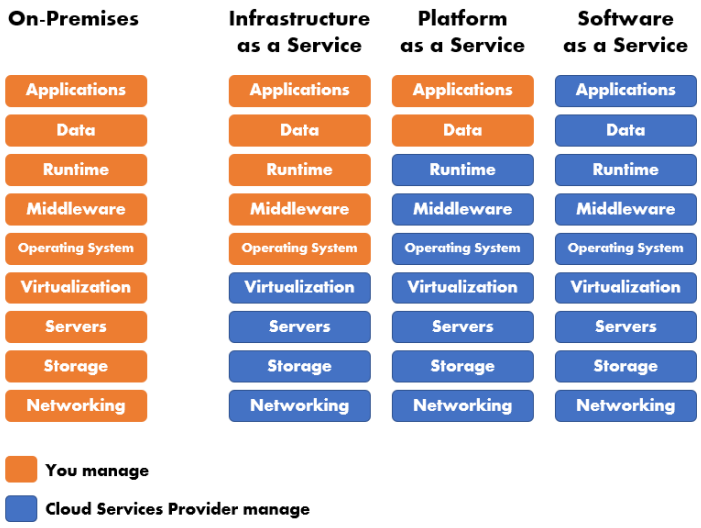

Figure 2.3. Cloud Service Models

2.3 Deployment models

When selecting a cloud strategy, a company must consider factors such as required cloud application components, preferred resource management tools, and any legacy IT infrastructure requirements.

The three cloud computing deployment models are Full Cloud, Hybrid and Multi Cloud.

Full Cloud

In a cloud-based deployment model, the customer (i.e., an organization or an individual who starts adopting the cloud computing) can migrate existing applications to the cloud or can design and build new applications in the cloud to meet the business needs. The customer can build those applications on low-level infrastructure that requires an IT staff to manage them. Alternatively, he can build them using higher-level services that reduce the management, architecting, and scaling requirements of the core infrastructure [2].

Hybrid

A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud. The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure, to extend and grow an organization's IT infrastructure into the cloud while connecting cloud resources to the internal system [2].

Multi Cloud

Since there are so many different types of workloads, each with its own requirements, many businesses end up using a combination of services from different Cloud Service Providers, including their own private cloud resources. This is known as a *Multicloud* approach.

Multicloud gives the customers more flexibility over different price points, service offerings, capabilities, and geographic locations. With careful planning, a multicloud strategy can create consistency across the organization, independent of the services being consumed. Moreover, a Multicloud approach requires a software layer to deliver management and orchestration of workloads across cloud environments [29].

2.4 Global Infrastructure

A Cloud Computing infrastructure is the set of hardware and software elements necessary to enable cloud computing. It includes computing, networking, and storage capabilities, as well as an interface that allows users to access virtualized resources. Virtual resources mirror a physical infrastructure, with components such as servers, network switches, memory, and storage clusters [30].
Customers will use these virtualized IT resources to meet business needs. However, customers might be concerned about potential issues with the physical infrastructure of the Cloud Services Provider interfering with the delivery of services.
Cloud Services Providers, such as Amazon Web Services (AWS), Google Cloud and Microsoft Azure, offer a Global Infrastructure providing high level of performance and reliability of their services. This Global Infrastructure allows the customer to deploy application workloads across

the globe with a single click for resiliency purpose or to build and deploy specific applications closer to end-users to reach a single-digit millisecond latency.
The Global Infrastructure of a Cloud Service Provider is usually made up of Zones. A Zone is a single or a cluster of data centers with redundant power, networking, and cooling resources inside a Region. A Region consists of multiple, isolated, and physically separate Zones within a geographic area.
Zones make it possible to partition applications to obtain high availability. If an application is partitioned across Zones, companies are better protected from issues such as power outages, lightning strikes, tornadoes, earthquakes and more since Zones are physically separated by a meaningful distance.
Therefore, a Global Infrastructure allows to achieve a high level of Resiliency. Resiliency is the ability of a workload to recover from infrastructure, service, or application disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions, such as misconfigurations or transient network issues [11].
Moreover, a Global Infrastructure enables companies to be extremely flexible and take advantage of the conceptually infinite scalability of the cloud. Customers used to over provision to ensure they had enough capacity to handle their business operations at the peak level of activity. Now, they can provision the amount of resources that they actually need, knowing they can instantly scale up or down along with the needs of their business, which also reduces cost and improves the customer's ability to meet their user's demands. Companies can quickly spin up resources as they need them, deploying hundreds or even thousands of servers in minutes.
The Global Infrastructure of the above-mentioned Cloud Services Providers are designed to meet the most stringent security requirements to comply with any regulations, such as GDPRs for European companies. Furthermore, any infrastructure belonging to the Cloud Services Providers is monitored 24/7 to help ensure the confidentiality, integrity, and availability of the customer data. In addition, customers will always have the control their data, including the ability to encrypt it, move it, and manage retention at any time.
The Figure 2.3 shows AWS Regions across the world in 2022 [31].

Figure 2.3. Amazon Web Services (AWS) Regions in the world in 2022.

3. Cloud Architecture

3.1 Cloud dynamic infrastructure

Traditional IT governance models are usually based on up-front design, rigorous change review, and strictly segregated responsibilities. Companies prefer to add extra work up front, hoping to reduce the time spent making changes later.
However, with cloud computing, there are no longer physical IT resources, having transformed them into virtual constructs that the company can create, duplicate, change and destroy at will. This transformation has led to a different way of design and use computing resources. Today, there are several principles for designing and implementing infrastructures on cloud.
For instance, considering that any organization needs to patch and update systems as well as resize the IT resources, redistribute load and troubleshoot problems, a modern cloud-based infrastructure must be designed for providing uninterrupted services while underlying resources change.
Moreover, while designing and implementing a cloud-based infrastructure, an important principle to follow is to create a recoverable system. A system is recoverable if you can rebuild its parts effortlessly and reliably. This will allow to make testing environments consistent with production environments, replicate systems across regions for availability purposes, add resources on demand and replicate systems to give each customer a dedicated instance. However, any system generates data, content, and logs, which cannot be defined ahead of time, but they must be considered as part of the replication strategy.
In addition, a cloud-based infrastructure allows to add, remove, start, stop, change, and move the parts of its system. This creates operational flexibility, availability, and scalability. It also simplifies and de-risks changes. This is also the main idea behind the cloud native software.
At this purpose, there is a popular expression to understand the disposability of servers in cloud: “Treat your servers like cattle, not pets”.
Nevertheless, the easiness of making changes might lead to a configuration drift. Configuration drift is variation that happens over time across systems that are supposed to be identical. For example, you define a simple component and create many identical instances of it, then you can easily understand, change, and fix it. To make this work, you must apply any change you make to all instances of the component. Otherwise, you create configuration drift.
As a result, with a cloud adoption, companies must embrace a new mindset considering that the Cloud allows to make changes easily, safely, quickly, and responsibly to adapt the infrastructure to business needs [19].

3.2 Cloud architecture pillars

Amazon Web Services (AWS) stated that when building technology solutions on cloud, if the customer neglects six pillars of operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability, it can become challenging to build a system that reach expectations and requirements.
Incorporating these pillars into your architecture helps produce stable and efficient systems. This allows customers to focus on the other aspects of design, such as functional requirements. The six pillars are described illustrating the design principle and the best practices.

Operational Excellence

The principle of operational excellence concerns how organizations support business objectives and the ability to execute workloads effectively, obtain insights regarding their operations, and continually improve processes and procedures to deliver value added.

There are five design principles for operational excellence in the cloud.

Operations as code

In the cloud, it is possible to define applications and infrastructure as code and update them with code. Customers can implement operations procedures as code and automate their execution by triggering them in response to events. By performing operations as code, human error will be limited and there will be always consistent responses to events.

Frequent, small, reversible changes

Design workloads considering components to be updated regularly. Changes must be small increments that can be reversed if they fail without affecting end-users if possible.

Refine operations procedures frequently

Processes and procedures previously defined must be reviewed and validated frequently, seeking improving opportunities. Indeed, since workloads evolve, also processes and procedures are supposed to evolve over time.

Anticipate failure

Cloud customers should perform a proactive analysis to identify potential causes of failure in order to eliminate or mitigate them. In cloud environment, this can be done by testing error scenarios in order to fully identify their impacts. Also, response plans should be tested periodically to assess their effectiveness and to make teams know how they are performed.

Learn from all operational failures

Improvements can be driven by lessons learned from all operational events and failures. These must be shared across teams and through the entire organization.

BEST PRACTICES

Organization

All the teams inside the organization need to have a shared understanding of the entire workload, their role in it, and shared business goals to set the priorities that will enable business success. At this purpose, well-defined priorities will maximize the benefits of the efforts of the organization. This can lead to make the organization able to evaluate stakeholders needs, considering external factors, such as regulatory compliance requirements and industry standards.

Moreover, it is necessary that teams evaluate threats to the business such as, business risks and liabilities, and information security threats. Then, they should evaluate the impact of risks, and tradeoffs such as accelerating speed to market for new features and cost optimization. Considering benefits and risks allows teams to make informed decisions and where to focus efforts.

Furthermore, teams must understand their part in achieving business outcomes. Teams must understand their roles in the success of other teams, the role of other teams in their success, and have shared goals. A clear and shared definition of responsibilities, ownerships and decision-making processes, definitely contributes to maximize the benefits of efforts of teams.
Finally, experimentations must be encouraged to accelerate learning and keep team members interested and engaged. Moreover, this will allow workers to grow their skill sets so that they can support changes in demand and responsibilities. However, in order to achieve this, they must receive resources and tools to continuously learn and eventually, to support the organization business outcomes. Cross-functional teams inside the organization can help to achieve different unique perspectives and increase innovation.

Prepare

Cloud customers must design workload so that it can provide useful insights necessary to understand the internal state of the system, such as metrics, logs, events, and traces in support of observability and investigating processes. This will lead to the risk identifications and definition of response plans as well as for continuous improvement.

Operate

For cloud customers, a successful operation of a workload will lead to the achievement of business outcomes. Thus, cloud customers must be able to identify metrics to determine if workload and operations are successful. Based on these metrics, the customer can prioritize actions to be taken considering their business impact. Moreover, to reach operational excellence, customers must monitor the operating status of their workloads through dashboards or alerting systems.

Evolve

Operational excellence must be sustained over time by making continuous incremental improvements. Cloud customers should continuously perform post-incident analysis to identify the contributing factors and preventative actions to limit or prevent recurrence. Then, these critical factors must be shared across the organization. Moreover, they must regularly evaluate and prioritize opportunities or requests for improvement of workloads or operations procedures, such as feature requests, issue remediation, and compliance requirements. Cross-team retrospective analysis of operations metrics are always useful in identifying opportunities and methods for improvement.

Security

The security pillar in cloud architecture is a topic of great interest to many cloud customers operating in different industries. It concerns the ability of protecting data, assets and systems exploiting cloud services.

There are seven design principles for security in the cloud.

Strong identity foundation

Customers are supposed to implement the principle of least privilege (i.e. assigning always the minimum number of authorizations to users) and enforce separation of duties with appropriate

authorization for each interaction with cloud resources. Moreover, identity management should be centralized with the aim to eliminate reliance on long-term static credentials.

Traceability

Customers must consider that cloud-based resources can be easily monitored and automations can be used to investigate and take actions, such as make changes to the cloud environment in real time, in response to log and metric collection.

Security at all layers

Defenses with security controls must be applied to all layers of the infrastructure, such as network, compute service, operating systems, applications.

Automate security best practices

A secure cloud infrastructure includes controls that are defined and managed as code. This will also improve the ability of security scale resources rapidly and cost- effectively.

Protect data in transit and at rest

In cloud data must be classified based on sensitivity and protected by encryption, tokenization and access controls.

Keep people away from data

Mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data must be used in order to reduce the risk of loss, modification and human error when handling sensitive data.

Incident strategies

Cloud customers must define an incident management process and investigation policy as well as run incident response simulations and use tools and automation to increase speed for detection, investigation, and recovery.

BEST PRACTICES

Security

Segregating different workloads by account (i.e. set of cloud resources), based on their function and compliance or data sensitivity requirements, is highly recommended.

Identity and Access Management

To ensure that only authorized and authenticated users and components will access cloud resources, cloud customers should define principals and build out policies aligned with these principals. For example, there must be defined what action a user can do in a specific account. Cloud services providers provide Identity and Access Management (IAM) service so that customer can apply granular policies, which assign permissions to a user, group, role, or resource.

Detection

Customers are supposed to use detective controls to identify potential security threats or incidents. They can be used to support a quality process, a legal or compliance obligation, and for threat identification and response plans.

Infrastructure Protection

Customers must apply methodologies and tools for defending each cloud resources which the cloud infrastructure is made of. This must be done for organizational or regulatory obligations.

Data Protection

Practices that influence data security are data classification, which provides a way to categorize organizational data based on levels of sensitivity, and encryption which protects data by making it unintelligible to unauthorized access. These practices can prevent financial loss and they are used to comply with regulatory obligations.

Incident Response

Customers are supposed to apply security threats controls and preventive actions but still incidents might occur. At this purpose, customers should put processes in place to respond to and mitigate the potential impact of security incidents, named incident response plan.

Reliability

The Reliability pillar concerns the ability of a workload to perform its intended function correctly and consistently when it is expected to. This includes the ability to operate and test the workload through its total lifecycle.

There are five design principles for reliability in the cloud:

Automatically recover from failure

Monitoring a workload for key performance indicators (KPIs) is an essential practice, it can trigger automation as a response when a threshold is reached. These KPIs should be a measure of business value, not of the technical aspects of the operation of the service so that they can be easily and quickly understood. This also allows for automatic notification and tracking of failures, and for automated recovery processes. Automations can even prevent failures.

Test recovery procedures

In the cloud, customers are supposed to test workload as well as recovery procedures. Automations can be used to simulate different scenarios that led to failures with the aim of reducing risks.

Scale horizontally to increase aggregate workload availability

Cloud customers should distribute workloads across multiple small resources instead of using one large resource, so that they will not share a single common point of failure.

Stop guessing capacity

Cloud customers can monitor demand and workload utilization, and automate the addition or removal of resources to maintain the optimal level to satisfy demand without over- or under-provisioning.

Manage change in automation

Cloud customers are supposed to make changes to infrastructure by using automation considering that they can be tracked and reviewed.

BEST PRACTICES

Foundations

Cloud customers should create a cloud infrastructure that can handle different workloads or project. Therefore, there must be some foundational requirements to be considered while architecting a system that might influence the reliability of services. However, resources provided by the largest cloud services providers already incorporates these foundational requirements. For instance, cloud services provider can provide the customer with always sufficient networking and computing capacities, while the customer can resize resources to meet its own demand.

Workload Architecture

To guarantee highly scalable and reliable workload, customers should implement a service-oriented architecture. This is a practice to make software component reusable as well as smaller and simpler. Moreover, customer should consider that distributed systems, made of multiple small components, rely on networks which might imply data losses and latency. These considerations can lead to mitigate the possible impact of these impairments and improve the mean time to recovery (MTTR).

Change Management

Customers must design workloads considerations that changes should be anticipated and accommodated to achieve reliable operation of the workload. Changes can include those to manage peaks in demand as well as new features deployment or security patches.

Adding and removing resources in response to changes in demand can be done via automations that not only increase reliability but also ensures that business success does not become a burden.

Failure Management

Customers must consider that failures might occur, and they can have an impact on the services availability. Rather than trying to diagnose and fix a failed resource that is part of production environment, cloud services providers suggest replacing it with a new one and carrying out the analysis on the failed resource later out of band. This can be done because cloud allows to recreate temporary versions of the system quickly and at low cost. Moreover, in cloud, customers can also use automated tests to assess the recovery process. These considerations must be kept while defining a Disaster Recovery plan.

Performance efficiency

Performance efficiency pillar concerns the ability of to use computing resources efficiently. There are five design principles for performance efficiency in the cloud:

Exploit advanced technologies

Customer should consider delegating advance technology implementation in cloud to the cloud vendor. In cloud, it is always possible to consume technology as a service. Technologies such as non-relational databases or machine learning require specialized expertise. In the cloud, these technologies become services that teams can easily consume.

Go global in minutes

Customers should consider deploying workloads in multiple regions around the world to provide lower latency and a better client experience at minimal cost.

Use serverless architectures

Serverless services provides resources that allows to carry out traditional compute activities without the need to run and maintain physical servers. This removes the operational burden of managing physical servers and can lower transactional costs because managed services operate at larger scale by the cloud provider.

Experiment more often

Cloud customers should exploit the virtual and automatable resources to quickly run and test different type of instances of resources and different configurations.

Understand cloud services

Cloud customers should understand how cloud services can be consumed and use a technological approach to manage workloads. For example, customers should consider data access patterns when selecting databases in cloud.

BEST PRACTICES

Selection

Cloud services providers' resources are usually available in different types and configurations. Customers should use an appropriate approach to select resources that match workload needs, such as data-driven, even-driven or pipeline approach.

Review

Customers must ensure that workload components are meeting performance and cost objectives. Also, customers should consider evolving and continuously improving performance of the workload components. These can be achieved through a frequent review process. Technologies such as machine learning and artificial intelligence can be used to reimagine customer experiences and innovate.

Monitoring

In order to guarantee different objectives and improve the system, customers are supposed to monitor metrics. These metrics can be used to raise alarms when thresholds are breached and to activate response plans.

Tradeoffs

Customers architecting and selecting cloud resources are supposed to consider tradeoffs to eventually identify the optimal solution.

Cost Optimization

Cost optimization pillar includes the ability to run systems to deliver business value at the lowest price point.

There are five design principles for cost optimization in the cloud:

Implement Cloud Financial Management

In cloud, a new cost model, commonly known as “pay as you go” has been introduced. Thus, to achieve financial objectives, it is needed new cost optimization approaches.

Adopt a consumption model

In cloud, customers will be charged only for the real consumption of resources. As a consequence, customers should increase or decrease usage based on business needs without use elaborate forecasting.

Measure overall efficiency

Customers should use instruments to measure the business output of the workload and the costs associated with it.

Stop spending money on undifferentiated heavy lifting

Cloud customers can exploit managed services reducing the risks of wasting capital to operate servers.

Analyze and attribute expenditure

In cloud there are a lot of instruments to accurately identify and allocate IT costs. This will help to measure financial indicators such as return on investment (ROI) and identify opportunities for reducing costs.

BEST PRACTICES

The cloud financial management is performed through innovative models such as the FinOps approach.

Sustainability

The Sustainability pillar concerns the environmental impacts, especially energy consumption and efficiency.

There are six design principles for sustainability in the cloud:

Understand the impact

Customers are supposed to measure and model the environmental impact of cloud workloads. This should include all sources of impact, including impacts resulting from end-user products use, and impacts resulting from their eventual decommissioning and retirement. These models can be used to optimize the environment impact of the cloud workloads.

Establish sustainability goals

Customers should establish long-term sustainability goals for their cloud workloads, such as reducing the computing and storage resources required or improving their usage efficiency while growing the infrastructure.

Maximize utilization

Customers should define the right size of resources for workloads and implement efficient design to ensure high utilization and maximize the energy efficiency of the underlying hardware. This implies to eliminate or minimize idle resources to reduce the total energy required to power workloads.

Adopt new and more efficient hardware and software

Customers should consider new and more efficient hardware and software to reduce the environmental impact while guaranteeing the same performance.

Use managed services

Using managed services implies to share services across a broad customer base, which helps maximize resource utilization and reduces the amount of infrastructure needed to support cloud workloads.

Reduce the downstream impact of cloud workloads

Cloud customers should reduce the amount of energy or resources required to end-users to use their services. This is possible by testing and assessing the impact from using the cloud-based service.

BEST PRACTICES

Region Selection

After having set sustainability goals, cloud customers should select regions where workloads can be run meeting business requirements and sustainability goals.

Resources patterns

Customers should implement patterns for performing workloads smoothing and maintaining consistent high utilization of deployed resources to minimize the resources consumed. They should consolidate underused components, retire components that are no longer needed and optimize components that consume the most resources.

Development and deployment patterns

Cloud customer should reduce environmental impacts associated to development, test, and deployment practices [6].

3.3 A new provisioning model: Infrastructure as Code approach

Organizations increasingly rely on their ability to deliver and operate software systems to achieve their goals. A recent research by a Google Cloud team has identified four metrics for evaluating software delivery and operational performances:

(1) Delivery lead time: the elapsed time it takes to implement, test, and deliver changes to the production system
(2) Deployment frequency: how often the organization deploys changes to production systems
(3) Change fail percentage: what percentage of changes either cause an impaired service or need immediate correction, such as a rollback or emergency fix
(4) Mean Time to Restore (MTTR): how long it takes to restore service when there is an unplanned outage or impairment

Therefore, organizations that perform well against their business goals, such as revenue, share price, or other criteria, also perform well against these four metrics, and vice versa.

To perform well on these metrics, any organization can exploit the dynamic nature of the cloud computing, however, this requires a fundamental change of approach and new ways of thinking about change and risk [32].
According to the "operational excellence" pillar, a widely used and innovative approach to managing cloud systems is Infrastructure as Code, that embraces continuous change for high reliability and quality.
Infrastructure as Code can be defined as an approach for provisioning and managing the IT infrastructure through machine-readable definition file. Therefore, it is based on practices from software development.
It makes provisioning, managing and changing the infrastructure and configuration of the resources as consistent and repeatable activities. Customers are supposed to make changes to code, then use automation to test and apply those changes to the systems.
Organizations adopting Infrastructure as Code to manage dynamic infrastructure may achieve some important benefits. In particular, it reduces the effort and risk of making changes to infrastructure, creating systems that are reliable, secure, and cost-effective. Moreover, the source code defining the infrastructure can be seen by different developers making governance, security, and compliance controls visible. Furthermore, it improves the speed to troubleshoot and resolve failures.
In addition, any system must change and evolve over time under a continuous improvement perspective and Infrastructure as Code allows to make changes both rapidly and reliably.
The latter benefit has been considered as the most important by cloud customers since it allows them to achieve a shorter Time-To-Market meaning a more rapid delivery of value to the final clients.
Actually, there are easier ways to provision infrastructure. The customers can always use the web-based platform of the Cloud Services Provider, which provides an intuitive web interface. Also, the customer can drop to the prompt and wield the vendor's CLI (command-line interface) tool to obtain new IT resources. However, these are not optimal methodologies since they can introduce human errors, they might turn out to be time consuming and they do not allow to exploit above-mentioned code advantages, such as reusability, consistency, and transparency.
Furthermore, using Infrastructure as Code rather than web-based console for the resources provisioning and management, the customer can gain:

Traceability: a history of changes useful for debugging problems.

Rollback: when a change breaks something, it is useful to be able to restore things to exactly how they were before.

Correlation: keeping scripts, specifications, and configuration in version control helps when tracing and fixing problems, correlating causes and effects with tags and version numbers.

Visibility: each change committed to the version control system is visible, the team has a situational awareness.

Actionability: script can trigger an action automatically for each change committed.

Today, the most common infrastructure as code tools that allow to build, change, and version infrastructure safely and efficiently are: HashiCorp Terraform, AWS CloudFormation, Azure Resource Manager, Google Cloud Deployment Manager, OpenStack Heat, Pulumi.
Since an increasing number of cloud customers is selecting a multi-cloud deployment model, HashiCorp Terraform is becoming widely used since it allows to manage resources on cloud platforms of different cloud services provider.
Providers define individual units of infrastructure, for example compute instances or private networks, as resources. Then, the customer can compose resources from different providers into reusable Terraform configurations called modules, and then, manage them with a consistent language and workflow.
Terraform configuration language is declarative, meaning that it describes the desired end-state for the infrastructure, in contrast to procedural programming languages that require step-by-step instructions to perform tasks. Terraform providers automatically calculate dependencies between resources to create or destroy them in the correct order.
As an example, to deploy infrastructure with Terraform, cloud customer simply has to carry out the following steps: identify the infrastructure for the project, write the configuration for the cloud infrastructure, install the plugins Terraform needs to manage the infrastructure, plan the changes that Terraform will make to match the defined configuration and finally apply the planned changes [33].

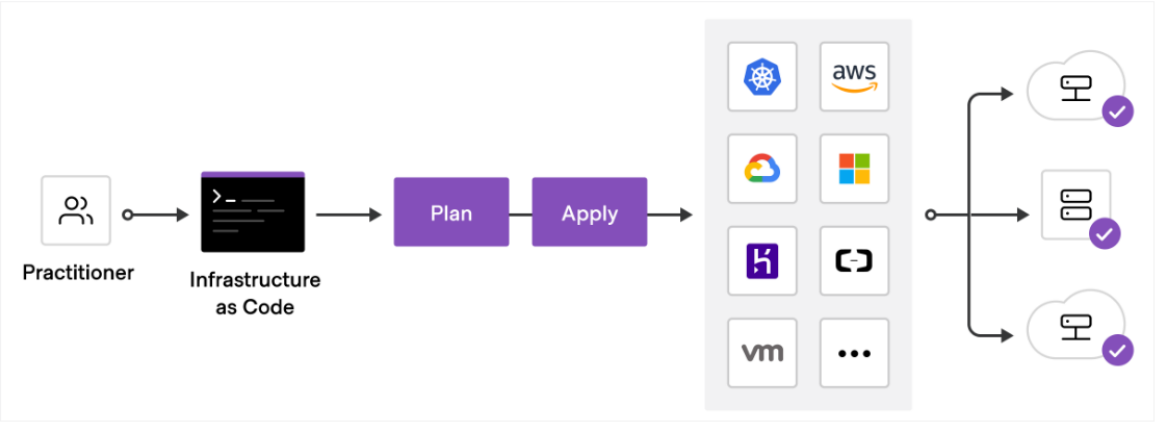

Figure 3.1. Procedure for provisioning and managing the cloud infrastructure with Terraform.

4. Cloud roles and responsibilities

4.1 Shared Responsibility Model as a new paradigm

When an enterprise runs and manages its own IT infrastructure on premises, within its own data center, the enterprise is responsible for the security of that infrastructure, as well as the applications and data that run on it. While moving on Cloud technologies, organizations rely on third-party IT resources.
As a consequence, security and compliance must be a shared responsibilities between the cloud services provider and the customer.
According to this model, cloud services providers always operate, manage, and control the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.
Instead, the cloud customers should carefully consider the services they choose because their responsibilities vary depending on the services used, the integration of those services into their existing IT environment, and applicable laws and regulations. The cloud customer can always enhance their security to meet their more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection and prevention, encryption, and key management. It is in the nature of a cloud shared responsibility model to provide the flexibility and customer control that permits customers to deploy solutions that meet industry-specific certification requirements.
Amazon Web Services (AWS) stated that a Cloud Services Provider is responsible for the security “of” the cloud, while the customer is responsible for the security “in” the cloud.
Therefore, the cloud services provider will be solely responsible for the security of the software, hardware, and the physical facilities used to provide cloud services. Whereas the customer is always responsible for a secure configuration and use of the cloud services selected.
For instance, a service such as a Virtual Machine is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all the necessary security configuration and management tasks, including:

- Data protection: encrypting data at rest and in transit.
- Network security: defining network rules, managing routing tables and the access control lists.
- Identity and the access management: defining users with their credentials, roles and policies for the resources access.

The latter is actually a clear example of a shared responsibility since the cloud services provider must have built several layers of security features to prevent unauthorized access to the resources, including multi-factor authentication; then, it is the customer’s responsibility to make sure multifactor authentication is enabled, particularly for those users with the most extensive permissions.
Customers that deploy a virtual machine instance are responsible for management of the guest operating system (including updates and security patches), any application software installed by the customer on the instances, and the configuration of the firewalls on each instance. Cloud services provider is responsible for protecting the infrastructure that runs the service offered

through the cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run cloud services.

Generally, shared responsibilities include:

- Patch Management: cloud services provider is responsible for patching and fixing bugs within the infrastructure, while customers are responsible for patching their guest Operating System and applications.
- Configuration Management: cloud services provider maintains the configuration of its infrastructure devices, while customers are responsible for configuring their own guest operating systems, databases, and applications.
- Training: cloud services provider trains its employees, while customers must train their own employees for a correct and secure use of the cloud services [21].

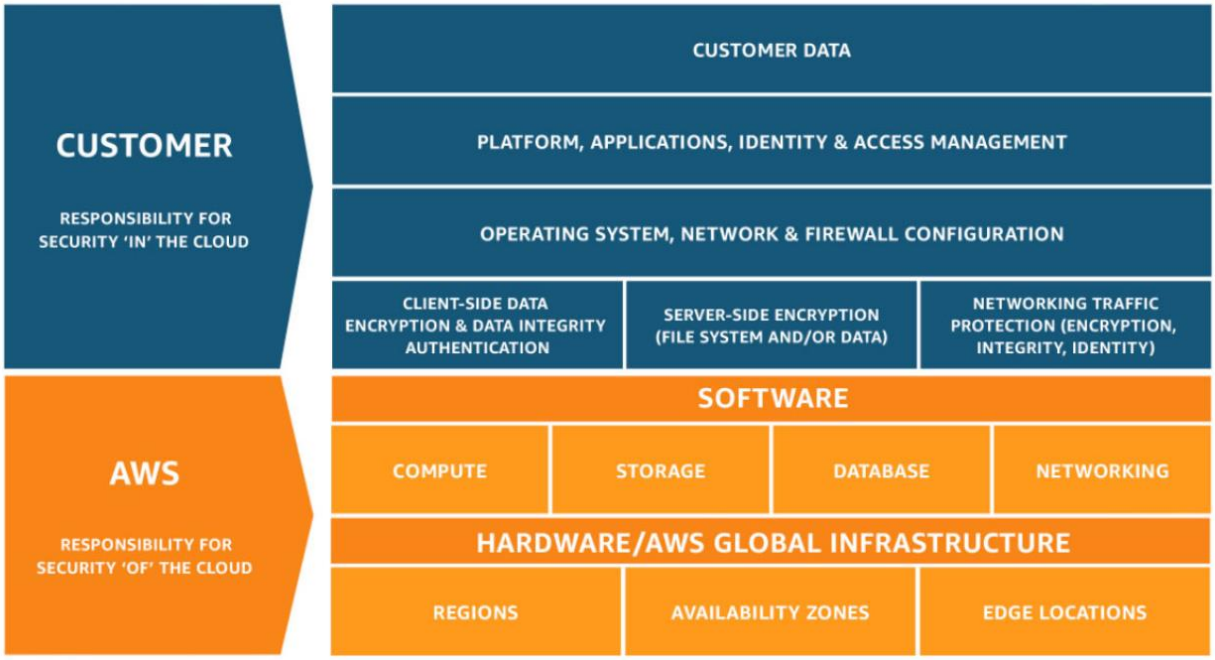

Figure 4.1. Amazon Web Services shared responsibility model for a IaaS solution

For SaaS solutions such as Office 365 and Dynamics 365, Microsoft Azure as cloud services provider offers capabilities to protect customer data, such as Office Lockbox and Data Loss Prevention, but ultimately customers must manage, classify, and configure the solutions to address their unique security and compliance requirements [17] [24].

5. Building a Cloud Center of Excellence (CCOE)

5.1 The Cloud Center of Excellence

The transition to cloud represents a significant transformation for the core IT. Multiple complex activities that concurrently happen during migration readiness require subject matter expertise that is often dispersed throughout an organization. Large enterprises beginning a transformation journey, noticed that good practices from isolated corners of the enterprise cannot transform the rest of the organization. To accelerate the journey to the cloud, a dedicated cross-functional team should be committed to conceiving the cloud strategy aligned with the organizational strategy and consider how the business transforms as a result of a technological change. This team is usually referred to as Cloud Center of Excellence (CCOE) who establishes the initial set of cloud services and helps with the migration activities. However, a CCOE is not only a team of experts who can be consulted for understanding how to operate in cloud, but it must be seen as the driver of change across the enterprise and as the focal point for the cloud-enabled IT transformation.
Thus, a CCOE can be defined as a centralized enterprise architecture function that leads and governs cloud computing adoption within an organization [8]. When this function is properly structured and supported, it can accelerate innovation and migration efforts while reducing the overall costs of change and increasing business agility. Moreover, when a CCOE is correctly implemented, it can lead to a significant reduction in time-to-market.
Its responsibilities include to set the foundation for a successful cloud migration, encourage a culture of collaboration and knowledge sharing, advise on and implement solutions providing both thought leadership and hands-on support.
In practical terms, a CCOE is responsible for:

Develop the cloud strategy and architecture Design a cloud platform determining how it should be setup, configured and consumed.

Execute initial migration activities Migrate the initial waves of applications into the cloud environment.

Develop standards & templates Build and maintain reusable templates and standards such as Infrastructure as code templates for provisioning the infrastructure.

Develop and provide foundational cloud services Develop cloud foundational components such as network and security components.

Drive the adoption of cloud services Share the knowledge across the organization through training programs to accelerate the journey to the cloud.

Provide financial governance Manage, control and provide financial stewardship of the cloud assets and resources.

However, since the priorities and the capabilities of the business that drive the structure and scope of the CCOE, each CCOE will look a little different. Moreover, the current state of cloud maturity of the organization will determine the CCOE activities.

One of the main concerns of enterprises starting their cloud-based transformation regards how to build up a CCOE inside the organization. Actually, there is not an optimal approach when designing a CCOE. Below the main steps to create have been illustrated:

1. Assess where the organization is on its cloud journey and where it wants to go.

2. Identify the figures with technological background and key people for the transformation, who can drive choices aimed to move to the cloud environment strategically.

3. Design the CCOE structure and develop a talent strategy to account for missing capabilities.

The CCOE is also responsible for defining a cloud mindset and practices within the organization and leveraging them for a successful cloud adoption across the organization. Therefore, CCOE provides:

Community leadership: the CCOE encourages members of the organization to adopt cloud-based solutions and collects members feedbacks. It also shares results and successful stories to the Chief Executive Officer, the rest of the organizations and to other stakeholders.

Virtual collaboration: the CCOE provides a forum for the members to exchange ideas and best practices, ask for and receive advice, and collaborate on cloud-related cross community projects. This can use various internal collaboration mechanisms.

Community documentation: the CCOE can use sharing tools to actively solicits the community to contribute to create new best practices.

Community code repository: the CCOE usually makes up an open-source code repository that contains templates, code libraries and other artifacts shared within the organization.

Community events: the CCOE plans and facilitates in-person or virtual meetings that allow members to share and learn from each other.

Cloud training: the CCOE cloud architects may directly lead training, collaborate with an internal or external training team to make the rest of the organization develop cloud skills and knowledge.

Future Projects: the CCOE creates an important talent pool for future cloud projects and for continuously improving cloud-based solutions.

The increasing collaboration within the Cloud Center of Excellence can drive tremendous value such as faster adoption, faster time to value, more effective governance and program management; fewer hand-offs and accelerated decision making [4] [13][22].
From an organizational point of view, the Cloud Center of Excellence team will be placed within organizational structure of the enterprise. Consequently, it will be essential to understand the current organization by representing and defining: IT organization chart and the mission of the IT functions represented in the organization chart.

The organizational transformation of the enterprise due to the introduction of a cloud competence center goes through a transition phase, called the ramp-up phase, followed by a phase of team consolidation based on the experience acquired, called the stable phase.
The formation of the CCOE always involves the definition of new roles and skills to be placed within the current organizational structure.
Therefore, the organizational transformation can take place through:

- Identification and representation of the roles and IT functions impacted by the formation of a Cloud Center of Excellence in the ramp-up and stable phase;
- Definition of new roles to be placed within the organization in the ramp-up phase and in the stable phase.

5.2 Assessment of the actual organizational structure

In complex organizations it is common to have IT functions with an organizational structure in "silos", in which, areas or functions distinct by competence.
For example, an area of competence of networking separated from the area of competence of security, in turn separated from the area of competence of applications. An empirical example is shown below in figure 5.1.

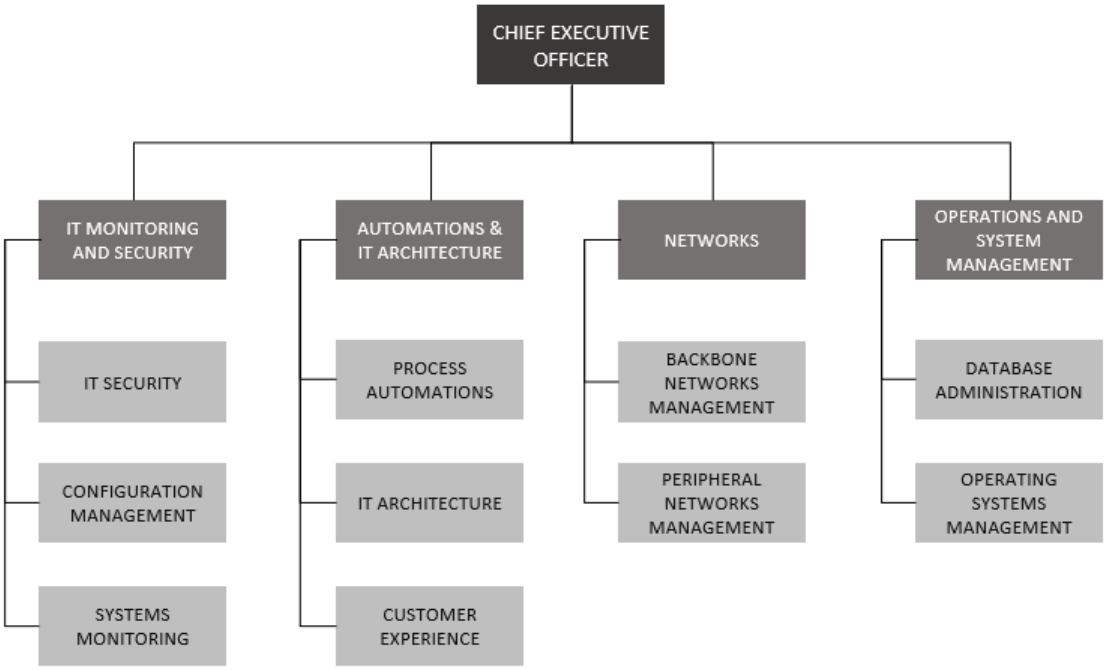

Figure 5.1 Example of IT organizational structure in "silos"

Teams belonging to different IT functions, in an organizational model "in silos", are focused only on their own outputs and their interests may not be aligned with the interests of other functions and teams belonging to the same organization.

This organizational structure leads the company to seek a local optimization rather than an overall optimization.
Moreover, different areas tend to adopt a perspective of separation, in which collaboration is reduced to an input-output mechanism in a model based on a rigid sequence of activities, like an assembly line or a waterfall process. Consequently, the organization needs specific and consolidated requirements before starting the sequence of activities.
In some cases, this approach is referred to as a "customer-supplier" logic. It was often employed by organizations operating in sectors based on economies of scale, stable markets and highly standardized processes.
However, in software development projects or implementations of cloud-based solutions, characterized by high uncertainty, need for rapid innovation and change, share of objectives and risk reduction through collaboration, this organizational model is not optimal.
Organizational silos can increase costs and times, and reduce the quality of service to final users. Software development requires the progressive acquisition of knowledge, and different skills to collaborate systematically throughout the project.
Another possible negative consequence of these organizational models for software development projects is the absence of an overall responsibility for the project. The functions in silos often lead to conflicts and negotiations between the various teams, reductions in efficiency and to a non-focus on the customer.
Therefore, the CCOE must introduce a new cultural mindset, based on greater collaboration among teams belonging to different IT functions, as well as new skills and competences, to arrive at a new organizational model that allows to exploit all the advantages of the technology.

5.3 Definition of Roles and Competences

The Cloud Center of Excellence can really differ across different enterprises. However, the CCOE team should start small, and it should be composed of people who are: experimentation-driven, which means to able to learn from failures and iterate quickly, not afraid to challenge the status quo of the organization, resulted oriented, customer focused and able to influence the entire organization.
Furthermore, CCOE team is usually composed of engineering with a strong technical skills and business strategy-oriented profiles that can improve the chances of creating a broad perspective.
In order to influence the organization, define the best practices for implementing and managing cloud-based solutions for the business and help with the migration of activities, the Cloud Center of Excellence introduces also new roles and competencies inside the organization that starts its cloud journey.
These can be built within the organization with training sections, which are likely to have a positive influence across the rest of the organization or they can be obtained from new hires or strategic partners. This will lead to gain the expertise and confidence to help organization understand and embrace the changing technology landscape.
The most common cloud roles and competencies, that will be deeply discussed in the following paragraph, are the following:

Stream	Cloud Role	Sourced from
Architecture	○ Cloud Enterprise Architect ○ Cloud Operations Architect ○ Cloud Security Architect	○ Enterprise Architect ○ Operations Architect ○ Security Architect
Infrastructure	○ Cloud Infrastructure Engineer	○ Compute Engineer ○ Storage Engineer ○ Network Engineer ○ Middleware Engineer ○ App Platform Engineer
Operations	○ Cloud Operations Engineer	○ Build/Release Engineer ○ Capacity Planner ○ Incident Management
Security	○ Cloud Security Engineer	○ Security Engineer ○ IAM Engineer ○ Policy & Compliance
Applications	○ Cloud Solutions Architect ○ Cloud Software Engineer	○ Enterprise Architect ○ Solutions Architect ○ Application Developer
Data	○ Cloud Data Engineer ○ Cloud AI/ML Engineer ○ Cloud Data Scientist	○ Data Platform Engineer ○ Database Admin ○ Data Architect ○ Data Scientist
Business/IT Alignment	○ Product Owner	○ Relationship Managers ○ Portfolio Managers ○ Senior Business Analyst
Project Management	○ Agile Scrum Master	○ Project Manager ○ Product Manager

Figure 5.2. Cloud Roles

5.4 Skills Gap Analysis

The roles and skills required for a successful cloud transformation are of particular interest to enterprises beginning their journey to a cloud-based transformation. As mentioned in Figure 5.2, the cloud roles and competences needed to set up a cloud center of excellence can be obtained from roles and competences typically present within an enterprise, through adaptation mechanisms, such as reskilling and upskilling plans, or through workforce onboarding plans.
At this purpose, a skill gap analysis can enable the enterprise to identify and match the skills needed to establish a Cloud Center of Excellence and reach a successful cloud-based transformation.
In order to conduct a skills gap analysis, the cloud roles with the related necessary competences, and how the latter differ from the skills potentially present within an organization have been illustrated.

Architecture

The *Cloud Enterprise Architect* works together to define business goals and creates the business infrastructure that supports those goals. Job responsibilities may involve assisting in the creation and execution of the information technology architecture roadmap. The Enterprise Architect must ensure that the right business infrastructure is created and that new applications meet all business standards.

Traditionally, an enterprise architect has competences in designing traditional architecture, such as multi-tier.
In cloud environments, a cloud enterprise architect must comprehend cloud architecture design, workflows, integrations and inter-service communications, native cloud application and managed services with their related integrations.

Infrastructure

The *Cloud Infrastructure Engineers* design and develop systems and networks in cloud environments. They develop cloud networks that store data remotely and on systems related to connecting clients to the cloud. Since they work with systems that access and store data online, they are also involved in making decisions regarding data storage and security.
In more legacy and traditional environments, competences regarding how to design and manage an IT infrastructure are held be several specialists that can be defined as compute engineers, storage engineers, network engineers, middleware engineers and app platform engineers.
In cloud environments, a team of cloud infrastructure engineers must combine the previously defined competences. Moreover, a cloud infrastructure engineer must develop knowledge regarding cloud managed services and related integrations, cloud basics, cloud network management, cloud storage management including how to define a backup strategy.

Operations

The *Cloud Operations Engineers* are in charge of supporting cloud-based software applications. They manage the resolution of system change requests, use infrastructure monitoring tools to respond to alerts and continually improve system stability. The DevOps approach, generally adopted, simplifies daily activities through the automation of operations.
Traditionally, specialists who are responsible for the IT infrastructure operation have networking backgrounds and knowledge regarding operating systems and cyber security.
In cloud environment, they must broaden their skills by embracing knowledge regarding:

- Cloud Basics
- Operations of IaaS solutions such as Virtual Machine recovery
- Managed service operations including knowledge in database as a service, native load balancing, autoscaling
- Native managed services dashboards such as metrics and alert
- Monitoring PaaS solutions
- Cloud storage management and operations such as resize volume, restore storage objects
- Disaster Recovery management

Security

The *Cloud Security Engineers* are responsible for identifying cloud platform security requirements and complying with risk management control objectives. They provide standardized solutions to facilitate continuous security and compliance within application stacks and the cloud environment. Finally, they integrate security standards and oversee products and offers.

Traditionally, IT security engineers are present within the organization, and they have competences in cyber security, identity and access management and active directory management.
In cloud environment, they must acquire knowledge regarding principles of cloud architecture, cloud security design, integration and functionality of managed services.

Application

The *Cloud Solution Architect* is responsible for global cloud technical architecture. He collaborates with the Product Manager to translate customer requirements into technical results. Furthermore, he is responsible for the technical deliver and establishing the technical direction. Traditionally, a solution architect has competences in scripting and in designing traditional IT architecture such as multi tiers. Moreover, he has knowledge of operating systems, networking and cyber security.
In cloud environments, a cloud solution architect owns skills and knowledge regarding:

- Cloud architecture design including autoscaling and automatic recovery
- Native cloud application
- Managed services and related integrations such as PaaS solutions
- Cloud base design including account definition strategy, virtual network design and security principles
- Cloud governance such as Access Control Lists and Identity and Access Management
- Cloud monitoring implementations
- Cost control and optimization
- Cloud adoption approach and plan

As far as the applications are concerned, the *Cloud Software Engineers* are responsible for coding and development of applications with knowledge of best practices of the cloud architecture. They are also involved in deploying and debugging cloud-based applications.
Traditionally, software engineers own knowledge of operating systems and capabilities in designing software.
In cloud environments, they must acquire competencies and knowledge in cloud native applications, in particular in scaling applications leveraging cloud resources and integrating managed services such as PaaS solutions for objects storage.

Data

The *Data Platform Engineer* provides continuous support for any coding needs for data processing and system interfaces. It must understand how machine learning will change data acquisition, system requirements and performance, as well as the customer experience for the systems, services and applications they support.
This profile develops the data architecture to acquire and process data and works directly with the data scientist to create documented goals, capabilities, time horizons, outputs, and other data-centric activities.
Traditionally, data platform engineers own competences in designing data pipeline and storing data.

In cloud environments, cloud data platform engineers must acquire skills and competences in: designing cloud architecture, native cloud applications, cloud data platforms and storing data in cloud.

Completely new roles, that cannot be sourced from existing IT roles, are also necessary. The most important ones are:

Cloud DevOps and Automation Engineers responsible for deployment of artifacts and stacks infrastructure as well as applications and their operations through the use of pipeline and CI/CD platform, configuration management platform, artifact/code repository and many other automation tools.
They have skills and competences regarding: cloud basics, managed services and related integrations with preexisting environments, infrastructure provisioning automations tools (Infrastructure as Code) and CI/CD approach.

Cloud Governance e Cost Control role oversees process in cloud such as cloud computing policy definition, cloud provider selection and relationships, cloud solution architecture designing, workload placement, and governance. It provides both guidelines and constraints that improve outcomes and manage risks. This profile defines and disseminates best practices within the organization.
This role is characterized by skills and knowledge regarding cloud basis, cloud architecture and cloud managed services.

5.5 Transformed organizational structure: Ramp-up phase

During the ramp-up phase, the CCOE, responsible for the research within the company of enthusiastic people, should be established together with a Cloud Governance team which in turn is responsible for the creation and acquisition of internal Cloud competencies to develop Cloud standards.
For almost every enterprise well established in the market, it is not common to have a dedicated CCOE team on day zero since it can alter the current organizational structure and corporate governance.
Moreover, it is advisable to establish at least one Cloud Center of Excellence head and a central Cloud Governance team. Then, the CCOE advises the internal teams which enthusiastic people to insert in the different fundamental roles for building the CCOE itself.
This will allow the team to both develop and build the necessary cloud skills and define cloud standards and policies internally to implement and manage cloud-based solutions.
From an organizational point of view, during the first phase, called ramp-up phase, the CCOE team is placed parallel to the current IT functions present in the organizational structure of the company. As a consequence, there will not be a strong impact on governance and on the AS-IS processes and organization, but still the team can positively influence and bring the cloud skills necessary for a successful transformation.
The Figure 5.3 shows an example of a part of the organizational structure of an enterprise, which is well-established in the market, with the allocation of the CCOE and Cloud Governance team during the ramp-up phase.

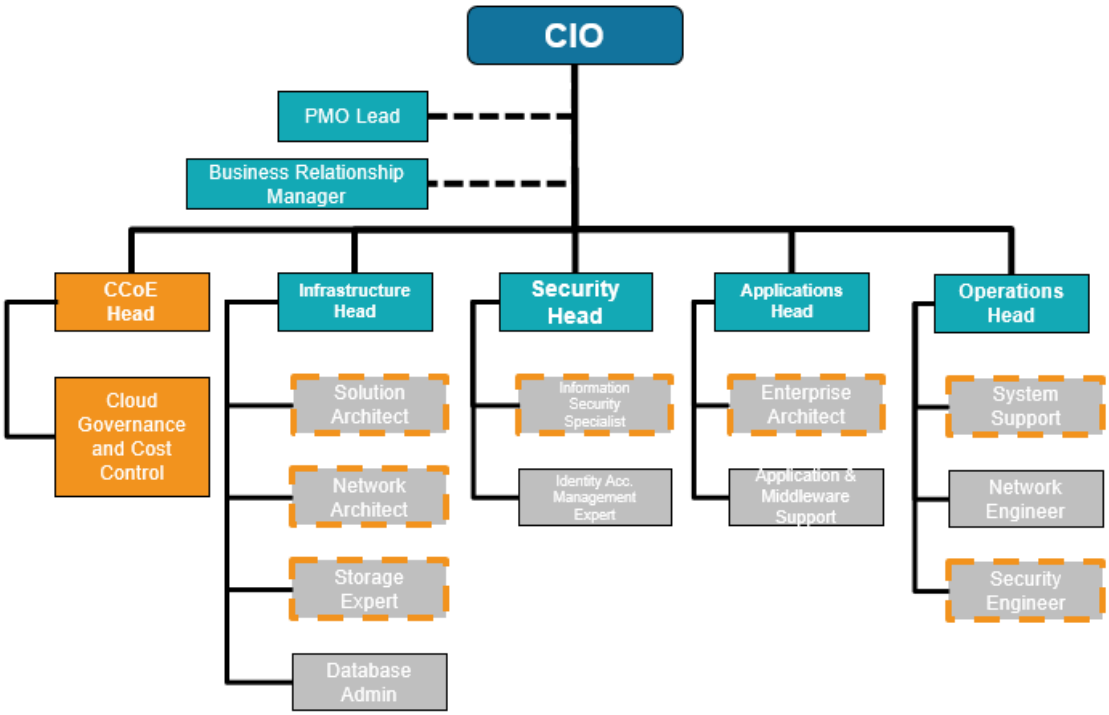

Figure 5.3 Cloud Center of Excellence in the rump-up phase.

In Figure 5.3, the gray boxes represent an IT role already present within the organizational structure of the enterprise before the adoption of cloud computing, while the orange boxes represent the roles and skills that the cloud competence center introduces. The graphic representation shows the IT roles that develop new skills and competences, and therefore are impacted by the introduction of the CCOE as gray boxes with a dashed orange border.
In this empirical example it can be noticed as the Cloud Center of Excellence, parallel to the IT functions and hierarchically below the Chief Information Officer, presents a CCOE Head and a function responsible for defining cloud governance and controlling costs.
The cloud competence center that provides standards and skills to the rest of the organization, positively influences and impacts other IT functions that will have to adapt their skills to be able to design, implement and manage cloud-based solutions in order to exploit all the advantages that this technology can offer compared to traditional IT infrastructures based on technologies on-premises.
In this study, it emerged that in the very first phase the IT Infrastructure function is particularly impacted by the CCOE building. In particular, in the roles of Solution Architect, Network Engineer and Storage Engineers, in accordance with the skill gap analysis.
The second particularly impacted function was the IT Security function, in particular, the role of Information Security Specialist, since it must correctly define the security policies and tools in the cloud.
Even the function that deals with software applications is immediately impacted, as the skills and abilities necessary to develop an application in the cloud can vary with respect to traditional

development methods. In particular, the Enterprise Solution Architect role will have to develop new competences and skills in accordance with skill gap analysis.
Finally, the Operations function is also impacted by the cloud competence center as the tools and practices for responding to alerts or tickets, that report IT infrastructure issues, change significantly in the cloud, especially thanks to the use of automation and cloud provider managed services.

5.6 Transformed organizational structure: Steady phase

The Cloud Center of Excellence allows to spread the cloud skills and competences within the organization and to define the standards for the design, implementation and management of cloud-based solutions. During the initial phase, the ramp-up phase, the CCOE team is usually placed parallel to the IT functions in the current organizational structure of the company.
Moreover, once some initial projects have been successfully completed using cloud approaches and practices and skills and competences have been successfully acquired, the rest of the organization should become eager to leverage the CCOE's services, tools and expertise for specific needs and problems.
However, companies must carefully plan this last critical step of scaling the CCOE function in the rest of the organization. The CCOE team placed in the organizational structure in parallel with the IT functions, could become a bottleneck for the rest of the organization in the adoption of cloud practices. Consequently, it will be necessary to consolidate the team based on the experience gained.
The new dedicated roles such as the DevOps engineer, Automation Engineer and Cloud Cost Optimization Expert must be permanently allocated in the organizational structure of the enterprise and no longer represent a separate team.
In Figure 5.4 below, the Cloud Center of Excellence is represented during the stable phase, which no longer represents a team separated from other IT functions, but it is a set of new roles and capabilities that the organization has adopted for a successful cloud-based transformation.

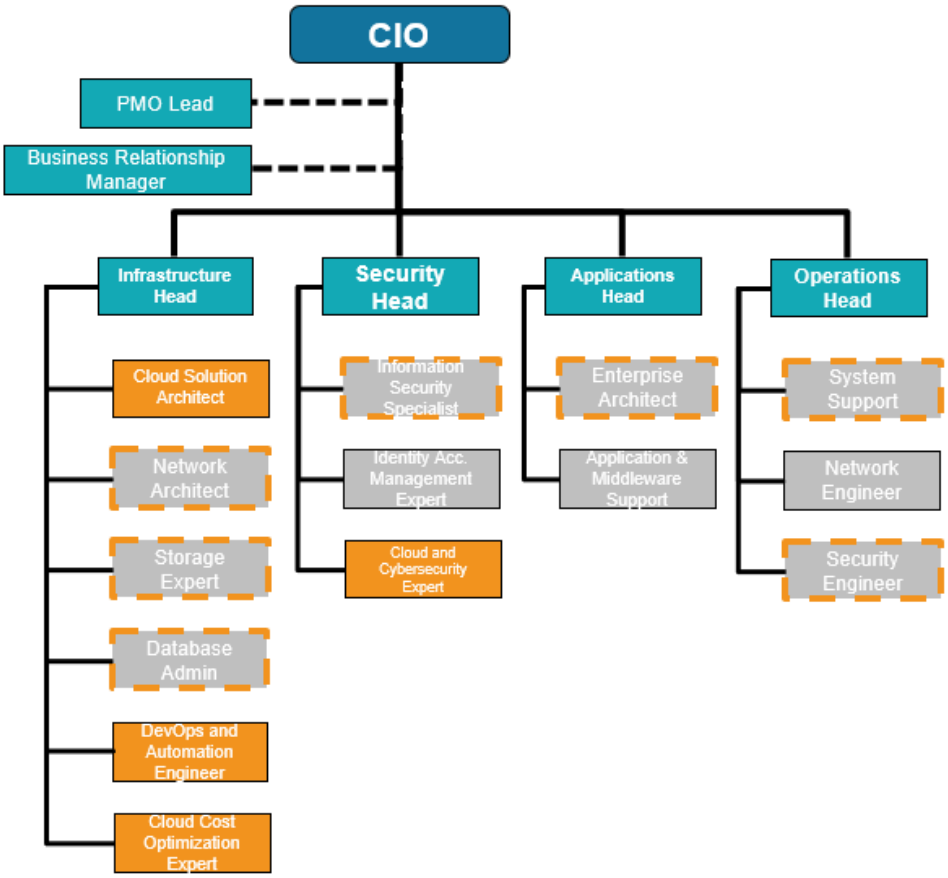

Figure 5.4 Cloud Center of Excellence in the steady phase.

In particular, the role of the DevOps and Automation Engineer who, through Infrastructure as Code, deal with infrastructure provisioning were introduced in the example shown. The role of Cloud Cost Optimization Expert, responsible for managing the costs of services and cloud infrastructure, is also part of the infrastructure function and it is no longer part of an external team.
Furthermore, in this empirical example, the figure of Cloud and Cyber Security Expert has been allocated who introduces policies, practices and tools necessary for IT security of cloud, according to the Shared Responsibility Models and based on enterprise's requirements.
Finally, it is important to notice that business roles can also be impacted by the introduction of the CCOE. In particular, the project manager must be able to manage projects with an agile approach, iterating and rapidly introducing changes several times to arrive at optimal solutions, rather than defining a rigid plan and control phases according to the more traditional waterfall project management methodology.

6. Cloud practices and methodologies

6.1 DevOps

A change of mindset for the organization necessary to exploit the advantages of cloud computing can be achieved by embracing the DevOps approach.
DevOps is a software development methodology that provides an organization with the ability to develop applications and services with greater agility and speed than traditional software development and infrastructure management processes.
According to a DevOps model, software development and production teams no longer act separately. In some cases, on the contrary, the two teams are merged into a unit responsible for the entire life cycle of the application, from development and testing to distribution and production. As a result, DevOps team members gain a range of skills that are not limited to a single IT function.

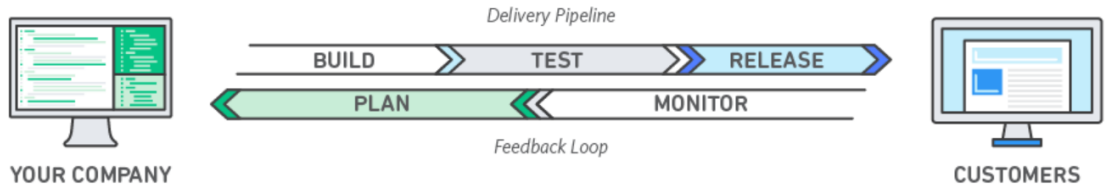

Figure 6.1. DevOps Model

Often, the same DevOps team is also in charge of product quality control and ensuring security at every stage of the software lifecycle, so the team can be called the DevSecOps team.
DevOps, in addition to bringing together software development and operation functions, rely heavily on automation to speed up processes. The DevOps team employs technologies and tools that enable them to develop, run and evolve applications quickly and reliably. These tools also help the team complete tasks, such as code distribution or infrastructure provisioning, that would normally have required the attention of other business units, further increasing efficiency of the organization.
Therefore, DevOps model introduces the following advantages:

Speed: more agile software lifecycle management processes to improve efficiency, innovation and better adapt to market changes.

Rapid distribution: increase the frequency of new releases to increase innovation and improve products. The faster release of new features and bug fixes can lead to an advantage over the competition by meeting customer needs first.

Reliability: faster processes and the use of automation for performance monitoring and control, ensure application updates and infrastructure changes that are always compliant with quality standards to ensure reliability and productivity without sacrificing the end-user experience.

Scalability: the consistency between different phases of the product life cycle and the use of automations allow to manage complex systems that are subject to change efficiently and containing risks. In a DevOps model, Infrastructure as Code is used to manage development, testing and production environments in a more efficient way and to allow iterations.

Improved collaboration: development and production teams can collaborate much more, share responsibilities and integrate their workflows. Moreover, causes of inefficiency are reduced and execution times are improved by reducing non-value-added activities.

Security: the DevOps model allows to increase the speed and agility of processes without giving up security, allowing the implementation of compliance policies, granular controls and configuration management techniques also through the use of Infrastructure as Code with which it is possible to monitor compliances at large scale [34].

6.2 CI/CD pipelines

Continuous Integration and Distribution pipelines (CI/CD) are procedures designed to optimize software delivery through the DevOps approach.
A CI/CD pipeline is divided into distinct subsets of activities, each of which constitutes a phase of the pipeline. Typical pipeline stages include:

- *Build*: the compiling phase of the application.
- *Test*: the stage where the code is tested. Here automation can save time and effort.
- *Release*: the stage in which the application is delivered to the repository.
- *Deployment*: in this phase the code is distributed to the production department.
- *Validation and Compliance*: The steps to validate a build depend on the needs of the organization.

Figure 6.2 CI/CD Pipeline

Continuous Integrations (CI) is an automation process for developers. Continuous integration process include phases for which new code is regularly built, tested and merged to a shared repository. CI helps find and address bugs quicker, improve software quality, and reduce the time to validate and release new software updates.
Continuous Delivery is a process that includes changes to an application done by developers. These changes are automatically tasted and uploaded to a repository or a container registry. The code can then be deployed into a live production environment.
Continuous delivery expands upon continuous integration by deploying all code changes to a testing environment and/or a production environment after the build stage. When properly

implemented, developers will always have a deployment-ready build artifact that has passed through a standardized test process.
Continuous Deployment, instead, refers to automatically releasing changes done by developers from repository to the production environment. Continuous Deployment process can really accelerate the reception of feedback from the final customer [20] [26].
An important advantage companies can gain from the adoption of DevOps models and CI/CD pipelines is the reduction of the lead time for changes, which represents the time spent from code commit to code successfully running in production environments.
Moreover, the combination of DevOps models and CI/CD pipeline can result in reduction of the change failure rate, which represents the percentage of changes committed to the production environment and results in degraded services requiring remediations, such as service impairment, outages [32].

6.3 FinOps

The introduction of cloud computing leads to a new cost model, named "pay as you go". Thanks to this cost model, the cloud customer avoids incurring massive investments in physical servers that could be underused and therefore represent an inefficiency and a waste of capital. Cloud customers are charged only for the actual use of IT resources.
However, this model has transformed capital expenditures (CAPEX) into variable expenses, or operational expenses (OPEX), which must be managed and controlled through new cost management methodologies to avoid incurring excessive expenses.
Most of the companies that had adopted the cloud computing risk exceeding their budget. This is due to loss of control and visibility of costs, unpredictable costs, wrong estimations and huge effort for manual processes.
A widely used model for cost management in the cloud is FinOps.
The FinOps model is a set of standards and best practices developed to help cloud professionals to manage and optimize the variable cloud economy, to facilitate collaboration, to make informed decisions and to bring value to the business.
This model introduces the FinOps Role, which is based on the idea of combining financial accountability with autonomous team delivery. Therefore, the FinOps team combine technical profiles with cost management roles.
Delivery teams can be made responsible not just for delivering, operating, securing and making sure that cloud-based solutions accomplish their objectives, but also for managing their costs, both fixed and variable.
In particular, the FinOps team is responsible for:

- Resource controls, which can be automated based on policies, that govern who can deploy resources and the process for identifying, monitoring, and categorizing the resources.
- Cost allocation to teams using cloud resources. This can shift the emphasis from the "IT as cost center" mentality to one of shared responsibility.
- Budgeting processes, which include reviewing budgets and realized costs, and then acting on them.

- Architecture optimization with the aim of continually refine workloads to be more cost-conscious to create better architected systems.
- Tagging and tagging enforcement to ensure cost tracking and visibility across organization lines.

FinOps model for cost management in cloud goes through 3 phases: inform, optimize and operate.

Inform: cloud costs can be extremely fluctuating over time. Thus, this phase offers cost visibility to all stakeholders by reporting the allocation of total cloud expenses. Cost visibility can be provided through the use of dashboards, reports and continuously monitoring the cloud services. However, cloud services can have complex pricing structures, centered around performance and resource availability time. The FinOps team must understand these cost structures and cross-reference them with operational requirements.
This phase leads to a granular cost allocation and tracking, allowing to define trends and analyzes for benchmarking and budgeting purposes.

Optimize: in this phase the team must take informed decisions to meet the organization needs. It is important to ensure that the size of resources matches operational needs, also leveraging automations. Furthermore, the team must rationalize the use of the cloud resources, for instance considering storage spaces and backup volumes, and ensure that all cloud resources are effectively used. This will lead to remove unused resources and rightsizing cloud resources and services. During this phase, the team also compares costs for different solutions, including refactoring the applications running on the cloud infrastructure, to meets both technical and business requirements.

Operate: the team must gain visibility of future needs of the organization, that can help to bargain discounts with the cloud services provider as well as define better governance and controls for cloud resources usage while continuously improve the efficiency and the innovation. The aim of this phase is to align financial, operational and governance goals in a continuous improvement perspective [36].

7. Cloud Target Operating Model

7.1 Traditional IT Operating Model

When accountability and processes are undefined or unknown, organizations risk both not addressing necessary tasks in time and employing redundant and potentially conflicting efforts to respond to customer needs. For this reason, organizations define their own operating model. The impact of the cloud-based technologies affects the entire organization including the information technology delivery structures. Therefore, establishing an operating model is critical to reach a successful adoption of cloud and delivering greater business agility [5] [7].
Introduction of a new technology can lead to a transformation of processes which in turn needs an organizational transformation. However, companies could continue to maintain their operating models by improving and adapting them to the presence of new technology. However, the improvement of operating models leads to an upper limit. To truly achieve a competitive advantage, it is necessary to embrace a new organizational mindset to define new operating models to support the corporate strategy by leveraging cloud technology.
Generally, drivers for the change of operating models might be:

CHANGING CUSTOMER RELATIONSHIP OR EXPERIENCE

For example, in banking sectors there will be less and less physical branches because banks services are delivered through mobile phone because of cloud computing. Thus, they are creating new digital products and services to serve customers in this new relationship.

CHANGING TECHNOLOGY

With the cloud adoption the way companies deliver products and services to customers has changed.

COMPETITION

There might be more competitors because of lower barriers to entry due to new technologies. Therefore, new competitors might provide customers with better product or services.

However, in the definition of a new operating model, it can be noted that the Business and IT functions pursue different objectives.
The perspective given by the business is always to increase the value of the company, increasing the market share, entering new markets and gaining new customers that allow the organization to increase profits. The business functions, therefore, pursue objectives such as: rapid marketing of innovative products and services, increasing the agility of processes in order to enter new markets and obtain new customers to increase the value of the company.
The IT operating models, on the other hand, aim to create technological solutions that are highly performing, secure and economical.
As a consequence, a Cloud Target Operating Model should also define how the Business and IT align their capabilities, processes, and workforce to reach strategic business outcomes.

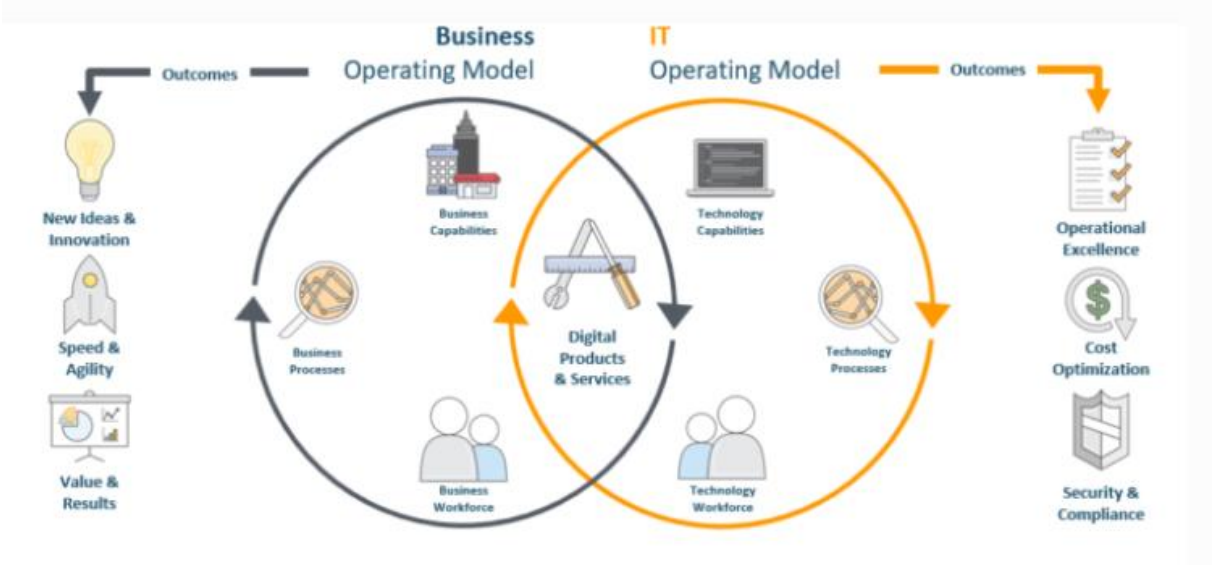

Figure 7.1 Operating Model from Business & IT perspective.

With the introduction of the cloud computing, the focus shifts to digital assets, rather than physical ones, and the workloads they support. Consequently, one of the purposes of the operating model is no longer to ensure the functioning of physical assets to meet business requirements, but to ensure consistent, reliable and secure operations.
Furthermore, traditional operating models can have many inefficiencies, slowdowns and bottlenecks. The team responsible for developing applications to meet business requirements have to communicate with the team in charge of providing computational, storage and network resources that build the IT infrastructure which the application will run on. The separation between engineering teams and the teams responsible for ensuring the operation of the product, represents a further inefficiency of the process. As a consequence, in many organizations there is the desire for greater collaboration among teams with the aim of improving the efficiency of processes by leveraging technology. However, it emerged that it is very difficult to eliminate the barriers between the “Engineering” and “Operations” teams as well as between “IT Infrastructure” and “Application” [35].

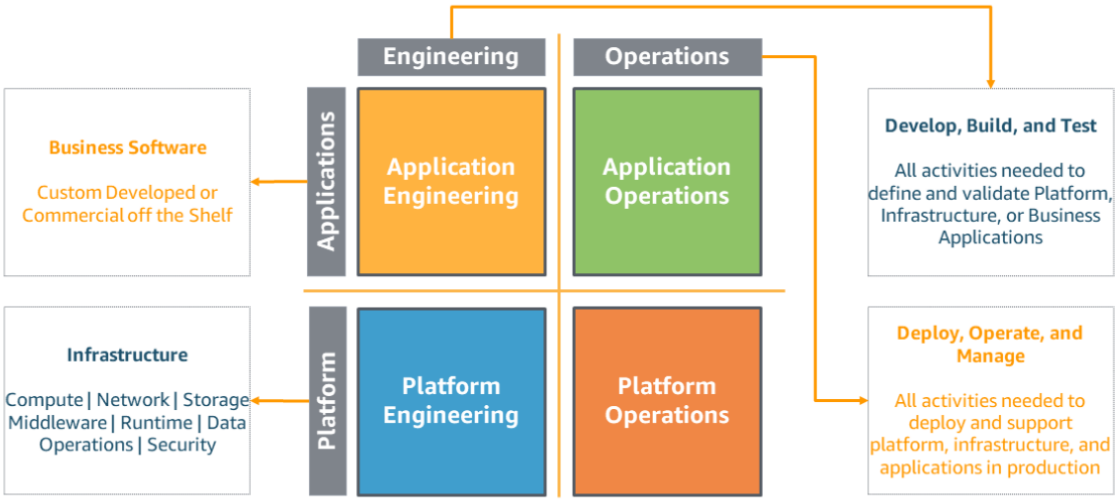

Figure 7.2 Traditional Operating Model

Figure 7.2 shows a traditional IT operating model. On the vertical axis, the distinction between applications and infrastructure has been presented. Applications refer to the workload involved in a business outcome and may consist of custom developed software. Infrastructure refers to physical and virtual IT infrastructure and other software that support that workload.
The distinction between engineering and operations phases has been represented on the horizontal axis. Engineering phase refers to the development, implementation and testing of applications and infrastructure. Operations consist of the deployment, updating and ongoing support of applications and infrastructure [35].
It is important to note that, in a traditional operating model, each box represents activities carried out by different teams separately. Work is transferred from one team to another through mechanisms such as job requests, work queues, tickets or using an IT service management system (ITSM).
Requests from other teams tend to be postponed until they become a priority. Defects identified late may require significant rework and a second step through the same teams and their functions. If there are incidents that require action from the technical teams, their responses are delayed by the delivery activity.
When business, development, and operations teams are organized around the activities or functions performed, there is a greater risk of misalignment. This can lead teams to focus on their specific responsibilities rather than on achieving business results. Teams can be highly specialized, physically isolated or logically isolated, hindering communication and collaboration [7].
Widely used Cloud Target Operating Models have been discussed in the following sections.

7.2 Transitional Model

To overcome the problems of the traditional operating model, it is possible to adopt operating models that take advantage of cloud-based infrastructure.
A widely adopted operating model, arises from the evolution of traditional operating models, while leveraging the advantage of having a virtualized IT infrastructure. In this model, often

referred to as the “transitional” model, cloud technologies have enabled infrastructure engineering teams to be responsible for both the design and operation of IT platforms to support the application teams. Therefore, this model, as well as the next models that will be discussed, follows a “you build it you run it” methodology.
This greatly reduces the complexity of processes, the number of non-value-added activities and delays during the implementation and management phases of the IT infrastructure.

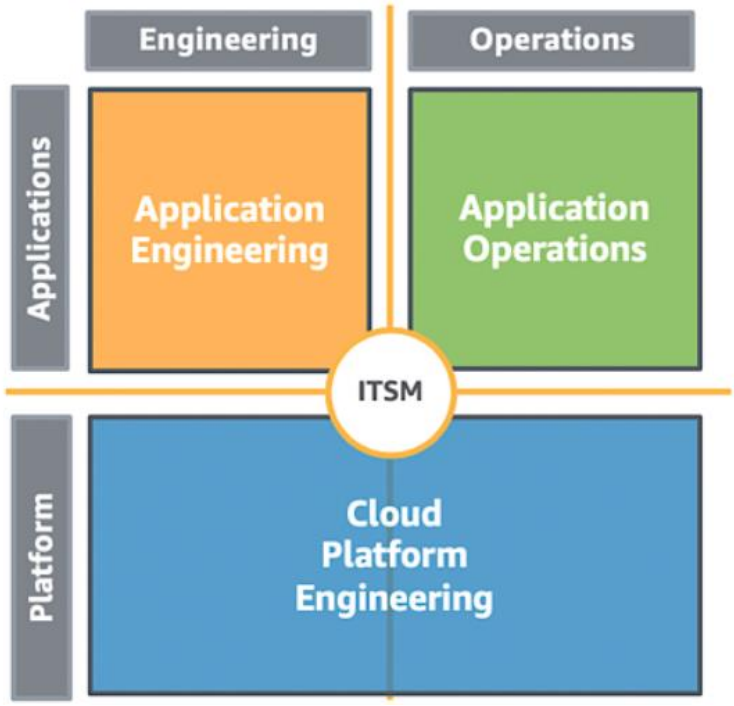

Figure 7.3 Transitional Cloud Operating Model

This operating model still involves collaboration and interaction between different teams. The management of IT processes is often done through the use of the ITSM discipline [10].

7.3 Centralized Model

The most used model presents an application engineers team who is responsible for the design, implementation, and operability of its own workloads. Similarly, the infrastructure team performs both the engineering and operations of the cloud platform to support the applications team.

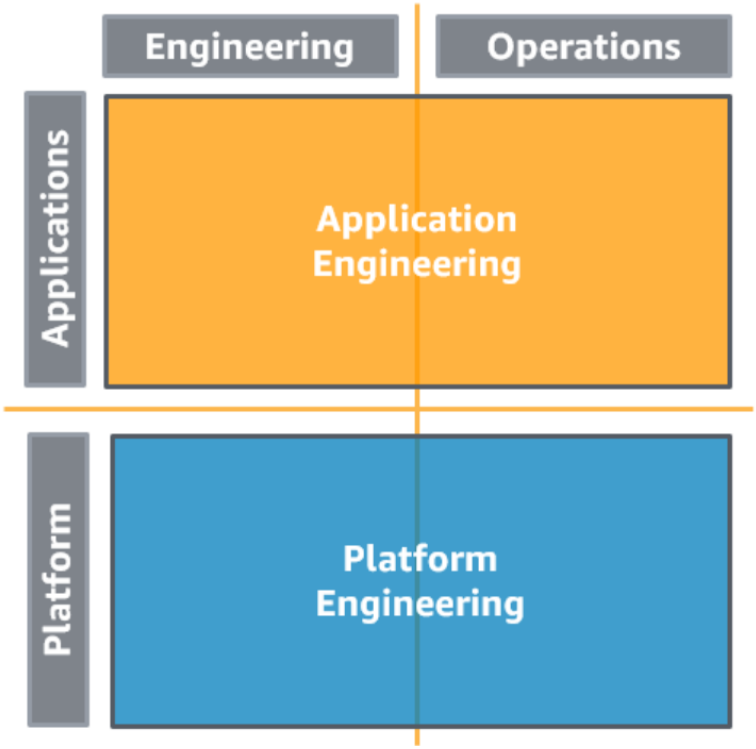

Figure 7.4 Centralized governance cloud operating model.

This model is defined as "centralized" governance as the standards and policies for the configuration, access and use of infrastructure resources are defined, distributed and shared centrally by the cloud platform engineering team.
Moreover, according to this model, the platform engineering team provides a standardized set of services, such as development tools, monitoring tools, backup and recovery tools, network configurations to the application team.
This model also fosters communication between application teams and infrastructure teams. In fact, the cloud platform team provides the application team with complete visibility of the infrastructure stack allowing them to distinguish problems related to application components from problems infrastructure components consumed by the applications. In addition, the cloud platform team can also support in configuring the cloud services used by the application teams and guide them on how to improve the operation of applications.
This model also ensures greater collaboration between the applications team and final customers. Workflow management can take place through direct or indirect interaction with customers, for example through requests for new features or requests for support. This increased exposure of the applications team to the end customer allows for a customer-centric approach from the earliest stages of application development, to address problems more quickly, and to achieve faster innovation [7].

7.4 Centralized Model with Managed Services

According to this model, the application team is responsible for both engineering and workload operations.

However, the organization may not have the skills to support a team that have to deal with the engineering and operations of a dedicated cloud platform. Additionally, many organizations prefer to have a platform team responsible for building resources that will differentiate the business and to transfer undifferentiated day-to-day operations to an outsourcer.
Managed service providers provide experts who implement the cloud environment, support security aspects and compliance requirements, and help organization achieve business goals through the cloud computing.

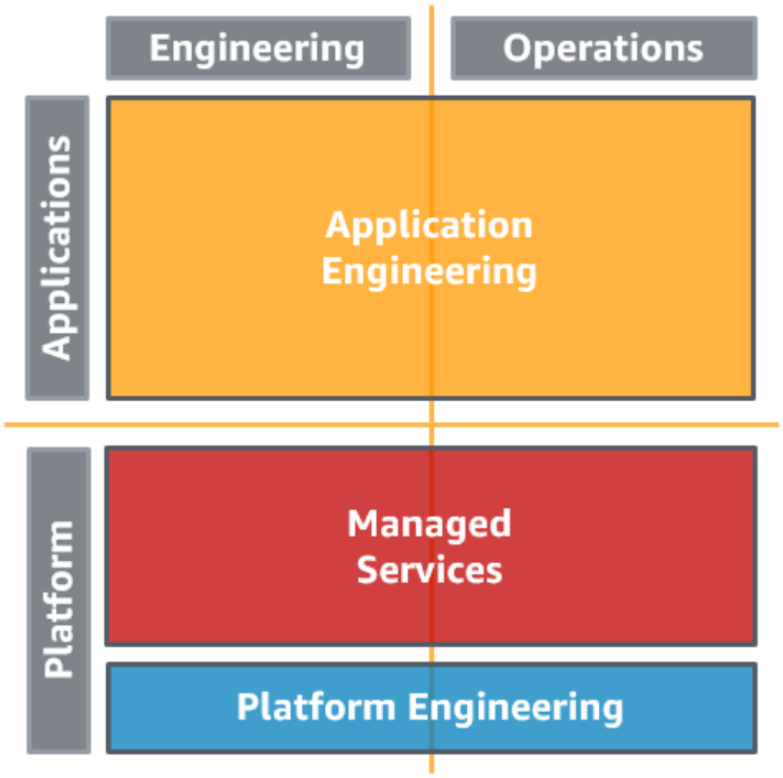

Figure 7.4 Centralized governance cloud operating model with managed services.

This model requires changing the work mechanisms to efficiently collaborate with the managed services provider. This cannot solve the bottlenecks and delays created by the transition of activities between teams, including the service provider, nor the potential rework related to late identification of defects.
However, it is possible to take advantage of the standards, best practices, processes and skills provided by managed service providers.
Therefore, the addition of managed services to the operating model allows to keep the teams lean and focused on the strategic results that differentiate the activities of the organization rather than on the development of new skills and functionalities [7].

7.5 Decentralized Model

In this model application team is responsible for developing and operating applications, but in order to avoid stifling innovation for high-growth areas of the company, they are empowered to build out infrastructural resources that have not yet been standardized by the Cloud Platform

Engineering team. The Cloud Platform Engineering team is still responsible for engineering and operating the cloud platform and provide standard policies that prevent Application teams from configuring Services from scratch.

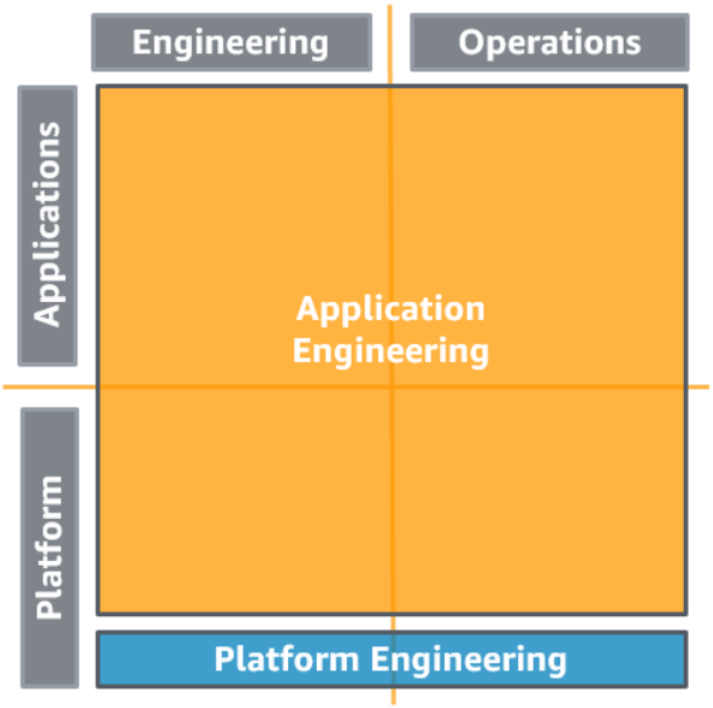

Figure 7.6 Decentralized governance cloud operating model

This operating model is defined as decentralized governance as the standards and policies for the configuration, access and use of infrastructure resources are still defined, distributed and shared to the application team by the platform team, but the application team may request additions and changes to these standards.
It is important to note that these requests for changes in standards and policies could also benefit other application teams.
In addition, the application team needs to develop new skills and potentially employ new members to define and support the additional functionalities of the platform. The risk of significant rework could otherwise increase if skills and capabilities are not adequate and defects are not recognized early.
The platform teams may provide direct support for these additional infrastructural functionalities, which in turn represents an effective support for business outcomes.
This model limits the constraints on innovation through the acquisition of significant skills by the application team. It helps reduce bottlenecks and delays created by the transition of activities between teams, while promoting the development of effective relationships between teams and customers.
It is important to note that whenever the application team is responsible for both the development and the operations of the application, the DevOps approach takes place. Therefore, the application team is usually referred to as DevOps team [7].

7.6 Transformational Steps to build a Cloud Target Operating Model

As already stated in previous section, the correct introduction of the Cloud Competence Center allows the organization to facilitate, support and accelerate the delivery of business outcomes by leveraging the advantages of cloud technology. The CCOE must be able to establish a new mindset within the organization to finally define the correct target operating model that allows the organization to truly achieve a competitive advantage.
Some of the most important principles that the CCOE must be able to establish within an organization to allow them to define a successful target operating model are described below.

Customer Centric Approach

One of the main objectives of the operating models is to provide the customer with an innovative, cost effective, reliable and secure product by leveraging the processes, resources and organizational structure of the enterprise.
Organizations that provide software solutions very often do not know what their customers need and what they consider as valuable. Consequently, these companies will have to rely on statistical estimation and inference techniques to gain a better understanding of customers. However, these approaches lead to a high probability of error.
To be a company with a customer centric approach, it is necessary to know the needs of customers, their pain points. It would be necessary to have and use data to make more informed decisions. This can also be achieved by providing products that can be easily modified with an agile approach. Furthermore, many studies have shown how important it is to create customizable solutions and at the same time innovative, without however jeopardizing the security and reliability of the cloud-based products consumed or used by cloud customers for business needs [10].

Product-based approach

Almost all successful cloud operating models have a peculiarity since they are based on a product-based approach. The product-based approach allows the organization to significantly reduce process inefficiencies and non-value-added activities. According to this model, each component of a system can be considered as a product. As a result, it will be possible to establish cross-functional product teams that have full responsibility for all aspects of the product throughout its life cycle. This greatly limits the number of interactions and the need to communicate between different teams, making processes more streamlined and flexible that can better respond to changes and customer needs.

According to Amazon Web Services (AWS) an IT product must:

1. Perform a limited number of tasks
2. Allow to define its inputs and outputs
3. Be useful to more customers
4. Continuously improvable to meet customer needs.

The teams responsible for the product life cycle will be able to understand and solve related problems and increase the perception of the product by customers.

For many organizations, the creation of product teams could be very complicated as they are used to working on a design basis or on a set of more complex systems. Therefore, to correctly establish a product-based mindset, the organization must be able to define products for which a single small team is responsible as well as spread a culture of accountability, empowerment, and self-reliance for each product team with the aim to exceed expectations regardless of any dependencies or other leveraged products or services.
It is important to note that product teams need to be small. Product teams are created with the aim of significantly increasing communication and collaboration between members responsible for product delivery and management. The ability to deliver software solutions that quickly meet business needs can really be a differentiating factor for the organization. Consequently, when a software product needs to be released, fixed or improved, the organization has to introduce rapid processes that reduce time-to-market. Hence, a small team allow to achieve this by encouraging better communication, coordination and collaboration between members who own the product and between the different product teams.
This new cultural approach appears to be very similar to the one that led to the introduction of the DevOps model which has also broken down organizational silos, the main cause of slowdowns in processes and product innovation.
Successful product-based operating models must ensure that all processes, tools and skills needed by the product team to have full ownership of the product have been consistently established. Therefore, each product team will have to present all the roles and skills necessary to deliver the product and to improve it over time.
Product teams introduced a further change in organizational mindset. The product teams, in fact, encouraged product experimentation. If an undesirable result can be immediately recovered by introducing changes to the product, then the product team is encouraged to experiment. This will lead to accelerates learning and innovation.
This organization of teams around products encourages cross-functional team members to maintain and expand their skills to adopt new technology solutions for the product. The expansion of skills is often a source of satisfaction for team members and supports innovation. The cross-functional team also allows members to acquire transversal competences that reduce the risk of under-skilling of the product team in the event of the loss of a member [10].

Iterations and Automations

Adoption of a new operating model is a process that usually evolves over time according to the principle of continuous improvement.
Product teams are responsible for their own products but to ensure the correct functioning of the entire system, as a set of products, the product team must guarantee and meet some standards of operations. The measurement of product standards remains an activity for which the product team is responsible. To ensure compliance of the products with the defined policies and standards, the product team will have to carry out periodic tests and eventually make changes, iterating on the solution until the optimal solution is reached in compliance with standards and organizational policies.
These tests and changes to the product in the cloud are supposed to be carried out through the use of automation and using the Infrastructure as Code approach, which allow for more lean, agile and rapid processes, reducing process inefficiencies [10].

7.7 Aligning IT operating model with Business goals

Most companies nowadays have started their transformation to become a digital business by serving their customers and employees through digital resources. This does not necessarily mean that the products or services are digital, but it does mean that the consumer and employee experience is becoming increasingly digitized.
Digital transformations occur in every industry, such as financial, manufacturing, government that are using digital resources to improve the customer and employee experience or to gain a competitive advantage.
A good example is the banking sector. Today each bank has digital services that give access to banking services and products.
This digital transformation relies on software applications to provide the digital components and foundation for digital business. Applications can be considered the engine of a digital transformation.
Therefore, topics such as application development or modernization and application hosting location define the application strategy that supports companies need to become a digital company [3].
The adoption of cloud computing allows the organization to migrate application workloads to a virtualized infrastructure that allows for advantages such as scalability, flexibility, reliability and cost reduction.
However, there are several methods of migrating workloads to a cloud platform.
The simplest methodology is called Rehosting. This methodology consists of running the same software application on the cloud infrastructure, without making any changes or optimizations. However, this methodology allows to obtain advantages given by the elastic infrastructure that could reduce the total costs of ownership of the application.
The second methodology, that is usually adopted to migrate preexisting workloads to the cloud, is called Replatforming. This methodology performs application optimizations without affecting the core code.
An application workload migration methodology widely adopted by organizations is called Refactoring. This methodology involves reimagining how the app can be redesigned and developed using cloud native features. Refactoring is always driven by a strong business need to add features, scale or other performance needs that would otherwise be difficult to achieve with current IT infrastructures running the app. These huge architectural changes can be a big benefit as well as expensive.
An alternative methodology for migrating application workloads is called Repurchase. This repurchase of apps indicates the traditional Software as a Service model. For example, it is possible to terminate the CRM contract and switch to a new service completely in the cloud.
It is important to note that some software applications may take time to implement and may require upfront costs, even though the several benefits could be reached in the future.
It is also important to mention the Retire and Retain methodologies, respectively with which the application is discharged or maintained on the current traditional infrastructure on premises for a limited time span.
Application workload migration methods must be considered when choosing the target cloud operating model. This choice represents an important opportunity to align business objectives with the objectives of IT functions.

At this purpose, it is possible to note that the traditional operating model is appropriate for rehosting migration strategies, as no changes are made to the application. However, the team responsible for the infrastructure is in charge of building the cloud infrastructure, therefore it is possible to create only one team that, with the help of automation, can be responsible for the provisioning and operations of the cloud infrastructure.
If the organization needs to optimize the application workload by leveraging cloud technologies and using a migration strategy that improve the application, an operational model that introduces the role of DevOps responsible for both development and operations is more likely to be adopted.
Amazon Web Services (AWS), following these considerations, proposed the following operating models based on the migration to cloud strategies of the application workloads to align the business and IT objectives, as shown in the Figure below [1].

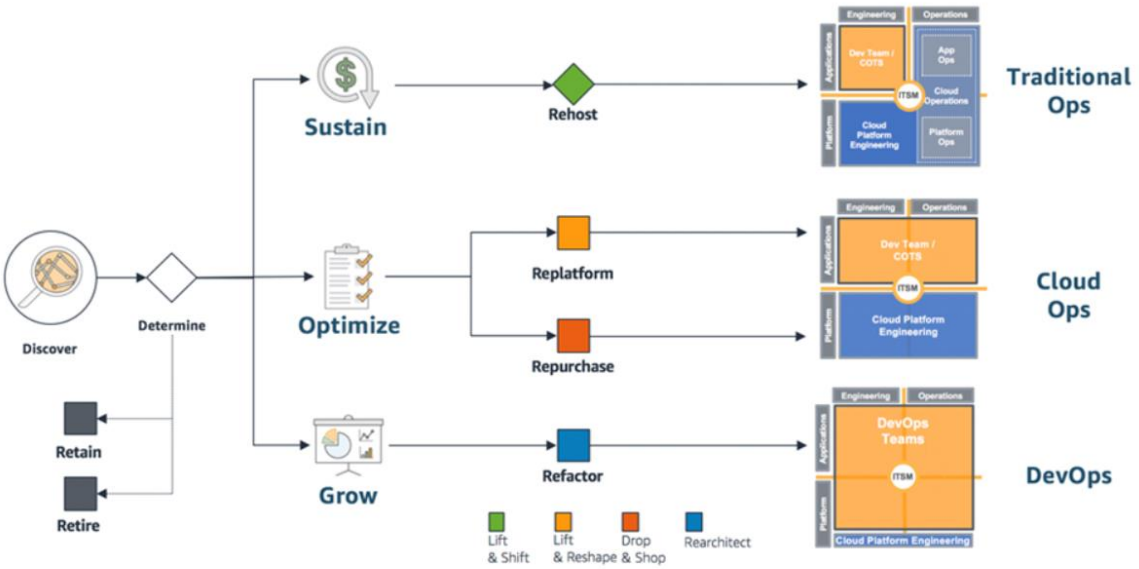

Figure 7.7 AWS strategies to align business and IT goals.

8. Spotify Organizational Framework

8.1 Introduction to the Spotify Organizational Framework

Digital transformations, such as the adoption of the cloud computing, impose the need to continually adapt and respond appropriately to frequently changes in the markets by leveraging the technologies.
The target cloud operating models presented in the previous section are intended to provide the organization with agility, speed and flexibility.
The adoption of the cloud has allowed the organization to manage the virtual infrastructure as software to meet business needs.
Software development projects have always been considered characterized by complexity and uncertainty. Agile practices and organizational redesign have been widely adopted in software development environments as opposed to traditional project and organization management methodologies, to deliver higher quality products and services to the end customer quickly and more frequently.
Agile methodologies attempt to reduce the risk of failure of the product created, by iterating on the solution and providing small increases in the functionality of the product, allowing the organization to retrace its steps or adapt to the real needs of the customer without particular complications.
The formalization of the principles and practices on which agile methodologies are based have been the subject of the work of a group of software designers and have been formalized and are now present in *The Agile Manifesto*.
Some of the most important practices reported into *The Agile Manifesto* are: formulation of value stories, removing complexity, shortening release cycles to incorporate customer feedback, and the estimation with story points to reduce effort estimation complexity.
Agile practices and a product-based approach are the fundamental principles that the entire organization must fully understand and adopt in order to achieve a new organizational mindset necessary to define and embrace a successful cloud operating model.
For this purpose, an organizational framework widely adopted by enterprises starting their journey to cloud is called the Spotify Model.
Spotify is one of the largest and most popular audio streaming services in the world. A key success aspect of this company has been its unique approach to organizing work to improve team agility. The organizational mindset proposed by this company was originally based on the idea of maintaining the agile and product-based approach despite the organization was scaling over to an increasingly number of teams involved in products development across the world [9] [15].

8.2 Squads, Tribes, Chapters and Guilds

The Spotify model defines the *Squad* as the smallest unit of an agile organization. The squad is very similar to a Scrum team. Scrum is the most adopted agile framework in software development where it is very difficult to plan.
Therefore, Squad are completely autonomous teams that represent a mini-startup. Squad members have all the skills and tools needed to design, develop, test, and release to production.

They are a self-organizing team and decide their own way of working, indeed, some use Scrum sprints, some use Kanban, some use a mix of these approaches.
Each Squad must define a long-term mission such as increasing the application client satisfaction.
Squad always operate with an agile approach, for instance, they are used to building an MVP (Minimum Viable Product) in order to collect customers feedbacks.
The main aspect of the Squads is the need to be a completely autonomous, cross-functional team, with full responsibility and a minimum of dependence with the other Squads. This model also employs very small teams, in this case called Squads, to facilitate the efficiency of processes, communication and coordination. They always present the following agile roles:

Product owner (PO): who represents the customer and ensures that the product delivers business value. He acts as customer and prioritizes work. The PO defines and accepts the products features.

Scrum master: who ensures that Scrum is understood and enacted. He facilitates the Scrum methodology by supporting team events and coaching.

Operative team members: who are able to design, build, test, integrate, maintain, and operate the product.

For instance, a Squad can be made responsible for an entire application life cycle.

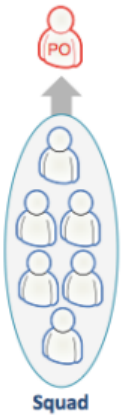

Figure 8.1 Spotify Squad

After Squad based on product have been set up, it can be possible to define a *Tribe*.
A Tribe is a group of squads with similar business interest and responsibility for a product area consisting of several related products. A tribe usually consists of 8 to 12 squads.
Spotify has defined its Tribe as an “incubator” for the Squads. Each Tribe has a Tribe Lead who is responsible for ensuring the best operating conditions for the Squads within the Tribe. The Tribe Lead has strategic responsibilities for pursuing business objectives within the assigned budget, managing the teams, and the creation and delivery of the products and services through the coordinated work of the Tribe. Tribe Leads from different Tribes meet to discuss progress, potential problems, joint plans and portfolio management of initiatives.

It is advisable that Squads belonging to the same Tribe are located within the same building, with the Squads physically positioned close to each other to facilitate collaboration and decision-making processes.
The definition of completely autonomous small teams, however, has the disadvantage of losing economies of scale.
In addition, the squads, despite being autonomous teams and almost not dependent on other teams, can communicate and collaborate with other teams within the organization to share knowledge, feedback and suggestions.
At this purpose, *Chapters* can be defined inside this organizational model. They promote team collaboration and innovation and ensure methodological consistency across Squads or Tribes. Chapters usually form around functional skills.
As an example, very often each product team, that is the Squad, has Marketing skills. Therefore, all the members of different squads can form the Marketing Chapter.
Each chapter present a chapter lead. The chapter lead is line manager for his chapter members, with all the traditional responsibilities such as training employees and setting salaries. However, the chapter lead is also part of a squad and is involved in the day-to-day work, which helps him stay in touch with team members.

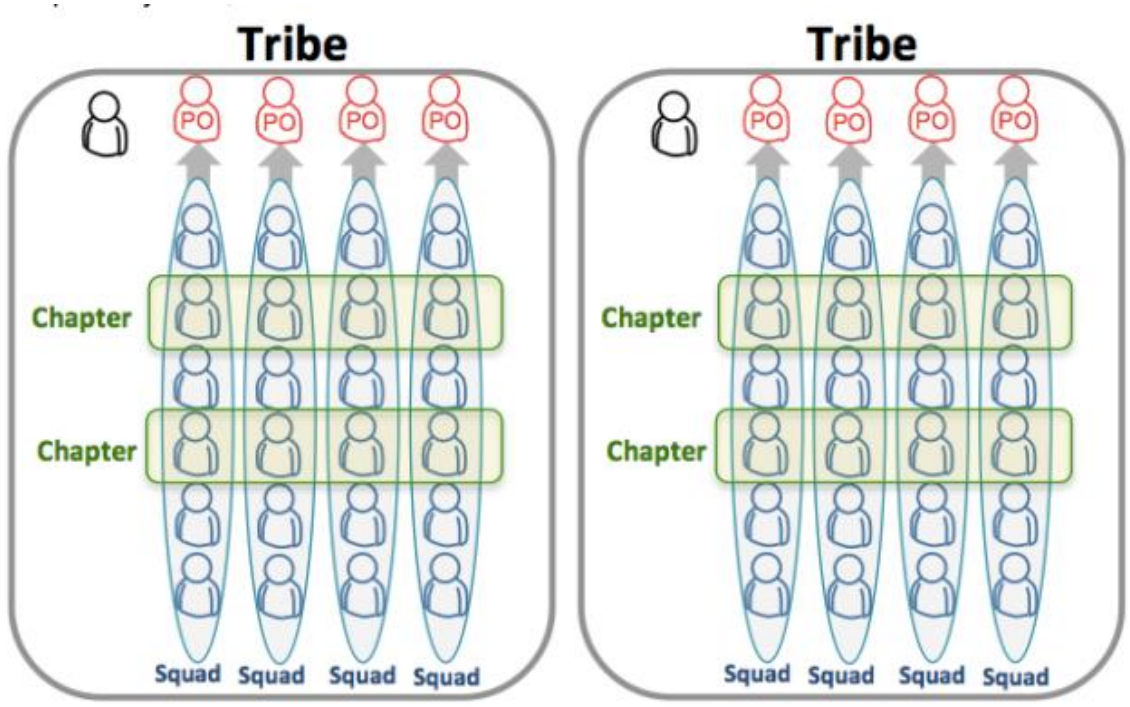

Figure 8.2 Spotify Tribes, Chapters and Squads

The sharing of experiences and knowledge acquired, according to the Spotify organizational model, are also favored by the formation of the *Guilds*.
The Guilds consist of groups of people, belonging to any area or tribe of the company, who share a common interest and meet, self-organizing, to increase their knowledge and share new practices and approaches.

It is important to notice as Chapters are always local to a Tribe, while a Guild usually cuts across the whole organization. Some examples are: the web technology guild, the tester guild, the agile coach guild.
Actually, a Guild often includes all the chapters working in that area and their members, for example the testing guild includes all the testers in all testing chapters, but anybody who is interested can join any guild.

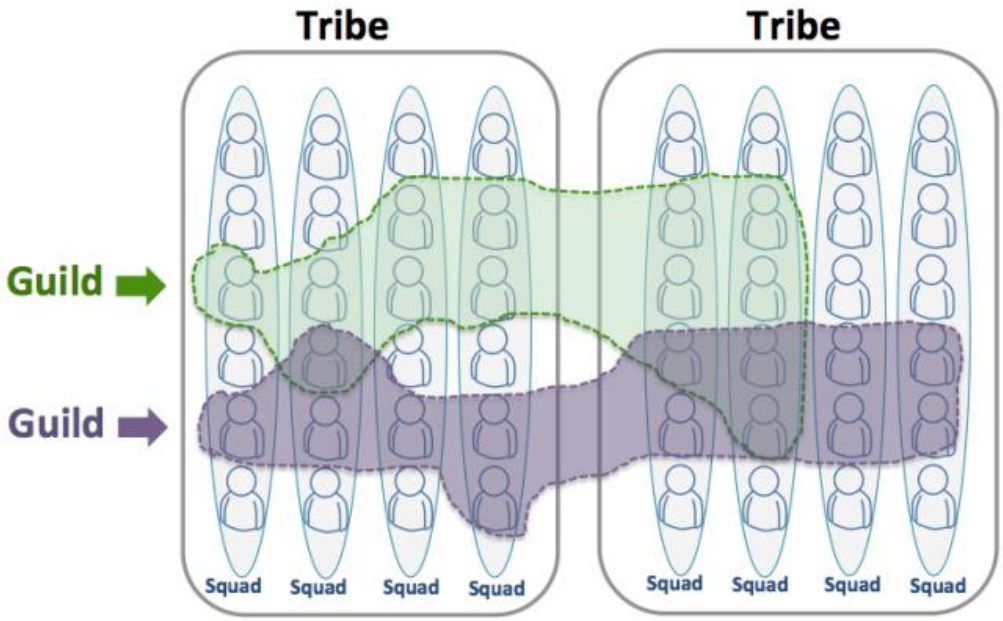

Figure 8.3 Spotify Guilds

The organizational framework proposed by Spotify is widely adopted for cloud-based transformations as it allows the technical teams to understand the contribution they offer in achieving business results. It also allows team members to understand decision-making processes, focus efforts and optimize business processes.
In addition, the definition of product teams through the adoption of the Spotify framework allows the organization to adopt different operating models based on the number of product teams.
It can be concluded that the organizational model proposed by Spotify has the following advantages:
First, the teams have all the necessary resources to make decisions related to the product. This greatly speeds up decisions making and implementation processes because all valuable decisions can be made within the team. Second, the problem of "functional silos" is reduced as teams are made up of all the human resources needed to cover the product value chain. Third, team members have a common interest in realizing valuable product since all of them would suffer from defective product.
However, the model also has disadvantages: while teams would ideally have all the resources and skills needed for product delivery, teams might depend on specialists for specific needs. In addition, the full autonomy of the teams for all decisions relating to the product includes complete freedom in defining IT architecture or in the DevOps toolchain used. This could lead to a lack of standardization and synergies between teams [15].

9. A real case study

9.1 Business needs

This chapter describes a cultural, organizational and process transformation following the adoption of cloud computing starting from the real needs of the company followed during the thesis experience.
The project followed as consultant intern to write this thesis was conducted for a client-company operating in the Financial Services Industry. The project was based on defining a cloud strategy and understanding how to implement it.
The project started from the definition of the following requirements, which were also the reasons why the company decided to adopt cloud technology for the management of its workloads:

- Products modernization
- Reliability of services
- Costs saving
- Global distribution
- Reduction of operational management
- Increase in security of services
- Scalability and performance of services
- Imposition by the CEO
- Compliance with regulations
- Time-to-market reduction

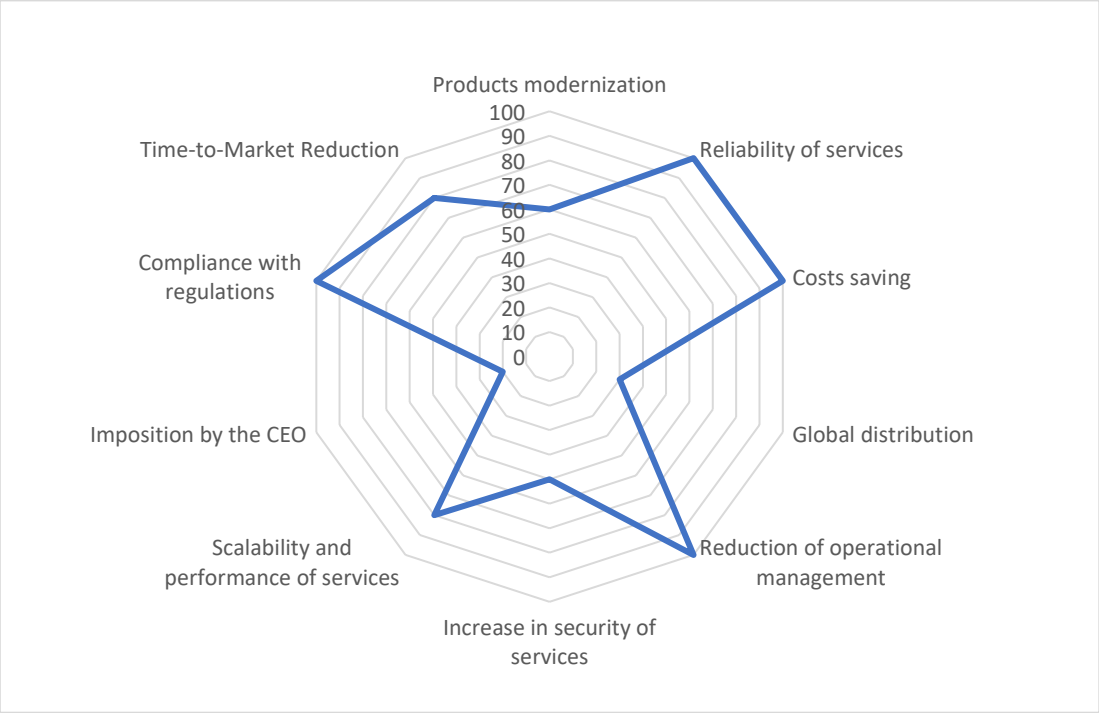

Figure 9.1 Company requirements and concerns that guided the cloud strategy.

For the company operating in the Financial Service Industry, which is a really regulated sector, *compliance with regulations* and *reliability of services* provided to end customers have been the most important requirements, as shown in Figure 9.1, for this cloud adoption project.
Moreover, the figure has shown that also *cost saving* and *reduction of operational management* have been considered highly important for the company. The reason for that is the increasing digitalization of the sector. Indeed today, online banking, online insurance services and other digital services have increasingly taken place in this sector leading to an increase in costs and operational efforts for companies. However, due to this rapid digitalization of the market, the company has considered *time-to-market reduction* and *scalability and performances of services* important to reach more customers and gain market shares.
Product modernization has been considered as medium-priority requirements since the company was already running new digital products to serve the market. Furthermore, digital products provided by the company were already very secure, therefore the organization found no reason to improve the *level of security*. Finally, the potential *global distribution* of the products and the *imposition by the CEO* were considered as the lowest-priority concerns for taking the cloud adoption project by the company.
The reasons for choosing cloud computing and how cloud-based solutions have met the company needs are described below.

9.2 Approaches and methodologies adopted

The company studied in this business case provides two types of products:

1. IT infrastructure on which the end customer develops and manages his own applications.
2. Software solutions developed and managed on behalf of the end customer on IT infrastructure.

As previously stated, it operates in the Financial Services Industry, therefore it provides products to customers such as banks, insurance companies and financial institutions. These end customers use specific services nationwide, so even if cloud-based software products could have been spread globally, the company preferred to employ a single Region of the Cloud Services Provider to manage its workloads.
The cloud adoption project has been considered as strategic in a view of digital transformation, by the top-executive and the CEO of the organization and supported by its IT departments who have made their own technological considerations.
The first fundamental requirement that the company exposed, considering its end customers, was the need to provide solutions that comply with regulations, including the GDPR. The selected Cloud Services Provider (the possibility of having multi cloud solutions in the future has not been excluded) has provided all the documentation audited by third parties to provide solutions that comply with current regulations.
Another fundamental requirement that the company expressed was the need to provide products to its customers that were extremely reliable and at the same time flexible and performing. In particular, it emerged the need to provide software solutions based on an infrastructure that scales if the workload increases or decreases without losing any request from end customers.

As reported in the previous chapters, a cloud infrastructure allows customers to achieve some advantages, which is the reason why the company has decided to adopt this technology.
In particular, a cloud infrastructure is considered elastic as it can increase and decrease the amount and capacity of resources to run application workloads. As a result, in the peak demand periods that software applications must handle, the infrastructure would have been able to scale to handle those requests.
The cloud infrastructure is also considered more reliable than a legacy IT infrastructure managed by the company on premises. The reason is that if a machine inside the cloud services provider's data center failed, the workload is immediately managed by another machine according to a clearly defined business continuity plan. Consequently, even the software applications developed and managed on top of the cloud infrastructure would have been more reliable and performing.
The security requirement was also particularly important for the company. As stated in the previous paragraph, the digital products provided by the company before the adoption of cloud computing were already very secure so it was necessary to maintain at least that level of security.
Regarding this aspect, security has actually increased due to the shared responsibility model. In particular, the company chose to initially purchase IaaS and PaaS solutions. According to the shared responsibility model, the company has reduced the burden of responsibility on the security of its products as the Cloud Services Provider has contractually guaranteed, by providing documentation audited by third parties, the physical security of the hardware and a virtualized provision of these. The security of the stacks above the virtualized hardware, starting from the operating systems (in the case of IaaS solutions), has remained a responsibility of the cloud customer who, however, will now be able to use new cloud native security solutions to increase system security.
These considerations were made to demonstrate how the use of cloud technologies was the correct solution. However, this was not immediate. In designing a cloud-based architecture to meet all the needs described above, it emerged that the company did not have the necessary skills and competences. In particular, it was unable to define new, more streamlined, agile and efficient processes to reduce operational effort, time to market and increase product reliability by leveraging cloud technology.
The company could not effectively leverage the cloud for its digital transformation as it lacked a number of core organizational skills as well as technical expertise on technology.
As a result, there was a need to undertake a cloud center of excellence (CCOE) building project. In a first phase, the team consisted of the head of the IT architecture team and external consultants who together formed the CCOE as a separate team parallel to the current organizational structure of the company during the ramp-up phase. In a few months, the CCOE was able to bring a new organizational culture within the organization, allowing them to understand all the architectural pillars, described in the previous chapters.
The training of the CCOE also allowed an upskilling and reskilling of the organization’s personnel, who already had strong technical skills, necessary to design and implement a cloud-based architecture.
However, the technical training of the staff was not sufficient to exploit the advantages of the technology. The definition of a cloud architecture according to the architectural principles described in the previous chapters introduced the need to define new processes around cloud

computing. In turn, the definition of new processes has led to the need to define a new organizational model.
The needs of the company, such as costs saving, reduction of operational management and the ability to know how to exploit the scalability of the system to define new more efficient processes for the delivery of software products, led the CCOE to re-evaluate the current operational and organizational model of the company.
It emerged that the current operating model of the organization was a very traditional model that presented a clear separation between the teams responsible for IT infrastructure and the teams responsible for applications, which in turn presented a clear separation between the teams in charge of design and those in charge of operations, just as shown in chapter 7 in figure 7.2.
This operating model together with a siloed organizational structure, which the company has always used for the structuring the IT departments, would never have made it possible to achieve those goals.
Consequently, on the basis of the chosen cloud solutions and the skills that the CCOE was able to perpetrate, three possible operating models with the related organizational consequences were proposed.

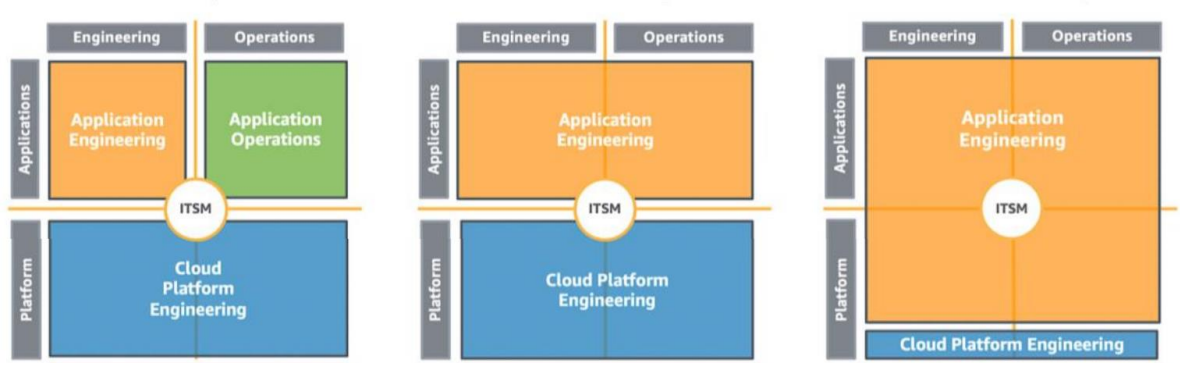

Figure 9.2 Cloud Target Operating Models chose by the client according to best practices

It is important to note that all three operating models require an organizational structure and a more agile allocation of skills than the current operating model. The peculiarity of the three operating models is the combination of design and operational skills of the virtualized cloud-based infrastructure to support applications. In this way, the single team is able to consider the operational requirements of the infrastructure in the early design stages.
Based on the types of products that the company places on the market, in these operating models the teams responsible for the applications may not belong to the organization of the company, that is, if the company has to create an infrastructure product then he will only need the cloud platform engineering team.
The company initially opted for the operating model that still has two separate teams for developing and operating the applications, as shown in Figure 9.2, not because the organization did not understand the potential of the other operating models, but for reasons of aversion to change.
Indeed, this operating model compared to the as-is model, in addition to presenting the single team for the platform, also presents a strong synergy between the team responsible for the operation of the application and the single platform team. That is, the cloud platform engineering team actively provides support to the team responsible for responding and

managing application changes and issue, shown in the figure as the “application operations” team.
The choice to initially adopt this model was also based on technological considerations. The company had initially decided to use only IaaS services for the development and management of cloud-based products. IaaS services, such as virtual machines, still require a lot of configuration and management activities of the technology stack to run application workloads. This has led the company not to opt for an operating model that is too different from the current one in which there are many specialized skills.
In addition, the company decided to migrate applications to the cloud, initially without making improvements, a “lift and shift” migration strategy. This was a further motivation for the use of the model, as the platform team can build and manage a scalable, high-performance and secure infrastructure with virtual machines, while the applications are still managed in a legacy manner.
Therefore, we can see how the company initially adopted a very risk-averse and not very innovative approach from a technological point of view, which led them to adopt an operational and organizational model that is not very disruptive compared to the as-is model.
However, the other two models have defined a future target. The organization has considered the second model, for the optimization of the applications that will be subsequently migrated through the use of the DevOps model. Furthermore, the third model represented an even more future target, for the continuous improvement of applications, for developing native applications for the cloud and for the use of PaaS infrastructure solutions.
The latter target model, through the use of the DevOps model, will present a completely different IT mindset. DevOps defines a single team responsible for designing and operating cloud native applications, but also for managing part of the infrastructure to support their applications.
This model represented the most future target because it is necessary that the CCOE has disseminated the necessary technological skills and has allowed the entire organization to understand the new processes that leverage the new technology.
A problem that emerged with the use of strategic operating models was the use of the DevOps model to streamline the development and operation processes of applications.
The use of the DevOps model significantly reduces non-value-added activities, such as waiting and slowdowns caused by activities that can represent bottlenecks. However, it emerged that to properly implement the DevOps model, the Development and Operations teams can be still separated but they must define a clearly expressed shared goal, such as providing reliable and frequent changes through the use of CI/CD pipelines, and cooperate. It emerged that the members of the Operations team must feel considered while collaborating with developers and developers must take operational features seriously and really include their inputs in the implementation of solutions. This proved to be particularly complex to understand from a cultural point of view.

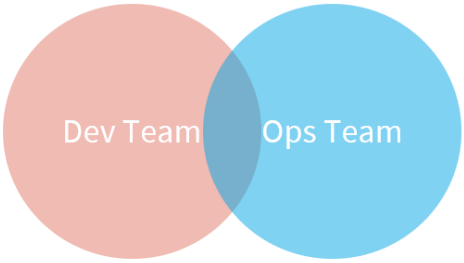

Figure 9.3 Collaboration between teams in a DevOps approach

In all three target models, the cloud platform engineering team is present. However, it is important to note that this has responsibilities that vary according to the cloud technologies used, such as IaaS rather than PaaS, according to the shared responsibility model in the cloud.
Furthermore, after an analysis of the current skills in the organization, the ITSM (IT Service Management) approach was considered for the delivery of IT as a service to internal departments or to external customers of the organization. A typical scenario belonging to the ITSM approach is the request for a new infrastructure component sent by the company via a ticketing system that will allow the specific function to take charge of the request and process it. In general, the processes that the ITSM approach embraces are Incident Management, Change Management, Problem management, Configuration Management, Workflow and talent management.
The major issue for the company remained to define how to effectively organize itself to achieve a target operating model and finally operational excellence, the ability to manage highly flexible and performing services and cost reduction.
The organizational approach adopted turned out to be very innovative but at the same time necessary. The Spotify organizational approach was used, based on the definition of virtual product teams responsible for the entire product life cycle. By following this approach, the DevOps model can also be implemented correctly. Indeed, the temporary and very small team of DevOps may eventually introduce a high level of enthusiasm, coordination and collaboration for the creation and management of a product, while eliminating non-value-added activities.
All these models and approaches have led to the organizational change of the company which, to satisfy its business needs by leveraging cloud technology, is now organizationally structured as described below.

9.3 Organizational transformation

The target operating models chosen led to the reorganization of the IT departments. In accordance with the methodologies and approaches described so far, the company was able to define the following Talent Pools (i.e. Chapter of the Spotify organizational framework): Architectures, Infrastructures, Security & Networks and Governance.
The architecture team has the skills necessary to design an IT architecture using both traditional physical resources and cloud-based architectures. Within this talent pool there are the members of the CCOE. The Infrastructure talent pool has combined different figures with skills related to: IT infrastructure engineering, operations, monitoring, change management experts and business continuity experts. The Security & Network talent pool reports skills and competences to secure resources and network traffic in cloud. Finally, a centralized governance talent pool

has been defined which includes the skills necessary for demand management, budget management, project management and provides services such as help desks, trouble ticketing and customer service.
Starting from these talent pools it has been possible to define the product teams (i.e. Squad of the Spotify organizational framework). Each product team has been then allocated on the operating model chosen on the basis of the type of product and application migration strategy.
The product teams have been categorized on the basis of the type of product to be created and managed. As a result, the "infrastructure" product teams and the "software" product teams have been defined. The product teams have been schematized in the figure below.

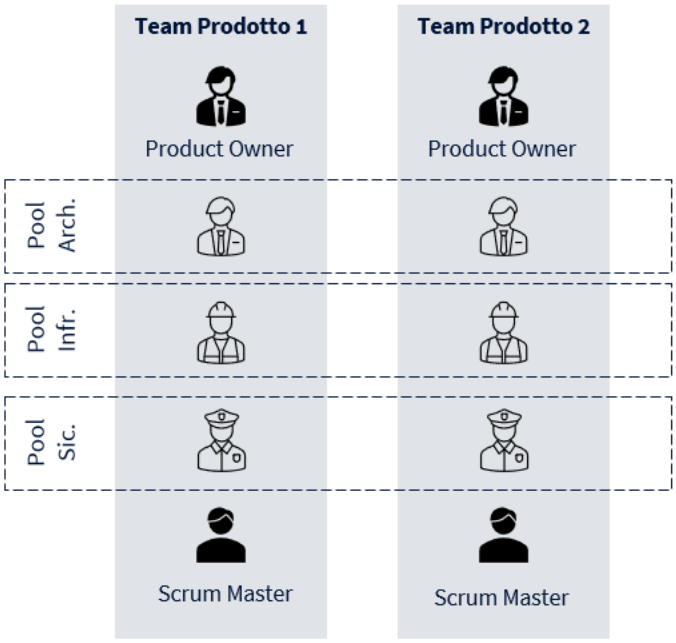

Figure 9.4. Product teams of the company

The allocation of product teams on operating models was essential to define how the teams were organized in the development and management of applications and IT infrastructure.

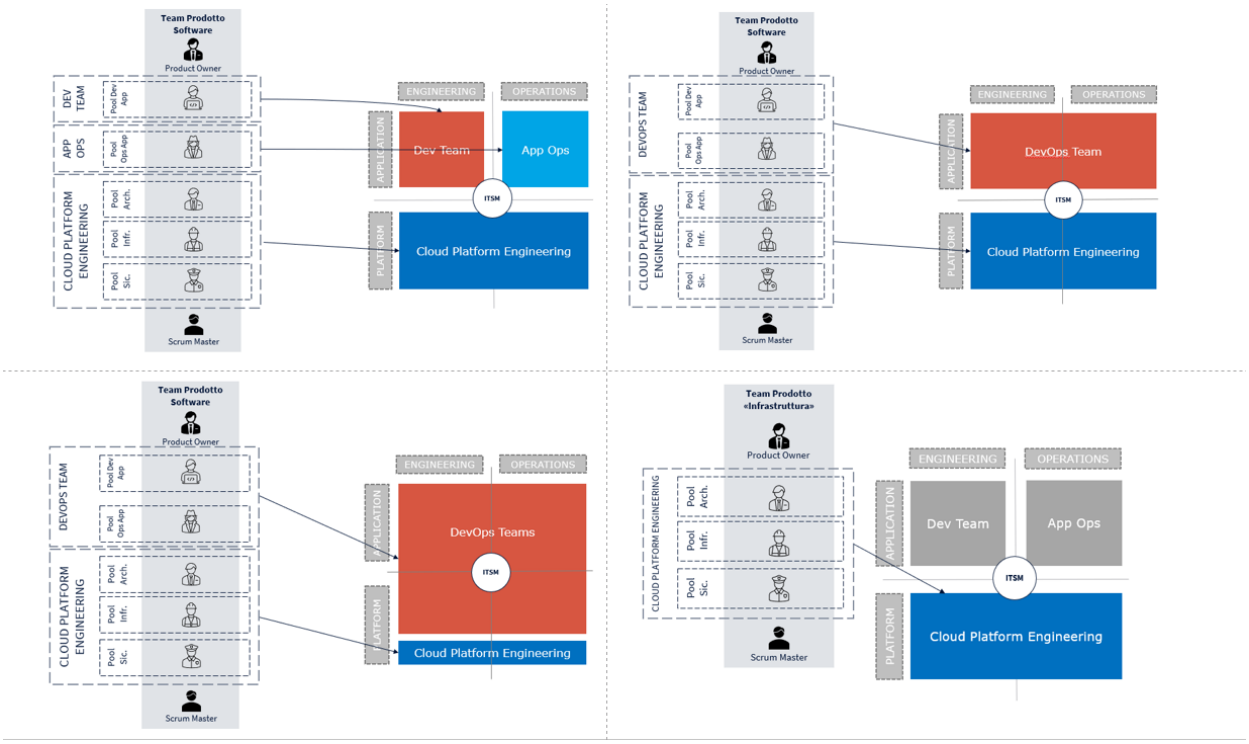

Figure 9.5. Allocation of the product-teams onto Cloud Target Operating Models

It is possible to notice how the roles and skills of the product team change based on the model adopted. In the case of an "infrastructure" product, shown in the lower right quadrant of Figure 9.5, the team has only cloud platform skills, as the software applications will be developed and managed by end customers, consequently the team remains unchanged on the basis of the model adopted.

It was possible to create these product teams thanks to the mindset but also to the technical skills introduced by the CCOE. Each product team is a cross-functional team, as it possesses skills and competences belonging to different Talent pools. In addition, each product team is a virtual team created dynamically just-in-time. Each team has all the technical skills and also a Product Owner responsible for defining the product backload and a role responsible for managing the project, who in this case was a Scrum Master.

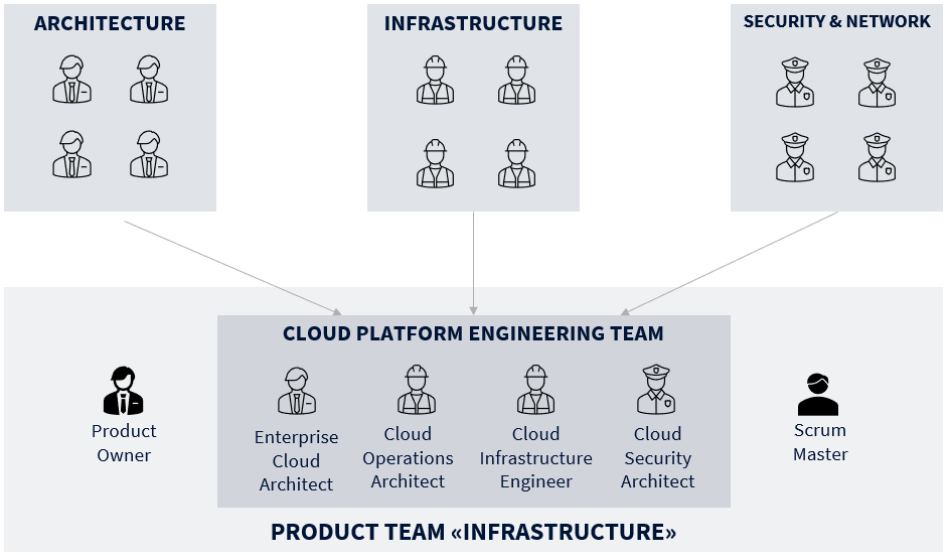

Figure 9.6. How a client product-team has been created

As shown in the figure, the product team employed the technical skills that represent the cloud platform engineering team who together with a product owner and a scrum master defined an infrastructure product team.
It is important to note, as the cloud platform engineering team which is itself part of the product team, employs the skills introduced by the CCOE. In particular, the skills already present within the organization through training sessions have introduced the roles of:

Enterprise Cloud Architect belonging to the Architectures talent pool

Cloud Operation Engineer belonging to the Infrastructure talent pool

Cloud Infrastructure Engineer belonging to the Infrastructure talent pool

Cloud Security Architect belonging to the Security & Networking talent pool

The “software” product team (i.e. the team who realizes and manages a complete cloud-based software application and the underlying infrastructure), on the other hand, has skills regarding the development and management of applications as well as the cloud infrastructure. In this case, the application development and operations teams were introduced but they were not considered as talent pools of this project because they did not have to adapt their technical skills for the cloud computing, even though they started collaborating according to DevOps model.

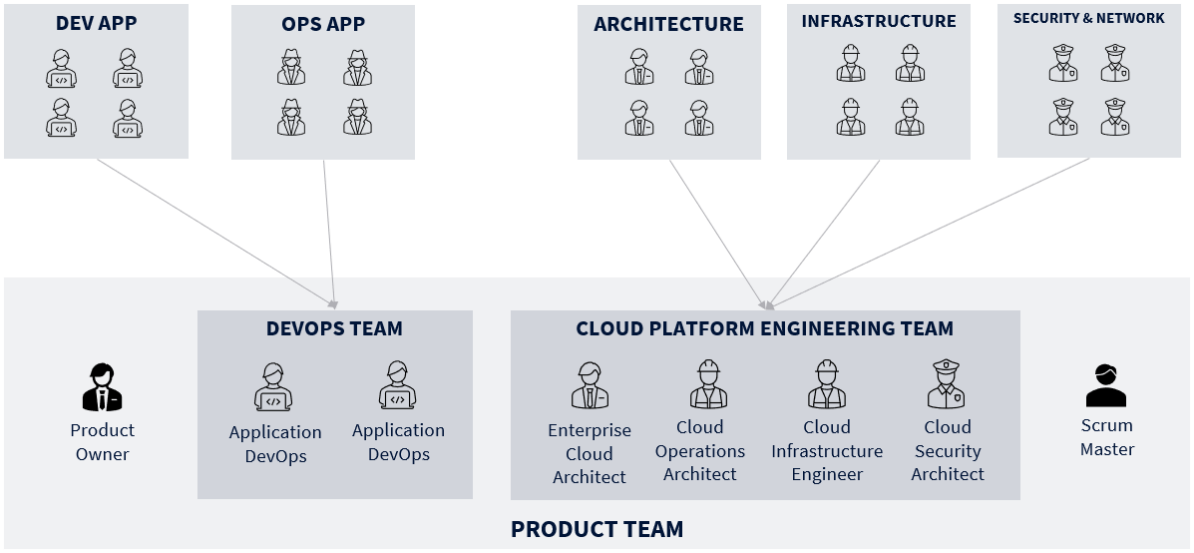

Figure 9.7. How a cloud-based application product-team has been created

The Figure 9.7 shows the creation of a "software" product team. In this specific case the product team has adopted the DevOps model also for the applications.
The exact sizing of the teams is strictly dependent on the complexity of the product to be created and managed. It should be noted that product teams are actually dynamically created teams, and members can be allocated and work on multiple product teams.
The product team must be small and should not exceed 7-10 members to ensure agile project management, collaboration and communication between cross-functional team members for rapid delivery of components and product changes.
A fundamental role is played by the centralized Governance team. The company has chosen to keep this team regardless of the operating models or products to be made. The first reason for this choice is to have a centralized entity that communicates with new customers and allows to understand what skills are needed to create a new just-in-time product team.

The need to adopt a new cost management and optimization model also emerged. Until then, IT functions had to make requests to purchase new IT resources. Requests had to be approved by the cost management teams. This model worked well with the organizational structure in silos because, despite the process inefficiencies given by the wait for approval of expenses, the costs of purchasing and managing IT products and services were very predictable, moreover they very often represented a long-term investment and therefore it was possible to apply the classic methods of cost management based on forecasting techniques.
Introduction of the product teams responsible for the entire product life cycle was supported by the FinOps model for cloud cost management and optimization. From an organizational point of view, it was initially taken for granted to place FinOps skills within the product team itself, so that the team would have had the full ownership of the product.
However, it emerged that the FinOps competences should have represented a centralized team and consequently be placed within the Governance team. There are several reasons for this choice.
First, FinOps is actually a technical figure that monitors application workloads and optimizes infrastructure resources to manage workloads efficiently and optimizing costs. FinOps therefore

uses tools and automation to optimize the underlying resources. Consequently, the use of FinOps within product teams independent of any other team would only have doubled the effort in creating such tools and automations.
Furthermore, in the cloud, the FinOps figure is responsible for evaluating all the most optimal cost solutions, such as requests for volume discounts or discounts for a multi-year commitment from the customer. These activities must be done centrally by a team accountable for the budget and cost management. In addition, the negotiation activities carried out within a very small product team would have subtracted the effort in optimizing resources and consequently costs.
Finally, another reason to allocate the FinOps figure in the centralized governance pool, has been the importance of managing the costs of resources shared between multiple cloud infrastructures, such as networking resources.
The use of the FinOps model has not always led to a reduction in costs, but certainly to the creation of value for the organization and an increase in margins.

Finally, these operational and organizational models based on the use of the skills introduced by the CCOE, on the use of DevOps and FinOps models and on the creation of product teams according to the Spotify framework presented a very important critical issue reported by the company.
The effort of the members of the product teams, allocated across multiple products, has increased exponentially. In particular, team members were staffed on too many products, especially during the operations phases, i.e. monitoring and resolution of product criticalities, also with a view to continuous improvement. These models were not sustainable.
The solution to this criticality was given by the introduction of the Site Reliability Engineer.
The Site Reliability Engineer (SRE) is actually a Software Engineer who designs and implements automations to replace or reduce human effort during the operations phases.
The SRE is a role that implements the DevOps model and has the main objective of automating manual, repetitive and technically automatable operations.
The reduction of time spent on these activities allows the DevOps team to be allocated to engineering activities, improving the performance and reliability of the service which in turn can reduce the causes of criticality and therefore the effort of the operations phases.
In particular, the SRE was used to develop automations to improve Change Management, Monitoring, Incident Response and Capacity Planning activities.
The tools and practices to develop the automations, for the operations phases, of particular importance used have been:

Post Mortem: a documentation made by the SRE that reports the records of the incidents. The records show the root causes of the incidents, the impacts, the actions taken in response and the subsequent preventive actions taken.

Runbook: documentation that contains all the information on how to respond to the alerts that are expected to be received.

Changelog: a file, usually .md, which contains all the changes to be released periodically. This is associated with the application and infrastructure repository and with a CI/CD pipeline each change is read and released automatically.

Finally, we can claim that the development and operations processes of the cloud-based infrastructure and applications turned out to be much more agile, flexible and efficient, reducing time-to-market, increasing performance and security of the products, creating more value for the business and also reducing the human effort.

10. Conclusions

The transition toward the cloud computing has already begun since years and companies are migrating their applications software and IT infrastructure on the cloud with a view of digital transformation to reach the several advantages, widely discussed in this thesis work, that this technology allows.
This thesis work tried to present the advantages of the cloud computing as a reason for companies to adopt this new technological solution and the important organizational consequences that this technology has required.
It has been discussed as companies need to employ the right people, processes and organizational models to take advantage of the new features. Differently, all the value of a cloud computing implementation project within a complex enterprise will be lost. In particular, organizations that do not optimize their approaches risk missing out on the benefits of the cloud, not only in terms of costs and efficiency gains, but also as a basis for innovation and for achieving a competitive advantage in highly complex, competitive and rapidly evolving markets.
This study integrated the literature with the needs, choices and approaches of a company that has adopted the cloud computing, allowing to conclude that the most important element necessary for a successful cloud transformation is the *Organizational Change* which includes defining new operating models, policies, processes and eventually a new mindset.
Other important elements seen are:

Executive Sponsorship: align the entire organization on business requirements and involve all the stakeholders;

Cloud Strategy: create a vision and incentivize team members to follow it;

Experiment: define architecture, patterns, governance and then measure, monitor and iterate to find the optimal solution;

Principle & Standards: publish guidance and best practices on how to adopt cloud successfully;

Cloud Center of Excellence: provide a centralized expertise and then guide decentralized innovations from the product-teams;

Adoption Roadmap: start small and iterate, measure, manage and update plan;

However, the models and approaches described in this work may take a long time to be fully understood by the entire organization and achieve visible benefits, which increases the risk of cloud adoption and migration projects failing due to frictions to cultural and organizational change.

Future improvements of this work, might include the change in data obtained in the long run, such as:

- Market share, customer satisfaction and process efficiency, for assessing the evolution of the organization over time by leveraging cloud technologies;
- Performance and security to evaluate from a technological point of view the improvement of cloud-based digital products compared to digital products based on on-premises technologies.

References

[1] Amazon Web Services, *AWS Prescriptive Guidance: Modernizing operations in the AWS Cloud*, August 2019.

[2] Amazon Web Services, *Overview of Amazon Web Services: AWS Whitepaper*, 2022.

[3] Baecke M., *Introduction to the VMware Cloud Operating Model*, VMware, October 2021.

[4] Blanchard B. et al*., Cloud center of excellence (CCoE) functions*, Microsoft, September 2022.

[5] Blanchard B. et al., *Understand cloud operating models*, Microsoft, September 2022.

[6] Carlson B. et al., *AWS Well-Architected Framework*, Amazon Web Services, December 2021.

[7] Carlson B. et al., *Operational Excellence Pillar: AWS Well-Architected Framework*, Amazon Web Services, August 2022.

[8] Costello K., *Execute Your Cloud Strategy With a Cloud Center of Excellence*, Gartner, July 2021.

[9] Dremel C., Gerster D., Kelker P., *Scaling Agility: How enterprises adopt agile forms of organizational design*, ResearchGate, 2018.

[10] Easter R., Savine A., *Building a Cloud Operating Model*, Amazon Web Services, July 2020.

[11] Eliot S., Livingstone A., *Disaster Recovery of Workloads on AWS: Recovery in the Cloud: AWS Well-Architected Framework*, Amazon Web Services, April 2022.

[12] Gartner, *Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $500 Billion in 2022*, April 2022.

[13] Google, *Building a Cloud Center of Excellence*, March 2019.

[14] Harvard Business Review, *Accelerating Forward: The State of Cloud-Driven Transformation*, 2022.

[15] Ivarsson A., Kniberg H., *Scaling Agile @ Spotify with Tribes, Squads, Chapters & Guilds*, Spotify, October 2012.

[16] Jelciana, Kumar R., Raj H., *Exploring Data Security Issues and Solutions in Cloud Computing*, Procedia Computer Science, v. 125, pp. 691-697, 2018.

[17] Kaczorowski M., *Exploring container security: the shared responsibility model in GKE*, Google, March 2019.

[18] Lewis M., Slack N., *Operations Strategy*, 5 ed., Pearson, 2017.

[19] Morris K., *Infrastructure as Code: Dynamic System for the Cloud Age*, 2 ed., O'Reilly, 2021.

[20] RedHat, *What is a CI/CD pipeline?*, May 2022.

[21] Roach B., Taggart M., Woods P., *Amazon Web Services: Risk and Compliance*, Amazon Web Services, March 2021.

[22] Schwartz M., *Using a Cloud Center of Excellence (CCOE) to Transform the Entire Enterprise*, Amazon Web Services, February 2018.

[23] Shahzad F., *State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions*, Procedia Computer Science, v. 37, pp. 357-362, 2014.

[24] Simorjay F., Tierling E., *Shared Responsibility for Cloud Computing*, Microsoft, October 2019.

[25] Wittig A., Wittig M., *Amazon Web Services in Action*, Manning, 2016.
[26] Zadgaonkar A. et al., *Introduction to DevOps on AWS: AWS Whitepaper*, Amazon Web Services, November 2020.
[27] https://www.statista.com/statistics/233725/development-of-amazon-web-services-revenue/
[28] https://researchhubs.com/post/computing/cloud-computing/cloud-elasticity.html
[29] https://www.intel.it/content/www/it/it/cloud-computing/deployment-models.html
[30] https://www.vmware.com/topics/glossary/content/cloud-computing-infrastructure.html
[31] https://aws.amazon.com/it/about-aws/global-infrastructure/?nc1=h_ls
[32] https://services.google.com/fh/files/misc/state-of-devops-2019.pdf
[33] https://learn.hashicorp.com/tutorials/terraform/infrastructure-as-code
[34] https://aws.amazon.com/devops/what-is-devops/
[35] https://pubcloudnews.tech/2022/05/20/what-is-a-good-cloud-operating-model/
[36] https://www.finops.org/introduction/what-is-finops/