Multi-Cloud Administration Guide

Manage and optimize cloud resources across Azure, AWS, GCP, and Alibaba Cloud

Jeroen Mulder

www.bpbonline.com

Copyright © 2024 BPB Online

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor BPB Online or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

BPB Online has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, BPB Online cannot guarantee the accuracy of this information.

First published: 2024

Published by BPB Online
WeWork
119 Marylebone Road
London NW1 5PU

UK | UAE | INDIA | SINGAPORE

ISBN 978-93-55515-551

www.bpbonline.com

Dedicated to

My wonderful wife Judith
and
My girls, Rosalie and Noa

About the Author

After his study in Journalism, Jeroen Mulder (born in 1970) started his career as editor for the economic pages of Dutch agricultural newspapers. From 1998, he got involved in internet projects for Reed Business Information, in creating websites and digital platforms. Highly attracted by the possibilities of the new digital era and the booming business of internet, Jeroen decided to pursue a career in digital technologies. In 2000, he joined the IT company Origin, as communication specialist in a group designing and developing cross media platforms. Origin evolved to AtoS where he fulfilled many roles, lastly as principal architect.

In 2017, he joined the Japanese IT services company Fujitsu as Senior Lead Architect, with focus on cloud and cloud native technology. From May 2020, he held the position of Head of Applications and Multi-Cloud Services for Fujitsu Netherlands, leading a group of frontrunners in digital transformation. Then Philips knocked on his door. In 2021 and 2022, he was assigned Principal Cloud Architect at Philips Precision Diagnosis. Yet, Jeroen returned to Fujitsu in the summer of 2022 as Principal Consultant for the Global Technology Solutions Business Group, focusing on hybrid IT.

About the Reviewer

Fouad Mulla is a seasoned Lead Consultant, Digital Leader, and Cloud Security Architect with 15 years of professional experience in the digital and software industry at global corporations. Fouad excels in designing and implementing comprehensive cloud solutions across multi-cloud platforms. He has assisted numerous businesses in effectively governing and safeguarding their information, proactively identifying cybersecurity risks, and enabling them to make informed and strategic business decisions. Fouad is CISSP, CISM, CASP+ certified.

Acknowledgements

First of all, I have to express my deepest gratitude to my beloved and wonderful wife, my girls and my entire family and dearest friends. This has been a difficult year with health issues whilst planning for the move to a new house. Thank you for standing next to me, even when I have not been the best version of me. I am truly sorry.

Next, I also have to thank my employer Fujitsu for granting all the time I needed to get well again. And thank you all at BPB for all the patience.

And of course: a big thank goes to you, dear followers and readers. You're making all the effort worthwhile.

Preface

Cloud first is not a strategy, but a statement at best. For starters, cloud first does not say anything about your business strategy. It does not say anything about the goals you want to achieve by using cloud technology. Yet, almost every company on earth is using the cloud in some form. And then the trouble starts: how do we manage our workloads in the cloud? A lot of companies find out the hard way that managing cloud is something different from managing the more traditional IT. That is what this book is about: managing workloads in multi-cloud.

In this book, the reader will get guidance and hands-on instruction on operating multi-cloud environments. We will discuss all the different aspects that come with mulit-cloud such as interoperability between different cloud environments, networking configuration, data integration, and of course security requirements. There is no way of talking about cloud without addressing security and compliance.

This book provides new adopters of the multi-cloud approach with numerous frameworks and ideas for an efficient and sound multi-cloud infrastructure. Throughout the book, you will hopefully find solutions, techniques, designs, and administrative guidance for various types of multi-cloud environments, using AWS, Azure, GCP and Alibaba Cloud. Why these? Because these are the most used clouds.

This book will hopefully help you in understanding the necessary steps in multi-cloud management. Let us now go over the chapters in the book.

Chapter 1: Using the Cloud Adoption Frameworks – provides an overview of the various **Cloud Adoption Frameworks (CAF)** that help in setting up and manage environments in AWS, Azure, GCP and Alibaba Cloud. CAFs contain pillars such as security, identity and access, cost and governance. We will discuss the CAFs of the major providers and show readers how to use them to get maximum benefit.

Chapter 2: Virtualizing and Managing Connectivity – covers all aspects about connectivity in cloud. Networking in cloud is software based. In this chapter, you will learn what cloud networking is, with guidance to software building blocks, deployment models and operating networks in cloud. Concepts such as SD-WAN, SD-LAN and edge will be discussed. We will also introduce micro-services and how network virtualization can help with this.

Chapter 3: Virtualizing and Managing Storage – explains one of the major benefits of cloud: the almost limitless amount of storage that is available to us. But cloud is a shared resource model, so we need to understand how storage works in cloud, how to make sure that we get the right amount of storage and the right type, with the right performance. Cloud architects and admins should know about I/O, pooling and the different storage types. All of that is covered in this chapter.

Chapter 4: Virtualizing and Managing Compute – covers the basics of compute, starting with virtual machines, but also discussing serverless and containers as cloud-native technologies. Public cloud providers offer a wide variety in compute power with different deployment models. We need to understand how compute in cloud works regarding for instance CPU and memory. In this chapter, we will also look at on premises offerings by major cloud providers.

Chapter 5: Creating Interoperability – explains why interoperability is one of the biggest challenges in multi-cloud. In this chapter, you will learn how to overcome these challenges between public clouds and between public and private clouds. The chapter discuss various solutions and frameworks such as Open Compute.

Chapter 6: Managing Data in Multi-Cloud – starts with defining a data strategy in multi-cloud. We need that strategy to determine where data is stored, who and what may access data, what the usage of data is as well as how to prevent events such as data-leaks and data loss. You will learn about data quality, security and integrity and data gravity.

Chapter 7: Build and Operate Cloud Native – further explores cloud-native technologies such as serverless and containers. Cloud native development offers solutions to create scalable applications using, for instance, micro-services, container and serverless concepts, and deploying declarative code. This chapter also contains an in-depth explanation of setting up micro-services architectures and how to manage these.

Chapter 8: Building Agnostic with Containers – covers all aspects of developing and managing containers in cloud platforms. Since Kubernetes has evolved to become the industry-standard, we will study setting up and managing Kubernetes clusters with Docker containers in more detail. Next, we will explore the requirements to monitor our containerized workloads.

Chapter 9: Building and Managing Serverless – helps in understanding the concept of serverless, providing guidance in developing and provisioning serverless functions. In this chapter, we will learn how to define our environments as functions, that we can deploy and manage as serverless environments.

Chapter 10: Managing Access Management – introduces the cornerstone of security in multi-cloud: access management. We do not want just anyone to be able to access data and applications in the cloud; we want to have control and hence, we need access management. The chapter provides an overview of various tools that we can use in multi-cloud, but also addresses concepts as privileged access management and Identity as a Service.

Chapter 11: Managing Security – discusses the principe of the single pane of glass view to monitor and manage security. With distributed environments, we must use frameworks that cover the various cloud technologies and tools that can handle various clouds.

Chapter 12: Automating Compliancy – starts with explaining why compliance in cloud might be more of a challenge than in traditional IT, where we have workloads mostly on premise. Governmental bodies, certification authorities and auditors are setting compliancy guardrails to allow usage of major cloud providers. In this chapter, we will learn how to use automation and even AI to ensure that our workloads in the cloud remain compliant.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/x7mjh27

The code bundle for the book is also hosted on GitHub at **https://github.com/bpbpublications/Multi-Cloud-Administration-Guide**. In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Using the Cloud Adoption Frameworks

Introduction

Welcome to the cloud. Or better said: welcome to the multi-cloud. The major public cloud providers, such as Azure and AWS, offer **Cloud Adoption Frameworks** (**CAF**) to help customers set up and manage environments in their clouds. Their usage should be secure and efficient. CAFs are good guidance for architects and engineers. These frameworks contain pillars such as security, identity and access, cost, and governance.

In this chapter, we will first discuss what multi-cloud is and next study the CAFs of the major providers, showing how to use them to get maximum benefit. We will also discuss monitoring, including keeping track of (business) **Key Performance Indicators** (**KPIs**). At the end of the day, we should be creating value from our cloud, and value needs to be measured.

Structure

In this chapter, we will discuss the following topics:

- Exploring the business challenges of multi-cloud
- Introducing CAF: how to use them

- Deep dive in the CAF of Azure and AWS
- Frameworks by GCP and Alibaba cloud
- Similarities and differences
- Monitoring multi-cloud and keeping track of value propositions

Exploring the business challenge of multi-cloud

Before we dive into the challenges of multi-cloud, we must define what multi-cloud is. Multi-cloud refers to the practice of using multiple cloud service providers to distribute an organization's computing resources and applications. By leveraging the strengths of different cloud platforms, such as **Amazon Web Services** (**AWS**), Microsoft Azure, **Google Cloud Platform** (**GCP**), and others, businesses can optimize their IT infrastructure for performance, cost, security, and scalability.

The rise of multi-cloud strategies has become an important topic in today's IT landscape for several reasons:

- **Flexibility and avoiding vendor lock-i**n: Utilizing multiple cloud providers allows organizations to prevent reliance on a single vendor, offering them the flexibility to choose the best services and pricing structures for their specific needs.
- **Optimal resource allocation**: Each cloud provider has unique strengths and weaknesses. A multi-cloud approach enables organizations to allocate resources based on the specific capabilities of each platform, ensuring optimal performance and cost-effectiveness.
- **Enhanced security and compliance**: Distributing data and applications across multiple cloud environments can help organizations reduce the risk of data breaches, meet regulatory requirements, and adhere to industry standards.
- **Increased resilience and redundancy**: A multi-cloud strategy can improve business continuity by providing redundancy in case of outages or failures in a single cloud environment. This ensures that critical applications and data remain available and operational.
- **Innovation and competitive advantage**: Leveraging multiple cloud platforms allows organizations to access cutting-edge technologies and tools, fostering innovation and providing a competitive edge in the market.

Most companies are multi-cloud, even when they have a single cloud strategy. The staff will work with Office365 of Microsoft, store customer contacts in Salesforce, the book travels through SAP Concur, and have meetings through Zoom. At the same time, the backend systems of companies might be hosted on a public cloud such as AWS or Azure or on servers in a privately owned data center. Thus, companies use **Software as a Service (SaaS)**, **Platform as a Service (PaaS)**, and **Infrastructure as a Service (IaaS)**, and all these different environments must be managed. This is the IT challenge of multi-cloud.

Multi-cloud strategies are motivated by the desire to optimize IT infrastructure using different cloud platforms' unique strengths. Benefits include flexibility, optimal resource allocation, enhanced security and compliance, increased resilience and redundancy, and access to innovative technologies. These advantages make multi-cloud strategies relevant and valuable in today's competitive digital landscape.

But what is the business challenge of multi-cloud? Amongst others, we can think of the following:

- **Cloud sprawl:** We discuss cloud sprawl when a company lacks visibility into and control over the spread of its environments in various clouds, including instances, services, or providers across the company.
- **Lock-in, including data gravity:** A mistake that companies often make is assuming that multi-cloud decreases the risk of lock-in. That risk still exists, but now it is spread over multiple clouds. This risk is directly related to portability. It is not as easy as it seems to migrate native services across different clouds. Next, the issue of data gravity plays an important role. Applications often need to be close to the data. Having data sitting in a different cloud than the application may lead to issues such as latency. Moreover, rules for compliancy can cause issues. Think of laws that prohibit companies from having data outside country borders, limiting the choice of clouds.
- **Lack of multilingual knowledge:** If a company uses various clouds, it also means that it has to know how to use these clouds. Although the principles of public cloud are largely the same, clouds such as AWS and Azure still do differ in terms of operating workloads on these platforms. The company will need resources, engineers, and architects to cover the different technologies used.
- **Dynamics of changing cloud features:** Cloud is evolving fast. During the yearly large conferences such as Ignite for Azure and re: Invent for AWS, these providers launch hundreds of new services. Over the year, even more, new features and services are added to the portfolio. Not everything might

be of use to a company, but it needs to keep track of features and releases of new services to be able to improve its own cloud environments. This is not trivial, and certainly not when a company is operating multi-cloud. In most cases, cloud providers will help their customers in getting the best out of the cloud by adopting the right technologies.

- **Integration:** Using environments on different platforms might lead to integration issues simply because workloads cannot communicate with each other. This can be due to network issues such as bad routing and because technologies are not compatible.

Of course, there are many more challenges to overcome. Think of network performance and latency, security and compliance, governance, and policy management, not to mention controlling costs and the cloud vendor relationship as part of the governance. All these items are captured in the cloud adoption frameworks. During the course of this book, we will discuss these items in more detail.

Following best practices and guidelines from CAFs can help to at least address these issues and design solutions to overcome them.

Introducing CAF: how to use them

What is a cloud adoption framework, and how should we use it? Maybe a better first question would be: why would we use a CAF? The answer to that question is: because the CAF will help as long as we follow the guidelines and guardrails as defined in the CAF, it will be a lot easier to get support from the cloud providers when we encounter issues. It is fair to say that the CAF provides a universal language between the cloud provider and the customer. The CAF is basically a set of documentation with guidelines and best practices on how we can best design and operate our cloud.

Before we dive into the details of the CAF for Azure and AWS, which are the leading public clouds, we will study the generic pillars of the CAF. The six pillars of the CAF are as follows.

Strategy

Moving to the cloud just because you can, is not a strategy. Cloud first, for that matter, is not a strategy. Using cloud technology should be valuable to a business. This means that there must be a business justification. We will discuss this in the section about similarities and differences between the various CAFs. A business will have an ambition laid out in business goals. The next step is to define how the

business can achieve those goals and, in the end, fulfill the ambition. The architecture will lay out what the ambition will look like (sometimes referred to as the North Star architecture), but more importantly, how to reach the goals. What steps must a business take, and in what order? That defines the business strategy.

Plan

Despite what a lot of people think, the cloud is not solely about the technology. Of course, technology is an important part of the CAF and the forthcoming architecture, but cloud adoption is even more so about aligning business processes, people, and technology. In adopting the cloud, we will likely move workloads such as applications to a cloud platform. Ask these questions in drafting the plan:

- What do we use?
- Why do we use it?
- Who uses it?
- When do we use it?

The answers will help in defining the strategy to migrate workloads and applications to the designated cloud platform. One essential question is: does it bring added value to move a workload to the cloud? Followed by the question: how will it bring that value? This is where the following five R's are important:

- **Rehost**: This is lift and shift. Workloads such as applications are not modified but migrated as they are to the cloud platform.
- **Replatform**: This is lift and shift too, but this time some modifications are done. For instance, a business chooses to keep the application as it is, but some parts are shifted to managed services by the cloud provider. Think of having the databases managed through a managed service such as **Relational Database Service** (**RDS**) by AWS.
- **Refactor**: By refactoring an application, the application is modified. Services are replaced by cloud-native services, for instance, using container technology or serverless functions. This often means a redesign of the application, for instance, from a monolith architecture to micro-services.
- **Retire**: An outcome of the strategy or planning phase might be that an application is obsolete and can be retired.
- **Retain:** There might also be workloads and applications that cannot be migrated to the cloud for various reasons. The application must be close to the data source or the machine that it operates, which is typically the case in **operational technology** (**OT**). Think of manufacturing or healthcare. There

might be restrictions to using public clouds because of legal compliance, or an application is critical to the business but simply too old to move to the cloud. These might all be reasons to retain an application, meaning that they are not touched at all.

Prepare

The next step is to prepare the cloud platform that will host the workloads and applications. Typically, this starts with setting up the landing zone in the designated cloud. The landing zone is the foundation. If we are building a house, we need to know what the house looks like before we can lay out the foundation. It is the same for the cloud. We have to know what sort of workloads we will be migrating to the cloud to define and design the landing zone. During the course of this book, we will discuss the landing zone extensively.

Adopt

This is the phase where the workloads are migrated to the cloud according to the plan and the migration strategy that we have defined. We can either lift and shift workloads as-is or transform the workloads and adopt cloud-native services.

Govern

We need an organization that is able to manage the cloud and the workloads in the cloud. These are necessarily the same thing. In the govern phase, organizations might want to form a **Cloud Centre of Excellence** (**CCoE**) with a specific platform team, which manages the cloud, and application teams that manage the specific applications in the cloud.

Operate

This is the phase where organizations will monitor the workloads and make sure that these are performing in the most optimal way, following the best practices of the cloud provider and fulfilling the business requirements.

Most CAFs have added two more pillars to these six: security and sustainability. These might be debatable since both security and sustainability should be intrinsic and taken into account for every workload that is migrated to a cloud platform. In other words, security and sustainability are part of all six stages in the CAF. Yet, both AWS and Azure have security as separate pillars in the CAF, as we will learn in the next section.

Deep dive in the CAF of Azure and AWS

First, we take a look at the CAF of **AWS**. We will recognize the generic pillars of the CAF, but AWS calls these the foundational capabilities:

- **Business**: The business perspective helps to set the strategy for digital transformation. The AWS CAF takes the need for digital transformation as the starting point. In other words: it is not the question of whether a business must digitize but how. The business perspective helps define how cloud investments can accelerate this transformation.
- **People**: The people perspective is mainly about transforming the culture of a business. Digital businesses need people with a growth mindset and people who are willing to learn continuously and change accordingly. One remarkable aspect of the people perspective is *cloud fluency*. People need to understand the cloud, in this case, AWS. It might require a workforce transformation.
- **Governance**: The governance perspective is all about project and program management, guiding organizations in their journey to AWS, and making optimal use of AWS services. This includes risk management and cloud financial management or FinOps.
- **Platform**: This is, obviously, about the cloud platform itself and how we build it in AWS. There is one golden rule that applies here: AWS is responsible for the cloud, the customer of what is in the cloud. AWS provides its customers with a toolkit to build a virtual private cloud on their platform. It is up to the customer to use these tools and build a scalable, resilient environment to host applications and data. The CAF will help with best practices for platform, data, and application architecture, including **Continuous Integration** and **Continuous Delivery** (**CI/CD**) through (automated) pipelines that integrate with AWS.
- **Security:** As said in the previous section, AWS, and Azure have separate pillars for implementing and managing security in the cloud. It includes **Identity and Access Management** (**IAM**), threat detection, protection of infrastructure, data, and applications, and the management of the security postures in the cloud.
- **Operations:** From the business, requirements will be set concerning performance and reliability. This must be monitored and managed. Typically, IT operators manage environments using IT service management frameworks such as ITIL, including incident, change, configuration, and problem management. Observability is key, next to fast detection and response. The

AWS CAF specifically mentions AIOps, predictive management through **artificial intelligence** (**AI**).

These capabilities are required to go through cloud transformation value chains. The value chains lead to the following business outcomes:

- Reduction of business risks
- Improved **Environmental, Social, and Governance** (**ESG**) values
- Growth of revenue
- Increasing operational efficiency

To reach goals in business outcomes, businesses must go through a transformation. AWS specified four transformation domains:

- Technology
- Process
- Organization
- Product

All these domains will continuously change and transform. But by using cloud technology, these transformations can become more agile: adaptable and scalable. If we put this all together, we get the CAF of AWS, as shown in the following *Figure 1.1:*

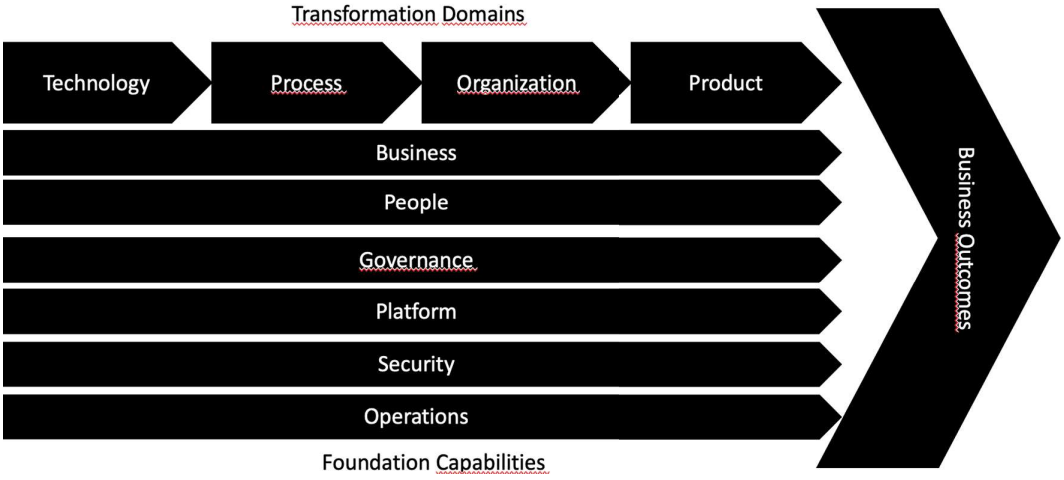

Figure 1.1: *High-level representation of AWS Cloud Adoption Framework*

A whitepaper about AWS CAF can be found at: **https://aws.amazon.com/professional-services/CAF/**.

As we will see in Azure as well, the CAF is not a one-time exercise but more of a lifecycle. That makes sense if we realize that the business, and the cloud itself, constantly changes with updates and new features. AWS presents this as the cycle from envisioning to aligning, launching, and scaling. The business envisions how the cloud can help in achieving business goals, aligns this with the foundation capabilities, launches the new services and products as **Minimal Viable Products** (**MVP**) or a pilot, and lastly, expands it to production. From there, the cycle starts over again.

Microsoft Azure presents the CAF as a cloud adoption lifecycle, too, starting with the definition of a strategy. The strategy is all about defining the desired business outcomes and the accurate justification to start the cloud journey. The Azure CAF is represented in the following *Figure 1.2:*

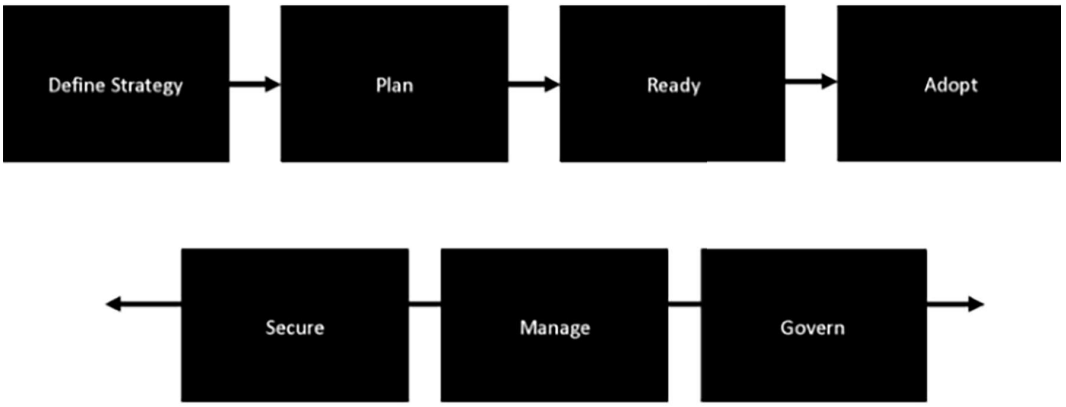

Figure 1.2: *High-level representation of Azure Cloud Adoption Framework*

To get started with the Azure CAF, Microsoft recommends working from scenarios. These scenarios have been chosen from various business standpoints. Perhaps one remarkable scenario is the hybrid and multi-cloud scenario. It is remarkable since this scenario focuses on businesses that will have more than one cloud and even cloud combined with on-premises environments. Using the CAF, businesses can establish unified and centralized operations across these different clouds and their on-premises data center. The CCoE is an important element in this scenario, combining knowledge of various cloud solutions and integrating these into one unified set of processes and best practices for architecture.

One other special scenario is desktop virtualization, allowing customers to migrate workplaces to **Azure Virtual Desktop** (**AVD**). Using the CAF guidelines, businesses can implement AVD instances in Azure and integrate this with Windows and Office365, the latter being a SaaS proposition.

These scenarios all follow the same approach that is set out in the CAF: strategy, plan, migrate, manage (operate), and govern. The business will formulate the ambition and the goals that are worked out in a plan. Next, the workloads – for instance, the virtual desktops – are migrated. An organization centralized in the governing CCoE will manage the workloads compliant with the business requirements.

The Azure CAF pays extra attention to so-called antipatterns. There is a list of antipatterns to be found on **https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/antipatterns/antipatterns-to-avoid**, but there are two in particular that we like to mention here:

- **IT as cloud provider**: This is the antipattern where the business treats its IT organization as the cloud provider. It is not the cloud provider; they are using the technologies in the cloud. Keep in mind that the cloud provider is responsible for the cloud, the customer of what is in the cloud. For example, the failure of a region in Azure or any other cloud is not the responsibility of the IT organization. Monitoring and managing the resiliency of specific workloads, where these failover to another region, is the responsibility of IT. That, however, starts with business requirements and the forthcoming architecture to design the resiliency of that workload.
- **Inaccurate out-of-the-box security assumptions**: Again, cloud providers offer a massive number of tools that will help organizations to secure workloads in the cloud. Public clouds are likely the best-secured platforms in the world, but that doesn't mean that workloads are secured by default. That depends on how the customer applies security guardrails, guidelines, and usage of tools to protect applications and data in the cloud. The assumption that the cloud provider automatically takes care of that is wrong.

The appropriate use of the CAF will help avoid these pitfalls and antipatterns. In the next section, we will study the CAFs of Google Cloud and Alibaba Cloud, which are a bit different from AWS and Azure.

Frameworks by GCP and Alibaba cloud

Google Cloud Platform (**GCP**) and Alibaba Cloud also have versions of a CAF. We will study these in this section. GCP defines its CAF in four themes and, with that, takes a completely different approach to cloud adoption.

Lead

This is about leadership from sponsors in the business, which supports the migration to the cloud. It also includes the teams themselves and how they collaborate and motivate one another in a successful transition and transformation to a cloud platform.

Learn

Cloud adoption is so much about technology but more about adopting a new way of working. Companies will have to learn how public clouds work. In other CAFs, this is typically gathered under people or as part of the operating model, including a center of excellence. Moreover, the staff needs to be trained and upskilled. This goes beyond technical skills.

A company and its employees also must learn to understand how, for instance, financing works in the cloud. What financial models are applicable in the cloud? Typically, organizations start with pay-as-you-go in the cloud, but there might be situations where reserved capacity might be a much better choice. Reserved capacity often means that a company still needs to invest or at least confirm and commit that it will use resources in the cloud for a longer period.

Migrating to the cloud is a learning process in many aspects. Not only is the technology different from traditional IT, but applications and data are managed differently in the cloud. Migrating to the cloud is a huge change and requires transformation and change management. Governance, security, development, operations, and financial management: these are all part of the transformation. In this book, we will mainly focus on the technical management of cloud environments, but it is good to keep in mind that cloud adoption involves more than just technology.

Scale

One of the most important and obvious reasons for companies is that the cloud offers scalability. GCP focuses on limiting manual processes as much as possible. Hence, automation is a major topic in the adoption framework. Workloads and services in the cloud must scale automatically but are always triggered by business processes. This is referred to as event-driven. For example, an event can be a customer that places an order on a website. That will trigger the process of payment and delivery

process of the product. When a company launches a new product, this might lead to a peak in orders. Using automation, the cloud services will automatically scale to facilitate the peak and make sure that the websites and associated applications keep performant. As soon as traffic decreases again, automation will also take care of scaling down, avoiding unnecessary costs.

Secure

Performance and cost control are important, but there is one more item that is at least as equally important or perhaps even more important. The fourth pillar in the CAF of GCP is, therefore, security. Security starts with identity and access management but also includes several tactics and techniques to protect workloads and services in the cloud.

Next, the framework addresses three levels of adoption: tactical, strategic, and transformational. Simply put, tactical concerns the individual workloads in the cloud, but there is no plan to leverage cloud-native services, enhancing automation and scalability. It is a simple lift and shift of workloads to the cloud, causing no disruption to the company. Basically, the cloud is used as a traditional data center.

On a strategic level, there is a plan to automate individual workloads and start decreasing the manual efforts to manage these workloads. On the transformational level, organizations use the cloud to innovate, using automated development and deployment pipelines to enable regular releases of new features to products or new products as a whole. The cloud now has become essential in shortening time to market, decreasing the cost of sales, and, with that, increasing revenue. The cloud is adding value to the business and, with that, has become part of the digital transformation of the business. We will talk about this in the final section of this chapter.

Putting the four pillars and the three stages together results in the cloud maturity scale that GCP uses. It can be seen in the following *Figure 1.3:*