ITIL®

ITIL® 4: Acquiring and Managing Cloud Services

AXELOS

ITIL® OFFICIAL PUBLISHER

a Williams Lea company

Published by TSO (The Stationery Office), part of Williams Lea,
and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0333 202 5070
Fax orders: 0333 202 5080
E-mail: customer.services@tso.co.uk
Textphone 0333 202 5077

TSO@Blackwell and other Accredited Agents

Axelos
Full details on how to contact Axelos can be found at:
https://www.axelos.com
For further information on qualifications and training accreditation, please visit:
https://www.axelos.com/certifications
https://www.axelos.com/archived-pages/becoming-an-axelos-partner/training-organization-and-trainer-accreditation
For all other enquiries, please email: ask@axelos.com

Copyright © Axelos Limited 2021

All rights reserved. No part of this publication may be reproduced in any form or by any means without permission in writing from Axelos Limited.
Applications to reuse, reproduce or republish material in this publication should be sent to the licensing team at: licensing@AXELOS.com
Registered office address: Suite 10, 121/122 Sloane Street, London SW1X 9BW, England

Axelos, the Axelos logo, the Axelos swirl logo, AgileSHIFT®, ITIL®, MoP®, M_o_R®, MoV®, MSP®, P3M3®, P3O®, PRINCE2®, PRINCE2 Agile®, and RESILIA® are registered trade marks of Axelos Limited.

Figure 4.1: Reproduced from https://cispe.cloud/website_cispe/wp-content/uploads/2020/06/CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v-EN-2020-05-11.pdf

Figure 8.4 is licensed under the Creative Commons Attribution 4.0 International licence (https://creativecommons.org/licenses/by/4.0/) from https://docs4.it/framework/04-06-development

First edition 2021

ISBN 9780113318186

Printed in the United Kingdom for The Stationery Office
Material is FSC certified and produced using ECF pulp, sourced from fully sustainable forests.

J003823300

Contents

List of figures vi

List of tables vii

Foreword ix

Preface x

ITIL Foundation recap xi

1 Introduction 1

1.1 What is the cloud? 3

1.2 The origins of cloud 3

1.3 Types of cloud solution 6

1.4 Deciding to use cloud services 10

1.5 Cloud as a key component of digital strategy 12

1.6 The role of cloud services in a digital transformation 13

1.7 Cloud services and sustainability objectives 14

1.8 Governance 15

1.9 How to use this publication 20

2 Explore: Can the organization benefit from cloud? 31

2.1 About the explore step 32

2.2 Understanding the cloud's role in strategy 33

2.3 Setting the strategic scope 36

2.4 Cloud strategic positioning 38

2.5 Value: outcomes, costs, and risks 43

2.6 Formulating the initial cloud strategy 53

2.7 Summary 61

3 Engage: Meeting a cloud service provider 63

3.1 About the engage step 64

3.2 Understanding the CSP landscape 65

3.3 Types of services to be considered 71

3.4 Defining requirements for cloud services 75

3.5 Request for information and proof of concept 84

3.6 Conducting a cloud readiness assessment 84

3.7 Engaging with cloud service providers 87

3.8 Reviewing the cloud strategy and cloud service requirements 92

3.9 Summary 92

4 Offer: Selecting the right services and service provider 93
4.1 About the offer step 94
4.2 Establishing a desired minimum return on investment 95
4.3 Communicating requirements 96
4.4 Request for proposal 96
4.5 Reviewing proposals 101
4.6 Determining the return on investment of the proposed cloud services 105
4.7 Defining and communicating a business case for cloud services 110
4.8 Summary 113
5 Agree: Negotiating and planning 115
5.1 About the agree step 116
5.2 Agreeing and planning value co-creation 117
5.3 Negotiating and agreeing a cloud service 118
5.4 Cloud service agreements 119
5.5 Shared responsibility model 120
5.6 Roles and responsibilities map 122
5.7 Charging models 124
5.8 Summary 125
6 Onboard (and offboard): Moving to the cloud 127
6.1 About the onboard step: general considerations 128
6.2 Migrating to cloud as a part of an onboarding initiative 134
6.3 Security and compliance considerations 140
6.4 Summary 143
7 Co-create: Enabling value 145
7.1 About the co-create step 146
7.2 Operating model alignment 147
7.3 The value co-creation map for cloud 149
7.4 Value co-creation drivers in practice 152
7.5 Managing the optimization of cloud service consumption 166
7.6 Managing cloud service quality 168
7.7 Using cloud tools for value co-creation 170
7.8 Summary 171
8 Realize: Measuring and improving 173
8.1 About the realize step 174
8.2 Maintaining operating model alignment 175
8.3 VUCA and the value co-creation map 176
8.4 Continual improvement and the value co-creation map for cloud 180
8.5 Summary 188
9 Conclusion 189

Appendix A: ITIL practices and the customer journey 191
Further research 203
Glossary 207
Acknowledgements 215
Index 221

List of figures

Figure 0.1	The ITIL service value system	xi
Figure 0.2	The ITIL service value chain	xii
Figure 0.3	The continual improvement model	xiv
Figure 0.4	The four dimensions of service management	xv
Figure 1.1	Cloud as the source of commoditized digital solutions	4
Figure 1.2	The governance cascade	15
Figure 1.3	The shared responsibility model	18
Figure 1.4	The customer journey	20
Figure 1.5	Value co-creation map for cloud	22
Figure 1.6	The cloud customer journey with feedback and feedforward activities	23
Figure 1.7	Cloud journey overview	26
Figure 1.8	The cloud usage strategy spectrum	27
Figure 1.9	Hub-and-spoke model	29
Figure 1.10	The cloud architecture and governance spectrum	29
Figure 1.11	Cloud use depends on cloud strategy position and architecture and governance position	30
Figure 2.1	The tiered relationship between business, digital, and IT strategies	33
Figure 2.2	A modern view of the relationship between business, digital, and IT strategies	34
Figure 2.3	Development of cloud strategy elements	55
Figure 3.1	The four areas of CSP implementation partner support	70
Figure 4.1	Cloud service procurement options	101
Figure 6.1	Decentralized infrastructure	136
Figure 6.2	Using migration and data pipeline integration tools	137
Figure 7.1	Operating model canvas	148
Figure 7.2	Co-creation driver priorities based on strategic objectives	150
Figure 7.3	Cloud consumption dynamics	166
Figure 8.1	The value co-creation map for cloud with a VUCA context	176
Figure 8.2	Delivery of cloud improvements	184
Figure 8.3	The Plan-Do-Check-Act (PDCA) cycle with baselining	186
Figure 8.4	Continual improvement with purpose	187

List of tables

Table 0.1	The ITIL management practices	xiii
Table 1.1	General strategies for consuming cloud services	6
Table 1.2	Architecture included in each cloud service model	7
Table 1.3	Deployment models	9
Table 1.4	Cloud features, benefits, and disbenefits	11
Table 1.5	Examples of feedback and feedforward activities within the cloud customer journey	24
Table 1.6	Examples of cloud usage strategy spectrum characteristics	27
Table 2.1	Risks related to the shift in roles and responsibilities	48
Table 2.2	Risks related to the unauthorized use of cloud services	49
Table 2.3	Risks related to the security of cloud services	50
Table 2.4	Risks related to API vulnerability	50
Table 2.5	Risks related to maintaining separation between tenants	51
Table 2.6	Preventing vendor lock-in	51
Table 2.7	Risks related to third-party contracting	52
Table 2.8	Risks related to migration	53
Table 2.9	Examples of strategic cloud objectives using the OKR framework	55
Table 2.10	Key cloud strategy elements and descriptions	56
Table 3.1	Overview of CSP types and their services	66
Table 3.2	Advantages of each CSP type	68
Table 3.3	Customer enablement services	69
Table 3.4	Examples of general service requirements	80
Table 3.5	Examples of data requirements	81
Table 3.6	Examples of security requirements	81
Table 3.7	Examples of people-related requirements	82
Table 3.8	Examples of service provider requirements	82
Table 3.9	Examples of cost reporting, billing, and payment requirements	83
Table 3.10	Examples of application/workload-specific readiness checks	87
Table 3.11	Consumer organization responsibilities versus CSP responsibilities	88
Table 3.12	Methods of accessing cloud services	90
Table 4.1	Cloud request for proposal format	100
Table 4.2	General service requirement assessment questions and actions	102
Table 4.3	Data requirement assessment questions and actions	103
Table 4.4	Security requirement assessment questions and actions	103
Table 4.5	People-related requirement assessment questions and actions	104
Table 4.6	Service provider requirement assessment questions and actions	104
Table 4.7	Cost reporting, billing, and payment requirement assessment questions and actions	105
Table 4.8	Examples of ROI assessment data	106
Table 4.9	Examples of benefits and costs used in ROI calculations	108

Table 4.10	Aspects considered when evaluating the benefits of moving to cloud	109
Table 4.11	Typical areas of conflict and uncertainty	111
Table 5.1	Three fundamental service relationship types	117
Table 5.2	The responsibilities of each entity	123
Table 6.1	Opportunities and ITIL guiding principles	133
Table 7.1	Overview of characteristics of co-creation drivers	149
Table 7.2	High-level responsibilities for strategy management	153
Table 7.3	High-level responsibilities for portfolio management	153
Table 7.4	High-level responsibilities for service level management	154
Table 7.5	High-level responsibilities for organizational change management	155
Table 7.6	High-level responsibilities for incident management	156
Table 7.7	High-level responsibilities for problem management	157
Table 7.8	High-level responsibilities for monitoring and event management	158
Table 7.9	High-level responsibilities for change enablement	158
Table 7.10	High-level responsibilities for availability management	160
Table 7.11	High-level responsibilities for capacity and performance management	160
Table 7.12	High-level responsibilities for architecture management	161
Table 7.13	High-level responsibilities for continuity management	161
Table 7.14	High-level responsibilities for service financial management	162
Table 7.15	High-level responsibilities for supplier management	163
Table 7.16	High-level responsibilities for information security management	164
Table 7.17	High-level responsibilities for data privacy	165
Table 7.18	High-level responsibilities for risk management	166
Table 7.19	Dimensions of service quality	168
Table 7.20	Cloud tools for value co-creation	170
Table 8.1	VUCA elements	176
Table 8.2	Addressing VUCA elements	177
Table 8.3	Addressing VUCA challenges in the context of strategic adaptability	178
Table 8.4	Addressing VUCA challenges in the context of consumer experience	178
Table 8.5	Addressing VUCA challenges in the context of operational excellence	179
Table 8.6	Addressing VUCA challenges in the context of reliability, resilience, and continuity	179
Table 8.7	Addressing VUCA challenges in the context of governance and control	180
Table A.1	Heat map of practices against steps of the customer journey	192

Foreword

The transformational capability of information technology (IT) is undeniable, and its impact continues to increase exponentially. Consumers demand more and better products and services in real time. Organizations strive to quickly respond to, and even anticipate, rapidly changing consumer needs and desires, often on a global scale and in highly data-driven ways.

IT service providers, therefore, have been required to far surpass their traditional roles as enablers and business necessities. Digital technology has simultaneously become a game-changing disruptor and a key differentiator for existing organizations, as well as for new start-ups; it is now considered to be an accelerating strategic imperative and essential for organizational survival. As a result, the need for a holistic, comprehensive, and relevant service management framework has never been greater.

Axelos has responded with the ITIL 4 specialist modules, which are a direct and practical application of the ITIL framework to evolving and emerging topics that are of critical importance to service providers and the organizations they serve. The ITIL 4 specialist modules are a continuation of Axelos's collaborative traditions, drawing on the combined knowledge, research, and real-world expertise of vendors, consultants, trainers, developers, business leaders, and practitioners who are shaping their respective industries. With digital transformation now at the forefront of organizations' strategies, Axelos aims to support the increasing numbers of businesses that need to acquire and manage cloud services if they are to meet their objectives and ultimately be successful.

ITIL training and certification continue to provide individuals with a structured approach for developing their competencies in the current and future workplace. The guidance provided in this publication will help organizations to take best advantage of cloud services, succeed in making their digital transformations, and create value for themselves and their customers.

ITIL is the most widely accepted approach to service management in the world. When it is applied to the specific challenges that organizations are currently facing, the result is use-case-based guidance that is realistic and proven. The ability to identify and achieve strategic organizational objectives and to optimize the daily operational activities that support them is, quite literally, in your hands.

Mark Basham
CEO, Axelos Global Best Practice

Preface

In under two decades, cloud computing has changed the world.

Early use of cloud technology provided users with access to data from any endpoint that had access to the internet. Many saw the cloud simply as an alternative way of provisioning infrastructure-based services, such as storage and workload processing, in a more flexible and efficient manner. But it didn't stay that way for long. Endpoints changed from corporate workstations to mobile devices, and cloud services expanded to deliver functionality as well as access. The vast computing power and data that drove huge organizations became available to everyone.

Applications and data that were previously only affordable by large corporations and government agencies started to become available to smaller organizations, eliminating barriers to entry to existing and new markets. Organizations were able to offer more relevant, flexible services and products to their customers.

The rules of society changed as individuals with unprecedented access to data and knowledge began to change the way they engaged with one another and with organizations. Individual consumers started using cloud technology to do everything, from keeping in touch with remote friends, to ordering consumer goods, attending classes, and even seeking a romantic partner. Amid a global pandemic, cloud services provided a way for organizations to survive as employees and customers worked remotely.

As impactful as cloud computing has been, the premise of cloud services is simple. Cloud service providers take complex, rich capabilities, usually developed by large, successful organizations, and make them widely available as commoditized, cost-effective services.

This does not mean that managing the cloud is a simple task. There are countless cloud services available in any market, and an even greater number of ways in which those services can be used. Those tasked with acquiring and managing cloud services must be able to navigate this complex landscape, while bringing the worlds of technology and business together in ways that were not possible just ten years ago. This requires a new set of skills and knowledge, not only about the cloud services themselves, but about the way those services have changed the context in which an organization operates. They will need to change operating and business models, redefine how supplier relationships are managed, and change the way employees work and how customers engage with the organization.

This publication is for consumers of cloud services, who are tasked with finding the best way for their organization to meet its objectives using technology. It is about acquiring and managing cloud services as part of an overall strategy which ensures that an organization stays relevant and successful in a rapidly changing world.

Acquiring and managing cloud services is not a single activity; it is a journey undertaken by an organization together with various types of service provider to find the best way to achieve its strategy. The publication is structured to reflect that journey, showing the stages an organization and its service providers will pass through as it seeks to realize value from using cloud services.

We hope that this guidance will prove to be a helpful tool in navigating these uncertain waters.

David Cannon
Lead editor, *ITIL® 4: Acquiring and Managing Cloud Services*

ITIL Foundation recap

This section provides a brief recap of the concepts introduced in *ITIL® Foundation: ITIL 4 Edition.*

The key components of the ITIL 4 framework are the ITIL service value system (SVS) and the four dimensions model.

The ITIL service value system

The ITIL SVS represents how the various components and activities of the organization work together to facilitate value creation through IT-enabled services. The structure of the ITIL SVS is shown in Figure 0.1.

The core components of the ITIL SVS are:

- the ITIL service value chain
- the ITIL practices
- the ITIL guiding principles
- governance
- continual improvement.

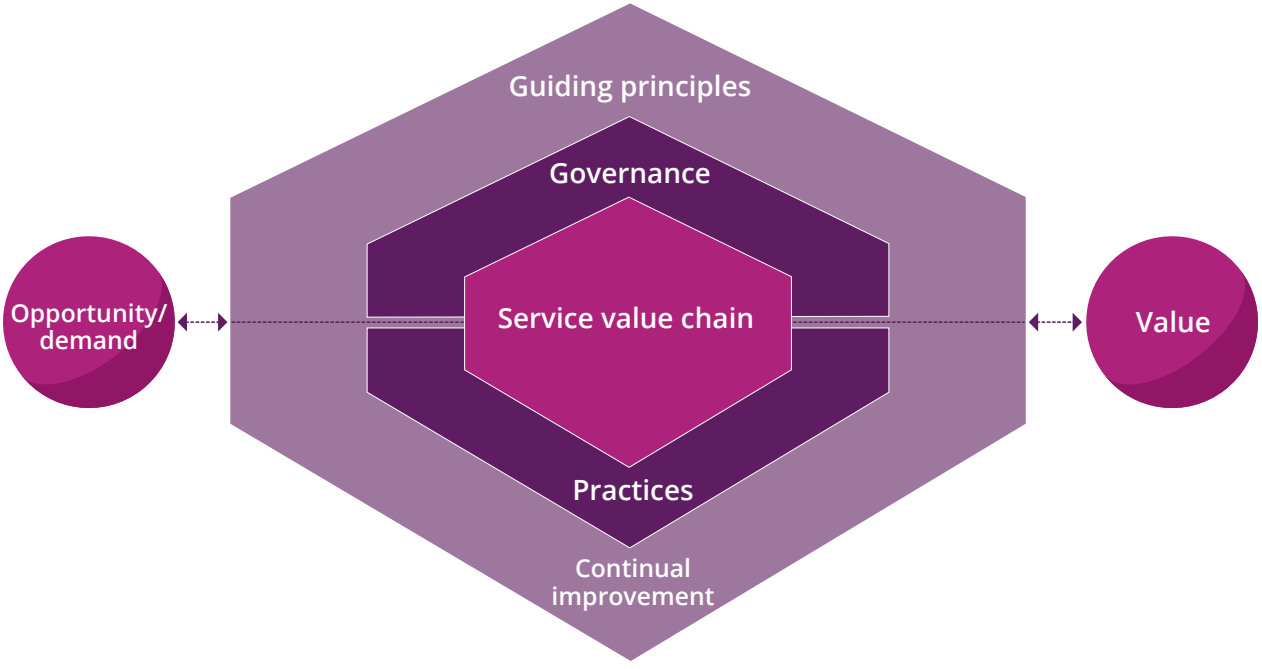

Figure 0.1 The ITIL service value system

The ITIL service value chain

The central element of the SVS is the service value chain, an operating model which outlines the key activities required to respond to demand and facilitate value realization through the creation and management of products and services. The service value chain is shown in Figure 0.2.

The ITIL service value chain includes six value chain activities which lead to the creation of products and services and, in turn, value. The activities are:

- plan
- improve
- engage
- design and transition
- obtain/build
- deliver and support.

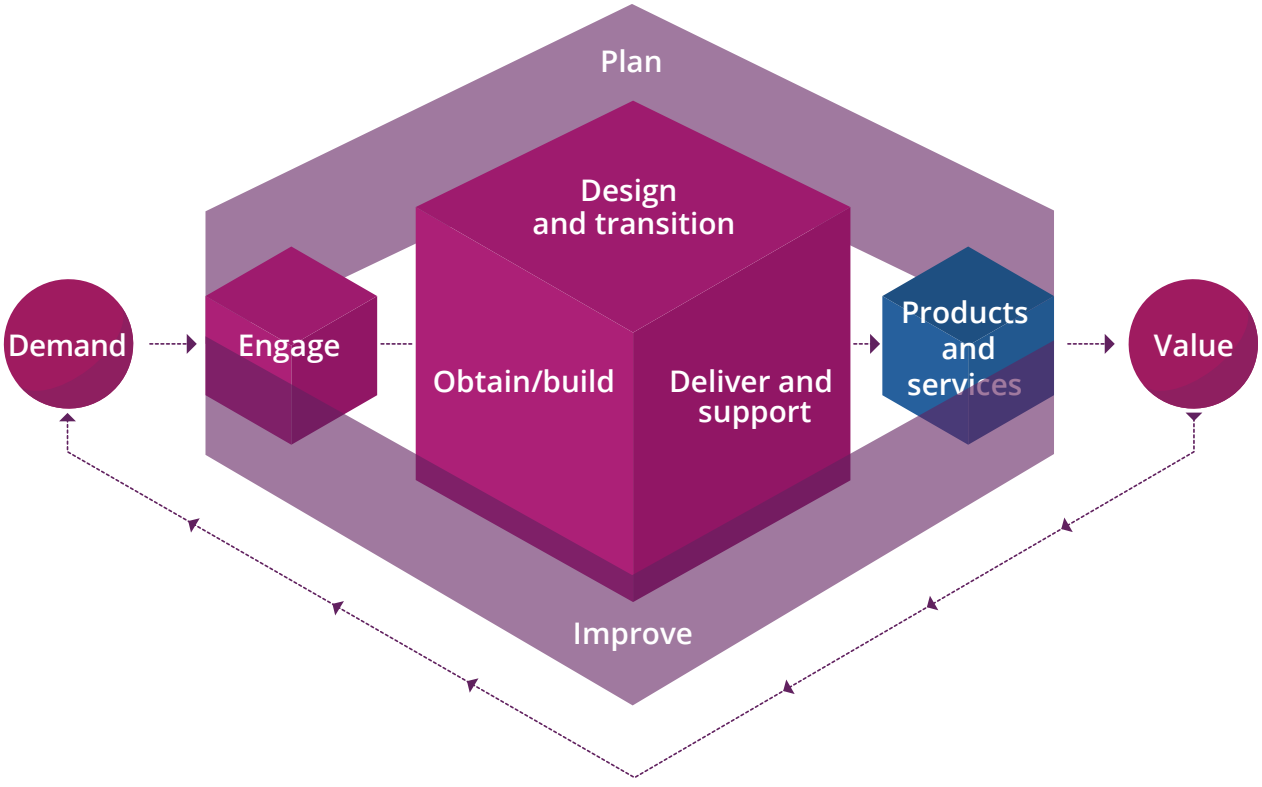

Figure 0.2 The ITIL service value chain

The ITIL practices

Practices are sets of organizational resources designed for performing work or accomplishing an objective. The ITIL SVS includes 14 general management practices, 17 service management practices, and three technical management practices. These are outlined in Table 0.1.

Table 0.1 The ITIL management practices

General management practices	Service management practices	Technical management practices
Architecture management	Availability management	Deployment management
Continual improvement	Business analysis	Infrastructure and platform management
Information security management	Capacity and performance management	Software development and management
Knowledge management	Change enablement	
Measurement and reporting	Incident management	
Organizational change management	IT asset management	
Portfolio management	Monitoring and event management	
Project management	Problem management	
Relationship management	Release management	
Risk management	Service catalogue management	
Service financial management	Service configuration management	
Strategy management	Service continuity management	
Supplier management	Service design	
Workforce and talent management	Service desk	
	Service level management	
	Service request management	
	Service validation and testing	

The ITIL guiding principles

The ITIL guiding principles are recommendations that can guide an organization in all circumstances, regardless of changes in its goals, strategies, type of work, or management structure.

The seven ITIL guiding principles are:

- **Focus on value** Everything that the organization does needs to map, directly or indirectly, to value for the stakeholders.
- **Start where you are** Do not start from scratch and build something new without considering what is already available to be leveraged.
- **Progress iteratively with feedback** Do not attempt to do everything at once.
- **Collaborate and promote visibility** Working together across boundaries produces results that have greater buy-in, more relevance to objectives, and increased likelihood of long-term success.
- **Think and work holistically** No service, or element used to provide a service, stands alone.
- **Keep it simple and practical** If a process, service, action, or metric fails to provide value or produce a useful outcome, eliminate it.
- **Optimize and automate** Resources of all types, particularly HR, should be used to their best effect.

Governance

Governance is the means by which an organization is directed and controlled. The role and position of governance in the ITIL SVS will vary depending on how the SVS is applied in an organization.

Continual improvement

Continual improvement is a recurring organizational activity performed at all levels to ensure that an organization's performance continually meets stakeholders' expectations. ITIL 4 supports continual improvement with the ITIL continual improvement model, outlined in Figure 0.3.

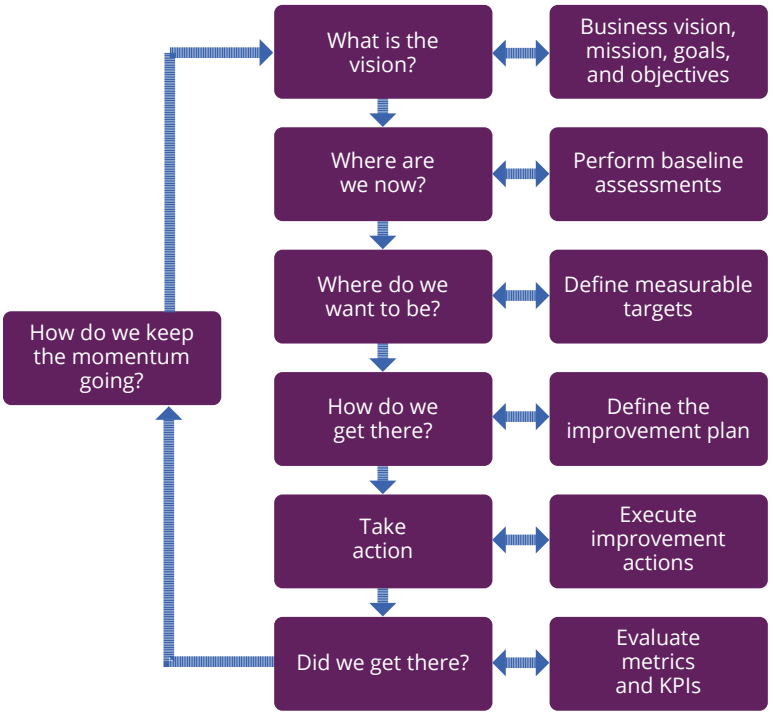

Figure 0.3 The continual improvement model

The four dimensions model

To support a holistic approach to service management, ITIL defines four dimensions that collectively are critical to the effective and efficient facilitation of value for customers and other stakeholders in the form of products and services. The four dimensions (shown in Figure 0.4) are:

- organizations and people
- information and technology
- partners and suppliers
- value streams and processes.

The four dimensions represent perspectives which are relevant to the whole SVS, including the entirety of the service value chain and all ITIL practices. The four dimensions are constrained or influenced by several external factors that are often beyond the control of the SVS.

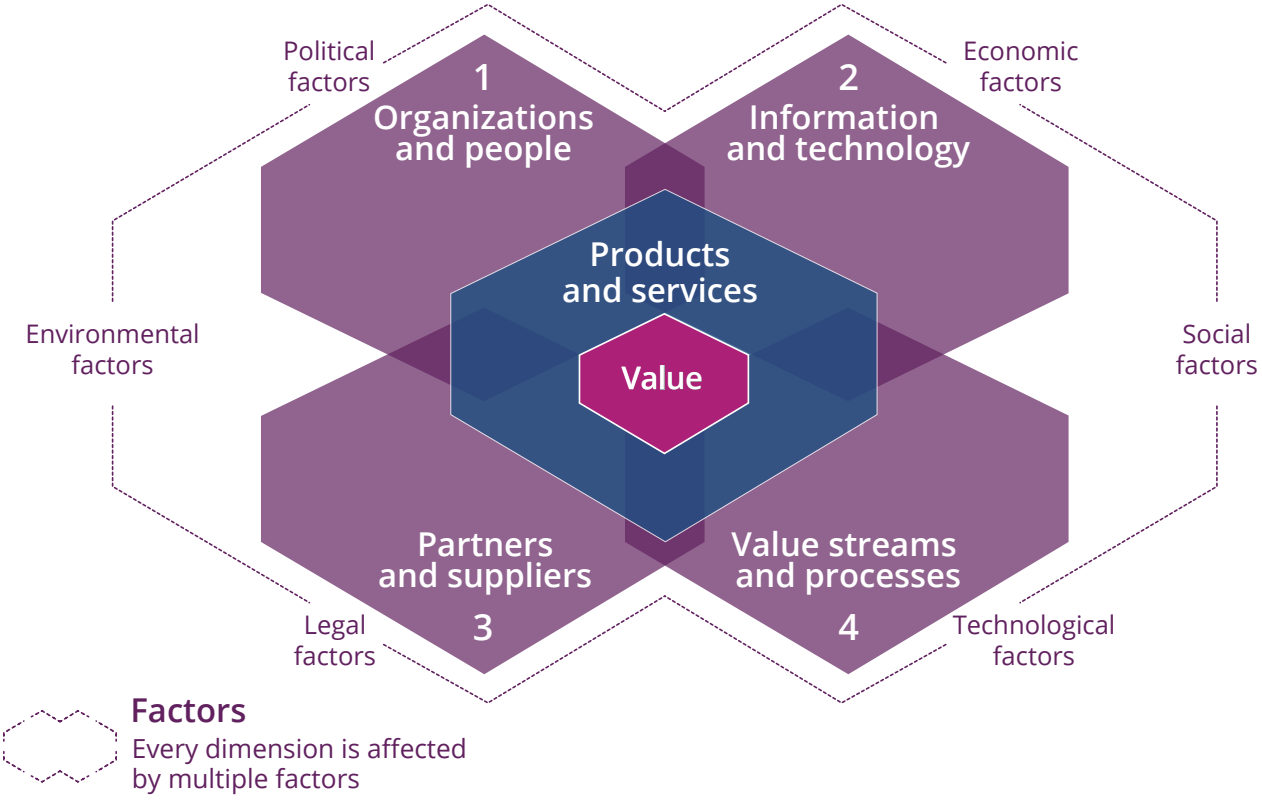

Figure 0.4 The four dimensions of service management

CHAPTER 1

INTRODUCTION

1 Introduction

Digital technology continues to revolutionize how organizations work and manage information. It also continues to create opportunities for growth, including expanding into new markets, developing new products and services, and achieving higher levels of operational excellence.

Modern technology enables organizations to respond rapidly to demand. Servers and database solutions are increasingly available. Almost limitless storage and data processing capabilities can support dynamic patterns of work. Emerging network and telephony advancements enable faster, more efficient services that can deliver information, dynamic media content, and remote collaboration capabilities to users worldwide.

A significant proportion of these successes have been facilitated by cloud technologies, which can fulfil the demand from organizations that need on-demand IT capabilities and resources that traditional in-house IT systems cannot offer. An organization's ability to 'go digital' depends on its ability to source and manage cloud-based solutions and partners that will enable it to leverage the opportunities that emerging technology offers.

Definition: Cloud service provider (CSP)

An organization that offers private or public cloud-based infrastructure, platforms, or applications on an on-demand (or pay-per-use) basis.

Although many IT organizations provide services using private cloud infrastructure, this publication focuses on managing those services obtained from commercial, public cloud service providers (CSPs). These providers can help organizations by providing:

- cost-effective and agile solutions (by pooling resources and optimizing them for availability and flexibility)
- ease of adoption and consumption (through standardization)
- advanced technical expertise (which can support organizations as they assess opportunities and risks).

Many publications about the cloud have been written from the CSP's point of view. They provide definitions and frameworks that explain how consumer organizations can work within their cloud computing architectures. Many of these are technology focused, and do not provide guidance about how these technologies should be used within service management and operational best practices.

This publication defines cloud services from the perspective of the *consumer* organization. The guidance will help consumers to use the capabilities offered by the cloud to identify and pursue opportunities, manage risks, and achieve their desired business outcomes.

Cloud services are no less applicable to small consumer organizations than to large ones; in fact, the cloud offers small organizations access to technology solutions that would otherwise be out of their reach in terms of complexity, affordability, and manageability. Because cloud services are critically important to the success of any organization, small consumer organizations should still be appropriately pragmatic. Small enterprises, micro-enterprises, and even sole proprietors should still approach cloud acquisition and management according to the customer journey, but most likely with less formality in the steps and activities described.

All consumers, regardless of type, size, and scope, should review the entire customer journey to make informed decisions for their organization.

1.1 What is the cloud?

Definition: The cloud

The provision of IT services that are available on demand, via the internet, from a pool of shared resources. These might be storage, processing facilities, operating systems, applications, functionality, development platforms, and/or IT management facilities.

Many organizations have defined cloud technology, usually from a service provider's viewpoint. Although each definition offers nuances of meaning, they all agree on the key characteristics of cloud computing, which include:

- broadly accessible via networks
- metered
- multi-tenant
- shared resource pooling
- on-demand
- self-service
- scalable, with high elasticity.

1.2 The origins of cloud

The first real cloud-like services appeared in the 1990s when commercial webmail was introduced. Service providers offered an email address and storage, with key features available to end users. This was a breakthrough: users did not have to ask their internet provider to set up an email box as a separate service (or for an additional fee). After only a quick registration via the service provider's

website, the customer could have a functioning email account, accessible from anywhere, regardless of their internet service provider.

Although this type of service did not meet all the characteristics of modern cloud services, it represented a shift towards remote, on-demand services via a global network. Early cloud services were a sign of IT commoditization and outsourcing, but CSPs have also been at the forefront of innovation.

1.2.1 Cloud as a result of commoditization

A technology is commoditized when it becomes a standard component that is easily available from multiple sources. When technology has been commoditized, its value is no longer questioned, and the focus shifts from innovation to finding optimal ways of sourcing and maintaining the technology.

For many organizations, the cloud has become the source of commoditized digital solutions, as shown in Figure 1.1.

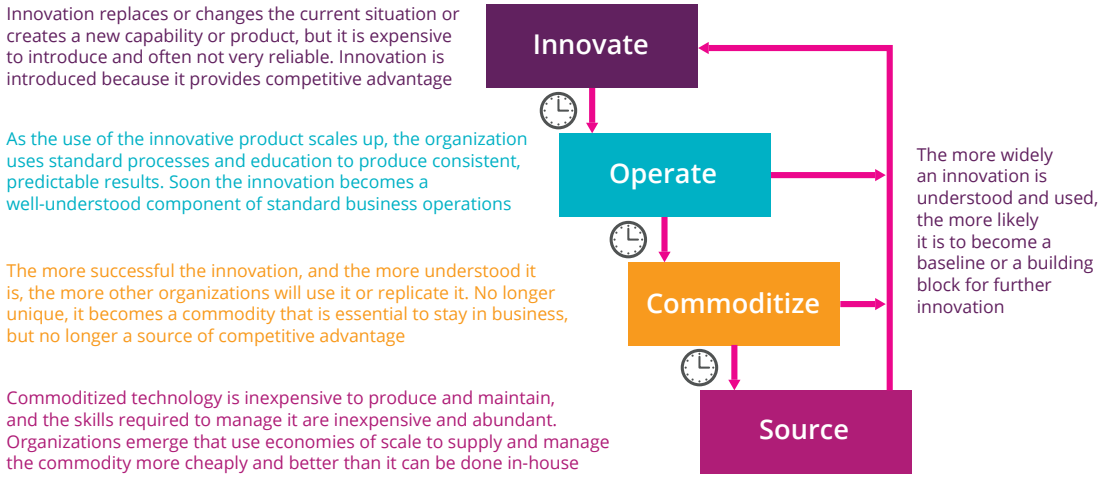

Figure 1.1 Cloud as the source of commoditized digital solutions

When organizations started automating their business processes, they began to need data storage and processing facilities. The earliest solutions were custom-made, and communication technologies did not enable remote accessing or processing of large amounts of data.

This led to many organizations investing in data centres (dedicated facilities that hosted their infrastructure and applications), and in the management and resourcing of infrastructure and facilities. In these situations, IT costs are high and mostly reflected as a capital expense. Because of the pace of innovation, most organizations had to continually invest in IT. The likely returns on investment were often unclear, and there was a lot of risk.

As a result, infrastructure and facilities were often either under-provisioned (resulting in frequent emergency purchases) or over-provisioned (resulting in expensive equipment being under-utilized).

The solutions to these challenges became the building blocks of cloud technology:

- **Technology commoditization** Specialized service providers developed standardized IT solutions when in-house solutions no longer offered competitive advantage.
- **New generations of communication standards** These made it possible to transport and process large amounts of data remotely, with high speed and reliability.

- **Virtualization** This made it possible to configure, restore, modify, and scale IT infrastructure quickly.
- **Orchestration** Middleware solutions introduced orchestration engines, which helped infrastructure providers to monitor and control their computing, storage, and network capacities, allowing them to adjust capacity as needed.
- **Self-service portals** These made IT services much easier to use. Software providers introduced new web-based self-service portals that allowed consumers to choose, change, configure, launch, use, monitor, and decommission services in one place and without external technological support.
- **Payment systems** Allowing international payments, and featuring predictable spend and flexible payment options, made it easy for consumers to pay for services and to see exactly what each service cost.
- **Metering and utilization tracking capabilities** These made it possible to introduce pay-as-you-go services, along with more accurate utilization reporting and root cause analysis. System utilization could easily be aligned with consumer activities and outcomes, allowing consumers to clearly articulate the value of the service. It also became easier to try, implement, use, change, or decommission a service quickly and at minimal cost. Providers could monitor their resource utilization in real time, and consumers could adjust usage based on their budgets and the value of the service.

These developments enabled the paradigm of cloud services: highly standardized IT resources that are available on demand and accessible from remote locations. Alongside other commoditized solutions, cloud became a foundation for the next generations of services, such as the IoT, edge computing, containerization, new hyper-converged infrastructures, and artificial intelligence.

1.2.2 Cloud as a result of innovation

CSPs do not only provide commoditized services; they often pioneer the development and use of emerging technology. Artificial intelligence, machine learning, virtual reality, and IoT technologies often depend partly or entirely on cloud services. Many of these technologies were developed by CSPs and offered to their customers as part of the overall set of services provided. This means that consumers do not have to develop their own solutions to benefit from the advances of emerging technology.

Even those CSPs that specialize in providing highly commoditized solutions are innovative in how they manage, deliver, and support those systems. Most CSPs would consider themselves a key component of their customers' modernization and innovation programmes, providing relevant platforms, skills, and knowledge.

1.2.3 Major differences between cloud services and in-house solutions

A move to cloud changes the way organizations think about managing technology. These changes include:

- **A different level of control over the underlying (physical) infrastructure** When an IT department becomes a customer, it is no longer responsible for managing technology components that are owned by the CSP. Its responsibility shifts to managing the outputs and functionality provided by that technology. Roles and responsibilities must be redefined using a shared responsibility model.
- **Different cost dynamics and approaches to managing costs** Moving to an operating expenditure model demands a better understanding of how IT services are used and funded. The organization must understand how costs are incurred, and define who can incur cloud costs and under what circumstances.

- **Different perspectives about the service quality** An IT department that used to measure system uptime as a measure of quality, for example, may need to measure the ability of a service to support certain activities and outcomes instead.
- **Differences in user experience** Using cloud services is often a different experience from using in-house solutions, including when requesting the service, using the service, and reporting and resolving incidents.
- **The process of changing a service is different** Cloud services and in-house solutions are both flexible, but they need different levels of investment, expertise, and support.
- **Applications need to be cloud-compatible** For example, legacy applications need to be adjusted to include buffers that accommodate latency in queries to the database.
- **Security management responsibilities** Managing the security of cloud services requires some actions to be taken by the CSP and others to be taken by the consumer organization (as defined in the shared responsibility model). In short, the CSP manages the security of the cloud, while the consumer manages security in the cloud (especially how and by whom the cloud service is used).
- **Scalability, flexibility, and elasticity** Cloud solutions are designed to be flexible and scalable. CSPs can manage demand dynamically across pools of shared resources. Most CSPs offer consumers the ability to scale up and down in seconds, move data around, and spin up and shut down resources as needed. Consumers can take advantage of disaster recovery through the existence of multiple data centres, redundant service design, and availability zoning. Although CSPs offer the ability to do these things, the consumer is responsible for controlling when and how they do this.
- **Governance and management control** The service provider is responsible for the control and management of systems used to deliver services, while the consumer controls and manages the services themselves. It is the consumer organization's responsibility to procure services that comply with regulatory requirements, but it is the CSP that designs services which help consumers to meet those requirements and provides secure systems which are well managed. Cloud services offer tools and instrumentation that enable the consumer organization to control how the services are used, and to apply its own standards of use that ensure appropriate governance and control.

1.3 Types of cloud solution

1.3.1 General approaches for consuming cloud service

Before considering individual types of cloud service, a consumer should define a general strategy for using cloud services to achieve its objectives. Table 1.1 outlines two general strategies for consuming cloud services.

Table 1.1 General strategies for consuming cloud services

General strategy	Description
Packaged solutions	A standardized solution that is designed for use with little or no customization, such as a subscription to an office automation software suite
Raw resources	A virtual environment for developing, testing, and/or running digital products and services. A collection of digital resources that the organization's IT specialists can use to develop and manage their own IT products and services

1.3.2 Cloud service models

Within these two broad approaches, consumers can choose from at least three basic types of cloud service, depending on what level of technology or business architecture they need to source. These service models (also called 'delivery models') describe the cloud service from an architectural level:

- **Infrastructure-as-a-service (IaaS)** This service model provides technology components, such as standardized infrastructure services, on a pay-as-you-use or reserved-use basis. For servers that can be provided using commoditized components in the cloud, IaaS provides an alternative to investing in on-site resources that are costly to purchase and maintain.
- **Platform-as-a-service (PaaS)** This service model provides an environment within which systems and solutions can be built. The consumers of these services tend to be developers. Basic functionality is provided, which saves time and money on writing extensive code from scratch. PaaS services are used to build and manage unique applications using standard platform features and functionality.
- **Software-as-a-service (SaaS)** This service model provides applications that can be used as they are, or with limited customization to suit a particular consumer. SaaS provides quick access to standard functionality for a particular area. This software can be accessed securely from anywhere and on any device that has an internet connection. These services are generally sold through subscriptions.

Service providers often discuss further categories, sometimes called *business-process-as-a-service* (BPaaS) or *anything-as-a-service* (XaaS). Although these are based on cloud services, they are usually a blend of cloud services and outsourced business activities.

Each of the three basic service models requires different levels of responsibility for the layers of the technology architecture. This in turn affects the organizational design, including the positioning and structure of an IT team within the consumer organization. This is illustrated in Table 1.2, which shows whether each layer of the architecture is provided by the consumer or by the CSP.

Table 1.2 Architecture included in each cloud service model

	In-house	Infrastructure-as-a-service	Platform-as-a-service	Software-as-a-service
Business activity	Consumer	Consumer	Consumer	Consumer
Applications	Consumer	Consumer	Consumer	CSP
Data	Consumer	Consumer	Consumer	CSP
Runtime	Consumer	Consumer	CSP	CSP
Middleware	Consumer	Consumer	CSP	CSP
Operating system	Consumer	Consumer	CSP	CSP
Virtualization	Consumer	CSP	CSP	CSP
Servers	Consumer	CSP	CSP	CSP
Storage	Consumer	CSP	CSP	CSP
Networking	Consumer	CSP	CSP	CSP

From a service consumer perspective, the choice of service model depends on how the organization expects to benefit from the key cloud service characteristics, balanced against a lack of customization and direct control.

Examples of the type of service typically offered through each service model are:

- **IaaS** Computing-, network-, storage-as-a-service
- **PaaS** Data-, function-, container-, code-as-a-service
- **SaaS** Enterprise resource planning, customer relationship management, office-automation-as-a-service, translation-as-a-service.

An important consideration for SaaS services is whether they will be customized, and how much customization will be allowed. Most SaaS services require some configuration (such as which features are available to which users). Customizations are changes that require coding, functionality and regression testing, deployment management, and so on. A heavily customized SaaS service may hinder the flexibility of the service, and the organization's ability to benefit from frequent updates to functionality and features.

Many digital and IT services meet the technical definitions of cloud, including those not perceived as 'cloud' by their providers and consumers. For example, office printing may have cloud characteristics, but is rarely perceived and managed as a cloud service. It is important that consumers evaluate the claims of the service provider to ensure that the services offered are truly cloud services. For example:

- A service provided from a standalone data centre or server room, no matter what architecture it uses, is not a cloud service.
- The fact that users can access an application from home, using the internet, does not necessarily make it a cloud service. Employees working from home and accessing in-house systems are not necessarily using cloud services.
- Some services can be delivered using characteristics of the cloud (such as metered utilization or virtual devices) but may not carry the advantages of pooled resources and redundant facilities and systems.

1.3.3 Standard and non-standard services

All categories of service vary in the degree to which they are available as standard or non-standard services. Standard services are offered through catalogues, and there is little or no room for negotiation about their features and performance. Non-standard services include cloud migration planning, support and consulting, and SaaS customization.

It is important that consumers understand the degree to which a service can be changed, so that they use the appropriate acquisition approach (such as purchasing from a catalogue or using a request for proposal) and to ensure that there is no misunderstanding about the ways in which the service can be used.

This difference between standard and non-standard services is described in detail in section 3.3.

1.3.4 Deployment models

Another common type of cloud service is the deployment model. These can be private, public, or hybrid deployment models. The key difference between these types is the level of multi-tenancy of the services, as outlined in Table 1.3.

The term 'deployment' is useful when thinking about how services are provided, but from a consumer perspective, it is more helpful to think in terms of resource- or capacity-sharing models.

Table 1.3 Deployment models

Service provider perspective: deployment model	Service consumer perspective: resource-sharing model	Characteristics
Private cloud	Fully dedicated	Based on customized consumer requirements Consumer-centric; each service is built specifically for individual consumers Expensive because of high direct costs Underlying infrastructure can be owned by the service consumer or an external service provider
Public cloud	Overall cloud infrastructure is shared with other consumers	Services are delivered using standardized components The overall infrastructure is shared; each individual service is private for each customer Product- or service-centric; consumers design, configure, deploy, and manage the services, and optimize how they use them Consumers can work with the CSP to request added features or to develop new types of service More affordable due to shared costs The underlying infrastructure is owned by an external service provider
Hybrid cloud	Mixed	A combination of bespoke and standardized services from several service providers Mostly consumer-centric, with some dependence on standardized services Consumers must ensure that dependencies between service components and contracts are coordinated Individual services are often more expensive because it is more difficult to achieve economies of scale Configuration is complex and requires in-depth interaction between consumers and service providers
Multi-cloud	Shared across multiple service providers	Multiple cloud services are used as part of a single architecture Could be a combination of public and private services Allows cloud services from different providers to be selected according to the task being performed, although this might reduce the potential discounts available when using a single CSP Purchasing frameworks of pre-authorized services and providers are set up, and consumers order the most appropriate service based on their current needs

Each of these models could be beneficial, depending on the context in which it will be used. However, most of the benefits related to cloud (such as higher security, lower costs, and access to more innovative services) are achieved through a public-cloud model. This means that, in practice, the term 'cloud services' usually refers to a public cloud. This applies to the following chapters, unless stated otherwise.

1.3.5 Types of cloud service provider

There are many types of CSP. Some specialize in only one type of service, while others provide a combination of cloud service models and deployment models. Some provide highly standardized services to a diverse range of consumers, while others provide customized services to individual consumer organizations.

There is no single best way of managing the relationship with this array of organizations. This publication will outline the major activities of acquiring and using cloud services, but they will need to be applied to the specific types of CSP on a case-by-case basis. The consumer of cloud services will need

to investigate the nature of the CSP and the services offered before concluding a contract. For example, large CSPs can offer cost-effective services because they are able to standardize those services and offer them at scale. These 'hyperscale' CSPs are unlikely to produce one-off, customized services. They will monitor the use of their services, investigate new technology, and conduct market research to make changes that benefit all their customers using those standard services.

Hyperscale CSPs rely on a network of partners to assist consumers in selecting the appropriate services, migrating to those services, and using them effectively. Some partners will even build customized functionality on top of the standardized services. It is important that consumers differentiate between the services provided by these partners and the CSPs themselves. For example, when acquiring standard services from a hyperscale CSP, there is little or no room for negotiating features or the price of standardized services. The opposite is true of a boutique CSP that provides customized instances of its SaaS solution. Although the overall steps taken to acquire and use these services are similar, the detailed process, benefits, and risks associated with each are very different.

More details about the types of CSP, partners, and cloud services are provided in sections 3.2 and 3.3.

1.4 Deciding to use cloud services

An organization needs to develop and maintain an effective strategy for sourcing and managing cloud services. This strategy should be aligned with the organization's business and technology strategy and architecture, risk management approach, information security policies, business continuity plans, and sustainability policies. It should also consider external factors, including regulatory requirements.

Strategic decisions about cloud are based on a detailed assessment of internal (the four dimensions of service management) and external (PESTLE) factors, including the following considerations:

- How can the organization benefit from cloud solutions, and what are the expected benefits?
- What level of the IT architecture is the best to source from the cloud?
- What cloud deployment model is best for the organization?
- How will the risks associated with using cloud solutions be managed?

Cloud strategies are discussed in more detail in Chapter 2.

1.4.1 Benefits and disbenefits of using cloud services

This publication refers to the benefits and features of the cloud throughout. Because its focus is on acquiring and using cloud services, it provides more information on how to obtain value from using cloud than on the reasons for not using cloud. However, readers should evaluate every option carefully, whether in-house or in the cloud. The benefits and disbenefits of using cloud services depend on the context. Every feature of cloud could be a benefit in one context, and a constraint or disabler in another.

The features, benefits, and disbenefits of using the cloud are outlined in Table 1.4.

Table 1.4 Cloud features, benefits, and disbenefits

Feature	Benefits	Disbenefits
On-demand, scalable, and elastic nature of cloud services	Supports an agile approach to strategic planning, making it easier for an organization to respond more effectively to VUCA contexts, which results in higher speed to market and to value realization	Organizations that are unable to extend the way IT services are managed into the cloud may experience cloud sprawl, which is the uncontrolled and unmanaged use of cloud services with little or no access control. This increases risk and costs, with effects that emerge too late to be prevented
Transitioning a significant part of IT costs from capex to opex	Supports shorter financial planning and evaluation cycles, and contributes to the organization's agility	Requires the organization to reconsider its budgeting, forecasting, and financial controls In some organizations, this change in culture might be resisted
Using pay-as-you-go models	Helps to optimize variable costs and accommodate experimentation and fluctuations in demand Helps to prevent over- or under-provisioning of IT resources	If workloads are not quantified in terms of user activity before the migration to cloud, costs are unpredictable, and sudden increases could catch the organization unawares Many CSPs provide cost calculators to assist consumers in predicting spend based on workload
Delegated responsibility for IT infrastructure	Allows the organization to focus on objectives rather than IT maintenance	Cloud services are standardized. They can be used in a flexible manner, but their functionality and performance are restricted to the terms of the contract with the CSP
Accessible emerging technology, functionality, and advanced technical expertise from CSPs	Greater ability to innovate	The use of new technology and tools can become an end in itself
Access to advanced skills and knowledge without having to hire expensive dedicated resources	Greater ability to innovate and apply the feature	These skills are typically available from CSPs or CSP partners on a contracted on-demand basis In-depth, organization-specific knowledge and experience cannot be replicated. Solutions that depend on these to be effective should not be considered prime candidates for cloud migration
A net reduction in the amount of IT equipment required and power consumed	More sustainable IT solutions, including a reduction in the customer organization's carbon footprint through reduction of in-house equipment, power consumption, and cooling capacity	Organizations that fail to extend responsible use and governance into the cloud are unlikely to achieve a net reduction in IT utilization costs. For example, a consumer that moves storage into the cloud will not achieve a net benefit if users store multiple versions of data or duplicated data, or refuse to archive data
Abstraction from the underlying technology and infrastructure	Reduction in administrative burden for internal IT personnel allows staff to focus on technical debt or other organizational goals and objectives	Significant limits placed on (or a reduction or loss of the traditional level of) management control
Ability to comply with various governance and regulatory requirements	Selecting the appropriate CSP can enhance the consumer's ability to meet regulatory requirements, such as location of data storage	Some elements of compliance may be less visible or controllable, as specific points may not be in the consumer's direct control. Instead, they must be taken from third-party audits or attestations

Table continues

Table 1.4 *continued*

Feature	Benefits	Disbenefits
A level of security based on current standards and proven techniques	The CSP may be able to provide an enhancement to the security measures and controls the consumer is able to implement	The consumer must rely on third-party audits to assure themselves that the CSP is providing the appropriate level of security. The consumer organization must retain responsibility for security and risk management of service in the cloud

Not all cloud services will lead to all of the benefits outlined in Table 1.4. Furthermore, the value of cloud largely depends on the organizational culture and appetite for innovation. The best approach involves balanced strategic decision-making that accounts for the organization's objectives.

1.4.2 Risks of using cloud services

Alongside benefits and disbenefits, cloud consumption can potentially introduce risks and constraints. These are described in more detail in section 2.5.3, but can be grouped into three main categories:

- **How organizations use and manage cloud services** Many organizations are unprepared for the change from IT service provider to cloud service consumer or service broker. Associated risks include:
  - Using cloud services as a basis for pursuing new markets or developing new products may require a significant change to the organization's culture. Some organizations may find these changes too ambitious.
  - For some IT departments, the change from being a service provider to being a broker of services provided by a CSP can be challenging.
  - If an organization is looking to cloud to fix issues caused by a lack of governance and control, it will find it equally challenging to manage those issues for services in the cloud.
- **Failure to understand the unique nature of each CSP** Although many cloud services are based on commoditized technology, CSPs differentiate themselves by providing unique features and services. They do not determine their customers' strategies, but their services and culture can help or hinder an organization as it pursues its strategic objectives. Understanding the unique culture, offerings, and strategy of each CSP is critical for selecting a CSP and services.
- **Choosing the appropriate cloud service model(s) or deployment model(s):**
  - Organizations using highly commoditized SaaS services will generally find them faster and cheaper than other services. However, these services will not provide much advantage if all their competitors are also using them (in these cases, not using the service would put them at a competitive disadvantage).
  - A lack of understanding of what will be provided as part of the service may be an issue in cloud migrations. Knowing the trade-offs between in-house, IaaS, PaaS, and SaaS services is critical.

1.5 Cloud as a key component of digital strategy

ITIL® 4: Digital and IT Strategy describes digital strategy as 'a business strategy that is based all or in part on using digital technology to achieve its goals and purpose'. This definition reflects the significant and increasing role of digital technology in modern organizations' business and operating models. Because digital technology is largely dependent on the attributes of cloud technology, digital strategy will depend increasingly on the use and expansion of cloud services.

There is, and will continue to be, an increase in the use of cloud services. This will be fuelled mainly by organizations' needs for flexible solutions, the ability to optimize costs according to volatile industry conditions, and remote-access services.

However, having a digital strategy is not a prerequisite for using cloud services. Many organizations that do not have a formal digital strategy are using cloud services; these may have been introduced by an IT group, a shadow IT group in another business unit, or a grass-roots initiative involving several employees. Regardless of how they were introduced, these cloud services mark a significant shift in the way technology is being used in organizations. It is important to address their further use in a coordinated, strategic manner.

Digital strategy also defines how governance should be appropriately applied throughout the organization. This is not so much about control as it is about thinking and working holistically. This ensures that all parts of the organization are working together in the best possible ways to meet its objectives. A hands-off approach (where individual groups make sourcing decisions without guidance or coordination) can result in data loss, security breaches, duplicated services, contradictory contracts, and inefficient operation.

Chapter 2 provides further guidance on cloud governance and strategy. Readers should refer to *ITIL® 4: Digital and IT Strategy* for detailed guidance on digital strategy.

1.6 The role of cloud services in a digital transformation

No modern organization, regardless of industry, size, or business model, can avoid the need for digital transformation. Whether it is automating a single business activity, launching a new business to tech-savvy consumers, or modernizing an entire business, digital capabilities are essential. Although it is better if these initiatives are conducted as part of a cohesive digital strategy, many organizations prefer to perform them as one-off projects.

In either case, most digital transformation projects will use technology that either is based in the cloud or relies on cloud services in some way.

Definition: Digital transformation

The use of digital technology to enable a significant improvement in the realization of an organization's objectives that could not feasibly have been achieved by non-digital means.

The term 'digital transformation' is not specific to a particular type of transformation, and can be used to refer to any transformation that is digitally enabled. The transformed entity is often a combination of the organization's customer experience, products or services, business model, operating model, and employee experience.

Digital transformation often includes the introduction or expansion of cloud services that the organization consumes, and may also include the development and delivery of cloud services addressed to its customers. Although cloud service delivery is outside the scope of this publication, it is important to note that it can only be possible and successful if the underlying technology is managed

and used effectively and efficiently. In many cases, this underlying technology is a cloud service (IaaS or PaaS). Effective consumption of cloud services is, therefore, a critical enabler of a digital business.

Cloud adoption and management should be a key element of the organization's digital transformation programme. This is based on the effective management of the customer journey, as described in this publication.

1.7 Cloud services and sustainability objectives

Many organizations see cloud as a key component of their sustainability strategy because cloud services use shared resources and multi-tenant architectures in state-of-the-art, energy-efficient facilities.

However, simply migrating to the cloud does not automatically reduce an organization's carbon footprint or make it more socially responsible. *ITIL® 4: Sustainability in Digital and IT* provides detailed guidance on how to achieve sustainability objectives using cloud services.

'Sustainability' refers to an organization's continuing viability: specifically, ensuring that the environment in which it operates will continue to support its success. The more an organization nurtures the environmental factors that make it successful, the more it will thrive as that environment changes. This translates into social responsibility programmes, environmental programmes, political engagement, and so on.

The sustainability (or long-term viability) of an organization is one of the main objectives of its strategy. As such, this objective is carried over to the digital strategy and cloud strategy.

Cloud services support an organization's sustainability in many ways, including:

- **Replacing inefficient systems with efficient cloud services** Many CSPs provide information about the efficiency of their architecture as standard.
- **Reducing duplication by rationalizing applications and infrastructure and standardizing services** This involves understanding the full portfolio of technology-based capabilities and how they are used, then replacing them with capabilities that are sourced in the cloud.
- **Responsible use** Pay-per-use services encourage the efficient use of technology resources, such as storage, and ensure that organizations do not overprovide. However, this is only true if the costs are directly visible to the users of those services. Where IT departments move storage or computing workloads to the cloud and still try to pay for them from a centralized IT fund, they often find that usage and costs spiral upwards. This can only be managed with full cost transparency and effective governance.
- **Elevating career opportunities** As commoditized components and routine activities are sourced from the cloud, the organization can explore higher-order opportunities for employees. It will also need to embrace a culture of innovation and experimentation.
- **Staying relevant as customer and environmental needs change** Cloud services are agile and mutable, which allows an organization to respond quickly to rapidly changing situations.

1.8 Governance

1.8.1 Governance of cloud services

ITIL® Foundation: ITIL 4 Edition describes governance as a system by which an organization is directed and controlled, realized through three key activities: evaluate, direct, and monitor.

Governance cascades through the organization, from corporate or enterprise governance to business unit or team governance, and can also be applied to groups of resources (such as practices) or activities (such as projects). This allows the governance of small teams to remain aligned with the objectives of corporate governance.

Key message

Governance is not the same as management. Governance is focused on setting an organization's goals, directions, constraints (financial, legal, sourcing, and so on), and accountability. Management is focused on obtaining and allocating resources (technical and non-technical) and ensuring that day-to-day activities are aligned with the organization's stated goals and direction, and are compliant with any stated constraints.

An organization can be thought of as a collection of smaller organizations for the purposes of illustrating the governance cascade. Each of these organizations can be regarded as a service value system, which will include the governance component. In this way, practitioners can connect the governance of different projects and teams to the overall enterprise governance, as shown in Figure 1.2.

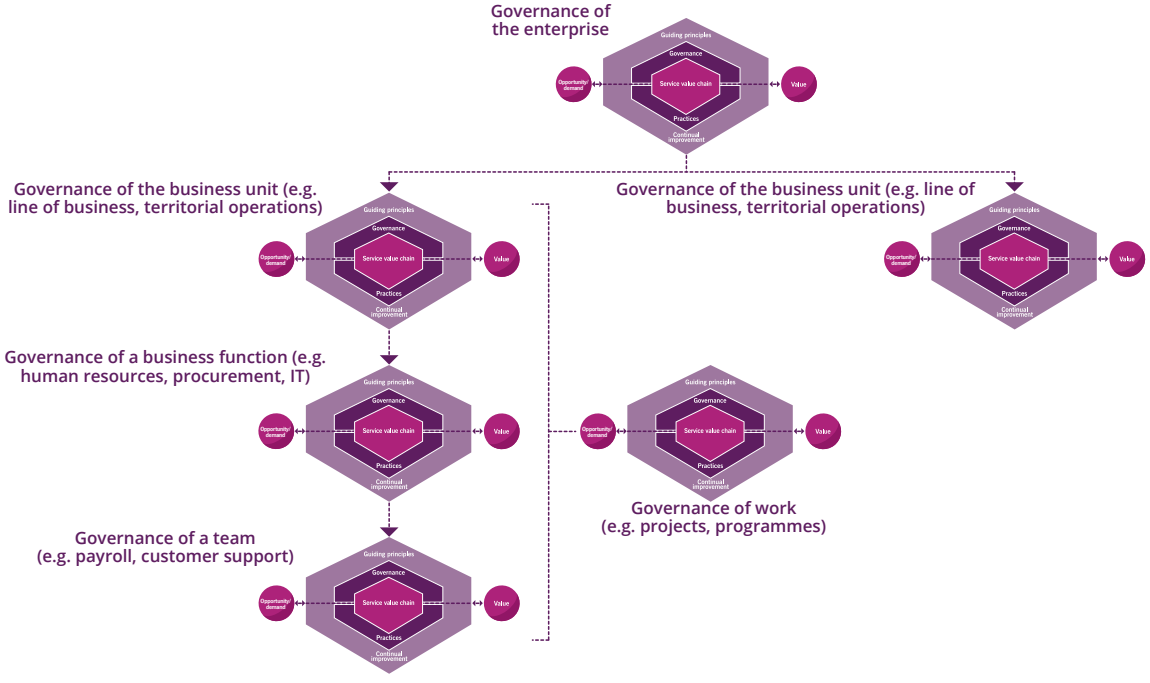

Figure 1.2 The governance cascade

As governance cascades across the organization, it should be contextualized to use the language of the relevant domains and teams. For example, the language of governance in a procurement team may be different from that used in the human resources department.

Cloud procurement activities vary in scope and scale, and therefore so do the scope and scale of governance. The acquisition of a cloud solution that is small in size and impact (such as an online mailing list platform) to meet the needs of a specific team or function might require only team and/or functional governance. An acquisition that will significantly impact multiple functions and teams (such as migrating from a data centre to a CSP) is more likely to be run as a project or programme, with its own dedicated governance.

The focus of governance (and thus the artefacts of governance) could also change as an organization progresses through the customer journey. Specific steps of the journey (or pieces of work within a step) might be subject to additional governance elements. For this reason, it is important that the governance elements of a cloud adoption journey are dynamic and flexible.

The elements of governance specific to each step of the cloud customer journey are:

- **Explore** This step focuses on understanding the organization's needs, defining value, and identifying potential CSPs. These activities are influenced by corporate and business unit governance. These levels of governance should have artefacts (such as a clearly articulated vision of how the organization will create value, or a list of sustainability commitments or objectives that will shape how the cloud-sourcing initiative defines value for the organization and its stakeholders) and identify CSPs that can help the organization meet the needs of multiple stakeholder groups.
- **Engage** This step focuses on building relationships with CSPs. These activities are influenced by corporate and business unit governance (for example, sustainability objectives covering sourcing of third-party products and services, or commitments to work with or exclude certain industries), and by functional or team governance depending on scope (for example, using only local service providers, or those owned by minority groups).
- **Offer** This step focuses on specifying, harmonizing, and consolidating requirements for the cloud solution. These activities are largely internal in scope, and are thus influenced by corporate, business unit, functional, and team governance (such as behavioural values and policies, governance around the use of tools and data to collaborate across stakeholder groups, or information security and data governance). Sometimes this step also includes proof-of-concept and pilot projects or programmes, which may require dedicated governance.
- **Agree** This step focuses on negotiating and agreeing service utility, warranty, and experience. Activities in the agree step are influenced by corporate and business unit governance (such as financial management and sourcing policies, and sustainability objectives), and by functional or team governance depending on scope (such as using only local contractors, reducing the amount of paper waste, or alignment with functional or team roles and responsibilities).
- **Onboard** This step focuses on transitioning to the CSP, and on offboarding from incumbent solutions and providers. Activities in this step are influenced by corporate, business unit, functional, and team governance (such as behavioural values and policies, governance around the use of tools and data to collaborate across multiple stakeholder groups, or information security and data governance). In large-scale cloud adoptions, this step will almost certainly be run as a project, or a work stream within a larger programme, and would thus benefit from additional governance by a steering committee or programme board.

- **Co-create** This step focuses on the ongoing consumption of cloud services and management of the relationship with the CSP. These activities are shaped by corporate and business unit governance, and by functional and/or team-level governance (for example, financial management and sourcing policies, alignment with functional or team roles and responsibilities, management of data).
- **Realize** This step focuses on tracking, assessing, and evaluating the ongoing co-creation of value with the CSP and the customer journey to date. These activities are shaped by corporate and business unit governance, and by functional and/or team-level governance (for example, financial management and sourcing policies, alignment with functional or team roles and responsibilities, management of data). If activities along the customer journey were managed as projects or programmes, there may be additional governance activities at that level (such as documenting and sharing lessons learned and recommendations for future activities, or documenting and publishing earned value calculations).

1.8.2 The shared responsibility model

The shared responsibilities in a cloud solution must be clearly defined. All stakeholders should understand which security and compliance tasks are handled by a CSP, and which are managed by the consumer organization. If a CSP partner is involved in any aspect of the acquisition, migration, and management of cloud services, its roles and responsibilities must also be clearly differentiated. The measures and areas of responsibilities will vary depending on:

- where the workload is hosted
- the type of service being consumed
- the involvement of a partner or service broker
- each CSP's terms and conditions
- CSPs' compliance with standards, which may cover only a portion of the consumer's end-to-end responsibility.

The acquisition of secure cloud services and secure usage of those services is the responsibility of the consumer organization. The consumer organization should:

- understand the level of security of the cloud service as it is provided by the CSP (because the CSP is responsible for security in the cloud). This might involve reviewing audit results and attestations from the CSP. A CSP that provides standardized services is unlikely to review and revise its security measures based on the individual requirements of each of its customers
- define how it will secure its use of cloud services, and how it will use the security-related tools and features provided by the CSP (because the consumer is responsible for security in the cloud).

When moving from one CSP to another, or when consuming services from multiple CSPs, it is important to understand the differences in how each CSP applies the shared responsibility model. In all cases, the consumer organization must first understand what its responsibilities would be if it were managing the solution in-house; all of these responsibilities should be specified and assigned in each shared responsibility model.

The areas of responsibility depend on various factors for different delivery models. These factors include, but are not restricted to:

- type of service relationship (the responsibilities of a CSP offering a range of IaaS, PaaS, and SaaS services may differ from those of a specialist CSP that only offers one type)

- packages of cloud services the customer can procure (such as a subscription to a software package or use of a development platform)
- customized or tailored services
- technology integration between the consumer and provider (such as where a cloud-based application depends on data held in-house)
- laws and regulations applied to specific services (such as privacy laws or industry-specific regulations).

A cloud consumer and CSP never share responsibility for a single aspect of security operations. The areas of ownership that the consumer controls belong to the consumer; for example, the provider does not dictate how its client secures its systems or data. Likewise, the cloud consumer does not control how the provider secures its applications (or portions of the applications), platforms, middleware, operating systems, or infrastructure stack. However, the cloud consumer has the right to access the provider's audit reports to check that its systems are secure. This means that the consumer organization should perform all of the necessary security configuration and management tasks in addition to the CSP solution.

The consumer organization retains responsibility for security as it moves applications, data, containers, and workloads to the cloud, while delegating some activities (such as securing the physical infrastructure) to the CSP. The shared responsibility model, shown in Figure 1.3, defines the line between consumer and provider responsibilities. It should be tailored based on the service and the organizational context.

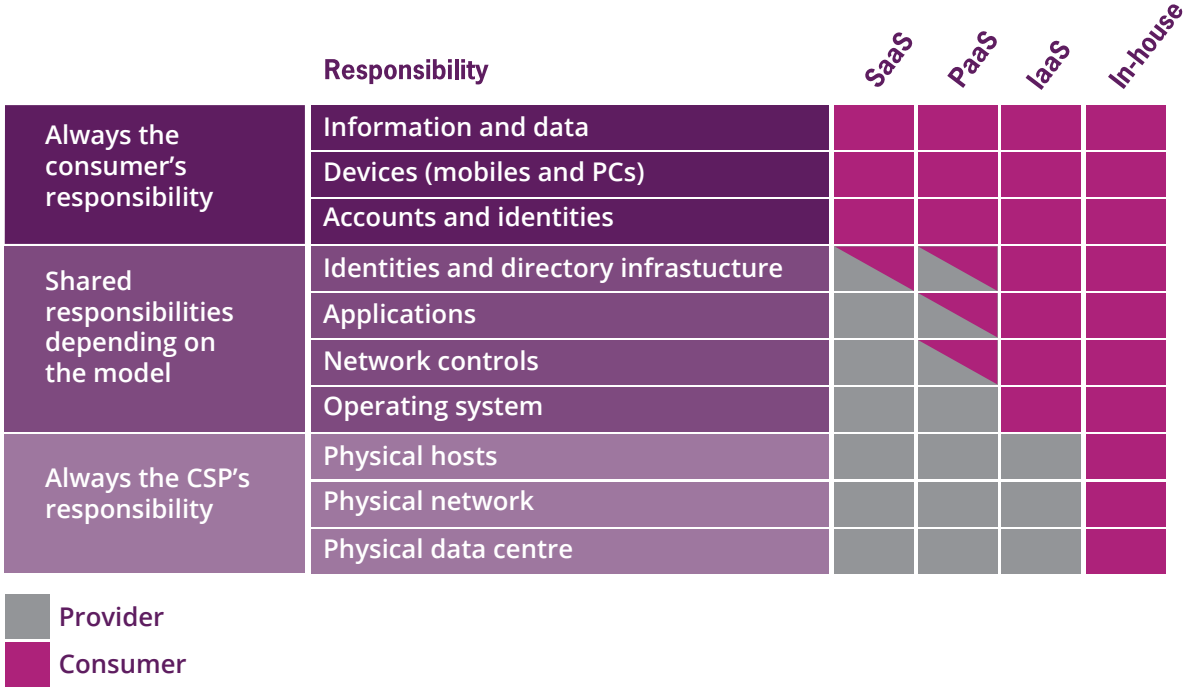

Figure 1.3 The shared responsibility model

In the shared responsibility model, it is important that the ownership of security is clearly defined, with each party maintaining control over the assets, processes, and functions it owns or manages. By working together with a CSP that provides a secure cloud environment and management tools, a consumer organization can meet its security management responsibilities with less operational overhead.

Each environment, application, and service will require a dedicated approach to the assessment and monitoring of security. The organization's overall security position is defined by its weakest link. If there is a gap in coverage in any one system, this increases the vulnerability across the entire stack and any connected systems.

Security measures provided by CSPs are often standard and proven to work, whereas consumer organizations' security measures are often developed as needed, but they must work within the constraints provided as part of the CSP's service.

1.8.2.1 Responsibilities always owned by the CSP

The CSP always controls:

- the physical security of the infrastructure, including equipment room location; power supply assurance; cooling facilities; protection against fire, water, shock, and theft; and surveillance (for details about security requirements, see related standards)
- the security of computing, storage, and network hardware
- the security of basic networks, such as firewalls and prevention of distributed denials of service
- cloud storage security, such as backup and recovery
- the security of cloud infrastructure virtualization, such as isolation of tenant resources and management of virtualization resources
- tenant identity management and access control
- secure access to cloud resources by tenants
- the security management, operating monitoring, and emergency response of technology under its control
- formulating and rehearsing service continuity assurance plans and disaster recovery plans for infrastructure
- the virtualization layer.

1.8.2.2 Responsibilities mainly owned by the consumer organization

The responsibilities that are mainly owned by the consumer organization include:

- defining and applying security policies for the configuration and use of cloud services
- user identity management and controlling access to service systems
- data security (in the European General Data Protection Regulation [GDPR] model, consumer organizations control the data and should be responsible for data security, while CSPs process the data and act as data controllers)
- security management and control of terminals that access cloud services, including hardware, software, application systems, and device rights
- business processes, policies, and roles; workflows; and procedures and their components integrated with cloud-based technologies.

1.9 How to use this publication

1.9.1 Intended audience

Anyone involved in defining cloud requirements, selecting a CSP, migrating to cloud, or exploring how to subscribe to standard cloud services to support their organization may find this publication useful. The guidance especially applies to those organizations that wish to use cloud services internally, or to use them as the basis for delivering services to their external customers.

1.9.2 The cloud consumer journey

This publication is vendor-neutral and focuses on the tasks, responsibilities, and good practices of a cloud consumer. It is based on the concept that cloud consumers follow a journey similar to the customer journey introduced and described in *ITIL® 4: Drive Stakeholder Value* and shown in Figure 1.4.

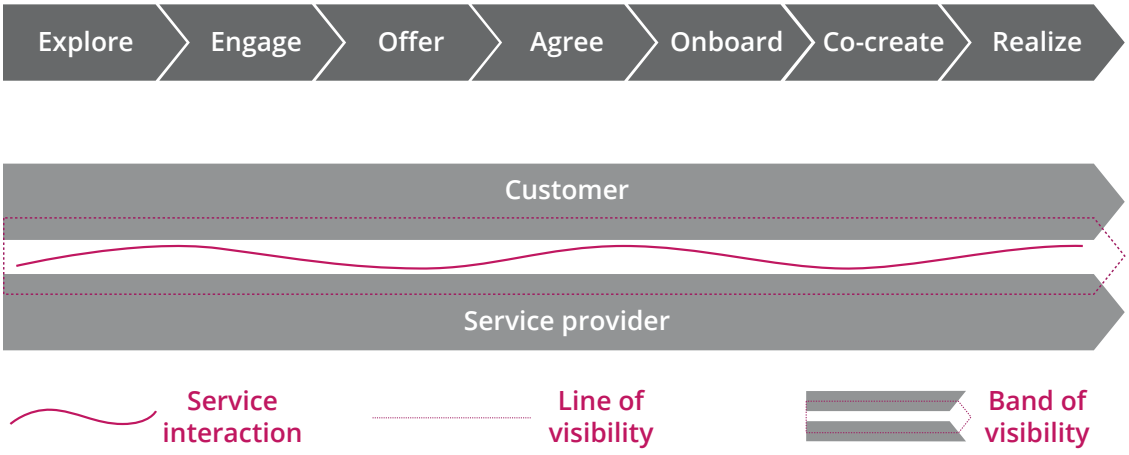

Figure 1.4 The customer journey

Definition: Customer journey

The complete end-to-end experience that service customers have with one or more service providers and/or their products through touchpoints and service interactions.

This publication is structured around the typical steps of the customer journey. However, some organizations may take different steps, or take the same steps in a different sequence. In the context of cloud, the journey illustrated in Figure 1.4 consists of the following steps and activities:

- **Explore** The organization explores how cloud could contribute to its success. This step involves:
  - reviewing the organization's strategy
  - assessing the role of cloud in meeting the strategic objectives
  - defining a scope of areas that will benefit from using cloud services.

- **Engage** The organization identifies potential services and CSPs, and works with them to define its requirements for cloud services. This step involves:
  - understanding the CSP landscape
  - defining requirements
  - conducting a cloud readiness assessment
  - meeting with CSPs.
- **Offer** The organization specifies and communicates its requirements for cloud services, usually in the form of a request for proposal (RFP). CSPs respond to the RFP and a solution is selected. This step involves:
  - specifying and communicating requirements
  - creating an RFP
  - evaluating RFP responses
  - determining the return on investment for the chosen solution, and creating a business case to obtain support.
- **Agree** The organization negotiates and agrees a contract with the service provider. This step involves:
  - negotiating a cloud service agreement
  - understanding the impact of the shared responsibility model
  - defining roles and responsibilities.
- **Onboard** The new services are onboarded. This step involves:
  - preparing to onboard cloud services
  - migrating to a cloud solution
  - implementing security and compliance measures
  - enabling users
  - elevating mutual capabilities.
- **Co-create** The service is delivered, supported, and consumed. This step involves:
  - aligning operating models
  - optimizing service consumption
  - managing service quality and performance.
- **Realize** The outcomes of the service are evaluated to ensure that the anticipated value has been achieved. This step involves:
  - tracking value realization
  - assessing and reporting value realization
  - realizing value in different settings
  - identifying opportunities for continual improvement.

Figure 1.4 also shows that there is a line of visibility beyond which customers cannot see the service provider's activities, and vice versa. This applies to internal and external customers and service providers. This guidance focuses on activities that are within the customer's line of visibility.

1.9.3 The value co-creation map for cloud

Throughout their cloud journey, consumers should consider how their cloud strategy will enable their objectives. Together with its customers and CSPs, the consumer organization will be co-creating value and becoming more successful as an organization. This idea is explored fully in Chapter 7, but achieving value co-creation in practice means applying it throughout each stage of the journey. Figure 1.5 provides an overview of the key elements of value co-creation for cloud services.

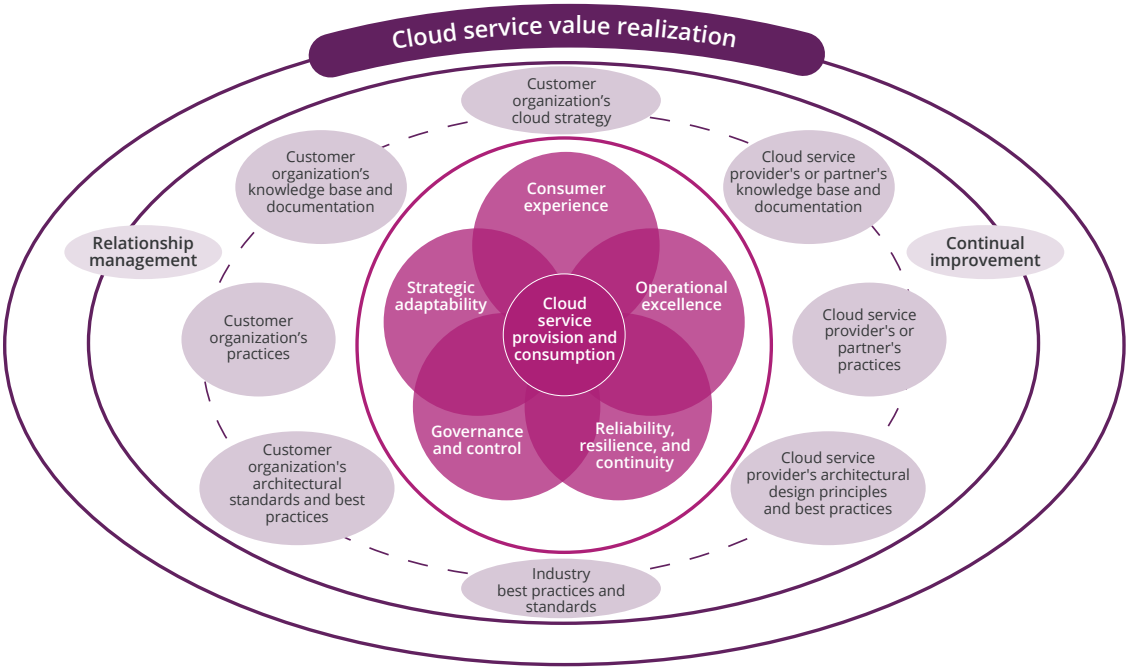

Figure 1.5 Value co-creation map for cloud

Figure 1.5 illustrates the key drivers for effective cloud service provision and value co-creation. It is an agnostic frame of reference that can facilitate effective conversations and therefore enable operating model alignment.

1.9.3.1 Cyclical activities in the cloud consumer journey

Many activities within the cloud customer journey are cyclical. For example, an organization may start defining cloud requirements as part of the explore step and continue to refine them throughout the engage and offer steps. However, information in the offer or agree step may cause it to return to the explore step and redefine some aspect of the strategy or high-level requirements.

A *feedback* activity is a process of using the results and outputs of a step in the cloud customer journey to modify the next instance of an earlier step. For example, the outputs of the realize step can be used to refine how the next explore step is conducted.

A *feedforward* activity is the process of using the interim results and outputs of a step to modify a later step before the first step is complete. For example, interim results from the onboard step can be used to modify roles or processes in the co-create step before all activities in the onboard step have been completed.

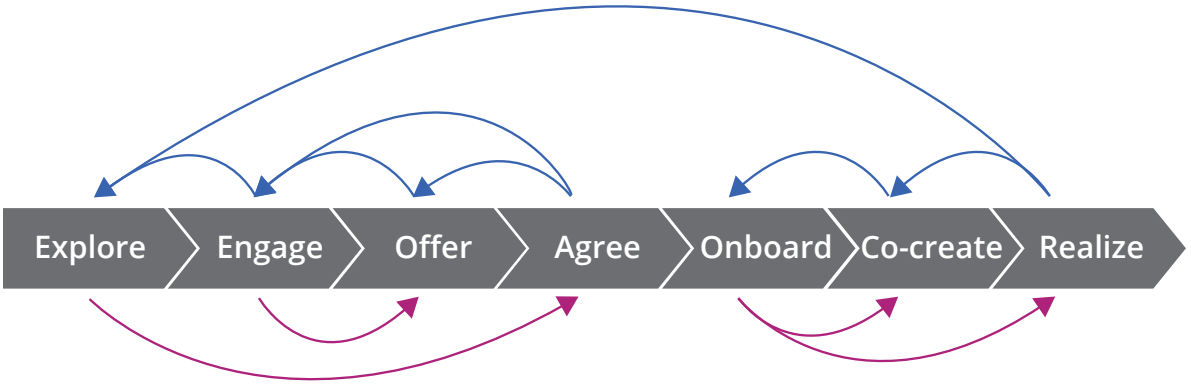

Figure 1.6 The cloud customer journey with feedback and feedforward activities

Figure 1.6 shows how the customer journey might look with feedback and feedforward activities included, although it does not illustrate every possible feedback or feedforward activity.

Table 1.5 also highlights how each step can interact with a past or future step. It provides examples of the feedback (blue) and feedforward (red) activities.

1.9.4 Cloud adoption and utilization scenarios

The subject of cloud can seem complex and diverse. This guidance describes a general approach to consuming cloud, but each organization must adapt the guidance for use in its specific context.

Two variables that may influence how readers approach the material in this publication are:

- **How the organization proceeds through the cloud consumer journey** To illustrate this, section 1.9.4.1 outlines four scenarios that describe organizations at different levels of experience and expertise in cloud.
- **How people use cloud services** To illustrate this, section 1.9.4.2 describes a spectrum of cloud use.

Table 1.5 Examples of feedback and feedforward activities within the cloud customer journey

		To						
		Explore	Engage	Offer	Agree	Onboard	Co-create	Realize
From	Explore				The definition of the organization's cloud strategy, available resources, and constraints will influence contract negotiations and commercial terms and conditions			
	Engage	Feedback on the initial vendor engagement efforts so that the scope of strategic requirements and market exploration can be further refined		The organization's activities to create relationships with targeted CSPs (and associated technologies) and the willingness of those providers to work with the organization will influence how tactical and operational requirements are defined and consolidated				
	Offer		Changes to tactical and operational requirements are fed back so that existing relationships can be refined or new ones initiated					
	Agree	Feedback regarding the pricing and commercial terms with a vendor can be used to refine and align business, IT, or digital strategy, leading to different perspectives and requirements when exploring the marketplace for potential solutions		Feedback regarding the pricing and commercial terms with a chosen vendor can be used to refine and align operational requirements and expectations				

From	Onboard				The activities, outcomes, and experience during onboarding the CSP and offboarding from the incumbent provider will define and evolve the BAU operating model	The effort, outcomes, experience, and lessons learned during onboarding and offboarding will influence how benefits are recognized and realized
	Co-create			Lessons learned from the consumption and management of operational cloud services and solutions can be used to improve how new users and customers are onboarded		
	Realize	An understanding of how cloud services are contributing to strategic or tactical metrics can help the organization refine its business, IT, or digital strategies, leading to different perspectives and requirements when exploring the marketplace for potential solutions			An understanding of how cloud services are contributing to strategic or tactical metrics can help the organization refine its consumption and use of those services	

1.9.4.1 Organizations progress through the cloud customer journey differently

Organizations will progress through the cloud customer journey in different ways, as illustrated in Figure 1.7.

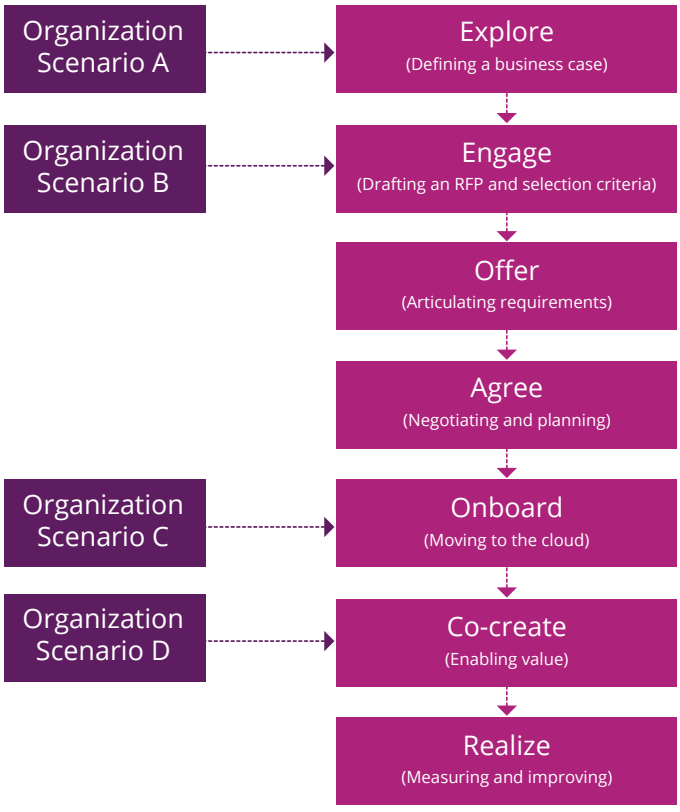

Figure 1.7 Cloud journey overview

An organization in Scenario A is approaching cloud for the first time. It needs to define a cloud strategy and understand the context of cloud within its organization. The explore step will help it to establish a clear cloud strategy.

An organization in Scenario B may not know how to best use the cloud. It may want to start engaging with CSPs (or, more commonly, CSP partners) to understand what services are available or to get help with establishing a cloud strategy. The engage step will help it to understand the context of cloud and have constructive conversations with CSPs.

An organization in Scenario C may be considering adding services to its existing onboarding agenda, or migrating a different part of the organization to cloud.

An organization in Scenario D is operating cloud services. If it has already established a cloud strategy, the explore step can be useful for validating this. If it does not, the explore step will help it to retrofit a strategy to its cloud efforts.

1.9.4.2 Everyone consumes cloud services differently

Each organization has unique requirements for cloud, and a cloud strategy will influence its operating model in different ways, as shown in Figure 1.8.

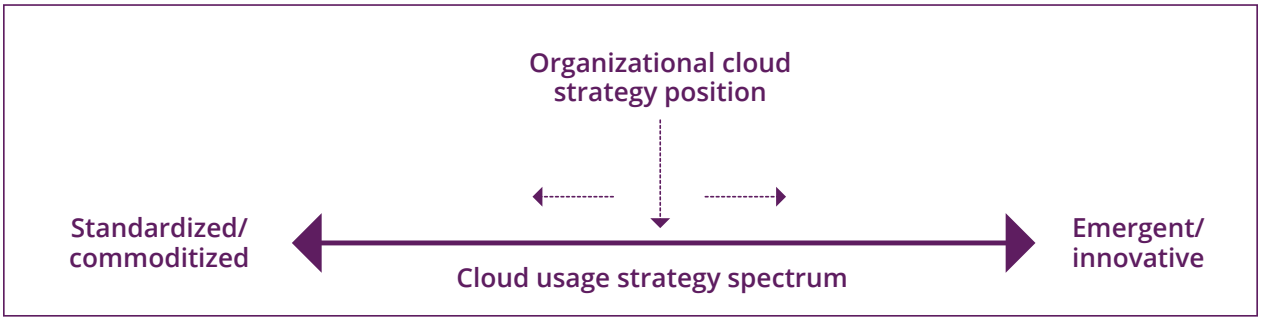

Figure 1.8 The cloud usage strategy spectrum

Figure 1.8 illustrates the cloud usage strategy spectrum. On the standardized/commoditized side of the spectrum, an organization may view cloud as an alternative to existing IT components or as an extension to the existing IT environment, with little change to the way it builds, supports, and delivers IT services. On the emergent/innovative side, it may use cloud to radically change its business model; for example, where the role of IT service provision is integrated into the business units themselves.

An organization may include teams that are in different places on the spectrum at the same time. For example, an IT department may use cloud as a sourcing option for traditional infrastructure services, while a product management team in the same organization may use it as a basis for building and delivering new services. Most organizations start their cloud journey on the left of the spectrum and evolve to use cloud for innovation as their use of cloud matures.

Some characteristics of standardized/commoditized and emergent/innovative usage patterns are outlined in Table 1.6.

Table 1.6 Examples of cloud usage strategy spectrum characteristics

Characteristics	Standardized/commoditized	Emergent/innovative
Nature	Stable (limited variability)/conservative/ commoditized	Emergent/progressive/innovative
Demand	Predictable	Unpredictable
Service customer	Internal supporting service, typically for application teams	Product/service owners or business customers
Service types	Infrastructure-type services (such as server provisioning and hosting)	Platform and microservices
System type	Systems of record and legacy systems of engagement (such as client relationship management)	Systems of engagement based on emerging use of technology (such as context-sensitive support)
Cloud workload type	Data centre migration (lift and shift)	Use of emergent cloud solutions for competitive advantage
Decision-making structure	Centralized governance and control	Autonomy
Pace of work	Relatively slow	Faster
Ways of working and operational practices	Relatively unchanged	Significant changes
Service requirements	Well known, predictable	Rapidly changing, lots of uncertainty and ambiguity
Architecture configuration	Prescriptive, modular, sometimes monolithic	Decoupled

An organization should not take an absolute left or absolute right position on the spectrum. Standardized infrastructure and services provide the organization with stability for its core systems, enabling it to be more robust and resilient. This forms the strong backbone needed to use emergent solutions successfully. Commercial organizations rely on emergent cloud usage to remain competitive. Public-sector organizations rely on cloud services to provide the most appropriate, cost-effective services to meet the needs of their consumers.

Positioning considerations include:

- **Regulatory compliance and security concerns** These may dictate that an organization needs to operate in a traditional, standardized way. For example, it would be too risky to use core banking systems of record with emergent technologies and untested practices.
- **Organizational culture** An organization that is new to cloud services and comes from a highly regulated or traditional in-house environment cannot become an emergent cloud adopter overnight. However, pressures to modernize can help to position it strategically for the future.
- **Highly competitive digital environment** If the organization competes strongly on digital platforms, there will be pressure for it to be emergent/innovative. This would result in an organization positioned on the right of the spectrum, but it does not devalue the importance of traditional, stable systems.
- **Organization with multiple business units with different strategies** In this scenario, each business unit may be positioned differently on the spectrum. The organization will therefore need to architect its cloud platforms and operating model to enable different business units to operate in different ways.

Emergent solutions are likely to be led by autonomous teams within an organization. These solutions typically evolve in one of two ways. One approach is to create a silo around the new technology to ensure that it cannot evolve or be replaced, thus ensuring the position of the team that manages it. A healthier approach is to start standardizing the solution as soon as it becomes part of the organization's operating model. This will mean formalizing the management practices and use of these technologies. These will eventually filter through to more centralized teams who will manage them on behalf of the autonomous teams, allowing the autonomous teams to continue to focus on new emerging solutions.

This is commonly referred to as the *hub-and-spoke* model, shown in Figure 1.9. The *spoke* is the autonomous team that is generally focused on a specific product or service involved with emergent solutions or practices. These teams do not scale well, so they usually standardize their practices over time and share their experiences with the central *hub* teams, which are built for scalability.

The hub teams provide broader support through the centralized service desk and management teams. These standardized services usually fall under global monitoring solutions and governance standards to ensure they are adopted at scale with minimum risk.

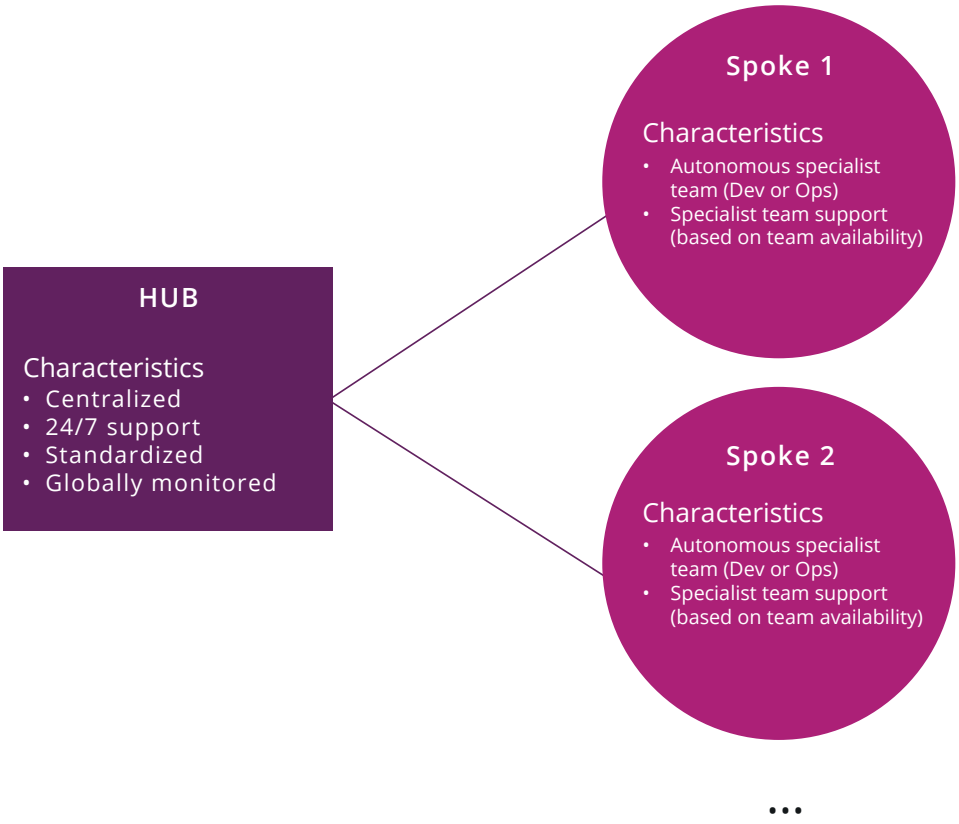

Figure 1.9 Hub-and-spoke model

An organization and its services will move along the spectrum at various times, depending on the current context. The strategy position can significantly impact discussions about how cloud technology needs to be architected and governed.

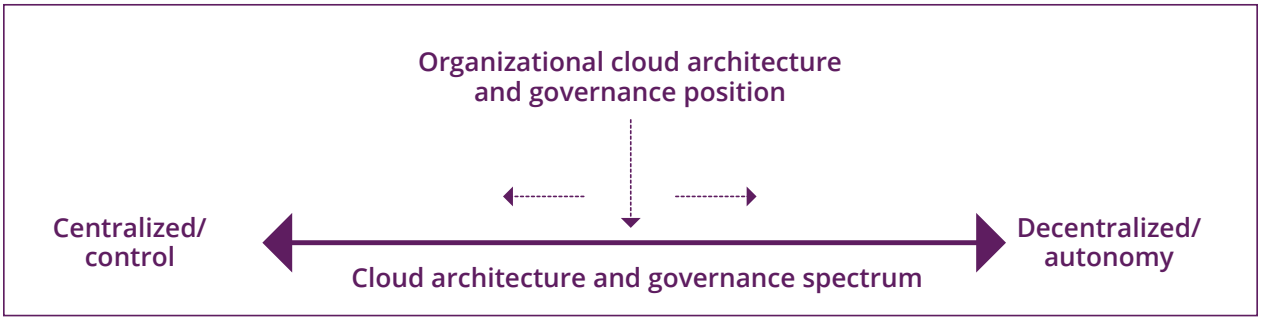

Figure 1.10 The cloud architecture and governance spectrum

As indicated in Figure 1.10, the cloud strategy influences how solutions need to be architected and governed. If the cloud strategy is more standardized, the cloud platform architecture needs to ensure all cloud solutions are heavily governed and controlled. The architecture will most likely be a centralized platform with clear control enforcement and automation. However, if the organization is more emergent, the business units or departments may shape and regulate their own cloud solutions without the use of a centralized platform to provide common controls and governance.

Figure 1.11 shows how cloud strategies differ depending on the organization's cloud strategy position and its cloud architecture and governance position.

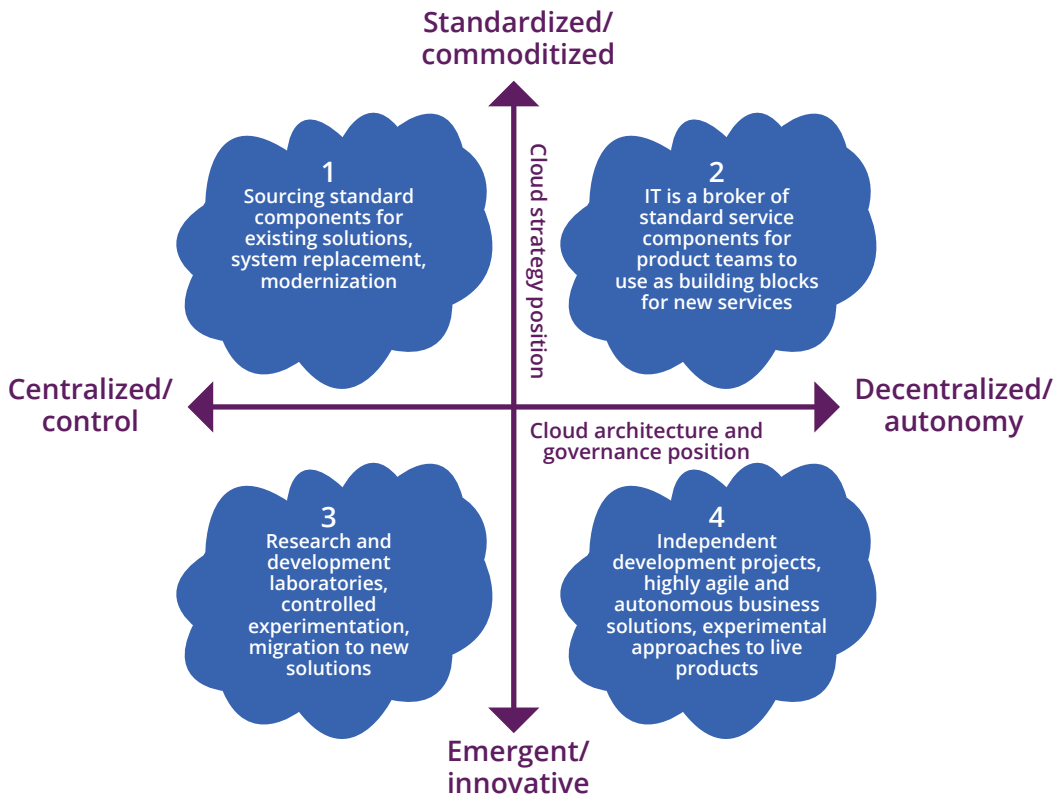

Figure 1.11 Cloud use depends on cloud strategy position and architecture and governance position

Figure 1.11 shows several ways in which an organization might use cloud services, depending on its strategy position and cloud architecture and governance position. For example:

1. An organization that is more conservative may tend to use cloud only to provide commoditized components to achieve greater efficiency, or cost savings in existing systems. It may also want to replace systems that are outdated, without changing the function or role of the service.
2. An organization that wants to maintain control of its core components of the organization, while allowing decentralized teams autonomy in how they use those components, may use its IT department as a broker and manager of the core components, while allowing the decentralized teams to manage solutions under their control.
3. An organization that depends on innovation to be competitive but needs to centralize control over all innovation will tend to use cloud for controlled experimentation and staged migration to new solutions in the cloud only after they have been proved to be effective.
4. An organization that has multiple, autonomous products or lines of business may encourage experimentation and agile development on several fronts at once, allowing each team to control the services it uses within a high-level framework to ensure strategic alignment.

CHAPTER 2

EXPLORE: CAN THE ORGANIZATION BENEFIT FROM CLOUD?

2 Explore: Can the organization benefit from cloud?

2.1 About the explore step

Most of the explore step involves learning about how cloud could benefit the organization. This step ends when the organization either has decided not to pursue a cloud strategy or has defined how it intends to use cloud services as part of its overall business strategy and operation.

The explore step involves understanding:

- the context in which cloud services will be consumed
- how cloud will support the organization's strategy and objectives: specifically the value, outcomes, costs, and risks involved in using cloud services
- which cloud services, or combination of services, would be most beneficial for the organization
- the opportunities offered by cloud services, such as new business opportunities (for example, entering a new market or developing new products and services) or opportunities to perform existing activities more efficiently and effectively
- how to define high-level requirements for the use of cloud services (the detailed requirements for the procurement of individual services will be defined in later steps)
- how to articulate the strategic importance of using cloud services.

Inputs to the explore step include:

- an assessment of internal and external factors that influence the potential benefits, opportunities, and risks involved in using cloud services
- the portfolios of applications, projects, and services in the organization
- articles, presentations, white papers, conferences, and research that outline trends in cloud usage
- input from other organizations that have used cloud services
- guidelines from existing cloud service providers (CSPs) and their partners.

The major outputs of the explore step include:

- an initial cloud strategy, including a high-level business case for using cloud services and a proposed approach for adopting or migrating to them
- a high-level scope, identifying which cloud services are likely to be used
- a high-level statement of requirements and policies associated with using cloud services.

The exploration of various options continues in the engage step as the requirements and scope are reviewed, revised, and expanded.

2.2 Understanding the cloud's role in strategy

Cloud adoption does not happen in isolation from the rest of the organization's ecosystem. To be as valuable as possible, cloud solutions need to be used in the correct context and address specific requirements. This means that the organization should understand the various strategies that cloud will support and enable.

2.2.1 What is digital strategy?

Definition: Digital strategy

A business strategy that is based all or in part on using digital technology to achieve its goals and purpose.

Many approaches to digital strategy are based on a tiered model, as shown in Figure 2.1. The organization's strategy is called the 'business strategy' or 'enterprise strategy'. The digital strategy is a subset of the business strategy, and applies to those parts of the business that will be impacted by digital technology. The IT strategy is separate, but supports both the digital enablement projects and the established parts of the organization.

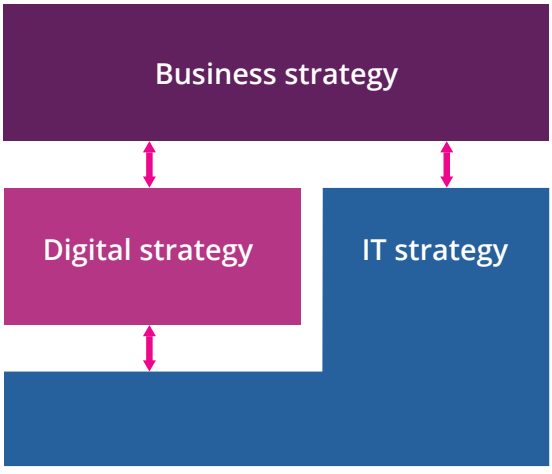

Figure 2.1 The tiered relationship between business, digital, and IT strategies

In this traditional model, the term 'digital strategy' refers to:

- the elements of the business strategy that are based on the use of digital technology
- a migration plan whereby an organization automates its activities or replaces outdated technology with digital technology.

Modern business strategies are largely composed of digital strategies that:

- exploit a market opportunity that has been created due to customers using new digital technology
- use digital technology to engage with customers and improve the customer experience
- relaunch existing products and services with new features and delivery methods enabled by digital technology
- use digital technology to improve the performance or efficiency of the organization's operations.

A better illustration of how digital, business, and IT strategies are related is shown in Figure 2.2, which shows how digital and IT strategies merge in response to an organization's growing reliance on technology. This is achieved by seeking new opportunities and maximizing the use of current capabilities.

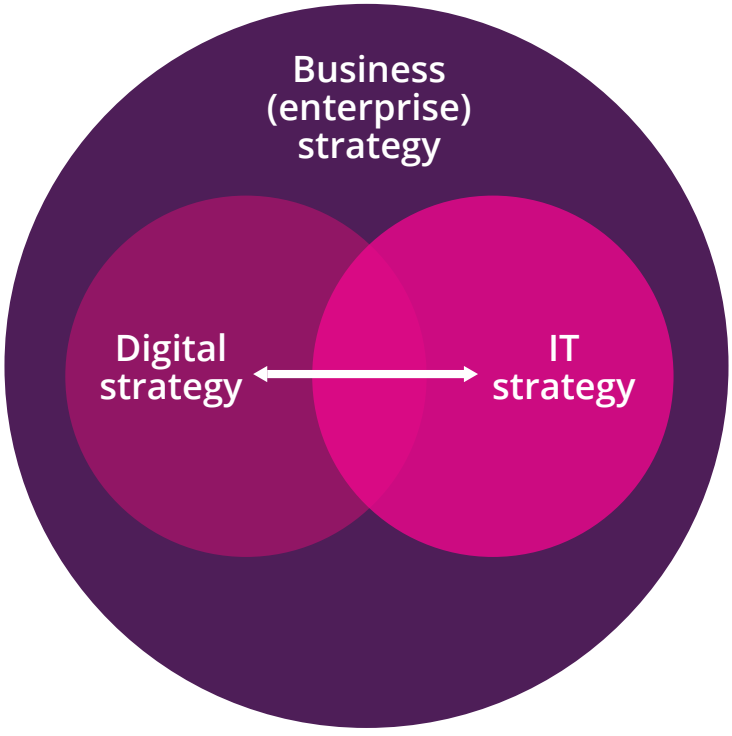

Figure 2.2 A modern view of the relationship between business, digital, and IT strategies

An organization with a successful mix of business and digital strategies is better equipped to achieve competitive advantage from understanding:

- how technology has changed, and how it has changed the environment in which the organization operates
- whether or not the organization needs to respond to changes
- how to identify opportunities in the digital world
- the risks involved with each opportunity
- how to exploit opportunities and mitigate or avoid risk.

An organization that views standardized IT services as part of its overall technology strategy will tend to have a single strategy that encompasses both digital and information technology.

Many organizations differentiate between an IT strategy and a digital strategy. This is typically the case where the IT department that provides a range of centralized, shared services is separate from units that deploy and manage business-specific, digital technology-based solutions.

Further information on digital and IT strategies can be found in *ITIL® 4: Digital and IT Strategy.*

2.2.2 Cloud strategies

Definition: Cloud strategy

The part of the digital strategy that refers to which cloud services will be used and how they will be acquired and used.

Although cloud strategies are generally tactical, and the services consumed are mostly commoditized and standardized, relationships with CSPs can be perceived as strategic by consumers. This is because:

- CSPs are often innovators of emerging technology and its use. This provides quicker and easier access to emerging technology so that consumers do not have to invest in the technology itself. For example, several CSPs make advanced artificial intelligence functionality available to their customers for experimentation
- the services provided by CSPs offer opportunities to redefine a business or operating model, which are strategic in nature
- cloud services are often used to realize existing business and operating models more effectively and efficiently.

Although a consumer organization might view their relationship with the CSP as strategic, the reverse is not always the case. The successful delivery of standardized cloud services does not depend on the CSP understanding the strategic role of the services in the consumer organization. It may be helpful for the CSP to conduct research into how cloud usage may change over time, or whether a new feature is being requested more frequently, but they typically do not establish strategic partnerships with individual customers of standard services.

Consumer organizations, on the other hand, often view the relationship with a CSP as strategic. Understanding the CSP roadmap of future services and features (if it is available) can help the consumer to achieve goals such as:

- developing new products and services
- reaching new markets
- complying with future regulatory requirements
- changing to an alternative when a cloud service is retired.

Some consumer organizations involve a representative of the CSP or one of their partners to participate in their strategic planning function. This might be an account manager, a consultant, or an adviser, although it should be noted that the more standardized the services consumed, the less likely the CSP will be to provide these resources as part of the service. For example, hyperscale CSPs rarely participate in the strategic planning process of their customers, although some provide this as a service through a separate professional services division.

A cloud strategy may be a standalone document for the teams responsible for moving the organization to cloud, and for those teams that deploy, use, and manage cloud services. However, a cloud strategy is always part of the organization's digital and/or IT strategy.

The following points, which may indicate that the adoption and use of cloud technology would be beneficial, should be considered in an organization's digital strategy:

- identifying candidates for cloud migration, such as workloads, solutions, or functionality, together with clearly defined migration criteria (it may no longer be cost effective to maintain resources or capabilities in-house)
- identifying resources and capabilities that are better positioned to meet the organization's objectives if they are not migrated to the cloud (some capabilities require unique equipment, skills, or knowledge that exist only within the organization)
- identifying which markets (consumers and locations) will be served by each cloud solution so that the appropriate policies can be applied
- identifying business opportunities that are made possible by using cloud services (for example, transforming existing products into 'smart' products enabled by the internet of things [IoT], or venturing into a new market that is dominated by a competitor dependent on brick-and-mortar facilities)
- identifying areas for increased automation and innovation
- using advanced cloud services (such as big data, artificial intelligence, IoT, or cognitive services) to address problems in more effective and innovative ways.

The decisions that result from these considerations are commonly used to develop an organization's cloud strategy. This is described in more detail in section 2.6.

2.3 Setting the strategic scope

When defining or assessing strategy, it is important to understand exactly what is in scope. The scope of a strategic assessment, as well as the scope of the cloud strategy itself, depends on how the organization plans to use cloud services, and which of its existing IT solutions cannot be moved to the cloud.

The scope of the strategy is likely to include both existing and new services, but each of these requires a slightly different approach. The strategy will therefore need to account for one or more of the scenarios outlined in the following sections.

2.3.1 Greenfield (or 'born in the cloud')

A start-up organization, or one that is establishing a new line of business, can consider cloud services as a part of every aspect of its operating model, because it is building the entire business model from scratch. Its cloud strategy will be formulated as a fundamental component of its business strategy.

2.3.2 Approaches to migrating existing services

Most organizations start their cloud journey by migrating existing services from in-house solutions to cloud services. There are three approaches in this category, each of which results in a different type of cloud strategy. They are:

- one-off migrations
- evolutionary migrations
- big-bang migrations.

2.3.2.1 One-off migrations

In this approach, individual systems, services, business processes, or functionalities are migrated into the cloud. There is no cohesive strategy for cloud migration, and each project is planned, costed, and executed independently by the team responsible for the item being migrated.

An organization using this approach should balance the benefits of quick, decentralized decision-making with a more centralized approach designed to ensure the consistency of performance and quality while reducing duplication.

2.3.2.2 Evolutionary migrations

This approach focuses on migrating components of the operating model to the cloud over time (using the guiding principle 'progress iteratively with feedback'). In this approach, the organization develops a vision of what it would look like if it used cloud services extensively. The organization knows which systems, services, processes, and functionalities would be best delivered using the cloud and which should be kept in-house.

The strategy focuses on migrating those components that are most obviously suited to the cloud or that need to be migrated urgently. Each migration is individually planned and migrated, but with reference to the cloud strategy. Each project is reviewed at closure, and issues are addressed in the next phase of the plan. The strategy is also reviewed regularly.

Organizations using this approach typically have established business practices and systems, especially where regulation requires that risk is strictly managed. This approach is good for organizations that use large volumes of data that can be managed in parallel between the cloud and in-house environments.

This approach allows the transition to new facilities to be planned smoothly. The legacy system can be offboarded when the new processes are functioning and can be managed with little risk.

2.3.2.3 Big-bang migrations

An organization facing a situation of disruption (for example, a competitor launching a service it cannot compete against) may need to create a new set of capabilities quickly. In cases of mergers and acquisitions, it is not always feasible to merge systems and then migrate them to the cloud over time.

This approach focuses on moving all identified components into the cloud as quickly as possible. It is generally riskier than other approaches, but may be the best option if the organization needs to re-engineer itself quickly or respond to an urgent and potentially catastrophic situation.

2.3.3 New services

Another approach is to keep all existing solutions in-house and only use the cloud for new services. As the organization learns more about how to manage the services in the cloud, it may consider migrating some or all of the in-house systems to the cloud using one-off, evolutionary, or big-bang approaches.

2.4 Cloud strategic positioning

To determine its position on the strategy spectrum and begin identifying the optimal approach to its cloud strategy development, an organization needs to perform an extensive assessment of its external and internal context. This is described in detail in *ITIL® 4: Digital and IT Strategy.*

The context of every organization, including the availability and nature of cloud services, continually changes, as does the organization's position on the strategy spectrum (see Chapter 1). A regular review of the organization and its external and internal context will ensure that the organization stays relevant and can afford the opportunities offered by emerging cloud services.

This cycle of review and revision is not unique to cloud services, and should already be one of the organization's strategic planning activities, as explored in *ITIL® 4: Direct, Plan and Improve*. Cloud exploration should be integrated into the organization's strategic review cycle.

An organization may need to collaborate with its CSPs, partners, and operational teams to understand strategic shifts and risks. This will allow it to enhance the effectiveness and speed of its strategic planning activities. Enabling autonomy in decision-making is a critical success factor and needs to be addressed in the organization's governance model.

2.4.1 Review of external factors

Cloud strategies typically focus on two external contexts:

- **External organizational context** This involves assessing the organization's external factors, such as its external customers and its competitive market space.
- **External IT context** This involves assessing the internal organization that is external to IT but still within the organization itself, such as internal stakeholder customers, organizational products and services and their value chains, and desired outcomes.

In some organizations, there may not be an external IT context; there may not be a formal IT department, but instead several IT platform teams and business development teams delivering products and services directly to customers.

Several external contextual factors are particularly important when exploring cloud services. These include:

- regulations and standards
- customer expectations and requirements
- industry and market opportunities and threats.

2.4.1.1 Review of regulations and standards

The use of cloud technology is largely affected by regulations and standards defined for:

- data storage and processing
- information security
- personal data protection
- disclosure and accessibility
- communication technologies and networks.

A thorough review of this area is important for two main reasons:

- Regulations and standards may have changed since the organization first applied them.
- Organizational policies and procedures do not automatically align with regulatory requirements.

Regulations and standards can restrict what the organization is able to do; for example, where data about customers can be stored. They often also result in higher costs, not only to become compliant but also because of the ongoing expense of reporting and auditing. A thorough understanding of this context will ensure that the organization can optimize its architecture, portfolios, and offering.

Regulations and standards also offer opportunities; for example, new ways of validating a customer's identity online, thus enabling the organization to provide services remotely. Changes to regulations may therefore mean that using cloud services is essential in competitive organizations. Voluntary compliance with a standard may provide a marketing opportunity, or allow the organization to qualify for certain types of contract.

One way of assessing how cloud can be used in organizations impacted by regulations is to understand how local or national governments are using cloud, and then determining whether this can be replicated. For example, the Federal Risk and Authorization Management Program (FedRAMP) is a framework that organizations can use to deliver secure, compliant cloud services to the US federal government.

2.4.1.2 Review of customer expectations and requirements

For a cloud strategy to be effective, the organization needs to understand the different customer journeys, including what customers are trying to achieve and how the products and services enable them. Because customers' needs continually evolve, the organization's evaluation of their journeys should be continually assessed and reviewed to ensure alignment.

Cloud service adoption or migration will impact customers. These impacts must be clearly articulated and understood in order to ensure the cloud strategy and subsequent requirements can be clearly defined and delivered against. A thorough understanding of the customer journey will allow the organization to prepare for and mitigate any negative impacts, and to promote and exaggerate positive ones.

Customer requirements and expectations, therefore, directly affect the organization's cloud strategy and choice of cloud solutions, CSPs, and services.

2.4.1.3 Review of industry and market opportunities and threats

Cloud services present organizations with opportunities and threats that need to be continually assessed. Different industries may use cloud services in unique ways, for example healthcare organizations may develop 'telemedicine' solutions that can be replicated by other healthcare organizations. Universities may develop remote learning and research capabilities that become an industry-standard approach for higher education.

Those who are responsible for defining strategy and evaluating the use of cloud solutions should continually monitor opportunities offered by their organization's industry and the market to ensure that they get optimal value from cloud technology and continually find new ways of competing or adding value. Opportunities or threats may trigger:

- the adoption of new cloud services
- a review of existing contracts

- a change of CSP
- migration to another platform or solution
- expansion to new markets with existing services
- the ability to host data in specific countries as required by appropriate regulations.

Most CSPs or providers of cloud-related consulting services (partners) can provide insights into the opportunities and threats within industries because they evaluate those opportunities and threats as part of their own product development. CSPs and partners:

- are diligent in monitoring the external environment
- understand trends in emerging technology and how they are being used
- understand and navigate complex regulations (for example, enabling data sovereignty across multiple global regions and accommodating various legislations) and enable consumers to address their own compliance requirements
- invest in research and innovation to grow their service offerings and expertise.

Trusted CSPs and partners can therefore provide valuable input to an organization's cloud strategy.

Most CSPs have a published roadmap indicating new features and products to be launched. These roadmaps highlight future capabilities to consumers, and can be used in an organization's cloud strategy to determine how new technology might impact customers.

Private-sector organizations also need to understand the competitive landscape. The insights obtained from analysing competitors should help to determine an organization's strategic position and cloud requirements.

Although competitive analysis is usually associated with external competition, it also applies to the external IT environment. In the context of cloud, organizational units may engage directly with software-as-a-service (SaaS) providers and completely avoid IT departments. This will not only undermine the department's value to the organization, but it will also introduce governance and architectural risks and challenges. IT departments must clearly establish the role they play and articulate the value they bring.

2.4.2 Review of internal factors

When defining a cloud strategy, an organization should combine its understanding of the external factors with a good understanding of its internal factors, including:

- strategic objectives and plans
- portfolios
- operating model resources, capabilities, and constraints.

2.4.2.1 Review of strategic objectives and plans

When an organization is considering cloud services, it needs to have a clear understanding of all of its existing strategic objectives and plans, both at an organizational level and from a digital strategy perspective.

Some important questions when evaluating existing strategic objectives while developing a cloud strategy are:

- What are the dependencies between current strategic objectives, and what are their influences and impact on external factors? How will the strategic cloud objectives align with these?

- What vital business processes or functions do the technology resources that are to be moved into cloud enable?
- Which applications are directly linked to the organization's strategic objectives?
- How effectively are we meeting or executing against the current strategic objectives and plans? What are the current challenges, risks, or impediments? How will we mitigate these issues for the strategic cloud objectives?
- Are the current strategic objectives and plans clear and measurable? If they are not, what will we align our strategic cloud objectives with, and how will we ensure they are clear and measurable?
- How could cloud services support or enable the existing strategic objectives and plans?

2.4.2.2 Review of portfolios

When considering cloud services, it is important to understand what is currently available within the organization and where investments and efforts are being prioritized. An organization should review its application and project portfolios in the following ways:

- **Application portfolio** The organization needs to understand what applications are in place and whether they are providing value. Important questions include:
  - Which applications will be replaced by cloud services and why?
  - Are those applications fit for cloud migration, or should they be replaced by an equivalent SaaS service?
  - What consolidation opportunities can the cloud provide for the application portfolio?
  - What cost-saving or stability and performance improvement opportunities does cloud provide against the application portfolio?
- **Project portfolio** The organization needs to understand its current resource and financial commitments. Important questions include:
  - Which projects are the most resource- and capital-intensive, and what are the expected outcomes?
  - What is the average health of projects across the portfolio? If projects are not being completed on time, on budget, and with the expected quality, how will this be addressed for the cloud migration or onboarding project?
  - How will the cloud migration or onboarding project be prioritized against the rest of the project portfolio?
  - What opportunities can cloud services bring to the project portfolio to provide quick wins?

2.4.2.3 Review of operating model resources, capabilities, and constraints

Adopting cloud technology often requires major changes to the organization's way of working, internal practices, and IT architecture. The scale of the changes depends on the:

- starting point
- type and complexity of the cloud services being adopted
- scope of the adoption (including the affected organizational units, products, locations, and so on)

- skills and job roles required to implement and manage the changed organization (many CSPs and partners will provide skills assessments and training services to ensure that this area is well understood and managed)
- cloud readiness of the operating model: that is, the ability of an organization's processes and practices to design, transition, support, and operate services for cloud.

When developing strategic objectives and plans for cloud services, the organization needs to understand how well it currently operates. An organization that has significant challenges with deployments in its current operating model may find that the speed of many cloud services exacerbates these issues.

Organizations should assess their operating models using the four dimensions of service management (see Figure 0.4 at the beginning of this guide). Important questions (grouped according to each dimension) include:

- Organizations and people:
  - To what degree is the organization set up for accountability; that is, are there assigned service owners, process owners, application owners, and so on?
  - What structures ensure that strategic directives are cascaded to the relevant teams within the organization, and to what degree do they enable effective decision-making?
- Information and technology:
  - Is there a clear overview of the current architecture, and is it well documented?
  - What are the current architectural challenges, and how could they affect the performance of cloud services?
- Partners and suppliers:
  - What are the organization's current partners and suppliers, and could there be a conflict of interest with incoming CSPs?
  - How strong are the relationships with partners and suppliers?
- Value streams and processes:
  - How robust and efficient are the current processes?
  - To what degree does the organization understand how value is created and where waste and bottlenecks occur?

Many consulting firms provide assessments that can help an organization to understand inefficiencies in its operating model. This understanding is important because it influences how the strategic cloud objectives and plans are defined.

Cloud readiness assessments are discussed in more detail in Chapter 3.

2.4.3 Practical guidance for strategic positioning

If an organization does not have a cloud strategy, or its strategic objectives are unclear, it could consider short-term strategic cloud objectives and focus them on addressing key organizational challenges or risks. This should be only a temporary measure; cloud cannot become a strategic tool if it is not delivering against organizational strategic objectives.

The external and internal factor reviews imply significant and comprehensive assessments. However, these reviews aim to identify actionable insights for the development of strategic cloud objectives and plans. Successful reviews may require only a meeting and discussion with a few key stakeholders, which may be enough to effectively define strategic cloud objectives. The organization needs to find a balanced approach to the ongoing assessment of the factors described.

2.5 Value: outcomes, costs, and risks

An important part of the explore step is estimating the value of adopting cloud technology by assessing the likely outcomes, costs, and risks (VOCR).

VOCR is considered when:

- defining the digital strategy
- assessing individual cloud services
- defining requirements for cloud services
- evaluating proposals from CSPs.

When assessing the value of a service, the following factors should be considered:

- What outcomes will be achieved by using this service? These should include:
  - outcomes that were not previously possible, such as entering a new market or developing a new online service
  - existing outcomes, but more quickly or efficiently, such as increasing the number of customers that can be served in an hour
  - fewer negative outcomes, such as penalties for failing to comply with regulatory reporting.
- What costs will be introduced or removed? These will include the costs of:
  - preparing to use cloud services
  - introducing the service
  - using the service
  - not using the service, such as if the organization continued to use its existing infrastructure and applications
  - decommissioning an existing service or migrating to a new service provider (including costs that might be reduced).
- What risks will be introduced or removed? These include:
  - risks involved in expanding the organization's digital footprint, such as by making data available in mobile applications
  - limitations or inflexibility in the service provided
  - risks involving data privacy
  - lack of knowledge and skills needed to use and manage cloud services
  - risks associated with moving to a pay-per-use service model
  - risks involved in managing security in a shared responsibility model
  - contractual lock-in.

The ultimate value of a service is assessed using a return on investment calculation (see Chapter 4).

2.5.1 Outcomes

Because there are so many cloud services that can be used in so many ways, it is impossible to list all of the possible outcomes of using them. However, some common outcomes that organizations want to enable are:

- cost savings through avoiding over-provisioning
- the ability to modernize a solution without expensive equipment or software replacements
- the ability to reach new markets
- the development of new cloud-based products and services
- the ability to respond rapidly to changing conditions, such as market changes or changes in customer needs.

Some less desirable common outcomes are:

- increased costs because of poor workload forecasting or failure to use budgeting and governance tools provided by the CSP correctly
- uncontrolled use of resources, such as storage, because there is no longer a central point of control and governance, or because access tools provided by the CSP were not used correctly
- proliferation of uncoordinated cloud-based projects (because a cloud strategy was not in place or because service governance was not extended to cloud services). Because many cloud services can be acquired directly by end-users, it is easy to set up and use cloud services without going through the appropriate acquisition process
- some solutions being migrated to cloud that would be better managed and used in-house (because a workload cloud readiness assessment was not properly undertaken prior to migration).

2.5.2 Costs

An organization should understand the categories of cost that are involved in cloud services. These costs will need to be considered when assessing the potential return on investment of engaging with a CSP.

The organization can research cloud costs in various ways:

- with a request for information (RFI)
- through research reports
- using the experiences of other organizations
- through informal research
- with specialized advisory consulting.

Consumers should expect CSPs, especially those who provide standardized services at hyperscale, to make the costs of their services publicly available. In addition, many CSPs offer a cost management tool to assist in estimating the cost of migrating specific workloads to the cloud and comparing the costs to in-house solutions.

Cloud costs are typically incurred in five areas:

- exploring cloud services
- onboarding and offboarding

- co-creation
- under- and over-utilization
- outages.

2.5.2.1 Exploring cloud services

The costs of exploring cloud services typically include:

- analysing the business and operating models, existing infrastructure, applications, and processes to determine where cloud could be beneficial
- changes in how the organization governs itself, such as from a hierarchical to a flat organization
- strategic assessments and the evaluation of multiple cloud options
- the evaluation of opportunities available when using cloud services (such as new products and markets, or improvements in operational efficiency).

For many organizations, cloud is not only about replacing existing systems with a faster, cheaper alternative. Rather, it is about being innovative and agile in order to stay relevant in a fast-changing market. For these organizations, the cost of exploring a cloud strategy is part of the costs of larger changes.

2.5.2.2 Onboarding and offboarding

Onboarding costs are the costs of preparing for and implementing new services, or migrating existing services from one environment (in-house) to another (cloud). Some of these costs relate to the service provider (these will be listed in the proposals), such as sign-up costs and the costs of creating application programming interfaces (APIs). Other costs are incurred by the consumer organization, such as the costs of preparing data for migration.

Sources of costs in the onboarding area can be mapped to ITIL's four dimensions of service management. They might include:

- Organizations and people:
  - changing the IT department to expand its ability to be a cloud service broker, including reorganization, training, hiring, and implementing new processes for cataloguing and requesting services
  - establishing a vendor management office to manage the ongoing contract definition, coordinate activities between different CSPs, manage disagreements, and so on
  - training staff on managing and using the new services
- Information and technology:
  - designing and piloting the migration to cloud
  - signing up to new services
  - creating APIs
  - migrating applications and/or data
  - implementing targets and testing for user acceptance
  - disposing of existing equipment
  - terminating software licences

- Partners and suppliers:
  - terminating contracts with existing suppliers
  - establishing formal channels of communication with new service providers
- Value streams and processes:
  - changing existing processes to work within the new service environment
  - applying the shared responsibility model to existing processes.

When a service needs to be replaced by another service, or decommissioned entirely, costs similar to those in the onboarding stage may be incurred.

2.5.2.3 Co-creation

Co-creation costs are the costs of the ongoing use of cloud services. This is where the most significant cloud costs are incurred. This cost area has the longest lifespan, which is typically measured in years, although there are valid applications of cloud services for shorter periods.

Sources of costs in the co-creation area might include:

- Capital expenditure (capex)
  - development of applications, using platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS)
  - in-house equipment for any part of the service that is not migrated to cloud
  - development of APIs between in-house systems and cloud services
  - setting up a cloud management office
  - network upgrades to support increased cloud usage
- Operating expenditure (opex)
  - use of cloud services
  - operational management activities (such as monitoring and control)
  - provisioning redundant services for high availability
  - disaster recovery and service continuity planning
  - security management
  - the cost of outages (including the resources and actions to resolve incidents)
- Staffing (internal and external)
  - consulting
  - architecture and design
  - governance (programme office, communication)
  - proof of concept (training, preparation, planning, remediation, management)
  - solution or service provisioning (RFI, RFP, vendor selection process, orders)
  - pilots (training, preparation, planning, remediation, management)
  - onboarding (training, preparation, planning, remediation, management).

The use of cloud services often shifts capital expenditure to operating expenditure. Because many of the costs of using cloud services are based on pay-per-use, CSP prices (usually available on the CSP's website or from responses to the RFP) will provide a cost for each unit of use, such as the cost per transaction or per terabyte of storage.

The end-user team can often account for and approve cloud expenses. However, the finance team must have oversight through management accounts.

Although a few services may be available at a fixed cost, most CSPs will not specify a fixed price for their services. This is because most CSP services are based on market pricing, which is dynamic. Therefore, it is the consumer's responsibility to monitor and manage costs (e.g. by using CSP tools to set up budgets and alerts for when those budgets are almost spent, or setting spending caps on individuals or departments).

2.5.2.4 Under- and over-utilization

If a consumer has a contract with a CSP committing to a certain amount of usage (as opposed to the pay-as-you-go model), there may be important cost considerations relating to the under- or over-utilization of cloud services. These may include:

- If a discount has been applied due to anticipated usage, there may be penalties associated with under-utilization.
- Over-utilization may be subject to penalties (although this is rare).
- Advance notification may be required for significant over- or under-utilization, and penalties may apply if notice is not provided in time.
- It is the consumer organization's responsibility to forecast its utilization rates, even if the CSP provides a service of estimating future workloads.

2.5.2.5 Outages

Outage costs can be a contentious issue. Consumers should understand their and the CSP's responsibilities when outages occur, and know whether the terms of the service agreement will prevent significant business loss. These terms relate to specified levels of redundancy, service continuity measures, and penalties for service outages.

At the same time, it is important to compare the cost and likelihood of outages in the cloud, which are less likely due to the resilient architecture, and the ability of the consumer to architect for high availability. Consumers should look at a CSP's history of outages to better understand which CSPs offer a reliable cloud environment of resilient architectures.

2.5.3 Risks

It is important to understand whether cloud services introduce, reduce, or remove risks. An organization should already have a defined risk appetite, and should know how much risk mitigation will be needed before a new service is introduced.

Typical areas of risk related to cloud services include:

- shifts in roles and responsibilities
- unauthorized procurement or use of cloud services
- security of cloud services
- API vulnerability
- maintaining separation between tenants
- incomplete data deletion processes

- vendor lock-in and switching costs
- third-party contracting
- migration.

2.5.3.1 Shifts in roles and responsibilities

When the consumer organization's technical teams are no longer responsible for physical assets, many of the activities that they previously performed shift to the CSP's operational management teams. Typical risk factors and mitigation actions are listed in Table 2.1.

Table 2.1 Risks related to the shift in roles and responsibilities

Risk	Mitigation actions
IT groups (generally those that are technology-centric) finding it difficult to shift their role to that of a service consumer, where monitoring and control are at the service level rather than device level	Carefully review the shared responsibility model Define the new roles and responsibilities of technical staff Provide training on the new roles and responsibilities
Service disruptions caused when IT staff do not understand the role of each asset, or when they rely on technical staff to source and fix faulty assets	Define a full-service architecture before migrating to cloud Identify how each cloud service is used in the organization's processes and activities Redefine service level agreements (SLAs) and processes, and provide training to IT staff
IT staff focusing on the management and performance of devices and applications without understanding how the organization uses them. As a result, the cloud service is defined to reflect those activities, rather than to enable the desired outcomes	Quantify the desired outcomes and performance required from each service, rather than the technical architecture that the CSP will use

2.5.3.2 Unauthorized procurement of cloud services

The on-demand, self-service design of cloud services makes them easy to procure and use. This becomes a risk when consumers do not put in place the controls and governance to ensure that only authorized users are able to spin up new services or access existing services.

Mitigating these risks involves implementing measures which ensure that cloud usage is consistent with the organization's objectives and policies. Stakeholders should define, communicate, and apply security, procurement, and usage policies. Consumers should use CSP-provided monitoring tools to understand and control usage, and to ensure that the organization achieves an optimal balance between performance and cost.

Organizations may consider using a cloud management office or centre of excellence to coordinate and control the overall use of cloud services. Typical risk factors and mitigation actions are listed in Table 2.2.

Table 2.2 Risks related to the unauthorized use of cloud services

Risk	Mitigation actions
Uncontrolled purchasing introduces several risks, including: ● essential features may be missing from the services, such as security countermeasures ● the organization may no longer qualify for discounts on consolidated purchasing ● the number of vendors increases, so the cloud services become more difficult to manage	Centralize purchasing for certain categories of cloud service if possible (many groups depend on the rapid procurement and deployment of cloud services) Define and communicate acceptable use policies and minimum acceptable service policies Use identification and access management tools to manage who can use each cloud service Define and enforce spending caps for individuals and departments for cloud services Use service catalogues to clearly communicate the features of authorized services so that they can be compared with new services Use a pre-authorized purchasing framework to streamline procurement Use CSP tools, such as budget alerts, so that purchases are closely monitored
Using cloud services outside of established controls and disciplines, resulting in inefficiencies and high costs	Establish and communicate clear controls Provide training on establishing clear processes for managing resources Where appropriate, audit the use of cloud services according to the established policies
Confusing the use of cloud services with the process of innovation	Establish clear use cases to guide the use of cloud services Differentiate between the purchase of approved services and the purchase of new services (the latter should go through a more rigorous evaluation process)
An increase in technical debt when cloud services duplicate functionality that is already provided in existing solutions	Establish appropriate governance and control measures for the use of cloud services If the culture does not support centralized purchasing, introduce a check into the decentralized purchasing process that requires an evaluation of the impact on technical debt

2.5.3.3 Security of cloud services

The security of cloud services is a shared responsibility between the CSP and the consumer (as defined in the shared responsibility model). CSPs use the highest required levels of security to protect the physical and virtual environment, which means that all consumers benefit when using cloud services from that CSP. In addition, CSPs use their own cloud capabilities, such as artificial intelligence and machine learning, to enhance how they manage security. They often offer consumers the ability to view security across in-house and other cloud environments to provide a single view of security and the management of security incidents.

Typical risk factors and mitigation actions are listed in Table 2.3.

Table 2.3 Risks related to the security of cloud services

Risk	Mitigation actions
Inconsistent security measures, tools, and practices	Define requirements that reflect the minimum level of security required for services Update security policies to account for cloud service usage The CSP should provide tools that offer the consumer the ability to manage and monitor security appropriately Integrate the use of CSP tools, monitoring, and reporting into the mechanism used to manage security in the consumer organization (such as a security operations centre)
Staff do not understand how to configure and use cloud services securely	Provide training to all staff and contractors on how to use cloud services securely
Misaligned understanding of security responsibilities	Ensure all stakeholders understand their roles and responsibilities in terms of the shared responsibility model Ensure that all security policies and procedures clearly state who is responsible for the activities outlined, and confirm that these are consistent with the terms of the contract
Physical access to data centres	Ensure that access to the CSP's data centres is restricted to CSP staff. Allowing staff from the consumer organization to access the multi-tenant environment represents unnecessary risk and serves no purpose. Instead, consumer organizations should review third-party audits and attestations of the security of a CSP's data centre Ensure that virtual access is limited to software, middleware, and operating system access, which is provided to specific end users with administrative rights. In this way, end users can access services without widening the risk of intrusion

2.5.3.4 API vulnerability

An API enables two systems to communicate with and pass data to one another. It is a potential source of vulnerability, especially when transferring unencrypted data between internal and external sources. Typical risk factors and mitigation actions are listed in Table 2.4.

Table 2.4 Risks related to API vulnerability

Risk	Mitigation actions
Unauthorized use	Ensure that data is properly secured, and that failures are quickly detected and managed so that data is not lost Specify and follow appropriate security measures The CSP should provide tools that offer consumers the ability to manage security in their environment
Vulnerable data storage and transfer	Identify the data's source, destination, and route, and ensure that security requirements have been established Review security policies, tools, and processes for all data under the control of the consumer organization Specify the minimum level of security required for environments managed by the service provider, and for the tools offered by the CSP to monitor and control data storage and transfer

2.5.3.5 Maintaining separation between tenants

Multi-tenancy enables CSPs to achieve economies of scale and make advanced technical resources available at a lower cost. It is also a potential risk, although CSPs go to great lengths to mitigate it, so that it is no longer considered to be a major risk. Typical risk factors and mitigation actions are listed in Table 2.5.

Table 2.5 Risks related to maintaining separation between tenants

Risk	Mitigation actions
Procedures are not adequately defined or applied, resulting in reports, workloads, and data being distributed to the wrong environment	Use the discovery process or RFP to ensure that the CSP has adequate measures and procedures in place to mitigate these risks
Unauthorized physical access to devices supporting a cloud service	If a shared data centre is accessed by staff from more than one consumer organization, physical security measures must be in place that prevent unauthorized access

2.5.3.6 Vendor lock-in

Switching from one CSP to another is not always easy. The consumer organization should ensure that the service provider is a good fit for its strategy, culture, and working practices. An organization that is considering switching should be aware of the following factors:

- Each CSP has a unique architecture and culture. What may be easy to achieve when working with one CSP may be difficult with another.
- There are costs for redefining procedures, interfaces, training, and so on.

The subject of vendor lock-in, and how to avoid it, is described in more detail in section 6.2.2, which covers the migration of services from one CSP to another. Typical risk factors and mitigation actions are listed in Table 2.6.

Table 2.6 Preventing vendor lock-in

Risk	Mitigation actions
Highly customized or unique services are difficult to move from one CSP to another	Reconsider the use of cloud services for unique, business-critical solutions that depend on in-house skills and development, unless the solution can be rebuilt using generic cloud services Specify the most common standards of environment, data formats, APIs, and procedures when anticipating the need to switch providers or to work with several providers Design services to be built using generic components A CSP should provide portability tools and services that enable customers to move data on and off a CSP's storage as needed at any time Build applications to be as flexible and loosely coupled as possible Evaluate the CSP's architecture for components or technologies that provide unique functionality

Table continues

Table 2.6 *continued*

Risk	Mitigation actions
The more a SaaS solution is customized, the higher the risk of vendor lock-in	Differentiate between configuration of SaaS software and customization, which requires adherence to whatever form of software development lifecycle the organization uses Evaluate the level of specialized knowledge and architecture required for the service, and ask: ● Is the solution's future roadmap consistent with the consumer organization's requirements? ● Does the CSP's culture match the consumer organization's culture? ● Does the CSP have the knowledge and expertise to support the consumer organization? ● If the service had to be moved, how would that be done? ● Are there components of the service that should remain generic?

2.5.3.7 Third-party contracting

CSPs work with partner organizations for three reasons:

- The CSP is focused on the delivery of the core services, and needs partners to help consumers to source, migrate to, manage, and optimize cloud services.
- A consumer may need a broader range of services than a single CSP offers. In some cases, the consumer organization will integrate the services itself, but in others it will need a cloud service integrator or broker to help.
- Niche service providers use generic services from a CSP to deliver specialized services to a narrow market. In these cases, the contract will be with the niche service provider, with little visibility of the base-service CSP's services. The consumer must ensure that all requirements are specified to the niche provider, which identifies any critical dependencies.

Typical risk factors and mitigation actions are listed in Table 2.7.

Table 2.7 Risks related to third-party contracting

Risk	Mitigation actions
The relationship between partners and the CSP is unclear, resulting in unrealistic expectations or confusion as to which organization has responsibility for certain actions	Evaluate the shared responsibility model and ensure that each party's responsibilities are clearly understood before an agreement is signed
Engaging with more than one service provider for different components of the same solution can cause confusion as to how the overall solution should be managed and supported	The consumer organization is always responsible for the management of a solution involving more than one provider. It should: ● architect the solution based on clearly defined services, specifying which organization is responsible for each aspect of the services ● understand its role in the overall solution ● specify how vendors will be engaged when there is an incident or problem that requires involvement from more than one vendor in the incident and problem management processes ● consider using a cloud management or vendor management office to facilitate inter-organization collaboration

2.5.3.8 Migration

Risks are incurred whenever there is movement between environments; for example, migrating from in-house to cloud or when switching between CSPs. Typical risk factors and mitigation actions are listed in Table 2.8.

Table 2.8 Risks related to migration

Risk	Mitigation actions
Migration creates opportunities for administrator and super-user credentials to be stolen	Ensure that identity access controls and policies exist and have been tested before migrating Include changes to credentialling processes and technology in the migration test and training Ensure that the architecture and security policies provided by the CSP meet the organization's needs
The cloud solution can be challenging for IT staff who are used to managing in-house solutions; changes may cause confusion and disruption	Good planning and an experienced partner will help the organization anticipate the level and types of change that will occur A skills analysis will identify which specializations will be required, and which existing staff will be best suited to each, based on their current skills and aptitude Communicate a staffing plan and a detailed training programme Identify areas managed by only one person because of their 'unique skill', and expand that skill set so that there is not a single point of failure
Abuse of authorized access occurs where IT staff use their credentials to perform activities for which they are not responsible. This is often done to speed up a task or solve an incident, but results in informal processes, which are not planned for in the migration and therefore do not work in the new live environment. This leads to service quality issues, disruption, loss of data, and so on	Create and check detailed operational procedures and security policies before the migration Use the identity and access management tools provided by the CSP Test service performance and functionality to identify non-standard activity or access
Data is particularly vulnerable during and after migrations. Loss can occur due to transmission failures, software or hardware issues, environmental factors, and human error	Ensure that the data is compliant with defined data retention policies before moving it Test the migration to identify any dependencies or points of failure Define and test contingency plans that include full data recovery and the mitigation of dependency failure
Some contracts fail because the parties agree on what services will be offered, but one or both do not fully understand the responsibilities created when signing the contract	Each party should perform a due diligence exercise to ensure that their responsibilities are understood and any ambiguous terms and conditions are identified

2.6 Formulating the initial cloud strategy

When an organization has reviewed the external and internal factors, the cloud's strategic value and potential use cases should become clear. These reviews should also highlight current challenges that could present risks or opportunities for cloud adoption. The next step is to define the strategic objectives and plans for the cloud. This leads to the formulation of the cloud strategy, which outlines how the cloud objectives will be met.

It is important to remember that the impacts of cloud services are not limited to helping an organization achieve its current strategic initiatives. New capabilities introduced by CSPs can provide opportunities

for growth. This means that a cloud strategy should never be developed independently of the business strategy and the associated digital strategy. Also, the cloud strategy should not become the organization's primary strategy. 'Cloud-first' is a helpful design principle, but it is not a substitute for thorough strategic planning at every level of the organization.

Cloud journeys should aim to enhance or optimize an organization's current objectives and plans. If the organization does not first understand its objectives and challenges, it may overlook important opportunities for cloud services, or try to use cloud in the wrong ways.

2.6.1 Defining the strategic cloud objectives and plans

To effectively establish clear strategic cloud objectives and plans, which outline what the cloud services need to deliver and in what way, the organization should ask questions based on a thorough understanding of the external and internal context discussed in section 2.4. Important questions include:

- How can cloud services address operational or technical challenges?
- How can cloud services enable and support business processes?
- How can cloud services help to position the organization competitively?
- How can cloud services help the organization to meet existing objectives and plans?
- How can cloud services highlight opportunities to innovate?
- How can cloud services optimize or enhance existing products and services?
- How can the organization ensure that services are migrated to cloud successfully?
- How should the organizational culture and skill set evolve when services are migrated to cloud?
- Where can cloud services serve unmet customer needs?

The answers to these questions should help the organization to articulate a clear set of strategic cloud objectives and plans.

Some organizations use the objectives and key results (OKR) framework when defining strategic objectives and plans.

Definition: Objectives and key results (OKR)

A framework for defining and tracking objectives and their outcomes.

The OKR framework is used to ensure that strategic objectives are actionable and measurable. It is discussed in detail in *ITIL® 4: Digital and IT Strategy*.

Two high-level examples of strategic cloud objectives that use the OKR framework are shown in Table 2.9.

Table 2.9 Examples of strategic cloud objectives using the OKR framework

Objective	Key result
Reduce and optimize IT infrastructure costs	Migrate 30% of current infrastructure to cloud hosting services within 10 months. Ensure that cloud cost thresholds and enforcement policies are defined and implemented within 6 months. Identify application owners, and make them accountable for infrastructure costs associated with their application within 16 months.
Increase delivery speed of IT development services	Reduce development lead time by 50% within 24 months. Map the value stream for the development service within 3 months. Benchmark all work in progress, cycle time, and lead time for the development service within 16 months. Identify toolchain blockages and deficiencies, and identify solutions to optimize the development and release toolchain within 12 months.

These objectives reflect the strategic business case for migrating to or using cloud. The strategic business case should not be confused with the detailed solution business cases that are used to obtain funding for each proposed service. These business cases are discussed in Chapter 4.

2.6.2 Formulating the cloud strategy

When the strategic objectives and plans are understood, the organization should identify how cloud services need to be used in order to meet them.

Cloud strategies can be broken down into individual elements. The organization should meet with stakeholders and subject matter experts to define each key element in the context of the strategic cloud objectives and the internal and external factor reviews, as shown in Figure 2.3.

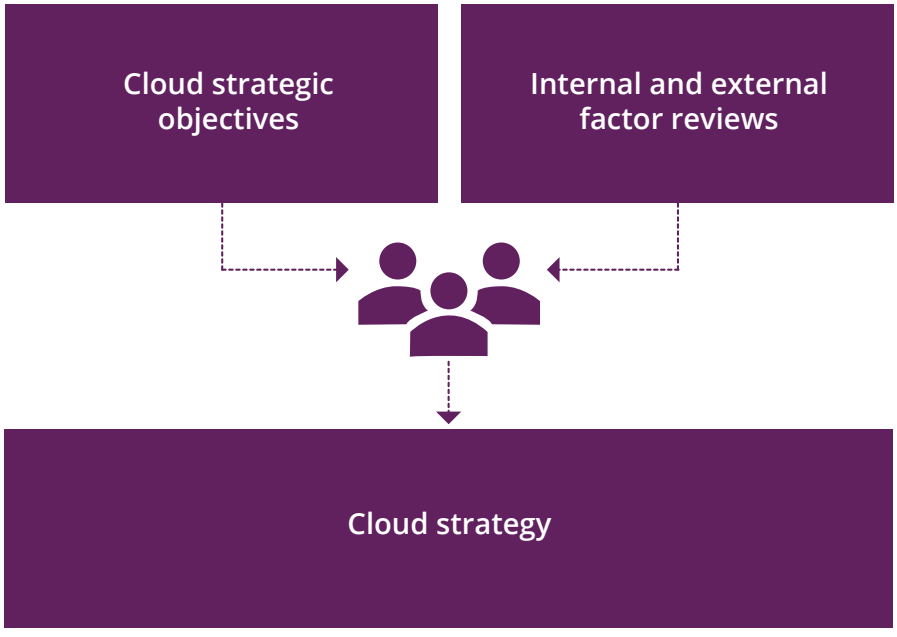

Figure 2.3 Development of cloud strategy elements

The recommended steps for defining the cloud strategy are:

1. Identify key strategy elements, and prioritize them based on the set of strategic cloud objectives and the internal and external factor reviews.
2. Identify key stakeholders and subject matter experts who can ensure that the strategy will enable the organization's objectives.
3. Plan a formal initiative to define the strategy. The outcome should be an articulation of how the strategy will enable the strategic cloud objectives.
4. Establish a review committee to review the strategy document.

Table 2.10 outlines a high-level example of key elements that are commonly found in a cloud strategy.

Table 2.10 Key cloud strategy elements and descriptions

Element	Description
Scope	A cloud strategy's scope is the set of areas that the strategy applies to. If there are multiple business units with unique cloud strategies, each strategy's scope will need to be applied to the business unit it serves.
Cloud vision, objectives, and key results	The cloud strategy should articulate the vision for the use of cloud within the organization. It should also define the objectives and key results for cloud usage, to ensure that the cloud strategy is actionable and measurable.
Cloud strategy alignment to other strategic plans	The cloud strategy should define how it supports or works alongside other important strategic plans, such as the IT, digital, digital transformation, and other cloud strategies. It should answer the questions: how does this strategy enable the other strategy's goals, and what impact or risks does it impose on other strategies?
Cloud deployment and service models	The cloud strategy should clarify which cloud deployment or service models will be favoured. For example, an organization may opt to not use public-cloud services and only make use of private cloud. The strategy should clarify how each deployment and service model will be used to enable the cloud strategy's objectives.
Guiding principles for cloud	This element defines the key guiding principles for how cloud should be adopted and used. Some examples of guiding principles are: ● SaaS should be the first consideration before other application migration options. ● All cloud services should have service models that are defined and assessed for readiness before they are deployed to operations. ● Information should not be shared beyond the organization's security perimeter. This element is usually completed after the initial strategy has been drafted.
Application migration criteria	This element should highlight the criteria that need to be met before an application should be considered for migration to the cloud. For example, an application should not be migrated to the cloud if it: ● processes or stores customer information ● can be replaced by a SaaS solution ● does not have the appropriate application architecture for optimized cloud usage.
Future state and roadmap of key initiatives	The cloud strategy should outline and articulate the future state of cloud usage within the organization, and define the roadmap and key initiatives that will get the organization to its desired future state.

Cloud operations architecture and governance	This element should outline: ● the decision-making body structure that will enable autonomous decision-making for cloud across the organization ● important data controls and security considerations ● the financial management approach to the cloud (for example, how will cloud consumption be reported on, and what accounting practices will be changed to accommodate cloud usage) ● the portfolio management approach, including how the portfolio will be rationalized for the cloud ● the approach to CSP, partner, and vendor management ● architecture and operational management considerations, including where the organization should be positioned on the strategy spectrum for optimal delivery ● single- or multi-cloud approach considerations (see section 3.3 for more detail).
Cloud culture and key adoption scenarios	This element outlines the training and hiring that may be needed to enable people to use and manage cloud. This may be associated with a change and adoption strategy to methodically transition the organization's culture to the desired cloud culture.
Supporting resources	This element contains current cloud information resources, outsource consultants, marketing research data, monitoring results, and cloud-related business analytics.

Every element of the cloud strategy can be difficult to define; it may take a significant amount of time to effectively do so. This may be achieved through collaboration between internal specialists or insourced CSPs or partners.

2.6.3 Practical guidance for strategy formulation

Separating strategies into elements as described enables an organization to approach cloud strategy development and review iteratively and responsively. It also enables it to develop its cloud strategy in parallel with the engage and onboard steps of the customer journey.

2.6.3.1 Managing multiple cloud strategies

Sometimes an organization has a cloud strategy complemented by other strategies, such as monitoring, technology, or DevOps strategies. All of these strategies should be aligned with the cloud strategy; their objectives and their impacts on the cloud strategy should be clearly documented in the strategies themselves, and their alignment should be reviewed regularly.

When there are different cloud strategies for different business units, it is important that the objectives and impacts of each strategy are documented to clarify how it delivers against or supports the organization's higher-level strategies.

2.6.3.2 Finding the right level of abstraction for strategies

Cloud strategies will also differ between organizations in terms of their level of abstraction. For example, some cloud strategies may explain in detail how cloud solutions should be architected; others may not provide any guidance around architecture at all.

An organization needs to balance detail and flexibility to make its strategies actionable. Strategy documentation should not include detail that is likely to change within a year, because doing so will make the strategy reactive. For example, a strategy that outlines specific technologies may have to be updated often as new features or technologies emerge.

The level of abstraction an organization chooses for its strategy may also be based on the maturity of the organization and the level of insight teams need. For example, an organization using cloud in an

innovative/emergent capacity may want more autonomy, and therefore a more abstract strategy. If many teams are involved in cloud service delivery, the cloud strategy may need to be less abstract to reduce ambiguity.

2.6.4 The differences between cloud services and in-house solutions

When an organization transitions to cloud services, it should fully explore and understand the differences between the old and new approaches. It should also evaluate whether cloud is the better option for new services, rather than provisioning them in-house. In both cases, it should clearly define how the services will be managed using the shared responsibility model.

Key areas of differences between cloud and in-house solutions include:

- backup and data recovery
- costs and cost dynamics
- dependency on service providers
- governance, management, and control
- managing security
- party responsibility
- people
- scalability and flexibility
- service quality metrics.

Some of these differences are explained in more detail in the following subsections.

2.6.4.1 Backup and data recovery

In-house data and system backups are complex tasks performed as routine IT operations procedures. They are subject to dedicated management and control, and recovery can impact business operations and productivity. Specialized backup software and storage solutions can be expensive, and recovery procedures can be even more so, especially when specialized data recovery expertise is needed.

Cloud services generally include the ability to perform data backup, recovery, and failover to redundant systems, but these are not automatic (and may even require an additional subscription). The consumer organization is responsible for its data, for defining the standards and requirements for the backup/restore and archive/retrieve functions, and for defining the data management policy. Consumers are also responsible for managing the data and services appropriately. For example, a CSP cannot be expected to take responsibility when a consumer organization deletes its own data.

A CSP may offer services with such features as 'close to zero-downtime' policies, disaster recovery, data retention standards, mirroring services, redundancy policies for its physical facilities, and data continuity provisioning. However, the consumer organization must specify where it needs these features to be activated.

Data governance remains the responsibility of the consumer organization. This includes ensuring the quality and integrity of data, and identifying who is responsible for making decisions about data; for example, how privately identifiable data will be managed, which data should be archived, how long archives should be kept for, and which data should be kept available for immediate retrieval.

2.6.4.2 Costs and cost dynamics

Although the costs of in-house solutions seem predictable, many aspects of managing them result in unpredictable, often higher-than-estimated, costs. These include:

- ongoing investments in hardware and software
- maintenance
- human error
- complex operational procedures.

Most in-house solutions also need to be over-provisioned to accommodate peak workloads.

Costs are sometimes difficult to quantify because they are split between different departments in the organization. It is also difficult to determine the costs of certain aspects, such as staff, facilities, and energy consumption of services. The cost of supporting untracked equipment (such as a server under the desk) is often unknown.

Cloud costs are tracked more simply because they are operational expenses (provided the CSP can provide clear information about how costs are incurred, and many CSPs provide tools that help consumers to predict, track, and monitor these). Although they vary based on utilization, they are more predictable, especially once the service has been running for a certain amount of time. However, the organization must be able to accurately forecast how a service will be used. Failure to do so will result in variations in use and the actual cost incurred. In many cases, the task of accounting for and approving cloud expenses can be managed directly by the end-user team according to financial management policies and oversight.

Issues can arise if the organization does not fully understand how cloud costs are incurred, if it does not impose a cap on spending for individuals or departments, or if there is no clear delegation of who can incur cloud costs and under what circumstances. For example, when decommissioning a data-processing service, it is important that the relevant teams understand whether the data storage will be automatically decommissioned as well, or will continue to incur costs.

2.6.4.3 Governance, management, and control

In-house data centres appear to offer more direct control over the technology investment than cloud solutions. Dedicated IT support and operations teams define and apply operational procedures, security polices, and disaster recovery measures.

However, this perception of governance is sometimes an illusion. Many IT operations and support teams do not understand how their organization uses their systems. Organizations pay to maintain systems that are not valuable. Service level agreements in these organizations tend to focus on uptime and response time, without indicating what business outcomes are being achieved. These situations demonstrate ineffective governance, even when stringent operational controls are in place.

Additionally, expensive resources are often used to manage and control systems that could be controlled more easily with commoditized components that have built-in control features, focusing on outcomes rather than performance.

Cloud services with remote data centres facilitate management and control from three perspectives:

- The service provider is responsible for the control and management of the physical infrastructure that is used to provide standard cloud services. The consumer organization must ensure that the contractual terms and conditions specified by the CSP for these services support its business

objectives. This is difficult to achieve if the consumer organization is not already measuring the relationship between the service components and the business outcomes.

- It is the consumer's responsibility to procure services that comply with regulatory requirements. CSPs will provide services that are architected to facilitate that process (or tools that enable the consumer to architect its services) and which meet the most demanding levels of security requirements for that class of service. However, they will not change standard services to meet an individual organization's compliance requirements, and thus invalidate the compliance of all other consumers. It is up to the consumer to ensure that the service meets its minimum required levels of security, and then architects the way it uses that service to be compliant.
- CSPs should offer tools and instrumentation to enable the consumer organization to control how the services are used, and to apply its own standards of use that ensure good governance and the appropriate level of control. The CSP ensures that its cloud services are secure, then provides the consumer organization with tools that allow it to use the services securely.

Every organization should establish a cloud governance model that specifies the roles and responsibilities for procuring and managing cloud services appropriately. The model should also identify the appropriate approach to managing situations where responsibility is shared.

Data governance is especially important when considering cloud migration. It remains the responsibility of the consumer organization. CSPs provide tools and services that help consumers to meet governance objectives (such as compliance with privacy legislation). The consumer organization retains responsibility for defining governance policies and procedures, identifying data ownership, and specifying storage requirements.

2.6.4.4 Managing security

In-house data centres require extensive physical and virtual security measures. Typically, only the largest organizations can afford to employ people with the breadth and depth of skills needed to provide high levels of protection. Additionally, the more personnel that need to have physical access to the data centre, the higher the risk. This means that there are more breaches at in-house data centres than there are of resources hosted in the cloud.

Managing the security of cloud services is a responsibility shared between the CSP and the consumer (as defined in the shared responsibility model). The CSP uses the highest-level requirements to protect the physical and virtual environments.

CSPs often use their own cloud capabilities, such as artificial intelligence and machine learning, to enhance the way security is managed. They often offer the ability to extend this security across in-house and other cloud environments, thus simplifying security and security management.

Access to a CSP's data centres is usually restricted to a small number of CSP staff. Allowing staff from the consumer organization to access the multi-tenant environment represents unnecessary risk and serves no purpose. Virtual access is limited to software, middleware, and operating systems, access to which is provided to specific end users with administrative rights. In this way, the CSP allows users to access the service without increasing the risk.

2.6.4.5 Scalability and flexibility

In-house solutions are typically not designed or engineered for high scalability or flexibility, and it can be complicated and expensive to scale them. It is even more complicated and expensive to design systems that can flex with variable demand. This usually requires investing in a solution that caters for

the highest expected demand, even if that demand occurs only for a short time. For the rest of the time, the expensive solution is under-utilized. Designing for disaster recovery is even more expensive, because a significant amount of equipment and facilities must be duplicated.

Cloud solutions are designed to be flexible and scalable. CSPs can manage demand dynamically across pools of shared resources. Most offer the ability to scale up and down in seconds, move data around, and commission and decommission resources as needed. There is a clear understanding of the costs and incentives involved in managing workloads. Consumers can ensure that appropriate disaster recovery is in place by taking advantage of features such as the existence of multiple data centres, redundant service design, and availability zoning.

CSPs with broader IT capabilities offer tools for monitoring and metering to allow customers to manage resources and utilization. This enables the prioritization of workloads according to business needs. The pay-per-use model means that the more effectively work is managed, the more cost effective the solution is.

2.7 Summary

The first thing a consumer organization should do is understand its own unique strategic drivers and scope for cloud service consumption. These activities, coupled with preliminary industry and market research, will produce key documentation, including high-level versions of a statement of requirements, business case, and implementation approach. Not only does this begin to illustrate the value proposition of cloud services, it also facilitates early understanding of critical elements of consumption, such as the shared responsibility model. The result is a cloud service customer that is better prepared both to refine its understanding as the journey progresses, and to engage with potential CSPs that are aligned with its goals and objectives.

CHAPTER 3

ENGAGE: MEETING A CLOUD SERVICE PROVIDER

3 Engage: Meeting a cloud service provider

3.1 About the engage step

The engage step of the cloud customer journey starts as soon as an organization has defined its strategic objectives for cloud services and is ready to meet with cloud service providers (CSPs). It ends when the organization has conducted a cloud readiness assessment and has updated its cloud strategy and detailed requirements in preparation for the offer stage.

This process is not always linear. As the organization engages with CSPs and their partners, it learns more about the opportunities that cloud offers. This ongoing discovery should be used to refine the strategy and define the requirements in greater depth. The engage step helps the organization to fine-tune its requirements and decision-making criteria related to cost optimization, operational excellence, resilience, reliability, security, and compliance.

The engage step of the cloud consumer journey involves understanding:

- the CSP landscape, including the different types of CSP and their partners and the services they provide
- the role of CSP industry bodies and regulators and how they shape the services that are available in their market
- the types of services that can be considered to meet the objectives of the organization's cloud strategy
- how to define the requirements for cloud services
- how to conduct a cloud readiness assessment
- the levels of engagement between CSPs, partners, and cloud service consumers, and how to engage with CSPs and partners
- how to evaluate a shared responsibility model to ensure that it is consistent with the way an organization needs to engage with a CSP
- how to research the cloud service options available in a market
- how to incorporate everything learned during the engage step in the cloud strategy.

Inputs to the engage step include:

- the initial cloud strategy
- any high-level requirements that were defined during the explore stage
- marketing and sales materials from CSPs and their partners

- detailed descriptions of available services, including technical specifications where appropriate
- collateral from cloud readiness assessment.

The major outputs from the engage step include:

- detailed requirements analysis for cloud services
- a revised cloud strategy
- a cloud readiness assessment report and any action plans needed to prepare for adopting cloud services.

3.2 Understanding the CSP landscape

3.2.1 Types of CSPs and their services

Many organizations offer cloud and cloud-related services. An organization that understands the range of services offered will be better able to:

- evaluate whether CSPs can support its strategy
- understand the capabilities and limitations of the available cloud services
- understand what skills and capabilities it needs to develop to manage its relationships with service providers
- validate assumptions and expectations about what cloud services are needed
- verify whether the available CSPs can support the required services or solutions.

There are two broad configurations of CSP types, both of which offer standardized services at scale, which may vary from limited scale (such as a limited market or number of customers) to hyperscale (for example, when the same standard services are delivered globally to an extremely large number of customers). These types are:

- **Aggregate CSPs** These providers are typically regarded as industry CSP leaders. They offer a comprehensive blend of cloud service models.
- **Cloud service model specialists** These providers specialize exclusively in one or two cloud service models, such as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), or software-as-a-service (SaaS). For example, some providers are exclusively IaaS providers and offer niche cloud services for specific industries or organization types.

Table 3.1 gives an overview of the CSP types and their services.

Table 3.1 Overview of CSP types and their services

Aggregate CSPs			
Provider of multiple or all cloud service models			
Cloud service model specialists			
IaaS provider	**PaaS provider**	**SaaS provider**	
Provider of primarily cloud infrastructure-related services **Examples** ● Compute services (virtual machines) ● Storage services ● Networking services ● Containerized services ● OS licensing ● Database licensing	Provider of primarily cloud platform-related services **Examples** ● Development teamwork ● Security services ● Application designing and testing ● Web and database service integration ● Cloud service integration ● Artificial intelligence/ machine learning	*Technical* Provider of primarily technical cloud software-related services **Examples** ● Disaster recovery ● Backup ● Security	*Business* Provider of primarily business function cloud software-related services **Examples** ● Sales ● HR ● Productivity
Professional services			
Additional complementary services that are provided to optimize the adoption, design, or usage of cloud services provided by either cloud service providers, their partners, or independent consulting firms **Examples** ● Accreditation and training ● Cloud readiness assessments ● Migration services ● Advisory/consulting services ● Industry-specific services			
Cloud service deployment models			
All cloud service providers will deliver their services through one or more of the delivery models listed below			
Private	**Public**	**Community**	**Hybrid**
The cloud resources are used exclusively by a single customer organization and are generally physically located in its on-site data centre	Owned by third-party cloud service providers, who deliver the cloud services over the internet	Cloud resources shared exclusively between two organizations such as government organizations or education facilities	Public or community cloud resources used in conjunction with on-premise resources

Both CSP types can and do provide professional services. However, some organizations, such as independent consulting firms, specialize exclusively in cloud professional services but are not CSPs as they do not offer cloud services (only the professional services surrounding them).

CSP types can also be categorized based on the cloud deployment models through which they deliver their services (private, public, community, and hybrid cloud), which are supported and maintained by the CSP, as shown in Table 3.1.

An organization should also consider multi-cloud and cross-cloud strategies when deciding on a CSP. Many legacy vendors use multi-cloud to create platforms that enable easier integration between different cloud environments and legacy systems. These are known as cloud service integrators (shown as PaaS cloud service model specialists in Table 3.1). Cloud service integrators are systems integrators that specialize in the integration of both cloud and in-house services.

Key message

Cloud service integrators enable organizations to provide, manage, monitor, and govern software applications across multiple environments in an integrated and automated fashion. Although they do not only integrate PaaS services, they are sometimes known as *integration platform-as-a-service* (iPaaS) or *hybrid integration platform-as-a-service* (HiPaaS) providers.

There are many types of cloud service integrators with specific niches and value propositions. However, cloud service integrators are typically used to provide an end-to-end solution by enabling:

- the integration of resources between cloud and legacy applications; for example, to enable the modernization of compatible legacy applications
- the integration of multiple cloud services and cloud environments across multiple CSPs and cloud models
- application integration between various applications.

Aggregate CSPs offer services that can work across other cloud environments. This can help to address the demands of modernization, geographic resilience, data privacy, security, and compliance. Consequently, many organizations have turned to public-cloud, hybrid-cloud, and multi-cloud strategies. Multi-cloud also supports service availability if one provider goes out of business or is acquired.

Although they are attractive, multi-cloud strategies have drawbacks, including:

- High investment is needed when specializing resources on individual platforms.
- There is significant effort and cost in adapting an organization's support model for multiple clouds.
- It is necessary to invest in multiple toolsets to ensure effective management, governance, and compliance.
- When customers no longer buy at scale from a single provider, there can be a reduction in available discounts.

The organization must select the most suitable CSP and service configuration to meet its needs. For example:

- If a cloud strategy and requirements focus exclusively on an IaaS service model, it may make sense to engage directly with an exclusively IaaS CSP.
- An organization seeking to automate and enhance a business function, such as sales, may benefit from engaging SaaS CSPs for a specific SaaS solution.
- An organization with a niche storage requirement that is currently engaging an aggregate CSP may choose a niche IaaS storage CSP to complement its existing service.
- An organization that uses multiple cloud services and wants to integrate several cloud and in-house services may use a PaaS cloud service model specialist, such as a cloud service integrator.

There are advantages and disadvantages associated with each CSP type and the services it offers, as shown in Table 3.2.

Table 3.2 Advantages of each CSP type

CSP type	Advantages
Aggregate CSP	Provides a comprehensive, integrated mix of all service models to address multiple current and future requirements Heavily regulated and certified in most security and quality standards Generally offers better continuity, scalability, and service level agreements (SLAs) due to the global data centre footprint Typically strong financial health means there is a minimal risk of bankruptcy
Cloud service model specialist	Can provide niche, tailored services to specific organizations, business functions, or industries Can be cheaper than an aggregate CSP

3.2.2 CSP partners

CSPs provide cloud services. By their nature, these services are generally standardized and offered to many customers. They do not always have the focus or resources to help every organization to plan and migrate to the cloud. Those CSPs that provide consulting and implementation services themselves usually do so for only a subset of their customers.

For this reason, most CSPs have developed a network of partner organizations that specialize in helping consumer organizations to plan for, prepare for, acquire, migrate to, use, and optimize cloud services. Types of CSP partner include:

- **Resellers** These partners sell the services of a particular CSP.
- **Brokers** These partners typically represent the consumer. They help the consumer to define its service requirements and then source the appropriate services from one or more CSP.
- **Consulting and advisory** These partners help consumer organizations develop their cloud strategy, conduct a cloud readiness assessment, and plan the onboarding of the service.
- **Implementation partners** These partners help the consumer organization to onboard new services or migrate existing solutions into the cloud.
- **Solution developers** These partners provide specialist support for the customization and use of SaaS services.
- **Managed service providers** These are partners who manage and provide technical support for a consumer organization's cloud services. Their services include security monitoring and control, performance monitoring, incident management, and backup and recovery.

The rule of differentiating between cloud services and labour

It is sometimes difficult to understand the roles of organizations involved in providing and supporting cloud services. A good rule is to distinguish between acquiring and using a cloud service (which is always provided by a CSP) and commissioning labour related to the cloud service (which is provided by a partner, or the professional services group within the CSP organization). This rule is especially helpful when defining requirements, evaluating risks, or evaluating a shared responsibility model. When defining these, ask 'What am I buying?' rather than 'Who am I buying from?'

CSP partners extend the capabilities and services of a CSP to a broader range of consumer organizations. CSP partners play an important role in pre- and post-sales activities, working with the CSP to accelerate the consumer's digital transformation.

CSP partners can guide an organization through its digital transformation journey, offering recurring solutions and earning rewards for driving value creation. CSP partners can build unique solutions for virtually any organizational need. They receive their designation by undergoing an extensive validation audit by the CSP or an industry body that demonstrates competency and a good track record. CSP partners can offer customer enablement services, as outlined in Table 3.3, that include targeted expertise that enables project initiation, high-performing application building, and continual cost optimization.

Table 3.3 Customer enablement services

Area	Entity	Common use cases
Support	People, programmes, and tools that go beyond reactive break-fix services to optimize the consumer organization's environment	Issue resolution, cost and performance optimization, architectural guidance, planning, and operational support for business-critical events
Managed services	Infrastructure management and operation for the organization to reduce operational overhead and risk, which leads to increased focus on business applications	Move and operate faster by ensuring security and compliance in the cloud
Professional services	Specialized skills and experience to help define and achieve results in the cloud	Digital transformation, large-scale migrations for data centre closure, and innovative application development
Expertise	Faster completion of cloud-oriented projects	Fulfilment of expertise-based services to help set business and technical strategies, including proactive architectural guidance, hands-on assistance for learning purposes about cloud services, planning cloud-based projects, setting up cloud services, migrating to cloud-centric services, and estimating and optimizing cloud spend
Training and CSP certification	Resources developed by a CSP partner to advance a team's skills and knowledge	Build cloud fluency throughout the organization, create a culture of innovation, develop adaptable and continuous learning, and reskill mechanisms in tandem with innovation

CSP migration and implementation partners offer support in four key areas: plan and design; build and migrate; run and operate; and optimize, as shown in Figure 3.1.

Figure 3.1 The four areas of CSP implementation partner support

3.2.3 CSP industry and regulatory organizations

Consumers must ensure that CSPs can provide the tools, services, and functionality that they need to meet the organization's articulated cloud strategy and regulatory requirements. Many CSPs are heavily regulated by various computing organizations to ensure they meet specific regulatory and security requirements, and are also regularly audited to ensure they meet various regulatory body requirements.

When selecting a CSP, it is important to review its association with the cloud industry and regulatory bodies, which include:

- **Cloud Computing Interoperability Forum (CCIF)** Formed to enable a global cloud computing ecosystem where organizations can work seamlessly together for the wider industry adoption of cloud computing technology and related services. A major focus is on the creation of a common framework that enables two or more cloud platforms to exchange information in a unified way.
- **Cloud Infrastructure Services Providers in Europe (CISPE)** A non-profit coalition of cloud computing leaders in Europe. The CISPE Code of Conduct helps organizations across Europe to accelerate the development of GDPR-compliant cloud-based services for consumers, businesses, and institutions.
- **Cloud Security Alliance** An organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.
- **Distributed Management Task Force (DMTF)** Creates open manageability standards spanning diverse emerging and traditional IT infrastructures, including cloud, virtualization, network, servers, and storage.
- **National Institute of Standards and Technology (NIST)** A non-regulatory federal agency whose mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- **Open Commons Consortium (OCC)** Manages and operates cloud computing, data commons, and data ecosystems to advance scientific, medical, healthcare, and environmental research for human and societal impact.

- **Open Grid Forum (OGF)** An open community committed to driving the rapid evolution and adoption of applied distributed computing. OGF accomplishes its work through open forums that build the community, explore trends, share best practices, and consolidate these best practices into standards.
- **Object Management Group (OMG)** An international group whose mission is to develop technology standards that provide real-world value for thousands of vertical industries. OMG is dedicated to bringing together its international membership of end-users, vendors, government agencies, universities, and research institutions to develop and revise these standards as technologies change over the years.
- **Storage Networking Industry Association (SNIA)** A non-profit organization made up of member companies spanning information technology. A globally recognized and trusted authority, SNIA's mission is to lead the storage industry in developing and promoting vendor-neutral architectures, standards, and educational services that facilitate the efficient management, movement, and security of information.

Specific industries are also interested in cloud standards. Industry groups typically provide guidelines for using cloud in their industry, and will also provide guidance on how to ensure compliance when using cloud services. Examples include:

- **Association for Retail Technology Standards (ARTS)** Aims to create an open environment where retailers and technology vendors can create international retail technology standards.
- **Telemanagement Forum (TM Forum)** A group whose goal is to work together to break down technology and cultural barriers between digital service providers, technology suppliers, consultancies, and systems integrators.

3.3 Types of services to be considered

There are many different types of cloud service that are offered in different ways. Standard services are offered through catalogues and are available for immediate use. Non-standard services and cloud-related consulting and implementation services need to be tailored to the specific needs of the consumer organization, and usually need to be fully scoped and priced in a proposal before the consumer plans to use them.

3.3.1 Standard service offerings

CSPs, especially hyperscale CSPs, offer services that are based on common, commoditized technologies or functionality. These are then offered at scale as cost-effective, high-performing, reliable services. This cannot be achieved if the services are customized for each customer, so it is not typically possible to enter negotiation for heavily customized services.

Some CSP partners specialize in providing customized solutions based on standard cloud services (e.g. a software module that adds functionality to a standard SaaS service). Consumers should clearly differentiate between standard services provided by a CSP and related services or solutions that are provided by a partner, and not expect the CSP to provide services above and beyond its standard service catalogue.

If an organization cannot identify a CSP that can fulfil its essential requirements, it might revise its original requirements and value proposition. Or it might opt for a private cloud build that will provide flexible resources while maintaining core commitments to its customers.

To understand the implications of using a CSP's standard services, the consumer should check various documents, including:

- **Master service agreements (also called customer agreements)** The consumer organization should focus on the elements of the service that will remain its responsibility (such as in relation to data protection) and the protection that will be given to the CSP (such as indemnification, liability limitations, and the temporary suspension process). Other important elements are the terms and conditions and the contract's termination conditions.
- **SLAs** SLAs often focus on availability, but the targets for security and performance also need to be reviewed. Each tier of a multi-tiered service should have an SLA that specifies the level of service offered for that tier.
- **Acceptable use policies** Services are usually restricted by acceptable or fair use policies. The penalties for breaches can vary between CSPs.
- **Privacy policy** How the CSP collects, uses, and protects information. A standard service should meet the minimum privacy regulations and requirements of the organization and its customers.

If a cloud integrator is used, the organization should ensure that the integrator's agreements and targets are at least as strong as those of the CSP.

3.3.1.1 Subscription services

Organizations often use software on a subscription or licence basis. In both cases, the more users there are who need access to the software, the greater the possible discount from the vendor and the more likely it is that an enterprise model will be chosen over one or more individual purchases.

An organization might pay more in the long term for a subscription service rather than a perpetual licence, but subscription services have other advantages, including automatic product updates and support, and small or non-existent up-front payments. To ensure optimal use of subscriptions, it is important to continue to use the same software asset management disciplines that are used for purchasing licences.

Consumers should be aware of the 10 fair software licensing principles articulated by CISPE. These provide guidance on how to ensure that the subscription model avoids some common pitfalls. The 10 principles are:

- licensing should be clear and intelligible
- freedom to bring previously purchased software to the cloud
- customers should be free to run their on-premise software on the cloud of their choice
- reducing costs through efficient use of hardware
- freedom from retaliation for cloud choices
- avoiding customer lock-in through interoperable directory software
- equal treatment for software licensing fees in the cloud
- permitted uses of software should be reliable and predictable
- licences should cover reasonably expected software uses
- permitting fair software transfers.

Considerations when negotiating for subscription services include:

- understand the requirements so that the correct tier(s) of functionality is/are selected
- understand how demand will scale or reduce over time

- align the subscription with deployment/release schedules
- assess the discounts available
- ensure that, for optional user software, business units understand the subscription costs and can justify the expenditure
- evaluate the structure of licensing; although it may seem cheaper to subscribe to a bundled set of products, it is often more expensive if most users use only one or two of those products.

3.3.2 Non-standard services

Some cloud services need to be customized for individual consumers. Some CSPs provide these services, while others depend on partner organizations to deliver them. Some CSPs do both. If an organization works with a partner, it is important to engage the partner organization as early as possible, as it will help determine requirements and give advice on CSP selection.

Examples of non-standard cloud-related services include:

- application rationalization and migration
- cloud migration
- cloud migration monitoring
- cloud management office
- training
- organizational change management.

3.3.2.1 Application rationalization and migration

An objective, data-driven analysis should determine whether the organization's current applications should be rehosted, replatformed, refactored, replaced, retired, or retained. This includes identifying those that should be hosted in the public cloud, in the private cloud, or in-house.

The organization should also consider which applications should migrate first and what the most appropriate migration approach is.

3.3.2.2 Cloud migration

Many CSPs offer migration services, which manage transfers of applications, data, databases, servers, and networks using application programming interfaces (APIs). CSPs and migration partners can assist with key aspects of the actual migration, such as:

- application and data portability and interoperability
- application and data security during live migrations
- bandwidth calculations
- online/offline data transfer
- service continuity.

3.3.2.3 Cloud migration monitoring

CSPs have tools that help organizations track, monitor, and report on the migration. There are two major stages of monitoring:

- **During migration** Common activities include checking for potential issues and monitoring response times.
- **After migration** Initial health checks should confirm, for example, that workloads are as expected, the CSP's SLAs are being met, and resource consumption is as forecast.

Cloud migration monitoring depends on a good understanding of how the applications perform prior to migration, so that any performance issues during or after migration can be understood in context.

3.3.2.4 Cloud management office

A cloud management office can serve as a permanent and scalable central point of decision-making and communication. If an organization has an existing vendor management office, this should be expanded to include the management of cloud service providers. The cloud management office should engage with the following teams and stakeholders:

- architecture management
- cloud engineering
- compliance and risk
- CSPs, cloud consultancy partners, and tooling vendors
- DevOps (including CloudOps)
- HR/training
- procurement
- information and security
- finance
- legal and contracts
- internal audit
- programme or project managers
- supplier management.

3.3.2.5 Training and employee development

New roles that are relevant to cloud are becoming increasingly common, such as cloud and platform architects, cloud engineers, automation architects, and cloud management office leads. These roles can be provided by a partner, employees can be hired using a specialized cloud recruiting organization, or current employees can be trained and certified using a third-party organization or partner.

To become proficient in these roles, practitioners should:

- develop new technical skills, such as cloud engineering, cloud infrastructure operations, platform operations, automation delivery, XaaS, and DevOps
- automate repetitive tasks and standardize services so that IT experts can develop skills to focus on strategic tasks
- learn to understand business goals and translate them into scalable IT planning
- focus on the end-to-end perspectives of services and partners' ecosystems
- establish informal mentoring and job rotation schemes
- build resilient, redundant skill sets and capabilities for teams and individuals
- develop standard training plans for new hires.

3.3.2.6 Organizational change management

The impact of changes to the organization because of the adoption of cloud services should be addressed and reviewed as early and often as possible. IT and business teams will need to work together to:

- assess current and future functions and processes
- build an organizational change roadmap that includes milestones and key performance indicators
- build a strong innovation culture: for example, structure time and activities to focus on innovation
- reduce time from idea to service, and improve workflows
- establish new ways of collaborating across silos and institutionalize informal learning
- communicate changes in roles and responsibilities and ensure that training and support are provided to those affected
- build strong collaborative relationships across traditional silos
- cultivate knowledge-sharing practices.

3.4 Defining requirements for cloud services

The process of defining requirements for cloud services generally starts in the explore stage and continues through the engage and offer stages, by which time the detailed requirements need to be communicated to potential CSPs.

An organization that has limited experience with cloud services may start in the explore stage by defining a high-level set of broad requirements. These organizations often use the engage stage to define more detailed requirements. Most CSPs and partners offer guidance and consulting during this step. Organizations that have more experience with cloud services tend to develop detailed requirements during the explore step, then use the engage step to validate and refine them.

When solutions are built in-house, an organization can task the IT team with understanding the business requirements as well as defining, building, and delivering the solution. Many organizations are therefore accustomed to adopting specific technical architecture according to their requirements. Defining the requirements for cloud services, however, is not about specifying a technical architecture. Rather, it is about mapping business needs to the functionality of cloud services.

The people involved in defining requirements need to have the required cloud competencies and understand which functionalities are provided by different cloud solutions. If an organization cannot effectively map its cloud solution requirements, a request for information, demonstration, or proof of concept can be used instead.

Some organizations may want to enlist specialist organizations to help them understand the scope of the requirements to be defined.

3.4.1 Utility, warranty, and experience

Service requirements can be divided into three categories: utility (fitness for purpose), warranty (fitness for use), and experience (fitness for feelings).

3.4.1.1 Utility requirements

Definition: Utility

The functionality offered by a product or service to meet a particular need. Utility can be summarized as 'what the service does' and can be used to determine whether a service is 'fit for purpose'. To have utility, a service must either support the performance of the consumer or remove constraints from the consumer. Many services do both.

Although utility is often associated with the functionality of applications and SaaS, it is equally applicable to infrastructure and platforms and therefore to IaaS and PaaS offerings.

IaaS utility is stated in terms of compute, storage, and network capacity. PaaS utility is stated in terms of IT functionality, and SaaS utility in terms of business functionality.

The consumer needs to determine whether the utility of the service will keep up with or, in the case of innovative providers, dictate market demand.

3.4.1.2 Warranty requirements

Definition: Warranty

Assurance that a product or service will meet agreed requirements. Warranty can be summarized as 'how the service performs' and can be used to determine whether a service is 'fit for use'. Warranty often relates to service levels aligned with the needs of service consumers. This may be based on a formal agreement, or it may be a marketing message or brand image. Warranty typically addresses such areas as the availability of the service, its capacity, levels of security, and continuity. A service may be said to provide acceptable assurance, or 'warranty', if all defined and agreed conditions are met.

The consumer should assess the available services and CSPs to understand how the warranty dimension of each service will keep up with market demand.

3.4.1.3 Customer and user experience requirements

Definition: Customer experience (CX)

The sum of functional and emotional interactions with a service and service provider as perceived by a customer.

The utility and warranty of a service affect how it is experienced. The combination of functionality, speed and ease of deployment, and operational performance often elicits a superior service experience, provided the service enables the user to achieve their intended objective. This, in turn, affects employee satisfaction, which correlates strongly with customer satisfaction and financial results.

Utility and warranty statements are relatively easy to assess, but experience is a more subjective element. It can be assessed in several ways:

- Correlate the existing level of experience with current levels of functionality, availability, and performance. If a cloud service can provide the same or greater levels at the same or lower cost, the experience is likely to be the same or better.
- Obtain reports or commission research from industry research organizations.
- Test the proposed service with consumer focus groups. This could be done as part of a proof of concept or demonstration of the cloud services, and is the most reliable method for evaluating experience.

As with utility and warranty, the consumer should assess the available services and CSPs to understand how the experience dimension of each service will keep up with market demand.

3.4.2 The impact of cloud services on existing customers

When defining requirements, it is important to consider commitments to existing customers. Cloud services impact organizations' customers at strategic and operational levels.

3.4.2.1 Strategic impact

At a strategic level, cloud services are used to replace or augment elements of the organization's business and operating models. The impacts on existing customers include:

- changes in the ways the organization positions its services and products and achieves a positive customer experience
- changes to existing services
- new parties becoming involved in delivering services, such as if aspects of some services are provided to customers directly by the CSP
- the addition of new services, which can replace or build upon the current ones
- the introduction of new methods of engaging with customers, such as online access to catalogues and order tracking.

These impacts need to be considered when evaluating the VOCR aspects of the service, as discussed in Chapter 2. Any changes to services or products must be carefully researched, as must any changes to the ways in which customers are engaged and their overall experience.

Negative impacts, such as unexpected changes and the loss of features, may result in lower consumer satisfaction. Also, emphasizing the new ways of working and new customers can make existing customers feel deprioritized. Positive aspects should be emphasized, such as improved service reliability, increased responsiveness to new requirements, and the addition of new features that customers have requested.

3.4.2.2 Operational impact

The operational impact of cloud services consists of changes in the performance, cost, and features of existing services.

A move to cloud should, at minimum, support the existing levels of services in SLAs with existing customers, unless the situation demands that the SLAs be renegotiated. Every service requirement must be defined with existing commitments in mind, as well as the anticipated future demand. When evaluating services, the ability to meet or exceed existing, agreed service levels must be a priority.

Opportunities to provide much-improved levels of service may not always be perceived by customers as positive. Sudden, unexpected improvements may threaten a positive, consistent customer experience. After the initial positive experience, customers may ask:

- Will this increase costs during the next negotiation?
- Will the service levels decline over time?

Aspects of operational impacts on SLAs include:

- availability levels
- engagement processes
- new service features
- privacy
- response times
- security.

An executive sponsor, product owner, or account manager should meet with existing customers when necessary to discuss potential changes to their service, to prepare them for the possibility of changes to their SLA, and to get confirmation that they will continue using the service. The results of these discussions should be fed back to those responsible for defining the cloud strategy.

3.4.3 Defining requirements based on outcomes, costs, and risks

A consumer organization can use the VOCR assessment from the explore stage to help define service requirements that will maximize the value of using the service. When reading through this section, it is helpful to remember that the VOCR statements will vary depending on whether the supplier is a CSP or a partner. The rule of cloud services versus labour is useful here. Services are provided by CSPs and labour is typically provided by a partner or the professional services group within a CSP organization.

3.4.3.1 Outcomes

The consumer organization is responsible for achieving its desired business outcomes, but the CSP is responsible for providing the functionalities that the consumer organization needs to be successful.

Outcome-related service requirements are defined using the following steps:

1. Identify the desired outcome.
2. Define what actions must be taken to enable that outcome.
3. Define the responsibilities of the consumer organization and the CSP.

4 Describe how the service should perform the necessary actions, including requirements relating to how, when, and where they are performed.

The service requirements that are eventually communicated to service providers are those listed in step 4, although some organizations include information about steps 1 to 3 as background information to ensure that the requirements are understood. It is vital that all aspects of steps 1, 2, and 3 are completed fully because:

- The requirements communicated in step 4 may not enable the organization to achieve its outcomes, even if the service is delivered as agreed.
- The information from these steps is used to evaluate whether the proposed service will fully meet the requirements.

3.4.3.2 Costs

When defining cloud service requirements, the consumer organization can account for any cost uncertainties. For example, by:

- defining a maximum budgetary amount
- defining an acceptable cost range, and narrowing the range when more information is gained
- benchmarking the current and future costs of not migrating to cloud, then only considering cloud services that provide cost savings or performance improvements over a certain value
- listing all cost categories and gathering more information throughout the assess step.

As with outcomes, not all cost requirements (such as the maximum amount the organization is willing to spend) are communicated to service providers. Rather, the consumer organization will ask the service provider to define the price of the service, including discount structures and any additional costs that will be incurred by using the service.

3.4.3.3 Risks

Service requirements should be designed to remove risk or mitigate it to an acceptable level. Consumers cannot expect CSPs to disclose confidential information about how risks are managed, but they can expect to be given information that assures them that risks are adequately managed, such as through third-party audits and attestations.

An additional aspect of managing risk is to balance the cost of mitigating it and the value of the risk itself. For example, an organization might identify that uncontrolled cloud usage is a risk, but that centralizing procurement and monitoring of all cloud services is a difficult and expensive task. That organization might decide to establish controls for certain categories of cloud services, and depend on policies to guide behaviour for other services.

3.4.4 Typical requirements

Because the use of cloud systems is broad and complex, it is impossible to provide a complete list of possible service requirements. However, some examples are listed in the following sections. These examples do not apply equally to all types of service and service provider, but provide an overview of important areas to consider when defining requirements. Up-to-date guidance on defining requirements for cloud services is provided by several industry groups, such as CISPE.

3.4.4.1 General service requirements

Example requirements for the general aspects of cloud services are listed in Table 3.4.

Table 3.4 Examples of general service requirements

Area	Requirement examples
Service functionality	The service should contain certain required functionalities Simple functionalities (such as 'Does the service support the operating system?') may be indicated in a list with a check box Complex required functionalities may require a detailed description and screenshots
Ease of use	The service should be accessible Standard tasks should be performed in a certain way; for example, how a virtual server is configured or the number of steps to open a ticket Performance levels should be adequate under varying degrees of demand
Interoperability with other systems and services	There should be a list of software products and platforms for which interfaces are required, and whether there are any requirements related to a particular use case or toolset Interfaces should be secured The consumer should be notified of changes or updates to the interfaces
Operational aspects	The service should be available at a certain level (emphasizing resilience in recovering from inevitable incidents). Include periods where availability is more critical, such as month-end Security breaches should be limited, and the service should be recoverable The service should maintain continuity when faced with extreme circumstances (specification of levels of redundancy and the maintenance of separate physical data centres) Service performance should be predictable There needs to be transparency in reporting outages, especially security-related incidents
Authorization to use the service	Access to the service should be controlled There should be protocols to determine that the person ordering the service has the authority to do so The service provider should include tools to manage access

3.4.4.2 Data requirements

Because consumer organizations lack direct control over CSPs' activities, they may have concerns and risks associated with data. These risks refer to the veracity of third-party data and to the security, ownership, and portability of the service consumers' data.

Example data requirements for cloud services are listed in Table 3.5.

Table 3.5 Examples of data requirements

Area	Requirement examples
Data governance	Tools should be available for the consumer to manage, audit, and report on data use There should be minimum data governance standards
Security of data at rest and in transit	The CSP should provide a certain level of security Tools should be provided to monitor and report on potential security incidents
Data ownership	Who owns the data and who is responsible for managing it (especially third-party data) should be clearly defined How data should be secured should be clearly defined How complete removal should be confirmed after the consumer organization has deleted it should be clearly defined
Backup and restore services	A person responsible for backing up and restoring data should be identified The consumer organization's standards should be automated Tools should be provided for managing and auditing data A certain level of redundancy and failover should be provided as part of the service
Veracity of third-party data	Where a cloud service includes the provision of third-party data, the CSP should verify its: ● accuracy ● completeness ● credibility ● timeliness
Portability of data to another CSP	Data should be returned to the consumer, or certification of its removal should be provided The consumer organization should be able to transfer data Details about data models and storage architecture should be provided The organization should be able to test data transfers and offboarding

3.4.4.3 Security requirements

Security is a standard feature of most cloud services, but the secure usage of those services is the responsibility of the consumer organization. The exact division of responsibility can vary, and it is easy for misunderstandings to occur. It is important to establish exactly what will be provided by the CSP, and what will be expected of the consumer organization.

Example security requirements for cloud services are listed in Table 3.6.

Table 3.6 Examples of security requirements

Area	Requirement examples
Security architecture	The service should have specific architectural elements to improve security
Security standards and policies	The CSP should comply with certain security standards, such as ISO 27001 There should be standard security policies for the service The CSP should provide templates or guidelines for implementing security policies
Security tools	Security monitoring and reporting tools should be provided
Security monitoring and auditing	Any audits that are required must be specified
Security incident management	The CSP must report security incidents that may impact the service The consumer organization should be able to assist the CSP in resolving security incidents
Privacy	Evidence should be given that data is stored in compliance with the relevant country's regulatory requirements

3.4.4.4 People-related requirements

Regardless of the type of cloud service, people need to understand how to manage and consume it. Typical people-related requirements are listed in Table 3.7.

Table 3.7 Examples of people-related requirements

Area	Requirement examples
Awareness and training	There should be communication with stakeholders about the service, what it is for, and how it will impact the current roles, responsibilities, and processes There should be training on how to manage (if appropriate) and use the service Any required certifications should be provided or enabled
Transfer costs	If migration to cloud requires a transfer of employees to another organization (such as a managed service partner), define how many and which employees need to be transferred Relocation costs should be kept under a certain amount, and who will bear them should be specified

3.4.4.5 Service provider requirements

Entering into a contract with a CSP is as much about consuming services as it is about entering into a relationship with an organization. An organization that relies on cloud services must be sure that:

- The service provider will continue to be in business for as long as its services are needed.
- The service provider will continue to deliver services in the required form and at the required level.
- The service relationship is healthy: communication is open, cultures are compatible, and changes are easily negotiated.

Typical service provider requirements are listed in Table 3.8.

Table 3.8 Examples of service provider requirements

Area	Requirement examples
Supporting service	The CSP should provide the option for certain levels of support in the following categories: ● support options ● hours of support ● level of knowledge and experience of those supporting the service ● the role of automated or self-help support
Technical capabilities	The CSP (or its partner) should provide resources and expertise if the consumer needs assistance There should be a defined process to engage technical support Some level of monitoring and reporting should be provided Tools should be available so the consumer can monitor and manage service performance There should be a formal process for requesting, approving, testing, and accepting changes Standard updates should be reported on and announced in advance Event management tools and reporting should be provided by the CSP, a partner, or the consumer

Relationship with the provider and communication channels	The consumer organization should have a main contact for the CSP or partner, depending on the type of service being provided Service reviews should be conducted at a certain frequency The shared responsibility model should be articulated appropriately for the type of contract CSP or partner staff might participate in some of the consumer organization's internal meetings, although this is not the norm for hyperscale CSPs that provide standardized services
Commercial terms and conditions	Wherever possible, the CSP's terms and conditions should be used. This is because of the standardized nature of the CSP's services Requirements around termination may include such aspects as: ● termination notification periods ● early termination penalties or other costs ● the process for providing notification ● the circumstances under which the provider may terminate or discontinue the service ● policies or regulations that apply to switching between CSPs
Regulatory requirements	The CSP should demonstrate compliance with the relevant regulations if appropriate (either through holding relevant accreditation or by showing equivalency)
Business health	The CSP or partner should: ● meet or exceed a certain standard of financial health ● carry appropriate insurance ● be able to provide a list of references

3.4.4.6 Cost reporting, billing, and payment requirements

Cloud service billing can be complex, especially if several services are used in the same contract. Cloud billing reports should be structured to show the customer organization its usage costs at a glance, and to discover and help analyse trends. Typical requirements for cost reporting, billing, and payment are listed in Table 3.9.

Table 3.9 Examples of cost reporting, billing, and payment requirements

Area	Requirement examples
Billing reports	Billing reports should follow a defined structure, with cost information itemized and communicated in a specific way The consumer organization should be able to analyse trends Reporting and modelling tools should be available to determine how changes to service utilization will impact cost
Purchase and payment authorization	The consumer organization should control who orders and pays for services
Billing and payment information	The CSP should provide a clear schedule of billing dates Payment periods, terms, and conditions should all be defined
Upscale/ downscale options	The consumer organization should be able to scale its usage up or down if actual costs exceed expectations or there is an increase in demand

3.5 Request for information and proof of concept

A good starting point for defining requirements is the list of current technologies used, including an explanation of what they are used for. A mature organization might have fully defined service portfolios and application portfolios that indicate the relationships between applications, infrastructure, and business activities. A less mature organization will need to perform an audit to gather this information. The audit must identify:

- business functions and the systems or services they use
- the business processes, procedures, and activities that are supported or enabled by technology
- specialist resources and knowledge required
- the technological functionality needed to support all of the above.

With this information, the consumer can compare the list of areas that need to be supported with marketing information about available cloud services. Further meetings may need to be held with CSP representatives or partners to get more information. This information can be further augmented by issuing a request for information or market survey. Responses can help the team to identify the options that are most likely to meet its requirements.

When it is unclear whether a service will fulfil the requirements, a proof of concept can demonstrate how the cloud service would provide the required functionality and whether it would facilitate the desired outcomes.

The end result should be a shortlist of potential CSPs, their partners, and their services.

3.6 Conducting a cloud readiness assessment

When an organization has defined its requirements for cloud, it should consider undertaking a cloud readiness assessment. This will help the organization to determine its current operating model's readiness for cloud services, and to define a target operating model. This assessment may also highlight additional cloud requirements that will need to be addressed.

A consumer organization entering into a shared responsibility model for the effective delivery of cloud services needs to ensure that its proposed operating models are cloud-ready by reflecting the roles and responsibilities of the shared responsibility model.

Being cloud-ready means that the consumer organization's existing operating models can effectively design, build, operate, support, manage, and govern cloud services, or that it has selected a CSP partner who can do this on its behalf. Organizations that understand their own cloud readiness can articulate their cloud requirements more easily than organizations that cannot.

Many proprietary assessment models are available from CSPs and their partners. Independent consulting firms also provide cloud readiness assessments.

When using a third party's proprietary assessment, an organization should be aware of the risk of assessment lock-ins. Assessment lock-ins occur when the assessment results only cover options from a single CSP, or require that the organization purchases more consulting work or other solutions from the assessment provider. Before agreeing to an assessment, the organization should understand exactly what the outcomes of the assessment will be. The assessment results should be actionable by the customer organization immediately, without any further steps needed.

3.6.1 Steps in conducting a cloud readiness assessment

The most important steps in conducting a cloud readiness assessment are:

- define the assessment scope
- assess current resources
- specify the desired scope of cloud services
- assess operational readiness
- produce an assessment report.

3.6.1.1 Define the assessment scope

The cloud strategy should define the intended scope and use of cloud services in the organization. The cloud readiness assessment could either assess all areas defined in the cloud strategy, or just a subset of them. This will ensure that the assessment indicates accurately whether the organization is ready to achieve the objectives set out in the strategy. If not, it will identify the appropriate corrective actions.

It is better to assess all initiatives in the strategy at once, so that if one initiative proves unfeasible, it is still possible to move ahead with other initiatives without repeating the assessment.

It is also important to ensure that the assessment includes a review of the current organizational culture to determine whether the people and working methods will support a move to the cloud.

3.6.1.2 Assess current resources

A full readiness assessment should consider:

- **Funding** It is important to determine whether funding will be available for the move to cloud services, even if the exact figures are unknown.
- **Executive management support** Even if funding is available, the initiative will not succeed unless executives are willing to visibly support it.
- **Applications** This includes an inventory of the applications that are in use and in scope, how they are currently architected, whether they can be replaced or migrated, whether they were internally or externally sourced, what licensing and maintenance contracts apply, and to what extent there is duplication.
- **Infrastructure** The organization should understand what IT capacity is currently being supported, including a list of servers, storage, and networking equipment, and how the equipment is being used (is there a map of which devices support which applications, virtual machines and so on?).
- **Workloads** It is important to determine which workloads will be migrated to the cloud, what resources they use (and how much of each resource), and how those workloads are likely to change over time.
- **IT staff** There should be an up-to-date inventory of IT staff's skills, which will help determine how much training they will need to use and manage the anticipated cloud services. It is important to determine whether they could migrate to cloud while managing the existing in-house solutions. The assessment should also evaluate whether the IT team knows how to migrate, manage, and optimize cloud services.
- **Security requirements** The assessment should outline what data needs to be protected and to what level, including what regulations apply to the anticipated cloud services.

3.6.1.3 Specify the desired scope of cloud services

When the organization's current state has been assessed, the desired future state should be defined. This includes defining:

- which existing solutions will be migrated into the cloud, and what level of migration will be considered (for example, replacing in-house solutions with cloud services)
- which new cloud services will be deployed
- which existing solutions (applications, infrastructure, and so on) will be decommissioned.

3.6.1.4 Assess operational readiness

The organization should perform a gap analysis between the current state and desired future state. This will highlight whether the organization is ready to move to the cloud; it will also indicate what changes need to be made if the organization is not ready.

Some examples of operational readiness assessment areas are:

- **Support readiness** Does the current service model adequately map the support responsibilities of the consumer organization and the CSP or partner to ensure all incidents are managed effectively?
- **Change readiness** Do the current change process and change models support the rapid, ongoing 'push' nature of CSP service updates and new features?
- **Financial readiness** Have financial risks for the cloud been clearly understood, and have adequate controls been established to manage the risks of uncontrolled cloud consumption costs? Do the organization's current financial model and practices align to the dynamic nature of cloud service, such as elasticity and agile budgeting practices?
- **Legal readiness** Do the CSP's or partner's SLAs align with the organization's requirements? Are other partners' SLAs and contracts aligned with the CSP's or partner's SLAs?
- **Skills readiness** Are the skill requirements for the cloud service understood and met?

Operational readiness assessments can cover other capabilities, such as the HR processes for recruiting, job changes, and leaving; and service design readiness (being able to design and architect cloud solutions).

3.6.1.5 Produce an assessment report

The assessment report should provide information on the scope of the assessment, and on the readiness of the organization to move to the cloud within that scope. The contents of this report help to define the requirements in the offer stage. The report should include:

- the actions that need to be taken before the organization can move to the cloud
- an action plan that details timelines and budget to prepare for implementing the services that are in scope
- a statement of what training will be needed
- a report on what changes need to be made to the organization (for example, establishing a cloud management office)
- a list of required migration tools and services.

3.6.2 Architecture readiness examples

As explained in section 3.6.1.2, part of the cloud readiness assessment is creating an inventory of the organization's current applications. Table 3.10 shows examples of application/workload-specific readiness checks.

Table 3.10 Examples of application/workload-specific readiness checks

IaaS/PaaS	SaaS
Application compatibility Has the application been coded for cloud infrastructure usage? Is it optimized for reading and writing operations, and can it cater for cloud latency, run in high-availability configurations, and scale?	**Data readiness** Has all of the data to be processed and stored by the application been appropriately classified and encrypted in transit and at rest? Does the data meet regulatory compliance in terms of location and processing regulations?
Application security Has the application been checked for vulnerabilities within a cloud environment? Is application data encrypted during transit and rest?	**SaaS security and compliance** Does the SaaS solution have the appropriate security and compliance controls required to configure and align to the customer organization's security and regulatory position?
Database compatibility Are the current application databases supported in the cloud?	**Performance** Does the SaaS solution perform adequately in the cloud? (For example, are response times within expected levels?)
Performance Does the application perform adequately in the cloud (for example, are response times within expected levels)?	**Continuity and reliability** Does the SaaS solution have appropriate backup and disaster recovery options, or does it accommodate custom or third-party solutions?
Continuity and reliability Has the cloud solution been architected with appropriate availability and scalability, and does it include appropriate backup and disaster recovery?	**Monitoring** Does the SaaS solution have suitable monitoring end points in order to effectively monitor the availability and health of the service?
Data readiness Has all data to be processed and stored by the application been appropriately classified and encrypted in transit and at rest? Does the data meet regulatory compliance in terms of location and processing regulations?	
End-point monitoring Have monitoring end points been defined in order to support the effective monitoring of the end-to-end solution as well as the CSP's cloud services?	

The organization also needs to ensure that its in-house infrastructure will provide sufficient access to the cloud solution. It is important to assess the following:

- **Network** Does the in-house network have sufficient capacity for the traffic that will be introduced by cloud? Have suitable failovers been established to ensure high-availability access to the cloud where appropriate?
- **Identity and security** Are the employees' identities integrated with the cloud solution (such as in a domain directory)? Is data being encrypted at rest, in-house, and in transit to the cloud?
- **Monitoring** Are the assets involved in cloud delivery being monitored for availability and health?

3.7 Engaging with cloud service providers

3.7.1 Evaluating shared responsibility models

Shared responsibility models are defined in Chapter 1. Each CSP has its own approach to shared responsibility models, so it is important to understand how they can differ. An organization should evaluate CSPs on the services they offer, including which management activities are provided by the CSP and which activities the consumer is required to perform, as well as which tools are provided to help them.

Unless they have specifically outsourced certain responsibilities to a CSP, cloud consumers should be aware that they will remain accountable and responsible for many activities. Table 3.11 outlines some examples.

Table 3.11 Consumer organization responsibilities versus CSP responsibilities

	Consumer organization responsibilities	CSP responsibilities
Support	Monitor the CSP's service health indicators, and send alerts to the service desk and support groups Categorize, own, and manage all cloud incidents on consumer-controlled solutions throughout their lifecycle Evaluate and triage cloud-related issues before they are escalated to the CSP Define a major incident response plan	Provide alerts and dashboards to indicate the current health of services by region Provide a knowledge base to assist with troubleshooting and resolving cloud issues Provide responses after the occurrence of significant incidents to CSP-controlled infrastructure
Change enablement	Define a process to monitor and track the CSP's roadmaps, and triage changes according to the correct business context Define appropriate change models, and log changes in the appropriate manner Define people adoption, and change plans to empower people to use and support the change	Map planned changes within an acceptable timeframe Distribute information about the change before it is deployed Encourage feedback on proposed changes
Service level management	Ensure that the end-to-end SLAs for a service are understood, and define appropriate quality and experience metrics Establish service monitoring plans so that all service assets can be monitored for end-to-end SLA alerting and reporting	Publish service descriptions and service levels
Governance, security, regulatory compliance	Only allow appropriate data into the cloud Adhere to all relevant regulations Establish and implement a cloud security policy and controls Ensure that the CSP's services align with the organization's data-sharing, regulatory, and security requirements, including using CSP tools and functionality to comply	Provide controls and capabilities for security, data, and regulatory compliance Ensure that the cloud service infrastructure meets the relevant regulatory, security, and quality standards as defined in the CSP's third-party audit reports, and that these are regularly audited
Cloud architecture	Ensure that cloud services are designed and architected according to the relevant CSP's best practices, and against the end-to-end SLA requirements Ensure that cloud services are architected for usability and accessibility	Publish architecture design patterns and cloud service best practices

3.7.2 Engagement level options

Using its strategic assessment with a clear understanding of its architectural and operational readiness, the consumer organization should determine at what level it will engage with a CSP or partner. This may reduce the number of viable CSPs and partners it will want to engage.

There are three broad engagement levels, which are defined in *ITIL® 4: Drive Stakeholder Value*:

- **Basic relationship** Focuses on support and efficiency, with engagement fixed at an operational level. For example, if an organization wanted to move an application into an IaaS cloud environment,

and it had the skills and resources to do so, a basic relationship would be the most practical option. Relationships with large-scale or hyperscale CSPs generally fall into this category.

- **Cooperative relationship** Focuses on improvement and effectiveness, and typically occurs across the operational and tactical levels. These are often trusted, advisory relationships with CSP partners. For example, if an organization wanted to optimize and automate a business function, such as human resources, it may choose a cooperative relationship that includes advisory services.
- **Partnership** Focuses on innovation and growth, where the service provider (usually a boutique CSP or a CSP partner) is a strategic partner with the consumer organization. For example, if an organization sees cloud as a strategic and competitive opportunity, it may consider partnering with a CSP and working closely with it at the strategic, tactical, and operational levels.

3.7.3 Acquisition channels

CSPs and their partners provide several channels through which consumer organizations can access their services. These include:

- **Through the CSP:**
  - **Online** Customers can use the CSP's website to self-help and start or terminate services. This is an option in a basic relationship with a CSP, unless further professional services are purchased through the online portal.
  - **Through an enterprise agreement** A customer organization can engage with a cloud provider representative and sign an enterprise agreement that entitles it to additional enterprise grade services and savings. This implies a cooperative relationship or partnership.
- **Through a CSP partner** Services can be purchased through an accredited CSP partner in a cooperative relationship or partnership. An organization might choose to work with a CSP partner over the CSP itself because it may:
  - offer lower prices due to mass discounts
  - offer more niche professional services
  - provide access to more experience and specialized skills, such as managed services, that further relieve customer organizations of their typical responsibilities across the shared responsibility model.

Within these channels, a consumer organization can access services using one of the methods described in Table 3.12.

Table 3.12 Methods of accessing cloud services

Acquisition channels/offers	Description	Value
Pay-as-you-go	Consumers can use a pay-as-you-go model that is provided directly by CSPs. They pay for actual usage, with no minimum quantity or up-front payment required. This is typically used for IaaS- or PaaS-based service offerings or software offerings that do not require licences to be purchased.	This method is flexible in terms of how organizations adopt and consume cloud services. Because no up-front investments are required, there is minimal risk.
Prepaid commitments	Consumers can purchase volume-based discounts or up-front enterprise agreement commitments with CSPs to make greater savings. For certain IaaS and PaaS services, they can also prepay (for an additional discount) for cloud resources, such as storage, up to 3 years in advance. For SaaS services, consumers usually purchase licences for a predetermined period.	Outside of SaaS services, prepaid commitments provide significant cost savings regarding the consumption of services through up-front investments. Volume-based licensing also provides cost savings for SaaS-type services.
Cloud service plans and professional services	This relates to specific CSP- or partner-specific services or service groupings, which generally include non-consumption professional services options along with proactive and reactive support, architecture services, and so on. Support options are generally purchasable online, but they and all other cloud services and plans can usually be obtained through the CSP's enterprise agreement or through the offerings provided by the CSP partners.	Consumers may consider specific plans or service groupings to access more advanced value offerings or professional services to help them adopt and manage cloud services. This is usually beneficial for consumers who are just starting their cloud journey, as it will help them establish best practices early on.

3.7.4 How organizations engage with CSPs and their partners

Organizations may engage with CSPs and their partners (based on the desired engagement levels) in several ways:

- individual consumer services
- as-needed engagements driven by IT teams
- large-scale engagements.

3.7.4.1 Individual consumer services

An organization may experiment with cloud services before deciding whether to use them long term or engage a CSP. These experiments are generally led by a single person, such as a cloud solution architect or senior engineer, who will provide feedback about the experience to the organization.

In some cases, individuals may purchase cloud services to bypass the IT department, perhaps to avoid delays. Because of the pay-as-you-go link to IaaS or PaaS, individuals can use their corporate or private credit to pay simply and easily.

The benefits of individual consumption are in the easy and immediate access to cloud resources, and flexibility of use. The risks, however, generally relate to the use of cloud services outside the defined governance and security structure.

3.7.4.2 As-needed engagements driven by IT teams

Some organizations have projects driven by IT teams or other organizational units that require temporary cloud capabilities. This scenario would usually require only a basic relationship with the CSP, but a cooperative relationship or partnership could be necessary in some scenarios; for example, if business units or IT teams run large-scale proofs of concept.

If the consumer does not define its requirements, there is some risk that these engagements may not meet corporate IT's security and compliance requirements, or that the work being performed is not part of a stated and agreed initiative.

3.7.4.3 Large-scale engagements

Private- and public-sector organizations that are more mature in their use of cloud services typically fall into this category, as they typically have an enterprise agreement with a CSP or partner or are using volume-based or up-front purchases to leverage cost savings.

These engagements are typically managed through a formal supplier management process. The consumer organization should align its operations (architecture and support capabilities) to ensure it can execute its shared responsibilities with its CSP or partner. This scenario necessitates a cooperative relationship or partnership.

3.7.5 Researching what services are available

Understanding what services CSPs provide requires a detailed investigation that evaluates available services within the organization's context. Important questions include:

- Are the organization's requirements fully understood?
- Are the services the organization needs available from one CSP, or will it need to engage multiple CSPs or partners?
- Are there services that the organization was not aware of that would be a better fit for its strategic objectives, operating model, or culture?
- Do any aspects of the cloud strategy or requirements need to be updated?
- Do the cloud services do what the organization thought they would do?
- Do the cloud services enable the organization to meet regulatory requirements?
- How well do the cloud services fulfil the organization's requirements?
- What combination of services will help the organization to meet its strategic objectives?

The most common sources of information about available services are:

- CSPs' websites, which will contain a catalogue of available services
- CSP sales staff
- CSP partners
- third-party consultants, who often promote available services after helping to define a cloud strategy or performing a cloud readiness assessment
- other organizations that have transitioned to cloud.

3.8 Reviewing the cloud strategy and cloud service requirements

When an organization has engaged with a CSP or partner, the CSP or partner can provide detailed insights into the organization's strategic cloud objectives and plans. The organization should encourage a full review of the cloud strategy and service requirements to ensure that it has incorporated everything it has learned.

The objectives of the review are to:

- update the cloud strategy based on input from the CSPs
- define detailed requirements based on input from the CSPs
- refine previously defined detailed requirements
- identify any aspect of the strategy that is unfeasible based on what has been learned.

3.9 Summary

In the engage step, high-level understanding is no longer adequate; consumers should pursue comprehensive internal and external awareness. Internally, high-level requirements should be refined through a detailed requirements analysis. This may result in a review and revision of the organization's cloud strategy. In addition, the consumer organization should assess its level of organizational and architectural readiness for cloud services. When gaps to cloud adoption are identified, an action plan to proactively remediate them can be developed. Externally, consumers should become familiar with the landscape of services, CSPs, CSP partners, and industry organizations. A formal return on investment could be utilized to initiate contact and interaction with a potential CSP and begin to develop a shortlist of candidates.

CHAPTER 4

OFFER: SELECTING THE RIGHT SERVICES AND SERVICE PROVIDER

4 Offer: Selecting the right services and service provider

4.1 About the offer step

Once an organization has defined its cloud strategy, evaluated its readiness to use cloud services, defined its service requirements, and started to engage with a cloud service provider (CSP) or partner, it is ready to begin the offer step.

The offer step is about evaluating the services available from CSPs to ensure that they will meet the consumer organization's requirements. The aspects of the services to be evaluated include:

- service features and specifications
- cost
- risks (and risk mitigation measures).

The offer step also involves evaluating whether each CSP can provide the agreed services at the agreed level as long as the services will be used. The evaluation is based on offers made through standard service catalogues and requests, such as a request for proposal (RFP).

The offer step involves understanding:

- how to specify requirements to be communicated to CSPs and/or partners
- the role of an RFP in acquiring cloud services
- how to use purchasing frameworks to procure cloud services
- how to evaluate proposals
- how to select a CSP and cloud services
- how to select CSP partners that provide cloud adoption and migration services
- how to calculate return on investment (ROI)
- how to create and communicate a business case to obtain formal approval and funding for the selected services.

Inputs to the offer step include:

- all requirements defined in previous steps of the cloud consumer journey
- CSP standard offerings
- the consumer organization's cloud strategy

- the consumer organization's procurement processes and policies
- the results of the cloud readiness assessment.

The major outputs from the offer step include:

- an evaluation of solutions and services proposed by CSPs and their partners
- a business case to accept the chosen proposal, including a definition of the anticipated ROI
- a selected offer, which will inform the agreement of terms and conditions
- a statement outlining the minimum acceptable services and service levels as a baseline for negotiation.

4.1.1 Elements of the offer step that are specific to cloud services

The offer step for cloud services involves several uncommon elements:

- An RFP is rarely used for simple, standardized services.
- Cloud services are rarely tailored for individual customers. Instead, CSPs bundle predefined services together for an individual customer or offer varied levels of service or support.
- Cloud services are standardized. They are defined in catalogues and sold as out-of-the-box solutions.
- Large-scale migrations often involve more than one organization, such as the CSP and one or more of its partners. The cloud services themselves are contracted separately from the work done to prepare for and conduct the migration.
- Most cloud services are provided based on market price (that is, their price can go up and down). When purchasing from a CSP, it is therefore not appropriate to use RFXs and business cases to determine a fixed price. It is more appropriate for CSPs to provide dynamic pricing to ensure that consumers can access all services and the latest features and functionality.
- Many cloud services are designed for fast onboarding and offboarding. Lengthy procurement and evaluation cycles are counter to the benefits and methods of using cloud services. It is therefore more appropriate to use a framework or IDIQ (indefinite delivery, indefinite quantity) contract vehicle with a direct award mechanism and provide a purchasing catalogue based on the CSP's console to allow for quick, easy, and dynamic purchasing by multiple consumer organizations, departments, or individuals.

4.2 Establishing a desired minimum return on investment

It is good practice to establish a minimum desired ROI before starting procurement activities. This ROI will identify the returns anticipated from using cloud services and will specify the maximum amount of investment that is available to acquire, migrate to, and use cloud services. It will ensure that the RFPs and so on articulate the appropriate requirements and that responses are in line with what is feasible for the organization. It will also ensure that those CSPs or partners that cannot offer services at the proposed levels of investment will not submit responses.

When the responses have been received, the specific details can be entered into the ROI calculations and a more accurate view obtained. This revised ROI will be used to articulate the business case to proceed with the agreed solution.

A detailed description of the ROI process and calculations is provided in section 4.6.

4.3 Communicating requirements

Organizations usually define requirements during the explore and engage steps. During the offer step, the organization will communicate its fully defined requirements to one or more CSPs. It is important to communicate with CSPs and their partners early and often, and to allow for requirements to be changed or adapted to ensure that suppliers can participate.

After a CSP has reviewed the requirements, it can submit a proposal that indicates whether it can provide a service that meets the requirements. If a requirement cannot be met, or if the price of the service is too high, the consumer may decide to redefine or eliminate the requirement before entering the agree step.

The service provider may suggest changes to requirements during the offer stage, such as architectural refinements or alternative solutions at different price points.

4.4 Request for proposal

Definition: Request for proposal (RFP)

A formal document that provides background information and requirements to a shortlist of service providers, and invites them to submit a commercial proposal for products and services that meet or exceed the stated requirements.

Public-sector consumers can create RFPs to procure cloud services. However, it is highly recommended that an existing cloud procurement vehicle should be used (for example, a cloud framework or IDIQ). Creating a fit-for-purpose cloud RFP can be complex and time-consuming, so for speed and ease, public-sector consumers should use existing vehicles wherever practical.

RFPs for cloud services are different from those for other types of solution, such as hardware, applications, and consulting and bespoke development work. Differences include:

- CSPs and their partners are unlikely to submit joint RFP responses because they provide different solutions, support, and services. CSP services are standard and provided directly to their customers, whereas CSP partner services are usually tailored. Because CSPs and their partners provide different things, consumers should purchase separately from these two groups and not try to combine an RFP for CSPs and their partners. It is important for consumers to remember that CSPs do not act as subcontractors to their partners.
- Standard cloud services (including details about pricing, discounts, features, terms and conditions, usage limits, and so on) are provided in the CSP's service catalogue. An RFP is not required to assess

whether these services meet the defined requirements. Rather, it is used as a way of complying with regulatory or legislative requirements and to enable a clear comparison between different CSPs using a common structure.

- The RFP should not only be used to procure services, but also to set up a dynamic mechanism whereby the consumer can order services as and when needed.

The RFP should reflect the outcomes the consumer wishes to achieve, including what tools and features are required to meet those outcomes, rather than simply outlining what service the CSP should provide. This allows for clearer understanding of whether requirements would be met, and where some requirements can be excluded in favour of a lower price.

In a cloud proposal, the CSP will provide information about its services, features, costs, licensing terms, conditions of use, and so on. It should also explain how utilization costs are calculated, whether there are caps to utilization, and whether there is any way of levelling costs over time if this is required by the consumer (such as by managing when workloads are performed or making use of reserved instances). Partner organizations will include information about the services they have been requested to provide, including migration activities, costs, and consulting fees.

If the consumer does not engage suppliers sufficiently before the RFP, these proposals often highlight service requirements or service limitations that were not identified earlier. In addition, for CSP partner proposals, the consumer organization may wish to eliminate or qualify some requirements to reduce the price of the service. This could lead to a second round of proposals, often to a subset of the original group of CSPs or partners.

The proposal should not be the only consideration when selecting a CSP. The CSP's reputation, culture, and financial health should also be verified, as discussed in Chapter 3.

It is good practice to engage CSPs early in the process, and to consider using their terms in crafting the RFP. It is also important to provide a specific response timeline when requesting proposals, so that all parties have a chance to submit.

4.4.1 When to request proposals

RFPs are suited to large, complex solutions, such as combinations of cloud services or a large-scale migration of in-house solutions to the cloud. Most public-sector consumers are required to use RFPs to request and evaluate all cloud services above a certain value, regardless of whether they are standard or customized.

RFPs are useful for evaluating whether cloud services meet stated requirements, and to compare various aspects of services from different CSPs. However, it cannot be used to negotiate customizations for standard services. Individual services and their service agreements are predefined and prices are dynamic. Discount structures based on volume are also predefined. To compare the details and prices of these kinds of services, organizations should examine CSPs' service catalogues, unless they are required to go through an RFP process.

If an organization has unique requirements, these are negotiated directly with the service provider during the agree step. This is very unusual for services provided at scale (such as IaaS services from hyperscale CSPs) but may be the norm for smaller-scale CSPs, boutique SaaS CSPs, and CSP partners. A request for information (RFI) or RFP could be an effective vehicle for communicating those requirements.

RFPs are also used for complex situations, such as large-scale migrations or solutions that require a combination of standard and non-standard services (for example, a hyperscale CSP has a professional

services division that will help the consumer to migrate to the new cloud services). In the latter case, two separate sets of requirements should be defined, as the procurement of cloud services is very different from securing services for assistance with migration.

In many cases, the required services cannot be provided by a single CSP. The RFP process will need to differentiate between services that are offered by a CSP, and those that are offered by one of its partners. Two of the options open to the consumer organization include:

- Issue several RFPs, each focused on one aspect of the solution and one set of service providers, such as CSP-provided cloud services or partner-provided migration services.
- Engage a cloud specialist to act as a broker. This typically happens when the consumer organization does not have the skills or knowledge needed to create the RFP. The cloud specialist is often engaged during the explore or engage step.

Both of these options, where the consumer organization is coordinating components from several CSPs, demand a supplier management approach. Many organizations create a vendor management office (VMO) or a cloud management office, specifically to manage these complexities. A VMO's responsibilities do not end with the procurement of services but continue throughout the cloud consumer journey.

4.4.2 The request for proposal process

As explained in section 4.4.1, this process is intended for large-scale migrations and complex solutions, especially where additional or non-standard services are required. It is also the required method for many public-sector organizations when acquiring standard and non-standard services.

Inputs to the RFP process include:

- the cloud strategy, which will identify the overall priorities and outcomes that the solutions are expected to achieve
- the results of the cloud readiness assessment
- defined service requirements
- information learned from the CSP about the nature of its services and the steps the consumer is required to take before onboarding those services
- the results of any RFIs, demonstrations, or proofs of concept conducted.

The typical steps of an RFP process are:

- **Market consultation** This typically lasts for 12 months before the RFP is released and includes open discussions with potential suppliers to understand what services and solutions are available and how best to procure these. This is part of the engage step.
- **Draft RFP** The structure of an RFP is outlined in section 4.4.3.
- **Pre-qualification** Certain CSPs or partners may be disqualified from submitting proposals; for example, if regulations require that the CSP is in the same country as the consumer organization.
- **RFP released** This typically occurs in two ways:
  - The RFP is sent to CSPs based on the research done during the engage step.
  - RFPs are posted publicly and any CSP or partner can respond (if a pre-qualification was not used).
- **Questions and answers** CSPs can ask questions about the RFP to clarify requirements and priorities. Many organizations host question-and-answer sessions to facilitate this. Consumers should consider their questions carefully and amend the requirements to correct errors or provide

further clarification. If market engagement has been conducted extensively before the RFP, this is less likely to occur.

- **Responses submitted** By a specified due date, CSPs will produce a proposal. The proposal should answer the questions in the RFP, and provide details of the proposed solution and the price for each of the services.
- **Proposal clarification** If further information is required, the consumer will request clarification.
- **Demonstration of proposed services** It is sometimes difficult to evaluate services without seeing them in action. Shortlisted CSPs may be asked to provide a demonstration of the proposed solution. This is a highly recommended step to gain clarity and understand the services involved in the proposal.
- **Proposal evaluation** Each proposal is evaluated according to how it meets the defined requirements and at what cost.
- **Shortlist** A shortlist of proposals that are closest to meeting all the requirements within an acceptable price range can be helpful. These proposals then undergo a second round of evaluation. This step may be recommended for large, complex, and tailored solutions from CSP partners, but is not appropriate when buying standardized services from CSPs.
- **Additional qualification** The evaluation process might involve defining more detailed requirements. It might also involve requesting a proof of concept to demonstrate that the solution works as stated.
- **Selection and negotiation** The consumer organization selects its preferred CSP and enters a negotiation phase (this is the beginning of the agree step). Often, a consumer organization will negotiate and award different parts of the solution to different CSPs.
- **Award contract** If terms can be agreed, the contract is awarded to the successful CSP. If not, the consumer organization may select the next provider on the shortlist and enter negotiations with it.

4.4.3 Contents of a request for proposal

Cloud RFPs are different from traditional IT RFPs. Cloud technology is not a like-for-like replacement for traditional methods of computing; it introduces a completely new way to consume technology. Well-designed cloud RFPs help consumer organizations to take advantage of the cloud quickly. This should be reflected in the content of the RFP and (where appropriate) the way in which it is used to establish a cloud framework agreement or IDIQ.

In the introduction to a cloud RFP, it is good practice to articulate:

- the business objectives and benefits the organization seeks to achieve by using cloud
- the scope of the services to be included (an RFP to a CSP for standard services is different from an RFP for a partner to provide non-standard services; large-scale CSPs do not submit a response as part of another organization's RFP)
- the company that is being requested to submit a proposal.

Cloud RFPs follow a standard format that helps the organization to set expectations on how CSPs should respond. Table 4.1 outlines this format.

Table 4.1 Cloud request for proposal format

RFP section	Purpose
Purpose statement	An overview of why the organization is adopting cloud services. It highlights the organization's major strategic objectives and may outline the problem the cloud solution is supposed to solve
Company information	An overview of the consumer organization and its industry
Timeline	Indicates the dates by which each cloud service should be available to deliver its intended value
Scope of work and standards	Outlines the anticipated project phases (if they are known), along with detailed objectives per project phase, and all performance and quality standards
Deliverables	An overview from the CSP or partner of the services it is proposing and how it meets the requirements defined across the explore and engage steps
Contract terms and conditions	Highlights any explicit legal and compliance requirements concerning data usage or security, and relevant supplier policies regarding subcontractors (if the supplier is a CSP partner). Consumers should incorporate CSP terms and conditions to the greatest extent possible
Evaluation and award process	Articulates the evaluation and award processes
Appendices	May include relevant: ● architecture diagrams or documentation ● design documentation

4.4.4 Using cloud framework agreements

Definition: Framework agreement

A catalogue of agreements that have been negotiated and approved by an organization on behalf of multiple customers within the organization. Customers can select the service they need from a list of preferred service providers at rates, terms, and conditions that have been pre-negotiated.

It can be time-consuming and challenging to use an exhaustive RFP when procuring cloud services that are relatively standard, or likely to be used repeatedly and with short lead times. Many organizations go through the RFP process once, then set up a predefined buying vehicle. Public-sector organizations in particular have defined buying frameworks that are designed to give easy access to cloud services using predefined catalogues, pricing, and use cases. Examples of this are the US General Service Administration (GSA) Multiple Award Schedule (MAS) and the UK government's G-Cloud.

The Cloud Infrastructure Services Providers in Europe (CISPE) organization's guide to buying cloud services in the public sector provides an example of these frameworks, as shown in Figure 4.1.

Figure 4.1 shows how the RFP process can be applied when procuring a cloud service:

- **Using a formal RFP process** This can be used for a single opportunity, or to establish a master agreement with a CSP to procure services that are likely to be ordered frequently more easily in future.

Figure 4.1 Cloud service procurement options

- **Using a cloud framework agreement** This allows the organization to identify a shortlist of standard cloud services that can be procured from pre-approved CSPs. Each service is provided using a master service agreement with negotiated discounts, terms, and conditions already agreed for a particular organization or class of consumer (such as government agencies, universities, or hospitals).
- **Selecting an option from the shortlist with additional qualifications and assessment** A call-off contract allows an organization to specify additional requirements for a service when it orders (calls off) a service from a standard catalogue. The organization can invite approved suppliers to respond to a list of additional requirements. This could also involve comparative service testing.

4.5 Reviewing proposals

After the RFPs have been communicated, CSPs and partners submit proposals. If the consumer organization did not complete the activities in the explore or engage steps, it may be difficult to determine whether the proposed service offerings would deliver the anticipated value. The consumer organization may also overlook a key element of the solution or a contractual risk.

The response should contain the following elements (depending on the type of service being acquired, and whether a CSP or partner is responding):

- a complete and detailed description of the solution or services that is easy to understand, informative, and functional
- a list of the service's features
- the availability of the service and any individual components
- a technological map of the service, but not a technical architecture, that demonstrates that the service is:
  - able to perform at the required levels
  - based on modern digital computing resources

  - easy to configure, control, and manage
  - on-demand, so that it can be switched on or off as required
  - responsive, flexible, and scalable
- specification of where the consumer is expected to provide IT specialists
- a description of the complete set of easily metered and paid functions, within planned budgets and development schemes
- a description of what will be monitored and reported on, and how they will be used
- specification of all the security requirements and measures
- a description of what continuity plans exist, and how the service has been made 'disaster-proof'
- a description of the offboarding service procedures and migration considerations
- identification of which tools and resources the consumer organization will need to facilitate the transition to cloud (if not included in the contract).

4.5.1 Sample questions for assessing proposals

Table 4.2 lists important assessment questions and actions mapped to general service requirements. Not all questions apply to all types of CSP and their partners. The exact requirements specified and the type of assessment conducted will depend on whether a cloud service is being acquired from a CSP, or whether a partner is providing labour-based services.

Table 4.2 General service requirement assessment questions and actions

Area	Service assessment questions and actions
Service functionality	Does the service support all the functionality requirements? Does it meet the minimum requirements? Is there an additional cost associated with some requirements?
Ease of use	How easy is the service to access? Are the interfaces intuitive? Evaluate benchmark performance statistics, or run a proof of concept for specialized workloads
Interoperability with other systems and services	Are the interfaces standard, or will they need to be developed? Is there an additional cost to obtain or build the interfaces? Who will maintain the interfaces, and how easy will it be? Are interface security measures adequate?
Operational aspects	Do the availability levels meet the minimum requirements? Are the incident response times and notification procedures acceptable? Are the minimum levels of security consistent with the levels required in the consumer's security policies? Are tools provided to enable the consumer to detect and react to potential security incidents? Is the level of recoverability consistent with the levels required by the consumer organization's continuity plans? Are change notifications and maintenance periods consistent with the levels of service the consumer organization is expected to maintain?
Authorization to use the service	Does the decision about who may access the service, and whether they have authority to purchase, lie with the consumer organization? How will the service provider allow the consumer to automate and manage policies and controls?

Table 4.3 lists important assessment questions and actions mapped to data requirements

Table 4.3 Data requirement assessment questions and actions

Area	Service assessment questions and actions
Data governance	Does the service include the ability to apply and manage data according to the consumer's standards of data governance? Does the service include the ability to manage and audit data? What tools are provided? Is there an additional cost for tools?
Security of data at rest and in transit	Are the CSP's security policies consistent with those of the consumer organization? Do the consumer organization's policies need to be revised? Which security tools does the CSP provide, and which will need to be provided by the consumer?
Data ownership	Ensure that ownership of data is not transferred by using the cloud service Evaluate the shared responsibility model to ensure that each party has a clear understanding of its responsibilities in managing and owning data Will data be shared with other organizations, and how will this be prevented? If using a CSP, what tools do they offer for consumers to manage and protect data? Does the CSP provide certification of data removal after deletion?
Backup and restore services	What tools are provided, and does the service allow consumers to use their own tools? Do the proposed redundancy and failover measures meet the required levels of availability and performance? Are there additional costs for backup and restore services?
Veracity of third-party data	Does the proposal provide credible details about how veracity is ensured?
Portability of data to another CSP	Can the CSP provide guidance and information about the removal or transfer of data? Is it possible to determine, from the information given, that a transfer is possible? Will it be possible to test the continuity of the service that includes the transfer of data?

Table 4.4 lists important assessment questions and actions mapped to security requirements.

Table 4.4 Security requirement assessment questions and actions

Area	Service assessment questions and actions
Security architecture	Does the architecture allow for compliance with the consumer organization's minimum security requirements?
Security standards and policies	Is evidence of compliance with standards or regulatory requirements provided? Does the service allow the consumer's security policies to be applied? Is assistance provided for setting up and configuring security aspects of the service? If so, at what cost?
Security tools	Does the service provide the necessary security tools, or does it allow the consumer to extend the use of established tools to the service?
Security monitoring and audit	What level of monitoring is provided as standard, and what additional work or tools will be required? Does the service allow consumers to view a CSP's third-party audits?
Security incident management	Is security incident reporting timely, and does it contain the information necessary to take appropriate action? Is there a transparent security incident management process in place? Is there additional cost in responding to security incidents?
Privacy	Can the CSP certify the location of data storage? Does the CSP notify the consumer organization of requests for access by foreign regulators?

Table 4.5 lists important assessment questions and actions mapped to people-related requirements.

Table 4.5 People-related requirement assessment questions and actions

Area	Service assessment questions and actions
Awareness and training	How will the service provider support consumer staff awareness (for example, through standard content and materials, marketing, and presentations)? What training is available, who will provide it, and what will it cost? Are any certifications required?
Transfer costs	Will all staff continue to be employed, and if not, who will be impacted? What is the cost impact of transfer and relocation to the organization?

Table 4.6 lists important assessment questions and actions mapped to service provider requirements.

Table 4.6 Service provider requirement assessment questions and actions

Area	Service assessment questions and actions
Supporting service	Does the provider have the appropriate level of experience and expertise to support the services? Is there a support option that fulfils the consumer organization's needs, and if so, what does it cost? Is self-help provided, intuitive, accessible, and appropriate?
Technical capabilities	Are the levels of technical expertise and experience adequate to provide the level of service required? How easy is it to integrate with the service provider's processes? Do reporting and notification periods provide enough time and information? What event monitoring and reporting tools are available, and at what cost?
Relationship with the provider	Is the level of engagement appropriate for the type and level of service being provided? If appropriate for the relationship, how are service reviews conducted, and what is their scope? How frequently are service reviews conducted? Is the allocation of responsibility clear, and is there a process to resolve situations where it is unclear? What are the results of reference checks, and research about the organization?
Commercial terms and conditions	Do termination terms and notification periods place any aspect of the business operation at risk? What are the costs associated with switching services? Does any subcontracted work expose the organization to risk or additional cost? How will legal and insurance issues be resolved?
Regulatory requirements	Does the CSP have evidence that it is compliant with the appropriate regulations or can it show equivalency? What tools does the CSP offer to help the consumer organization to remain compliant when using the service?
Business health	Is there any risk that the service provider will be unable to provide the service at the agreed levels for the duration of the agreement? Are contingency plans required, and if so, what needs to be included?

Table 4.7 lists important assessment questions and actions mapped to cost reporting, billing, and payment requirements.

Table 4.7 Cost reporting, billing, and payment requirement assessment questions and actions

Area	Service assessment questions and actions
Billing reports	Do the billing reports provide relevant information clearly and in a format that allows for analysis? Do they provide information that will enable utilization management?
Purchase and payment authorization	Is it possible to control the purchase of, and payment for, services, even if they are ordered individually? Is it possible to assign and control purchasing authority?
Billing and payment information	Are the billing frequency and payment periods consistent with the organization's policies? Can subscription spend be managed?

4.6 Determining the return on investment of the proposed cloud services

Definition: Return on investment (ROI)

A measurement of the expected benefit of an investment. In the simplest sense, it is the profit of an investment divided by the costs invested. Most calculations will also include qualitative elements, such as the impact on culture and the perception of stakeholders.

An ROI calculation can be as simple or complex as necessary to enable stakeholders to make a specific decision, so long as it evaluates all relevant variables and the interests of all key stakeholders. It involves understanding all the elements of a service, and often relies on discussion, workshops, analysis, and assessment. The results of the ROI should be included in the business case to support a proposed action.

ROI is used to evaluate potential:

- cost savings
- business growth (new products or services, new markets, and so on)
- business performance improvements.

4.6.1 The return on investment process

Published ROI processes, such as the Phillips ROI methodology, provide detailed guidance on ROI calculations. The typical steps in these processes are:

- define the purpose, objectives, and scope of the assessment
- collect data
- review and analyse the data
- calculate and report
- decide.

4.6.1.1 Define the purpose, objectives, and scope of the assessment

An ROI assessment is usually conducted as part of developing a strategy or running a project, or when solving a significant problem. The assessment must present relevant information and not include variables that confuse the situation. For example, deciding whether to move a business-critical system to cloud requires different information than deciding to move from one CSP to another.

The objectives and scope of the ROI assessment will be determined by the:

- objectives of the strategy, project, or problem resolvers
- nature of the choices that need to be made (such as technology, people, or processes)
- nature of the solution(s) being proposed
- stakeholders involved in decision-making.

The objectives and scope of the ROI assessment will determine:

- what data needs to be collected
- how the data will be obtained (such as through external research, anecdotes, or internal records)
- how the data will be used
- what metrics and calculations are appropriate (for example, net present value is not appropriate when considering operational expenses).

4.6.1.2 Collect data

Table 4.8 lists examples of ROI assessment data in four categories.

Table 4.8 Examples of ROI assessment data

Categories	Examples
Outcomes	Cost savings Increased performance Automation Increased revenue Higher productivity Less waste Increased regulatory compliance Improved continuity
Positive risks (opportunities)	The ability to develop new services or products The ability to enter a new market or appeal to a new demographic New distribution and delivery channels
Costs	Design costs Development costs Project costs Migration costs Operating expenses Licence costs Maintenance costs Staff costs, such as training, transfer, and hiring costs

Categories	Examples
Negative risks (threats and vulnerabilities)	Increased risk of exposing private data Increased attack surface Loss of control over key capabilities Vendor lock-in Uncontrolled purchasing Inability to innovate to meet changing market demands

4.6.1.3 Review and analyse the data

The data typically collected for an ROI assessment relates to value, outcomes, costs, and risks. It will also include data about the variables involved in the study, such as workload rates and how and why they vary.

Data review and analysis will determine:

- a baseline of the current situation
- intangible elements that will impact the cost, risk, or success of the solution (such as culture, perceived quality, and experience)
- the variables that could potentially impact the cost, risk, or success of the solution
- the costs of doing nothing and the costs of each proposed option
- the potential impact on the organization of the proposed solution
- the risks of doing nothing and the risks that would be introduced or reduced by taking each proposed option.

4.6.1.4 Calculate and report

When the data has been analysed, the ROI can be calculated. In its simplest form, the ROI calculation is:

$$\text{ROI (\%)} = \frac{\text{Net benefit of taking the action (expressed in relevant currency)}}{\text{Cost of taking the action (expressed in relevant currency)}} \times 100$$

This calculation yields a percentage. An ROI of 100% represents a break-even situation, so most organizations require a significantly higher ROI before proceeding with the initiative.

The ROI calculation does not include intangible elements. These can be included in two ways:

- Perform the ROI calculation, then list other variables (such as increased user satisfaction, ease of use, or ease of communication) and use scenarios to demonstrate where an increase or decrease in these aspects would affect realization of benefits.
- Devise a method to assign a value to intangible elements, and include this in the ROI calculation.

Neither method is totally reliable; however, because value is subjective, it is important that all stakeholders verify the importance of intangible elements and agree how they should be used in the calculation. Douglas W. Hubbard (2014) provides a range of methods to measure the value of intangible elements in his book *How to Measure Anything*.

Table 4.9 outlines some examples of benefits and costs that can be included in ROI calculations.

Table 4.9 Examples of benefits and costs used in ROI calculations

	Benefits	Costs
Tangible	Revenue from selling existing products in a new market Revenue from a new product or service Increased sales because of new features Reduced expenditure to achieve an existing outcome	Marketing campaigns Establishing new distribution channels Research and development Technology replacement or modernization Cost of migrating to the cloud Cost of using cloud services
Intangible	Increased customer loyalty Increased brand visibility Increased employee satisfaction Greater ease of use	Cultural change (could also be a benefit) Skill degradation (skills that are important in the current context are less important in the new context)

4.6.1.5 Decide

The ROI is presented to the stakeholders, usually as part of a business case for the strategy, project, or problem resolution. These stakeholders must include:

- decision-makers (those who will fund the solution and those who are accountable for its success)
- technical advisers who can help evaluate the details of the solution.

The results of the decision must be communicated using the communication plan associated with the strategy, project, or problem resolution team.

4.6.2 Return on investment of moving to the cloud

When defining a cloud strategy, an ROI assessment is used to answer such questions as:

- What is the value of moving existing workloads or services to the cloud? For example, will it reduce cost, improve operational performance, or provide additional functionality that enables business growth?
- What is the value of introducing new cloud-based services? For example, will the organization introduce new services, enter new markets, compete more effectively in its existing market, or improve customer loyalty?
- At what point should existing services be retired as the business evolves? For example, cloud-based services have grown to such an extent that services delivered using physical facilities are no longer as profitable. Can the organization afford to shut all its retail locations and work exclusively as a digital business?

This assessment can be applied to the overall cloud strategy, or to a single service or workload.

This type of ROI is not a general comparison of cloud services with in-house solutions. It is not accurate to talk about the 'ROI of moving to cloud'. Rather, the organization should:

- define a scenario
- evaluate the ROI of using cloud services in that scenario
- evaluate the ROI of using existing in-house solutions in that scenario
- if necessary, evaluate a third ROI of modernizing existing services and keeping them in-house in the same scenario
- compare the overall ROIs.

The ROI of moving to cloud is therefore a comparison between at least two ROI assessments. The decision should be made based on which ROI provides the best business case.

The ROI of moving to the cloud typically includes evaluating the aspects outlined in Table 4.10.

Table 4.10 Aspects considered when evaluating the benefits of moving to cloud

ROI component	Description
The cost of over- or under-provisioning	After they have been set up, cloud services incur costs only when they are used, avoiding the cost of over-provisioning and the impact of under-provisioning
Cost reduction versus adding value	Cost reductions can be achieved only if the utilization of cloud services can be predicted. Uncontrolled use (such as storage of data without data governance) and inaccurate workload forecasting can escalate cost
Constraints of system ownership	Cloud services provide a way of overcoming a situation when a rigid in-house system prevents the organization from pursuing opportunities. At the same time, if the organization relies on that system for unique functionality, it may not be advisable to replace it
Rapid provisioning and dynamic use	The ability to respond to changes rapidly, such as changes in demand or the need for new functionality Individuals can easily procure and use cloud services directly. However, if oversight or guidance is not provided, this could lead to cloud sprawl: over-utilization of cloud services through duplication and failure to decommission services that are no longer used
Risk and compliance	A comparison of the need for specialized security management skills and tools to manage in-house systems, as opposed to the use of secure cloud architectures
Sustainability	Does a move to the cloud represent a net reduction in the organization's carbon footprint?
Skills availability	What skills will be required to meet the organization's objectives and use emerging technology? Will it be more valuable to keep resources in-house or rely on a CSP or partner to provide them?
Time to ROI	The anticipated returns may not be immediate. It is important to model them over time to account for set-up costs, changes in the business, and so on

4.6.3 Return on investment to compare cloud options

An ROI calculation can be used to compare the value of cloud services over a meaningful period, such as 5 years. At least two, and ideally three, scenarios should be identified that will provide a similar level of service. The activities and SLAs for the planned operations (such as upgrades and changes) as well as unplanned operations (such as the resolution of outages) must be specified so that the services are evaluated on a like-for-like basis.

4.6.3.1 Data used to calculate the ROI

The data used to calculate the ROI includes:

- scenarios, which might include a comparison of cloud services, two or more CSPs, or the use of hybrid or multi-cloud options
- hypotheses and assumptions about the costs, workloads, and utilization
- hosting and migration costs
- workload and utilization data
- the required outcomes that must be achieved by using the service
- performance requirements
- additional costs, such as training, transfer, and security.

Cloud-specific cost information is usually obtained either directly from CSPs (based on a standard pricing model) or from cloud integrators (based on their experience with existing customers). If this information is inaccessible or unavailable, the organization can use industry averages.

Information related to hosting and migration costs can be difficult to obtain. Costs depend on several options, such as the architecture to be used, how it is configured, and what strategy is used for the migration. The best way to estimate costs is to use a building-block approach that defines a limited number of hosting configurations and migration strategies. These can then be modelled in different combinations to evaluate the most common use cases.

In a capital expenditure model, the ROI rarely depends directly on real workloads of IT resources. In an operating expense (pay-as-you-go) model, the ROI generally depends directly on the real workload (usage) of IT resources during the charging period.

It is important to understand whether the cloud consumption model charges are based on the cost of the IT resources that are reserved and/or allocated, or on the real usage (workload) of the IT resources. It is also important to understand and evaluate how IT resource consumption will be measured, reported, and billed, and whether there are limitations and specific conditions related to scaling up or down.

4.6.3.2 Making a go/no-go decision

After the ROI calculation has been completed, the organization should build a decision model based on a 'what-if' analysis for the key variables that have the most influence on the ROI results. For example, a key variable could be the cloud volume that will be charged according to different estimates of workload growth. The volume could be underestimated, overestimated, or accurately estimated.

A decision model can help the stakeholders to evaluate the ROI results for the worst-case, best-case, and most likely scenarios. Most CSPs provide decision models and ROI calculators to help with this decision.

4.7 Defining and communicating a business case for cloud services

During the explore step, a high-level business case for using cloud services is articulated in the cloud strategy. For some services, that business case is sufficient to enter into an agreement with a CSP, especially for standard services specified in the cloud strategy.

Now that more information has been gathered through the RFP process, it may be necessary to define a more detailed business case for the services selected, especially if several options were considered.

A business case is a justification for the expenditure of organizational resources, providing information about costs, benefits, options, risks, and issues.

The core of a business case is a financial analysis, evaluating an expenditure for profitability and risk. This analysis should consider both qualitative and quantitative aspects. A positive business case indicates that the expected benefits exceed the expenditures and risks.

The purpose of a business case is to establish a foundation for informed decision-making, but it is based on assumptions. These assumptions are subject to uncertainty and often conflicting needs and interests. Typical areas of conflict and uncertainty are highlighted in Table 4.11.

Table 4.11 Typical areas of conflict and uncertainty

Area of conflict and uncertainty	Examples of conflicting or uncertain areas
Value: understanding real needs	Who are the key stakeholders and how are their needs prioritized? The users of a service may have different needs and priorities from the customer or sponsor. Other stakeholders also may have conflicting needs
Outcomes: understanding benefits	Longer-term benefits are typically subject to more uncertainty and risk than shorter-term benefits.
Costs: understanding the impact of changes to capital and operational expenses	What kind of investment is needed for this product or service? What are the implementation, maintenance, support, usage, and training costs? What kind of organizational change is needed? How will the shift from capital to operational expense change the organization? How will it enable the organization to pursue new opportunities? Will it reduce or increase the overall costs, and what will the result, or return, be?
Risks: understanding uncertainty and impact	Will the service provider be willing and able to fulfil the service consumer's evolving needs? Is there a good relationship with the service provider, in which both organizations can communicate their future requirements or service roadmaps? Where appropriate, does relationship management focus on salespeople, as well as people who will be key resources for service provision?

4.7.1 Building a business case

A business case should clearly identify the proposal and the benefits and risks involved. It should answer the questions often asked by senior management, explaining why the proposal is needed and justifying the investment.

The business case for a cloud service should cover all the aspects of migrating to, managing, and using the service, as well as the relevant benefits, costs, and risks associated with it.

When constructing the business case, it is important to be realistic about what is possible within the organization's conditions or constraints, for example:

- **Pace of change** The magnitude of the proposed change must match the organization's ability to adapt.
- **Culture** The organization's culture will either facilitate of inhibit the change. An organization with inconsistent practices (such as traditional ways of working versus emerging use of cloud) will require a different timescale and approach to one with a high-compliance culture.
- **Resource availability and capacity** Depending on the available funding, changes may have to be delivered using existing resources. If more resources are needed, another plan and business case will be needed.
- **Budget restrictions** The available budget's source and amount will constrain the scope of the proposed changes. Also, it is important to ensure that the new service fulfils all of the relevant stakeholders' needs. Those funding the change may prioritize themselves, so the business case must explicitly communicate the needs of all stakeholders.

4.7.2 Business case structure

Although the structure of a business case may vary by organization, the following sections are usually required:

- **Executive summary** A high-level overview of the business case, highlighting the problem being solved, the nature of the solution, and the anticipated ROI. It will also indicate what decision or action is being requested.
- **Introduction** Provides context for the business case, and indicates who drafted it and who it is being presented to.
- **Statement of the problem** A description of the problem that needs to be solved and its impact on the organization.
- **Analysis** Indicates the nature of the problem and provides any information that indicates its root cause. It also outlines the actions that have already been taken in an attempt to resolve the problem, and the potential impact of not resolving it.
- **An overview of the proposed cloud or cloud-related service** (or a list of potential options) Includes:
  - **Description of the cloud service** (or of each option) Outlines the scope of the solution, for example whether it involves technology, a service, people, partners, or a process. It will also provide details about how the solution addresses the problem.
  - **Benefits** Outline of the benefits of the service for the organization. These may include its generic benefits (the benefits of using cloud services) and the specific outcomes that will be achieved.
  - **Cost** Includes the costs that are directly associated with implementing the solution and the costs of using the service (which will require detailed workload analysis).
  - **Risks** The risks that may be introduced or reduced by using the service (and details of any mitigation actions), compared with the risks of doing nothing.
  - **Timescales** How long it will take to move to the cloud service, and especially how long before outcomes will be realized.
  - **Anticipated ROI** The value of the solution after comparing all benefits with the costs and risks.
- **Recommendations** Specific actions and decisions that are recommended.
- **Conclusion** A reminder of why the service is needed.

4.7.3 Communicating a business case

A business case should be aimed at the appropriate level of senior management. If there is a business case approval process, it should be agreed via that process. The process should include guidelines on how to prepare the business case, and how to present and communicate it to the appropriate stakeholders.

The business case should be communicated to the following stakeholders:

- **Experts on areas covered in the business case** It is important to verify that the contents of the business case are complete and correct. Although it may have been drawn up by experts, experts who were not involved should read it and ensure that all assumptions are correct and nothing has been omitted. This needs to be done before the final business case is presented to the decision-makers.
- **Decision-makers** Those with the authority and budget control to decide whether to proceed with the recommendations. The business case will be given to them, and they should have enough time to understand it and make a decision. Factors to be considered include:
  - What would happen if the organization continued in the current situation?
  - If options were evaluated, what were the advantages and disadvantages of each?

  - What is the expected ROI?
  - What other factors does the organization need to consider if the recommendations are accepted (such as the impact on culture)?
- **Those impacted by the business case** Before a business case is presented to decision-makers, those who draft the it need to understand the potential impact on different groups of stakeholders. This can be achieved through interviews, surveys, and focus groups. After the business case has been approved, the decision and its impact should be communicated to those who will be impacted by it. This is usually done once there is a clear plan for the next steps to be taken.

4.8 Summary

The consumer organization may wish to communicate its detailed requirements to a shortlist of potential CSPs through a formal RFP. It also should consider any applicable cloud framework agreements that could present purchasing benefits or advantages. CSP proposals must be thoroughly reviewed against service, data, security, human, and financial requirements. A comprehensive review should result in the selection of a chosen proposal and the ability to calculate the anticipated ROI more accurately. A detailed business case can be then formulated and communicated to the appropriate stakeholders for approval and authorization to proceed.

CHAPTER 5

AGREE: NEGOTIATING AND PLANNING

5 Agree: Negotiating and planning

5.1 About the agree step

The agree step begins when the consumer organization has selected a proposed solution from a cloud service provider (CSP) and/or partner, and has the approval of key stakeholders to enter into a contract. It ends when a contract has been signed.

The purpose of the agree step is to align expectations between the CSP and the consumer organization, including establishing a shared view of the service's target scope and quality. This may necessitate a formal contract and the involvement of specialists, such as legal advisers or procurement and contract managers.

In the steps after the agree step, the actual scope and quality of the delivered services will be compared with the contents of the service agreement. Any deviations from the agreement will need to be addressed by either improving the service or reviewing the agreement.

The agree step involves:

- agreeing and planning to onboard the services
- understanding the roles and responsibilities of the consumer organization and service provider(s)
- as far as possible, agreeing and planning how value will be co-created between the consumer organization and the service provider
- negotiating and agreeing a cloud service agreement, including acceptable terms and conditions
- understanding how the organization will be charged for using the cloud services.

Inputs to the agree step include:

- an evaluation of the solutions and services proposed by CSPs and partners
- a selected offer, which will inform the agreement of terms and conditions
- a statement of the minimum acceptable services and service levels as a baseline for negotiation
- a business case to accept the chosen proposal.

The primary outputs of the agree step include:

- an accepted cloud service agreement signed by the designated representatives of the CSP and the consumer organization
- the identification and sourcing, if necessary, of the knowledge, training, tools, and guidance that will be essential for onboarding.

5.2 Agreeing and planning value co-creation

In most cases, CSPs offer their services on fixed terms and conditions and with standardized service offerings. The use of standardized offerings allows for better scalability, a higher level of assurance, and optimization of the costs of service delivery. However, it also reduces the scope of negotiable quality characteristics and targets. The ability to negotiate individual agreements and adapt services to each customer's unique needs is closely related to the type of service relationship between the consumer and the CSP, as well as whether the consumer is working with a boutique CSP, hyperscale CSP, or CSP partner.

ITIL describes three fundamental types of service relationship:

- basic relationship
- cooperative relationship
- partnership.

Some key characteristics of these relationship types are described in Table 5.1.

Table 5.1 Three fundamental service relationship types

	Basic relationship	Cooperative relationship	Partnership
Typical focus	Support and efficiency	Improvement and effectiveness	Innovation and growth
Typical organizational level involved in the relationship	Operational	Operational and tactical	Operational, tactical, and strategic to both parties
Typical service types	Commercial off-the-shelf services, out-of-the-box services, highly standardized commodity services, or goods supply	Services that have to be configured or customized to fulfil the service consumer's needs	Custom or bespoke services with unique value propositions
Typical types of agreement	Standard contracts, service level agreements (SLAs), and experience-based agreements, mostly for mass market	Advanced SLAs, experience-based agreements, or outcome-based agreements	Bespoke contracts, outcome-based agreements, or no agreement
Examples	Service consumers articulate their expectations quite clearly, as the service provider expects, or accept standard offerings from the provider, with limited options to choose from	Depending on the relationship between the service provider and the service consumer, it can be difficult for the provider to fully understand the outcomes that the consumer wants to achieve. In some cases, they work together to define the desired outcomes	Services based on service offerings and products that have been planned and built in accordance with requirements specified by the customer Agile product development where the service consumer and provider co-create the product in shared teams

The nature of the cloud industry results in some variability in how these relationships are defined. Although cloud services can be of critical strategic importance to the consumer organization, that does not necessarily mean that the service relationship is a partnership. The commoditization and standardization of these services, and how they are consumed and utilized tactically and operationally, is likely to align more with the basic or cooperative relationship types. CSP partners tend to align with the cooperative and partnership relationship types. Value can be co-created in all types of service relationships, as long as the role of all parties is clearly defined.

5.3 Negotiating and agreeing a cloud service

The customer's ability to negotiate the scope and quality of the service may vary according to the type of service and the type of service relationship.

With most cloud solutions, the negotiation is often limited to some predefined sets of terms and conditions that CSPs list as their standard offerings. The types of cloud services, their deployment and delivery models, the technologies used, and their development strategies characterize the offerings these providers bring to the market. Each provider's cloud specification is narrowed to a specific number of solutions it provides.

This brings certain limitations and constraints to the negotiation. However, the services these providers offer are reliable and popular because of the standard and proven technologies they are based on.

Examples of packaged groups of services provided by CSPs include:

- application programming interface (API) management tools (applications and systems integration instruments)
- artificial intelligence and machine learning suites
- biomedical and care systems, and artificial intelligence solutions in cloud
- cloud management tools and applications for self-service customer purposes
- cloud monitoring and operations (logging; tracing; infrastructure and system health management tools; audit, debug, and inspection tools; real-time application dashboards; and so on)
- data analytics solutions
- database services (relational SQL, NoSQL, databases for internet of things, and so on)
- internet of things solutions
- media and gaming (visual effects, rendering, animation, game centres, video content streaming, and so on)
- migration tools, instrument kits, and services (for bare metal systems, middleware, applications, data, and workflows)
- networking and networking security solutions (VPC/VPN, traffic control, access control, platforms for network discovering, publishing, connecting devices, and network monitoring services)
- object storage in cloud (data transfer, archives, backups, file storage, collaboration, access to data tools, and so on)
- SDK, IDE, and other code development environmental services (container registries, command line tools and libraries, serverless platforms, applications, and container management platforms such as Kubernetes)
- security solutions for cloud (visibility tools, compliance, telemetry, encryption, sensitive data storage and treatment instruments, firewalls, identity and access management, web security, fraud and spam control, and so on).

When considering these standard cloud offerings, consumers often have to adapt their requirements. This is because most customers are required to sign the CSP's standard contract (due to the standard nature of the services). In cases where the CSP signs a customer-defined contract, it requires the CSP's preferred wording and terms and conditions to be reflected in the contract. There is typically not much room for negotiation on standard services.

The agreements reached during the negotiation are documented. For cloud services, a dedicated form of agreement has been developed, often referred to as cloud service agreements (CSAs).

5.4 Cloud service agreements

Definition: Cloud service agreement (CSA)

A compilation of documents or agreements that contain the terms governing the relationship between the cloud customer and the cloud service provider (CSP). The CSA is the key output of the negotiation between a CSP and a service consumer.

In general, the CSA comprises three major artefacts:

- customer agreement
- acceptable use policy (AUP)
- SLA.

5.4.1 Customer agreement

The customer agreement outlines the relationship between the customer and provider. It is important that a formal agreement is reached on how roles, responsibilities, and processes are defined, and the customer agreement fulfils this need.

Some providers may refer to the customer agreement as the 'master agreement', 'terms of service', or simply the 'agreement'.

5.4.2 Acceptable use policy

An AUP is used by CSPs to prohibit activities that they deem to be an improper or illegal use of their services. Depending on the provider and its delivery models and package offerings, the exact details of acceptable use will differ; however, the scope and effect of these AUPs often have similarities. This area of the CSA typically needs the least negotiation

5.4.3 Service level agreement

A cloud SLA is a documented agreement between the CSP and service consumer that identifies both the requirements and expected level of service. For cloud services, this can cover areas such as availability, serviceability, and performance. The SLA outlines targets or thresholds, and any financial penalties that will be incurred should these expectations be violated. If designed properly, an SLA should help to significantly reduce potential conflict, and can support both parties in resolving issues before they escalate into disputes. SLAs are also used as a basis for the monitoring and management of the services.

The service level management practice guide provides recommendations on the structure and format of SLAs. Depending on the type of service relationship, an SLA can take the form of a memorandum, or a direct (consumer/provider) or indirect (consumer/third-party provider) legal contract.

5.4.4 Disputes

A cloud customer must pay close attention to the language and clauses in the CSA. A lack of due diligence when reviewing the CSA can lead to architectural errors, security vulnerabilities, and confusion about roles and responsibilities with tasks such as operational support.

All of these factors can lead to increasingly significant impacts and risks for the consumer organization, including from cloud technical debt, administrative burden, and interruptions of critical services. The review and negotiation of the CSA must be comprehensive, to avoid misunderstandings between the consumer and provider.

A consumer organization should:

- utilize the outputs from the previous steps of the customer journey and compare available offerings from other CSPs (particularly in a basic service relationship, where multiple offerings are often available and negotiation is mostly about the terms and conditions)
- understand stakeholder expectations
- understand the essential requirements and acceptable trade-offs
- review and understand the agreed responsibilities of all parties, as documented in the shared responsibility model
- ensure that the CSP's mechanisms for governance, risk, and compliance align with the organization's systems
- understand the methods and controls for service monitoring and reporting
- ensure the shared understanding of service consumption costs, including their correspondent payments and planned budgets.

5.5 Shared responsibility model

Organizations must ensure a shared understanding of the respective responsibilities of the service provider and service consumer. Although there may be differences in its execution among CSPs, the cloud industry has standardized the name for this document: the shared responsibility model.

The shared responsibility model defines which security, compliance, maintenance, and support tasks are handled by the cloud provider and which by the cloud consumer. The measures and areas of responsibility vary depending on where the workload is hosted. The model may be applied differently depending upon the types of cloud solutions to be used: software-as-a-service (SaaS), platform-as-a-service (PaaS), or infrastructure-as-a-service (IaaS) in public, private, and hybrid deployments. In other words, the level of abstraction that the consumer organization experiences will be reflected in the contents of the shared responsibility model, and vice versa. A simple SaaS solution will often be accompanied by a simple shared responsibility model, and a complex hybrid IaaS solution will be accompanied by a complex shared responsibility model.

Defining the line between consumer responsibilities and those of the provider is essential; it reduces the risks of the cloud environment. Regardless of the cloud solution, the service provider will never assume total responsibility. A consumer organization will always retain some responsibilities, and those must be thoroughly understood before the CSA is agreed.

The responsibility-sharing depends on various factors for different delivery models, including:

- the type of service relationship
- the package of services procured by the customer
- whether the services are customized or tailored
- how technology is integrated between the customer and provider
- any laws and regulations applied to the agreed services.

In an in-house data centre model, an internal IT service provider is responsible for security across the entire operating environment, including applications, physical servers, user controls, and even physical building security. In a cloud environment, responsibility for security is shared with the provider.

In the shared responsibility model, security ownership must be clearly defined, with each party maintaining complete control over the assets, processes, and functions it owns or manages. By working together with the cloud provider and sharing responsibilities for security, a customer can maintain a secure environment with less operational overhead.

A security gap in any one system increases vulnerability across the entire stack and to any connected systems. The security measures that the CSP provides are usually standardized and proven across other similar solutions. They will have been fully documented and can be implemented on demand. By comparison, the consumer organization's security measures are often less comprehensively developed and managed, narrow in their implementation scope, and unproven.

When entering into an agreement with a CSP, security should be included up front in the decision-making process regarding shared responsibilities. The following sections can act as a guide to facilitate the discussion, to understand the roles and responsibilities in implementing and securing the cloud services, and to agree them with a cloud provider.

5.5.1 Responsibilities owned by the CSP

The Cloud Security Alliance outlines the following areas over which the cloud vendor maintains full control:

- physical infrastructure security, including:
  - selection of location of equipment room
  - assurance of power supply
  - cooling facilities
  - protection against fire, water, shock, and theft
  - surveillance
- security of computing, storage, and network hardware that is under the CSP's management (not including the security of any component under the consumer's management and control)
- security of basic networks, such as protection against distributed denial of service, and firewalls
- cloud storage security, such as backup and recovery
- security of cloud infrastructure virtualization, such as tenant resource isolation and virtualization resource management
- tenant identity management and access control

- secure access to cloud resources by tenant
- security management, operating monitoring, and emergency response of infrastructure
- formulating and rehearsing service continuity assurance plans and disaster recovery plans for components under the CSP's management
- virtualization software that allows physical devices to be segmented into isolated and secure virtual devices (this software is seen as part of the configuration for the physical hosts used to provide IaaS services).

5.5.2 Responsibilities mainly owned by the consumer organization

The consumer organization typically retains responsibility for:

- user identity management and access control of service systems
- data security
- security management and control of terminals that access cloud services, including hardware, software, application systems, and device rights
- business processes, policies, roles, workflows, procedures, and components integrated with cloud-based technologies.

5.5.3 Shared responsibilities

Cloud consumers and cloud providers never share responsibility for any single aspect of security operations. The areas that the consumer controls belong to the consumer, and the provider does not dictate how those areas are managed. Likewise, a consumer has no control over how the provider manages the areas that it is responsible for. However, the consumer does have the right to access the provider's audit reports to verify that its systems are secure.

Cloud customers should perform all of the necessary security configuration and management tasks for items not under the CSP's management. For example, the consumer is usually responsible for managing the operating system, utilities and applications, data, and access management.

5.6 Roles and responsibilities map

An important part of the agree step is the negotiation of a responsibilities map that outlines the future cloud architecture and areas of ownership. A number of roles and responsibilities involved in the cloud service arrangements within the entities are listed in Table 5.2.

Table 5.2 The responsibilities of each entity

Entity	Responsibilities
CSP	Provides remote services of computing, storage, networking, software, business functions, and their combinations
	Continually develops and optimizes its own cloud infrastructure to offer cutting-edge technologies within the solutions
	Researches the market on possible client engagement and on latest technology innovations to stay competitive and effective
	Provides services as agreed in the CSA
	Develops and offers SLAs
	Contracts with the client and provides billing and usage information
	Delivers the services, based on the SLA
	Offers pay-as-you-go on-demand models for the delivered solution and bills based on metered usage
	Delivers technical maintenance and support for the services provided, based on the SLA
	Meters and bills the support services as agreed with the customer
	Provides security measures for the solution, based on the SLA
	Provides training on the use of cloud
	Offers the customer add-ons, such as reporting tools, cloud management tools, IT optimization scenarios, cloud migration programmes, and customer development proposals, as agreed or by up-sale
	Monitors and controls the functioning of services, based on the SLA, when within the CSP's scope of responsibility
Cloud customer	Realizes the need for cloud transformation for its company
	Seeks a cloud transformation solution
	Holds sufficient budget or engages the investment programme
	Researches the market for CSPs and studies the possible solutions. If needed, researches the market on possible cloud broker engagement
	Compiles a list of requirements based on market research and internal business needs
	Negotiates with CSPs or CSP partners about the required solution, agrees the solution, then maps the service requirements to the packaged services offered
	Contracts the service provider and/or its third-party agent for the agreed solution and agrees on payments, including schedule and amount
	Provides the means and opportunity for the CSP to deliver the solution
	Provides the payments according to the agreed terms and schedule
	Implements relevant security measures for the solution
	Receives training as agreed
	Considers add-ons offered by the CSP
	Monitors and controls the success of the solution, based on the SLA
Cloud broker	Educates consumer organizations about what is possible and enables the consumer organization to choose the correct vendor and solution according to its business needs
	Helps the consumer organization to negotiate terms and conditions, pricing, and other details
	Continually researches the cloud market and technology innovations
	Negotiates possible partnerships with the consumer organization
	Obtains the list of service requirements from the consumer organization
	Establishes contracts and agrees payments with the consumer organization
	Advises the consumer organization during its engage step
	Mediates deals on behalf of the consumer organization
	Mediates and/or participates in contracting the CSP or its third-party representative on behalf of the consumer organization
	Advises the consumer organization on the future of the contract
	Mediates the delivery and support of the cloud service

Table continues

Table 5.2 *continued*

Entity	Responsibilities
Cloud partner	Maps requirements for obtaining partner status from a CSP (or several CSPs) Continually innovates to sustain value, including cutting-edge technologies Provides remote services on behalf of CSPs Researches the market for potential customers Offers and demonstrates solutions to potential customers Negotiates and agrees solutions with customers Agrees contracts with customers, including payment schedules and amounts Delivers solutions Meters services and bills and receives payments from customers offering pay-as-you-go on-demand models Maintains and supports the services within the solution, based on the SLA Provides security measures for solutions, based on the SLA Provides training for customers Offers customers add-ons Monitors and controls the functioning of the implemented solution, based on the SLA
Regulator	Ensures that CSPs and partners comply with regulatory frameworks, such as HIPAA, SOX, and GLBA; examples include the Federal Trade Commission and Securities and Exchange Commission

5.7 Charging models

Although the price of selected services, as well as the payment terms and conditions, should already be well understood at the end of the agree step, final confirmation of the financial aspects of service consumption is crucial.

Many service providers and cloud service resellers offer a variety of pricing models for consumer organizations to consider and adopt. The pay-as-you-go model is the most widely used, due to its convenient on-demand and user-friendly buying instruments. The shift from capex to opex is one of the most compelling arguments for adopting cloud services; however, consumer organizations must also prepare for the possible negative consequences of this charging model, such as unpredictable expenses due to higher-than-expected utilization.

Many CSPs offer charging models designed to help consumers manage the unpredictability of costs. These include:

- Discounted service consumption rates based on guaranteed levels of utilization over a defined period; however, if these levels are not achieved, the CSP may impose financial penalties. An example of this model is reserved instances.
- CSPs may offer a discounted usage rate for customers who are willing to commit to a minimum level of utilization in a defined period.
- Prepayment for anticipated usage can also qualify for a discounted rate.
- Some CSPs offer variable rates based on the level of support needed at different stages of the utilization lifecycle (for example, higher levels of support during a software release).

Although the financial implications of cloud consumption are important, consumer organizations should never negotiate prices down to the point of compromising the intended outcomes.

When the negotiation process has been completed and the cloud service agreement has been signed, the customer and provider can plan the activities associated with onboarding.

There are a number of helpful resources that consumer organizations can request from CSPs in the agree step to help with onboarding, including:

- the CSP's cloud adoption frameworks
- documentation for recommended 'landing zones' from the CSP
- self-paced, on-demand, or instructor-led training classes
- migration or other technical implementation tools or toolkits.

5.8 Summary

The relationship between the CSP and consumer organization should be thoroughly documented in a CSA. The CSA will define the many terms and conditions of the relationship; however, depending on the nature of the services and chosen CSP, the cloud customer may or may not be able to negotiate or significantly influence its content. A typical CSA includes stated SLA expectations, an acceptable usage policy, and dispute resolution rights. The consumer organization must understand the entire CSA. Roles and responsibilities between the CSP and consumer should be mapped, and charging models should be understood before the consumer organization signs the CSA.

CHAPTER 6

ONBOARD (AND OFFBOARD): MOVING TO THE CLOUD

6 Onboard (and offboard): Moving to the cloud

6.1 About the onboard step: general considerations

The onboard step begins when the consumer organization has completed the purchase of standard cloud services or signed a cloud service agreement with a cloud service provider (CSP). Onboarding could take place immediately for standard services such as software subscriptions, or after extensive planning, preparation, and migration for more complex services.

The purpose of the onboard step is to facilitate the necessary activities effectively and efficiently for a service consumer to start using the services, and for the service provider or partner to be ready to deliver it.

Onboarding is often perceived as a series of activities performed by the service provider, with minimal involvement from the service consumer. However, successful onboarding could involve both the provider and the consumer, depending on the nature of the services (standard or non-standard) and the type of service provider (aggregate CSP versus niche partner).

For example, if the customer has opted to purchase non-standard services from a partner, onboarding is very collaborative. However, if the customer is purchasing standard services from an aggregate CSP, onboarding will almost entirely depend on the consumer organization. In either case, onboarding is often a complex process, with sequences of actions and dependencies to consider.

The onboard step involves the following:

- **Planning for onboarding** Determining the list of activities needed to start supplying and consuming the agreed cloud services.
- **Involving users in the onboarding plan** Creating the structure of business relationships.
- **Establishing communication channels** Providing user engagement and delivery channels.
- **Preparing users for the new services** Empowering users with specific skills needed to consume the services.
- **Elevating mutual capabilities** Developing skills and knowledge for managing cloud-based technologies and contracts (while the service provider learns more about the customer business and how it can provide the appropriate levels of support and ongoing development).
- **Offboarding customers and users** Creating predefined offboarding procedures as part of the cloud service design.

The major inputs to the onboard step include:

- a signed agreement containing terms, conditions, and parameters that will influence onboarding activities
- contact information for the consumer and provider organizations' technical representatives, who will facilitate and perform onboarding activities if appropriate
- best-practice documentation from the CSP, including its cloud adoption framework, well-architected framework, and defined landing zone or staging area templates
- documentation that specifies the services that will be onboarded, and the requirements they were designed to meet; this will ensure that they are implemented appropriately
- instructions or documented processes required for the services to be configured and managed effectively
- migration or implementation tools provided by the CSP or obtained from a third-party supplier.

The major outputs of the onboard step include:

- live or operational cloud services that have been designed, planned, prepared, and configured to be in an optimal state of readiness for value co-creation
- workloads that have been constructed for the first time in the cloud, or have been migrated to the cloud from the customer's in-house environment or the customer's previous CSP.

When cloud services have been onboarded, they can be commissioned or decommissioned immediately. However, initial onboarding of cloud services can take time. Most services cannot simply be turned on the day after the agree step is completed (apart from highly standard services such as software subscriptions). Cloud consumption, as well as cloud provision, should be planned, and both organizations should be prepared to accept their agreed responsibilities. Due to the importance and complexity of onboarding activities, organizations should develop and follow an onboarding plan.

6.1.1 Planning for onboarding

Each onboarding initiative should be carefully planned and managed. Most CSPs have established guidelines, checklists, and templates that customers can use to create an onboarding plan. Many CSP implementation or migration partners also offer this service.

The onboarding plan must align the required consumer organization activities with the service provider's onboarding plans, although many of the elements of those plans will be unique to the organization. Regardless of the method used to prepare it, the consumer organization is responsible for defining and implementing the onboarding plan.

Activities that should be considered include:

- finalizing contracts and administration, such as paying the provider as agreed, and signing contracts and agreements between consumer stakeholders and third parties, such as suppliers, partners, legal agents, and insurance companies
- establishing or changing policies, and defining and supporting the new processes and procedures required to consume the new cloud services (while minimizing the impact on current business models and activities)
- preparing technical conditions for the new cloud services; for example:
  - establishing and testing a sufficient internet connection

- equipping cloud users with necessary devices, with corresponding software or middleware interfaces
- dedicating technical resources (from both the customer and the provider) as agreed
- aligning support services with the provider's processes
- training staff who will use and support the services.

The CSP or partner may plan or, more likely, automate its own onboarding procedures, including:

- configuring technical resources according to the contract and consumer requirements
- establishing monitoring and reporting consistent with service level agreements (SLAs)
- turning on the services, making them available to use
- preparing staff to work with the consumer organization's team for service enablement, provisioning, and support
- invoicing, billing, and other financial activities to collect funds from the consumer organization.

The consumer organization must be prepared to work with the service provider to understand how it prepares for onboarding. The consumer may need to adapt to accommodate a specific practice or activity the CSP needs to perform. Time and other resources will be necessary for a CSP or partner to supply the services as agreed, especially for tailored services.

The onboarding plan should account for the:

- current status of the service relationship
- scope of the onboarding initiative
- current configuration of the resources
- associated risks.

An onboarding plan should answer the following questions:

- What are the goals of onboarding? For example, to:
  - ensure a smooth migration to the cloud services
  - support a consumer's migration from one CSP to another
  - ensure a smooth migration between services offered by the same CSP.
- What is the scope of the onboarding?
- What consumer resources are required for onboarding?
- What third-party resources are required for onboarding?
- When does onboarding start and end?

All these questions should be answered by the onboarding plan. Every onboarding initiative should have a tailored plan, depending on the scope of the initiative.

Cloud consumer activities reflect the four dimensions of service management:

- **Organizations and people** Ensuring cloud users are ready, technical staff are trained, and stakeholders are informed at all levels. The activities can include change enablement, user training, and role and responsibility changes or enablement.
- **Information and technology** Access to the provider's systems is granted to a consumer. The CSP's resources must be configured for customer use by the consumer staff or CSP partner. Customer data is migrated to provider facilities. Legacy and redundant customer systems are decommissioned or configured for offboarding.

- **Value streams and processes** Organizational processes are optimized for service consumption. Value streams are optimized to maximize value from the services. Redundant procedures (replaced or automated with the services) are removed or updated. SLAs are established and executed.
- **Partners and suppliers** Contracts with partners and suppliers are updated to fit the new processes and value streams. Contracts for redundant (replaced) services are cancelled or changed. New or changed requirements for the services are communicated to all the involved parties.

The onboarding plan should also outline how the onboarding process will be controlled and its success ensured. This will include agreement on the control and validation techniques, the definition of milestones, and the criteria used to measure the initiative's success. In many cases, the control of the onboarding is best defined as part of the onboarding approach. However, like other components of the onboarding approach, it should be reviewed and adjusted during planning.

Depending on the level of cloud experience within the consumer organization and the complexity of the solution, environments, and migration, a formal review of the completed onboarding initiative may be best practice. This may require the involvement of a partner or a consultant. Depending on the general approach to onboarding control, the review may include:

- formal confirmation that all planned onboarding actions and validation checks have been completed
- review of users', customers', and other stakeholders' satisfaction and experience levels
- review of outstanding actions and errors
- a risk assessment
- registration of improvements for the continual improvement practice.

6.1.2 Involving users in the onboarding plan

Successful onboarding means that users will be prepared and able to use the cloud service to facilitate valuable outcomes effectively and efficiently.

User cooperation and collaboration ensures successful onboarding. The level of involvement will depend on the type of service being onboarded, the type of CSP, and the nature of the relationship with the CSP. A close working relationship with users during the onboarding step will have a positive impact on how the service is consumed and whether value is realized. Examples of activities that promote user collaboration include:

- planning new user onboarding activities as part of every new service implementation
- practising organizational change management to identify and resolve sources of resistance
- involving cloud users in the definition and articulation of requirements
- involving cloud users in service testing and onboarding actions
- understanding and leveraging user experiences and their related expectations
- monitoring user satisfaction to improve service experience
- involving users in service assessments and reviews
- fostering user communities and actively supporting members
- performing service usage analytics for the profiling and proactive use of real-time end-user computing data
- fostering healthy business relationships between the teams procuring or onboarding the services and the users
- maximizing the level of collaboration between the CSP and consumer organization.

6.1.3 Establishing communication channels

In the onboard step, communication channels established during the previous steps of the journey must be expanded, and new channels must be established to facilitate communication between the service providers and users.

Cloud users can use channels such as social media, online chat functions, call centres, and email to interact with service providers (both internal, such as the IT department that brokered the service, and external, such as the CSP). Clear policies and procedures should be defined to indicate what should be communicated, between which parties, and under what circumstances. For example, users must know who to contact in the event of a service disruption.

6.1.4 Preparing users for the new services

Some cloud services require special user skills, such as being able to use certain applications or equipment, or understanding the rules of safe operation in the environment where the services are used.

The following should be considered when preparing users to use the new services:

- collecting requirements from relevant stakeholders
- applying actions to meet the service and usage requirements
- controlling implementation and continually checking the relevance of the requirements.

Some services need to meet specific organizational, environmental, or regulatory requirements before they can be used. For users to be able to use these services correctly, safely, and effectively, these requirements should be met before the user can start using them. This will help to improve the user experience, prevent confusion, and reduce information security risks.

These requirements may entail the need for:

- **Due diligence** Only people with a certain clearance level may have access to the information and technology provided as part of the services.
- **User training and certification** Only people with proven knowledge and skills may use certain services.
- **Safety training and certification** Only people with proven knowledge of safety procedures are allowed to use certain services.
- **Age control and identity checks** Only users of proven identity (including age restrictions) may access certain services or service levels.
- **Effective management of access** to services, service catalogues, and support interfaces.
- **Effective presentation of the service catalogue**, including the service request catalogue to familiarize users with the spectrum of services and their possibilities.

Many of these measures may be taken as a part of an onboarding initiative. Some may require regular confirmation as a part of ongoing consumption. Measures should be agreed by the service consumer and service provider during the offer and agree steps.

6.1.5 Elevating mutual capabilities

Service relationships are about value co-creation for all stakeholders. Each service interaction is an opportunity to elevate the capabilities of another party.

The onboarding step brings opportunities for cloud consumers, together with their service providers, to apply ITIL guiding principles that help them both to co-create value. For example, indicator metrics can be defined that help the service provider identify improvement opportunities. These, in turn, can form part of the ongoing improvement of service quality and features available to all consumers.

Table 6.1 gives examples of such opportunities to create value, and the corresponding ITIL guiding principles.

Table 6.1 Opportunities and ITIL guiding principles

ITIL principle	Opportunity
Focus on value	When those onboarding the cloud service understand how the users will use it to achieve specific business outcomes, they can identify areas for improvement that will enhance the user experience as well as the ability to achieve the desired results.
Start where you are	When users are engaged during the onboarding step and considered throughout the customer journey, service adoption can be smooth and predictable, without user resistance or problems.
Progress iteratively with feedback	Changes that will be adopted and managed by users should be continually reviewed and tested. Feedback from internal stakeholders should be welcomed throughout the service adoption process and communicated to the CSP or partner, and used by both organizations as opportunities for improvement.
Collaborate and promote visibility	The cloud consumer should collaborate with all the stakeholders involved in cloud service provision, such as CSPs, partners, and suppliers. This will help the consumer to resolve incidents safely, quickly, and effectively.
Think and work holistically	Cloud users at every level can influence value creation. Users must understand their own responsibilities, and how they fit into the general business landscape and the overall success of the service.
Keep it simple and practical	The consumer organization should collect feedback on the complexity and effectiveness of the service. Areas for improvement can be communicated to the CSP so that it can simplify the user interface and service functions.
Optimize and automate	Feedback from users can be used to identify opportunities to optimize, then automate.

6.1.6 Offboarding customers and users

Organizations and cloud services are continually evolving, and no organization can know that the service it uses today will still be consumed in the same fashion, or even that it will still be relevant, in the future. Offboarding services, however, is often an afterthought, or is left to become part of the onboarding plan for replacement services.

CSPs often have predefined offboarding plans designed for each of their services. The consumer organization should consider defining its offboarding plans when it plans the onboarding of the service. Offboarding initiatives should be reviewed following the same principles as onboarding initiatives, and should lead to improving the same areas of service relationships.

An important planning element for offboarding is information security and asset management. It is essential for consumers to ensure that, when a cloud service is offboarded:

- all consumer data is eliminated according to security protocols and duties agreed in the contract
- access to cloud resources is removed for users of the offboarded service
- any systems and services that were used as part of the cloud service are switched off
- if they were issued, CSP credentials, access keys and tokens, links, and configurations should be removed, returned to the appropriate party, or eliminated.

Offboarding a service does not necessarily mean terminating the relationship with the CSP. Commonly, many individual cloud services are onboarded and offboarded as part of the ongoing service relationship. For example, if a consumer organization needs a particular service only for certain events, it may have a contract with the CSP that enables it to onboard and offboard the service as and when it needs it. In some cases, such as a mass offboarding, extra planning and coordination may be needed.

Offboarding can include the following actions by cloud consumers:

- communicating the planned offboarding and associated responsibilities to the CSP
- organizing the termination of the practical use of specific users, or the user logging off from the cloud system and beginning the offboarded account archiving procedures (equipment hand-off and configuration archiving)
- deleting relevant data related to the offboarded service or offboarded user
- reporting the termination of services to stakeholders
- maintaining the formal offboarding records required by regulations
- performing relationship management actions, such as closing calls or meetings and composing letters of appreciation
- meeting with customers of the organization who might be impacted by the offboarding activities to ensure that their expectations are appropriately managed regarding performance and availability while the cloud services are offboarded.

The level of formality required for these processes depends on the service relationship. For example, when a service provider is internal to the service consumer organization, the level of formality may be lower and some actions may be performed by a service consumer representative, such as a user's manager.

Offboarding should not cause problems for any users, and should not impact the consumer organization's business. As far as possible, offboarding activities should be automated.

When a cloud consumer offboards as a result of dissatisfaction or a dispute, it is even more important that the offboarding process has been agreed in advance and prepared properly to ensure seamless offboarding.

Large-scale offboarding and switching of initiatives may need the organizational change management and project management practices to coordinate the offboarding actions and ensure that the change is successfully adopted in their organization.

6.2 Migrating to cloud as a part of an onboarding initiative

Cloud migrations are typically conducted in three scenarios:

- migrating from in-house to cloud solutions
- migrating from one CSP to another
- migrating away from the cloud (to either an in-house solution or a different form of outsourcing).

Migration projects for each of these scenarios will be based on one or more of the migration approaches outlined in section 2.3.2:

- one-off migrations
- evolutionary migrations
- big-bang migrations.

6.2.1 Moving from in-house to cloud solutions

For a small start-up organization with a 'cloud-first' mentality and no in-house legacy, onboarding equates to constructing the environment that will ultimately host its workload. In most other organizations, however, these workloads are located in-house and were never designed to be 'cloud-ready' in the future. A transformational effort is required to migrate existing workloads to a cloud-based architecture.

Many CSPs have developed resources to assist in this transition. Publications from the CSP, like the cloud adoption and well-architected frameworks, can provide critical best-practice guidance, and staging areas or landing zones can be used as templates for planning and design, as well as the preparation and configuration of cloud services. Although there are universal or platform-neutral versions of these resources, cloud customers should obtain specific or proprietary guidance from their chosen CSP.

Although technology has changed, the core technical responsibilities of IT teams (to monitor and measure the environment) are the same. The challenge is to achieve infrastructure and workload visibility, especially when the performance attributes and the required resources and data span a complex hybrid and/or multi-cloud environment.

Although cloud can unify, simplify, and standardize many workflows in the organization, it also brings additional responsibilities to stakeholders who did not historically measure, monitor, or manage technology-based services. More than ever, monitoring performance across hybrid architectures with appropriate tools that collect and correlate data from every service and service component is critical.

Organizations rarely move the entirety of their IT to the cloud in a single 'big-bang' approach. Usually, an organization starts incrementally with a new use case or a need for a new application. Sometimes this application can run independently in the cloud, but more often it utilizes existing data from the in-house data centre. This means that, for many organizations, a migrated application or workload is dependent on a hybrid-cloud solution.

Some typical examples of initial migrations are:

- a legacy application that uses an old database that the organization wants to migrate to a modern, secure cloud data store
- an obsolete application architecture that the organization plans to modernize by migrating to cloud-based microservices
- a mobile app that is to be deployed alongside a traditional application.

Significant changes are often an important driver for migrating an existing application to the cloud. If one migration is successful, the organization may begin moving additional use cases to the cloud environment, each potentially having an individual pipeline, pool of users, stakeholders, databases, workflows, automations, business logic, and reporting systems.

The process of slowly moving to the cloud can take years, even for a very progressive organization. Many organizations that champion the move to the cloud still continue to provide services from their own in-house data centres for many years.

This gradual migration process should be planned as early as possible. However, it may start with the migration of one application as an experiment or proof of concept without organization-wide planning. When this proves successful, though, the organization must develop and execute a migration plan for the continued iterative transition to the cloud. Onboarding will then become a significant ongoing activity.

The organization's security position must be maintained or improved during and after cloud migration activities. Abstraction from underlying technology produces benefits and disbenefits for the consumer organization; therefore the consumer has to understand a fundamental principle of the shared responsibility model: the CSP secures and protects the infrastructure of the cloud, but the customer must securely configure and manage anything placed in the CSP's environment. Security, therefore, must be considered as part of the planning and execution of migration and onboarding.

An organization that does not have a comprehensive and holistic migration plan will, either explicitly or implicitly, allow each team or department to conduct its own cloud migration. The likely result, as demonstrated in Figure 6.1, is a decentralized infrastructure that is ineffective, inefficient, and difficult to manage, which creates technical debt that will impede future transformation and organizational velocity.

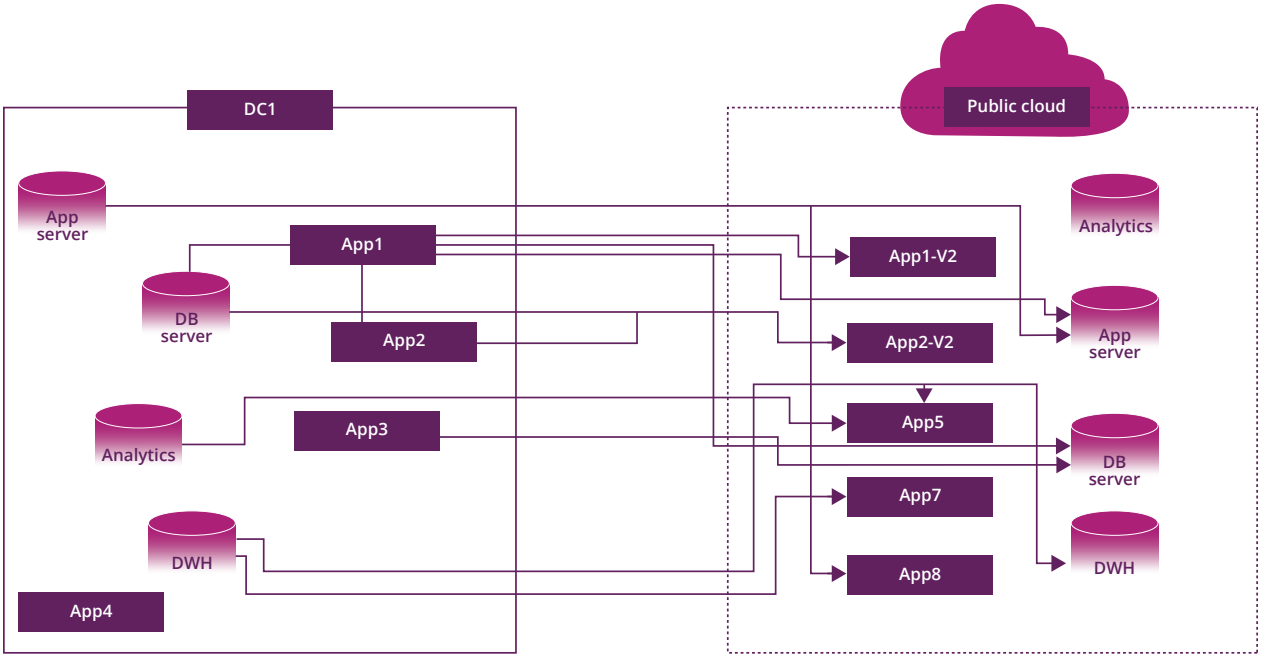

Figure 6.1 Decentralized infrastructure

Cloud migrations, particularly those that involve hybrid or multi-cloud architectures, can be planned and executed with one or more migration and data integration pipeline tools. This may require the use of third-party solutions and/or consultancy, but in many cases, these can be provided by a CSP or its partners. Using these tools, along with best-practice frameworks and staging environments or landing zones, makes the resulting environment more likely to be centralized, optimized, secured, and positioned for continued growth, as shown in Figure 6.2.

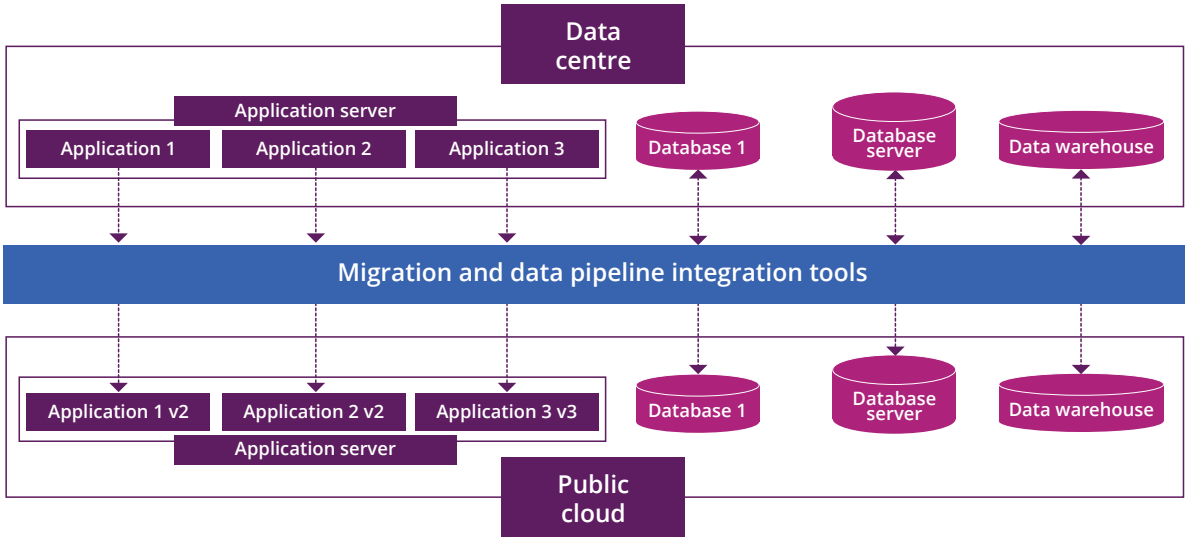

Figure 6.2 Using migration and data pipeline integration tools

Monitoring is a critical element of the cloud migration initiative. Before a migration to cloud begins, it is essential to measure the baseline in-house user experience and performance, and to define acceptable post-migration levels. Degradation in one performance area may be tolerated if it is balanced or offset by gains in another. To accurately verify the success of a migration, both the monitoring tool and the measurements captured should be consistent throughout the migration process.

During the migration to cloud, established performance and user experience metrics should be closely monitored. Variation from the baseline can be an early indicator of an issue. Dashboards and alerts can help to quickly and proactively identify issues before a business impact occurs, protecting valuable cost and time resources. Performance issues are far better identified during a migration, when it is easier to pause and make corrections, than after the migration is completed.

After completing the migration to cloud, the consumer organization should evaluate the effectiveness of its monitoring solution. On the one hand, using the same solution will allow it to verify that the service performs consistently with the in-house solution. On the other hand, the monitoring tools available through the CSP may provide better visibility into new aspects of the service. It is important that the customer journey is fully understood and service performance measured to ensure that service quality and user experience are maintained and improved after the migration. This will also provide the basis for lessons learned and more detailed forecasting for future migrations.

6.2.2 Migrating from one cloud service provider to another

When migrating from one CSP to another, the service components and workloads will be shifted through a highly coordinated combination of offboarding and onboarding, divided into two interconnected phases:

1. Offboarding the solution, services, and data from the existing provider
2. Onboarding the solution, services, and data to the new provider.

Although this type of migration is often planned and executed in a similar way as migrating from in-house to cloud solutions, moving between cloud environments involves unique challenges, including the differences in processes and procedures needed by the consumer organization (which can be resolved through appropriate change management and planning) and the possibility of vendor lock-in.

6.2.2.1 Avoiding vendor lock-in

Vendor lock-in occurs when an organization is dependent on a particular solution that will not work in a different environment without significant restructuring and/or re-engineering of assets, processes, and relationships.

The term 'vendor lock-in' is generally used to indicate two situations:

- A consumer has signed a multi-year contract with a supplier and cannot exit the contract without stiff penalties, even if that contract no longer meets its needs.
- An organization has invested in an expensive technology and cannot move away from that solution even though a better or more efficient option becomes available.

In the context of cloud, vendor lock-in typically occurs when a consumer or partner architects a cloud solution without considering the need for portability or interoperability. An example might be the extensive customization of a software-as-a-service (SaaS) service which means that data and functionality cannot easily be moved to an alternative SaaS solution. As a result of this growing awareness, more and more CSPs and consumer organizations are investing in a 'cloud-neutral' approach.

The necessity of interoperability and portability is now recognized by various vendor-neutral cloud computing alliances and CSPs. Cloud-specific standards such as OASIS CAMP for platform-as-a-service (PaaS) and TOSCA for infrastructure-as-a-service (IaaS) aim to enhance the portability and interoperability of applications across different clouds.

Until a universal set of standards is created and widely adopted, some strategies that can be used to avoid and mitigate lock-in risks when migrating to cloud are:

- selecting vendors that support both the creation of a set of cloud computing standards and the various inter-provider alliances needed to facilitate continued cooperation
- identifying and leveraging technologies, protocols, and APIs, such as containerization, that currently contribute to cloud service portability
- developing an acute awareness of the commonalities and dependencies among cloud-based services and solutions
- identifying clauses in the CSP contract that give the customer the agility and flexibility to transition to a different CSP or leverage a multi-cloud or multi-CSP approach
- using a comprehensive risk management framework to consider and mitigate the risks of vendor lock-in.

Key questions that can help consumers to evaluate whether a cloud service is prone to vendor lock-in include:

- Are there proprietary interfaces in the cloud service?
- Are proprietary communication protocols being used in the cloud service?
- Does the cloud service use proprietary data formats?
- Does the cloud service store data using a proprietary data model?
- Does the cloud service dictate where it is run?

Interviews and discussions with various IT and business stakeholders will also help to identify factors that minimize reliance on inflexible, immovable solutions. Such factors include:

- CSP proprietary cloud services
- interoperability and portability in the target cloud solution
- integration challenges
- data ownership
- security and privacy
- the frequency of change occurring within the consumer organization
- the internal and/or external nature of the changes that routinely occur within the consumer organization.

Several software developers are making significant advances and contributions to the cloud-neutral approach by offering tools that make it much easier for organizations to implement a multi-cloud architecture. This allows organizations to avoid any potential issues with a CSP and the geographical regions in which they operate. Utilizing a multi-cloud solution, a customer can split its workload across multiple CSPs, shifting as necessary. However, approaches such as multi-cloud and poly-cloud are not simple to implement, and at the time of publication these are still in the early stages of introduction and use. If an organization struggles to manage cloud services from a single CSP, the situation can be complicated by using services that depend on simultaneous use from multiple CSPs.

Vendor lock-in can be avoided by using best practices such as:

- ensuring that any decisions made before selecting vendors or signing cloud contracts are well informed
- supporting an open environment for continuous competition between providers in the cloud service market
- using standard software components with industry-accepted and proven interfaces.

6.2.3 Exit strategies and SaaS migration considerations

An organization migrating to the cloud should always have an exit strategy, even if it is unlikely to exit soon.

The organization can be flexible in its strategic use of cloud services by selecting vendors, platforms, and services that support a wide range of standards and protocols. This is crucial in the vendor selection process because it allows the organization to maintain a mix of cloud providers and internal support that works well for its circumstances.

These issues are not unique to organizations that implement PaaS or IaaS solutions. If the organization decides to change SaaS providers for any reason, it must consider data portability aspects. With SaaS, data formats and contents are abstracted away from the consumer and exclusively managed by the service provider, making data portability a major consideration.

The issue of critical importance in a SaaS migration is the compatibility of the functional interface presented to end users with any API made available to other customer applications. To help with this, the APIs that the SaaS provider makes available should be interoperable with both the interface of the in-house application and the data that is being replaced. Importing the data from one SaaS solution to another requires both applications to support a common format. This will also necessitate standard APIs for various application types. Should the APIs not be interoperable, customer applications or the data that uses them must be modified as part of the migration process.

6.3 Security and compliance considerations

To maintain security of cloud services, an organization needs to have an end-to-end view of user identity and behaviour at every application and database access point. This view should show unauthorized access, threat and attack vectors, and privilege changes. It should also provide critical knowledge as entry points are spread more broadly across platforms and geographies.

When migrating to cloud, security and IT teams are still responsible for the full protection of corporate data and clients' information. Technology teams should have a full view of the security position across different cloud architectures (especially if multi-cloud services are used), and be able to respond quickly to vulnerabilities and threats and produce timely and thorough audits.

Migrating to cloud can increase the complexity of the security landscape, but it does offer the ability to automate security, have greater control over security, and provide a more granular view of the environment. For comprehensive user activity monitoring across different cloud architectures, an organization should have easy access to log files and end-to-end tools that collect, correlate, analyse, interpret, and block any kind of suspicious behaviour.

Log files and monitoring tools provide visibility and analysis of user activity. They track the identities of users who submit, modify, and delete data, and the times when these events occur. They also reveal unauthorized access attempts, simultaneous logins from disparate locations, and changes to access privileges. They can even highlight inadvertent and malicious manipulation or extraction of data.

Dashboards within cloud monitoring tools can help visualize user identity and access events and create a foundation to analyse trends. Alerts and reports allow seamless transition from a reactive to a proactive response. Also, some tools offer predictive analytics and heuristics that provide security intelligence, helping to obtain a comprehensive view of the cloud infrastructure and security position. Many monitoring tools can help establish audit procedures and conduct compliance checks to ensure adherence to internal and industry standards and regulatory requirements. With audit trails, IT and security teams can rapidly troubleshoot a threat before it becomes a cybersecurity breach.

Issues can be overcome if they are fully understood. Some of the most common issues are:

- visibility
- compliance
- automation
- conflict between development and security priorities
- hybrid IT
- the role of SLAs with onboarded cloud services.

6.3.1 Visibility

When cloud services are adopted without coordination by individual users or teams, it is difficult to maintain visibility of who is using the services, when they are using them, and how. This has implications for the security of services, as well as how to optimize their use. Because services are easy to deploy, instances can sprawl unless they are controlled through effective management techniques. Also, some cloud resources have a very short lifecycle, such as load-balancing mechanisms that are instantiated during times of peak demand and later deconstructed when that demand subsides. It is also common for legacy practices to need manual intervention, or to lack support for any cloud or cloud-native security controls.

To manage this aspect, significant security and authorization controls are required. A comprehensive security policy established during the agree step can document the monitoring tools and processes, to allow the organization to have visibility of all deployed instances of the service. To reduce the likelihood of sprawl, an organization should consider utilizing practices such as:

- **Change enablement** To define the deployments that can be considered standard changes
- **Service financial management** To define the requirements for approving the additional costs
- **Service request management** To manage the workflow and document the authorizations required for the deployment of additional resources.

6.3.2 Compliance

Being compliant can be difficult even with in-house solutions, and the cloud adds an additional layer of complexity and abstraction. Because the CSP is responsible for securing its infrastructure, it can provide documented assurances of ongoing compliance for common regulatory requirements, such as GDPR, FedRAMP, HIPAA, and FERPA. This compliance, however, only applies to the cloud layer or to the CSP's side of the shared responsibility model. Because CSPs cannot be concurrently compliant with every security standard, award, or certification in all instances globally, consumer organizations may need to evaluate compliance based on equivalence rather than certification. For example, an organization that holds a certification in an ISO standard can demonstrate equivalence to the similar category of compliance for a country-specific security standard.

The cloud consumer organization is responsible for achieving and maintaining compliance for what it creates within the cloud environment. For example, a healthcare organization that is subject to HIPAA compliance must always know where any personal health information data is being stored, moved, or accessed, and ensure that it is properly secured and encrypted at all times. There are companies that specialize in helping organizations to achieve such compliance requirements.

Well-known best practices for enforcing compliance in traditional environments can also be applied in the cloud, although they need to be adapted. Descriptions of the tools and resources available to customers are often contained in the CSP guidelines, such as the cloud adoption framework and well-architected framework.

Cloud consumers must understand how the shared responsibility model applies to compliance, how to properly implement and maintain the required controls, and how to engage compliance agencies to provide general cloud compliance considerations and measures to support it.

6.3.3 Automation

Automation is sometimes mistakenly equated with a loss of control, so it can be seen as a risk to cloud security. However, automation can enable organizations to proactively detect and correct security issues before they can impact workloads.

The automation of security policies and changes can provide a means for the consistent application of security rules and measured compliance by organizations. When utilized correctly, automation can free up security professionals from mundane tasks so they can focus on higher-value (and often more interesting) activities.

6.3.4 Conflict between development and security priorities

Teams using modern development methods strive to create and deliver products and services as quickly as possible, while the security team works to ensure that nothing is deployed without being thoroughly reviewed to ensure it adheres to policy.

Individually, each team seeks to address its responsibilities and achieve goals that facilitate value co-creation. However, its processes and methods of working can contribute to a siloed mindset.

To resolve this issue, development teams should adopt common security rules to provide sprints with sound procedures and measures, so that the security team can monitor progress and compliance, giving continuous feedback and support.

6.3.5 Hybrid IT

Hybrid IT, with a mix of multiple security policies, is common. It can be complex, especially when there is a need for different security practices. Although existing security tools and practices in the organization may be predictable and well understood, they are often based on legacy IT infrastructure and applications. This means they might not apply to new efforts to transition to the cloud.

For example, in a traditional network, an internal IT team assigns IP addresses to physical and virtual machines. The workloads running on those machines remain consistent for a long time, so the IP addresses being used do not change very often, making these markers a simple way to keep track of events from a security perspective. By contrast, cloud-native workloads are highly dynamic and can be deployed at much larger scale than traditional applications. Moreover, cloud-native workloads are built from a set of services, each of which is deployed separately. As a security parameter, a static set of IPs is too rigid for such a fluid environment.

Mitigating this mixture of in-house and cloud environments requires a good understanding of the capabilities and use cases of each landscape, accepting that security practices and controls that work well for one environment may not work well for others, and creating and maintaining collaborative and complementary IT policies that work across the hybrid infrastructure.

6.3.6 The role of service level agreements with onboarded cloud services

SLAs are critical; they can dramatically impact the cloud consumer's security and business continuity initiatives. They set the stage for the required level of continuity and availability of service and ensure that the consumer's services are properly architected for availability and continuity. The SLA will also state what is not provided as part of the service so the consumer can ensure that it is not dependent on that particular aspect.

To develop effective SLAs, a number of essential parameters and criteria should be considered and reviewed, such as:

- availability
- performance
- security, compliance, privacy, and ownership of data
- disaster recovery and business continuity expectations
- location of the data

- access to the data
- portability of the data
- process for identifying problems and resolution expectations
- change enablement procedures
- dispute mediation process
- exit strategy (with expectations on the provider to ensure a smooth transition).

With a core set of criteria established, the next step is to evaluate the criticality of the cloud service and associated data. Almost any computing system can be made extremely reliable, but in the case of service failure, costs can be high. Reviewing and understanding the applicable SLAs enables the consumer organization to identify the key responsibilities and management activities that will lead to consistent and effective cloud service onboarding.

6.4 Summary

Onboarding cloud services requires holistic planning, user involvement, identification of any required tools, clear communication, and execution. Depending on the type of services selected, onboarding activities may be highly collaborative. If standard services are being implemented, nearly all of the onboarding activities will depend on the consumer organization. The activities associated with onboarding can also differ depending on whether the consumer organization is migrating from an in-house to a cloud solution, migrating from one CSP to another, or migrating from a cloud to in-house solution. Even if a migration from one CSP to another is not occurring, all onboarding plans should consider the process of offboarding and how this process could be triggered.

CHAPTER 7

CO-CREATE: ENABLING VALUE

7 Co-create: Enabling value

7.1 About the co-create step

The co-create step begins as the consumer organization starts using the cloud services it has onboarded to achieve its objectives. As they deliver and use the services, the cloud service provider (CSP) and consumer are involved in co-creating value that both organizations will realize.

In the co-create step, the consumer organization ensures that it can effectively operate and support the cloud solution in partnership with its CSP or partner in accordance with the shared responsibility model.

The co-create step involves understanding:

- how the services will be used to help achieve the objectives in the cloud strategy
- how the cloud service forms part of the organization's operating model, and how the operating model changes when cloud services are used
- all the elements required for the service to operate effectively
- the drivers of value co-creation
- how each stakeholder contributes to the effective and efficient operation of the services
- how industry guidance and best practice can be used to effectively drive value co-creation.

Inputs to the co-create step include:

- the cloud strategy
- the service agreement
- the shared responsibility model
- guidance and standards provided by the industry and CSPs
- the CSP's service architecture best practices
- the consumer organization's policies, guidelines, and practices.

Outputs from the co-create step include:

- services that operate as anticipated and as defined in the cloud service agreement
- achievement of the anticipated results of using the service
- service performance and quality reports
- compliance reports for regulated services
- recommendations for changes to service, the way it is delivered, or the way it is consumed.

7.2 Operating model alignment

7.2.1 What happens to an operating model when moving to the cloud?

When moving to the cloud, it is important to understand what happens to the consumer organization's operating model and its associated strategy. The consumer organization's and CSP's operating models should be aligned.

Definition: Operating model

A conceptual and/or visual representation of how an organization co-creates value with its customers and other stakeholders, as well as how the organization runs itself.

ITIL® 4: Digital and IT Strategy states that operating models are tools used to facilitate the design and configuration of an organization's operations, enabling value creation. They are contextualized by the organization's strategy; the purpose of an operating model is to ensure that operations are configured such that the organization's strategies can be executed successfully.

Operating models include the following components:

- value chain(s)
- suppliers
- locations
- organization
- information
- management system.

Figure 7.1 shows an operating model canvas.

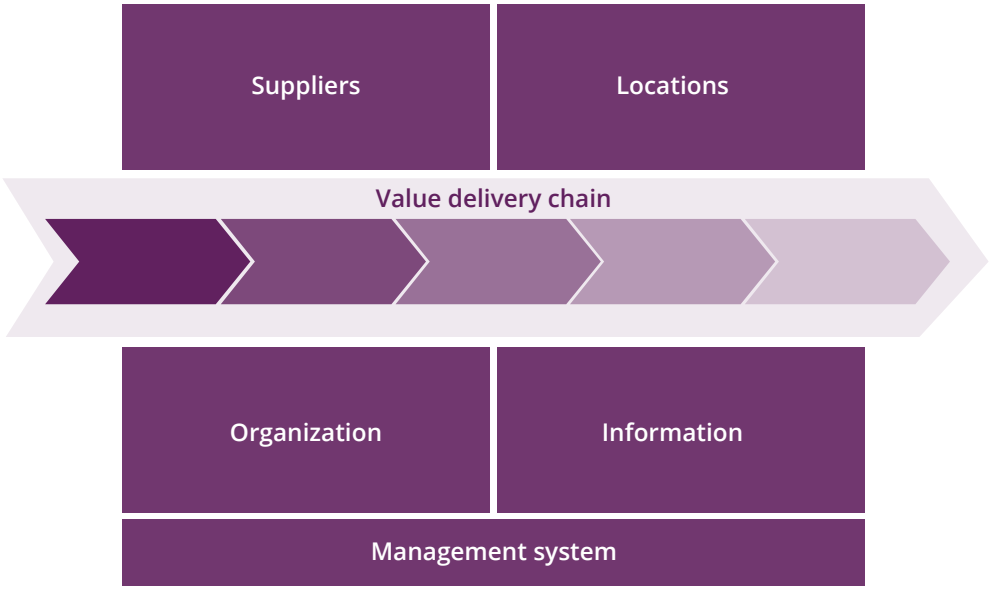

Figure 7.1 Operating model canvas
Reproduced with permission from Campbell *et al.* (2017)

An operating model is a framing tool for an organization, not for services. However, if it is not effectively defined, aligned, and optimized, an operating model will negatively impact the related services or products.

Cloud migration and the adoption of cloud services both significantly affect an organization's operating model. It is important to understand the dependencies, dynamics, and risks associated with an operating model and the outsourcing or insourcing of its components. When an organization outsources or insources cloud services, the dependencies within the current operating model need to be reviewed and updated to ensure they are fit for co-creation with CSPs.

The more an organization uses cloud services, the more it delegates control of its operating model components to the service provider. The outsourcing of these components means that organizations will start sharing responsibility for the creation of value.

7.2.2 Running multiple/parallel operating models

An organization can have multiple or parallel operating models; for example, if it has global divisions or business units that operate uniquely within its market. Parallel operating models can be categorized into four basic groups:

- **Cannibalism** The organization focuses on the rapid deconstruction of a strategy.
- **Erosion** A form of cannibalism where the organization uses the revenues of an existing (profitable) strategy to fund a new strategy.
- **Concurrence** The new operating model neither helps nor harms the existing strategies.
- **Synergism** The new operating model enhances or strengthens existing strategies.

For more detail, see *ITIL® 4: Digital and IT Strategy*.

An organization considering a new cloud operating model must determine how the change will affect existing operating models. For example, a cannibalistic model may lead to change that is too rapid, which will damage existing services or products. If this is the case, an erosive model would have been a

better choice. However, sometimes an erosive model is progressive enough to address competitive threats. The organization must be able to balance the risks of each type of model.

Determining how the operating model will be used for cloud provides insight into how a consumer organization and CSP can best co-create value. Two examples are:

- aligning an existing operating model to be more cloud-centric; that is, to design, deliver, support, and govern cloud services
- introducing a new cloud operating model.

7.3 The value co-creation map for cloud

Figure 1.5 in Chapter 1 provides an overview of the key elements of value co-creation for cloud services. It illustrates the key drivers for effective cloud service provision and value co-creation. It is a neutral frame of reference that can facilitate effective conversations, and therefore enable the alignment of operating models.

A cloud service's value potential is significantly impacted by the five drivers, which are outlined in Table 7.1.

Table 7.1 Overview of characteristics of co-creation drivers

Co-creation driver	Description
Strategic adaptability	In a highly competitive environment, cloud services can differentiate the organization from its external or internal market and make it more competitive
Consumer experience	Services that are delivered directly to consumers (internal or external) usually aim to provide a significantly positive experience in order to retain consumers
Operational excellence	Many organizations require highly optimized services in terms of cost, efficiency, and effectiveness. This is common for highly commoditized back-end systems
Reliability, resiliency, and continuity	Many services emphasize being available, scalable, and robust, especially core or backbone systems
Governance and control	Many services are highly regulated or involve sensitive information, such as child welfare technology services

These drivers are shaped by aspects of the consumer organization's and the CSP's or partner's ways of working. In Figure 1.5, these eight aspects are shown on the dotted line:

- customer organization's cloud strategy
- CSP's or partner's knowledge base and documentation
- CSP's or partner's practices
- CSP's architectural design principles and best practices
- industry best practices and standards
- customer organization's architectural standards and best practices
- customer organization's practices
- customer organization's knowledge base and documentation.

7.3.1 Applying the value co-creation map

The ITIL practices can help consumer organizations, CSPs, and partners to optimize each of the five drivers in an effort to maximize value co-creation. This involves defining the activities and responsibilities of both parties in each context.

Because there are 34 practices, a full review of this type is very time-consuming; an organization should focus on a prioritized minimal viable product (defined by what is needed to co-create value) and then iteratively enhance its ways of working over time.

The process of defining a minimal viable product for value co-creation has four steps:

1. Review co-creation drivers against the organization's strategic objectives.
2. Map and prioritize the ITIL practices to enable the drivers and strategic objectives.
3. Engage with the CSP or partner to define the co-creation model.
4. Prioritize the practice improvement backlog.

This approach is a simple starting point that a consumer organization can adopt and tailor according to its needs. The key outcome is always a clear definition of how the consumer organization and its CSP or partner will share the responsibility of creating value.

7.3.1.1 Review co-creation drivers against the organization's strategic objectives

Most organizations have a dominant driver based on their strategic objectives and the nature of the cloud services in their portfolio (current or planned). An organization can assign drivers to its strategic objectives, and then use that list to identify the ranking order of its co-creation drivers, as demonstrated in Figure 7.2. Organizations that are placed in different areas of the strategy spectrum or that are in different industries are likely to have very different driver priorities.

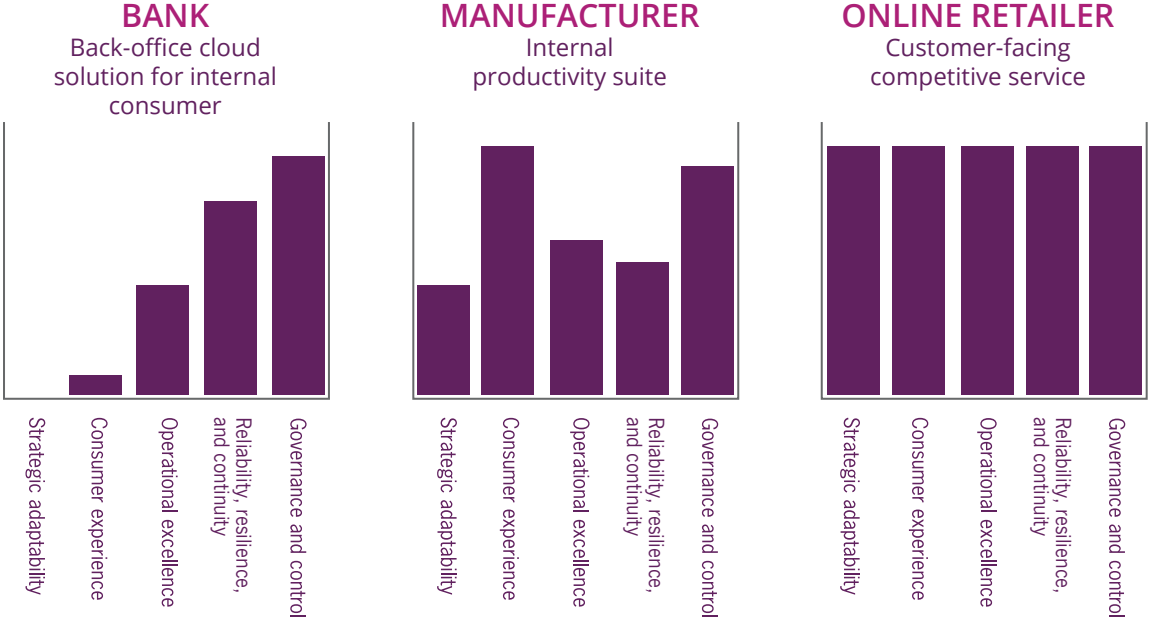

Figure 7.2 Co-creation driver priorities based on strategic objectives

If most of an organization's strategic objectives focus on governing and controlling cloud services, for example, due to a highly regulated environment, the governance and control driver should be prioritized highly. Some organizations may identify several drivers that are all high priority.

7.3.1.2 Map and prioritize the ITIL practices to enable the drivers and strategic objectives

The next step is to map the ITIL practices and organizational capabilities to each strategic objective. Any practice that is required to fulfil the objective should be mapped, and then those practices should be prioritized.

For example, the strategic objective of 'enabling and increasing collaboration across the organization' may involve:

- **Incident management** To ensure that incidents do not impede collaboration efforts
- **Problem management** To ensure that problems do not impede collaboration efforts
- **Knowledge management** To ensure that information is available and accessible, to foster collaboration
- **Organizational change management** To foster a culture of collaboration.

The list of relevant practices should be augmented by practices that are relevant to the prioritized list of value co-creation drivers. If the organization had identified the governance and control driver as a high priority, for example, it should also map practices such as information security management and risk management. These may be required to fulfil the strategic objective in the dominant context of governance and control.

7.3.1.3 Engage with the CSP or partner to define the co-creation model

The organization should understand the maturity of its current ways of working with regard to each of the ITIL practices that are mapped to its strategic objectives. This includes understanding the existing gaps in proficiency and how those gaps should be addressed.

The shared responsibility model provides the roles and responsibilities of each party relative to managing the services. For CSPs providing standard services at hyperscale, the role of the CSP in co-creating value should have been determined when acquiring the service, as there is little room for them to flex internal processes to accommodate the nuances of the operating models of individual customers. In other cases, gaps in the existing practices that prevent the co-creation of value should be determined by meeting with the CSP or partner to determine the co-creational roles and responsibilities of each party and to identify any tools that could assist in the higher levels of value co-creation.

These discussions should result in a clear indication of the gaps in the consumer organization's current practices and an understanding of how those gaps can be filled, either by the consumer organization or by its CSP or partner.

7.3.1.4 Prioritize the practice improvement backlog

The consumer organization should work with its CSP or partner to prioritize the list of practice improvements, based on each improvement's cost of delay. Each item on the list should be assigned to an owner (either the consumer organization or its CSP or partner) to ensure that it is managed through its lifecycle.

The next step is for the organization to identify which of the practice improvements are needed to establish a minimal viable product for value co-creation.

When this has been defined, a high-level roadmap can illustrate the anticipated milestones in the process of delivering the minimum viable product.

7.3.1.5 A different approach

Some organizations identify which ITIL practices will be needed to deliver against their strategic objectives without considering the five drivers. When this happens, the organization should agree what value co-creation will look like for each practice in the context of each strategic objective with the CSP or partner.

7.4 Value co-creation drivers in practice

7.4.1 Strategic adaptability

The strategic adaptability driver focuses on ensuring that strategic opportunities for cloud services are identified and defined, cloud services provide the expected return on investment, and deviations in strategic alignment and value delivery are addressed. From a value co-creation perspective, there are many opportunities for the organization and its CSP or partner to collaborate on this driver.

Two example ITIL practices can illustrate what value co-creation in the context of this driver might look like:

- strategy management
- portfolio management.

7.4.1.1 Strategy management

The strategy management practice ensures that the context of the organization and its market is clearly defined, allowing the organization to articulate the value proposition and strategic choices around its adoption and usage of cloud services. This facilitates informed decision-making about how organizational resources should be prioritized and positioned in order to enable the strategic objectives.

CSPs and partners can provide new capabilities that can differentiate the organization in its market. They may also have strategic insights that can help the consumer organization to better understand market context.

Table 7.2 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of strategy management and the strategic adaptability driver.

Table 7.2 High-level responsibilities for strategy management

Consumer organization	CSP/partner
Define the cloud strategy with an associated business case and justification for cloud services	Provide innovative features on an ongoing basis, published in a roadmap
Identify innovative business use cases for cloud service adoption	Publish industry- and market-specific case studies on the innovative application of cloud services
Evaluate the risk of competitive alternative cloud solutions within the consumer organization's environment	
Define cloud guiding principles for tactical and operational decision-making	
Align the cloud strategy to other strategic plans	
Define cloud governance controls	

7.4.1.2 Portfolio management

The portfolio management practice ensures that the organization understands its strategic investments and how cloud services can or should be used to maximize the overall portfolio's performance.

CSPs or partners can enhance the value of the portfolio by developing new capabilities and features in their cloud services and platforms, which the consumer organization can use. CSPs and partners can also help the organization to identify opportunities for portfolio enhancements through cloud.

Table 7.3 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of portfolio management and the strategic adaptability driver.

Table 7.3 High-level responsibilities for portfolio management

Consumer organization	CSP/partner
Assess the existing portfolio for cloud service opportunities, and define a placement model to identify which applications would be fit for cloud rehosting, refactoring, re-architecting, rebuilding, or replacing	Provide innovative features on an ongoing basis
	Publish architectural guidance on the compatibility and performance of applications and their infrastructure
Evaluate the ROI	
Identify opportunities to maximize the performance of the organization's portfolio with cloud services	

7.4.2 Consumer experience

The consumer experience driver ensures that the entire cloud service lifecycle is consumer-centric, including that the consumers are prepared to consume the service and the expected value and experience are delivered (and, where possible, exceeded). From a value co-creation perspective, the organization needs to be closely aligned with its CSP or partner to ensure that all touchpoints are carefully managed and that the consumer's end-to-end experience is positive throughout the customer journey.

The consumer experience driver is affected by a significant number, if not all, of the ITIL practices. Depending on who the consumer is and the overall strategy for consumer experience, some organizations may focus on a subset of ITIL practices that will have the most impact on value co-creation in the context of consumer experience.

Two example ITIL practices can illustrate what value co-creation in the context of this driver might look like:

- service level management
- organizational change management.

7.4.2.1 Service level management

The service level management practice ensures that the cloud service's utility and warranty are clearly defined, and that it delivers the agreed benefits and experience.

CSPs or partners should provide clear utility and warranty criteria and commitments, and the ability to measure and report on whether these are met.

Table 7.4 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of service level management and the consumer experience driver.

Table 7.4 High-level responsibilities for service level management

Consumer organization	CSP/partner
Identify the service components and configuration items needed to deliver the end-to-end service	Publish availability and performance service level agreement (SLA) details for all cloud services
Consolidate cloud service components (in-house and external) and review, negotiate, and agree the end-to-end availability and performance SLAs	Publish SLA details for support agreements
Negotiate and agree on operational-level agreements (OLAs) with appropriate internal stakeholders and underpinning contracts (UCs) with service providers, and on support agreements with CSPs and partners. Depending on the organization, the terms 'OLA' and 'UC' may not be used, but internal agreements or process handover points need to be reviewed. The UC in this case is the cloud service agreement	Publish historical SLA statistics for cloud services on request
Define, agree, and communicate the overall end-to-end SLA	Publish reference architecture and design patterns that can be used to design service solutions
Work with monitoring teams and service providers to establish OLA/UC monitoring and reporting	
Track and consolidate all OLA/UC statistics across the cloud service components, and report on overall end-to-end SLA targets	
Identify OLA/UC target deviations and escalate issues to the appropriate team or service provider	
Hold service reviews to discuss OLA/UC performance against the overall SLA with the relevant teams and service providers	
Conduct consumer experience surveys	
Review performance and adoption data, and discuss improvement opportunities with relevant stakeholders and service providers	
Withdraw the SLA/OLA/UC when services are no longer required	

7.4.2.2 Organizational change management

The organizational change management practice ensures that cloud service usage scenarios are clearly understood and that cloud services themselves are effectively adopted. This practice ensures that cloud consumers and the people involved in designing, provisioning, supporting, and governing cloud services are appropriately trained and skilled.

CSPs or partners co-create value in this context by providing material for new and existing features, such as online training, knowledge bases, and learning paths that facilitate onboarding and the appropriate use of cloud services.

Table 7.5 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of organizational change management and the consumer experience driver.

Table 7.5 High-level responsibilities for organizational change management

Customer organization	CSP/partner
Define the business case for change and the business success criteria Identify adoption scenario use cases for new cloud service features Determine people's readiness for new services, features, and updates, then resolve gaps in readiness before deployment Work with the service level management practice to understand cloud service adoption data and identify plans to improve adoption Define and establish appropriate adoption and change plans, including: ● communication plans ● resistance and risk plans ● sponsorship and stakeholder plans ● training and skills acquisition plans ● coaching and mentorship plans ● plans for appointment and management of change champions ● plans for monitoring and management of feedback channels Manage organizational change risk through its lifecycle Work with other practices to understand, measure, and manage consumer experience criteria Establish appropriate feedback channels, and ensure feedback is managed through its lifecycle	Provide training resources, formal certifications, and guides Provide new feature roadmaps and information before deployment Provide access to cloud service usage data Provide professional 'fast track' or adoption services to assist with cloud service adoption

7.4.3 Operational excellence

The operational excellence driver involves providing high-performing and optimized cloud services. From a value co-creation perspective, the organization essentially outsources portions of its value chain, architecture, and operating models to its CSP or partner. There must be clarity regarding which activities the organization retains, and which are outsourced. The consumer organization is usually able to leverage the CSP's or partner's industry experience.

Four example ITIL practices can illustrate what value co-creation in the context of this driver might look like:

- incident management
- problem management
- monitoring and event management
- change enablement.

7.4.3.1 Incident management

The incident management practice ensures that cloud services can be restored quickly when incidents occur. In the context of value co-creation, the challenge with incident management for cloud is in identifying where each incident has occurred.

A common misconception is that CSPs and partners provide a managed support service by default, that is, the CSP or partner will resolve all incidents without input from the consumer organization. Unless an organization has contractually procured managed support services, it will own incidents throughout their lifecycle. The organization will need to diagnose and troubleshoot incidents, attempt to resolve them, and only escalate each one to the CSP or partner when it has isolated the issue.

Table 7.6 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of portfolio management and the operational excellence driver.

Table 7.6 High-level responsibilities for incident management

Consumer organization	CSP/partner
Define appropriate incident models for cloud services	Publish health updates for each cloud service, with automated alerts when availability is impacted
Define incident SLA metrics against available SLA information from the CSP or partner	Publish support SLAs for relevant support agreements
Ensure that incidents are owned and tracked throughout their lifecycle	Provide a knowledge base to assist with incident resolution
Identify and categorize incidents	Provide a self-service means for consumers to log and track incidents
Provide initial incident diagnoses and support all cloud incidents before they are escalated	Provide incident categorization and prioritization criteria based on the SLA
Ensure that incidents have been isolated to the CSP or partner before escalation	Provide updates on incident resolution
Ensure that support diagnostics data and information are collected and submitted, and that the CSP or partner has access	Provide workarounds where possible
Ensure that incidents are categorized and prioritized with the CSP or partner	Provide post-incident review reports where applicable
Identify and define potential incident workarounds	Log high-level incident reports
Ensure that incident resolutions are tracked and captured	
Define resolution notes to aid rapid first-line resolution	
Report on cloud service incidents	
For major incidents	
Define major incident criteria to distinguish between normal incidents and high-impact, business-critical ones	Publish key contact details for support contract
Define a major incident response plan for the cloud service	Allocate appropriate resources to assist in the rapid resolution of the incident if related to the CSP infrastructure, or if this type of support has been purchased by the consumer
Allocate a major incident manager	
Proactively establish distribution lists and bridge systems in preparation for potential major incidents	
Identify and classify major incidents	
Assemble required resources for temporary teams to investigate and resolve incidents, including logging the incidents with the relevant service providers	
Communicate management with impacted stakeholders	

7.4.3.2 Problem management

The problem management practice ensures that the underlying causes of incidents are identified, and the organization's technical backlog for the cloud service is minimized. From a value co-creation perspective, the consumer organization will have ownership of and responsibility for problem management (unless it is contractually outsourced as part of a managed service). If the root cause of a problem is with the CSP or partner, an incident or change request should be logged and given to the CSP or partner to resolve.

Table 7.7 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of problem management and the operational excellence driver.

Table 7.7 High-level responsibilities for problem management

Consumer organization	CSP/partner
Define problem models for cloud services	Communicate information about known errors or vulnerabilities
Identify, classify, and prioritize problems	Provide post-incident review information for major incidents
Proactively identify problems through incidents or other sources of information and data	Provide diagnostic and advisory tools to help identify suspicious trends and deviations in the performance of cloud services and cloud configuration items
Review the cloud reference architecture and identify cloud configuration items that are likely to cause incidents	Provide reference architecture and design patterns for cloud solutions, to enable problem prevention or identification
Define workarounds to address known errors	Provide potential workarounds
Define and publish relevant knowledge articles	
Manage problems through their lifecycle	

7.4.3.3 Monitoring and event management

The monitoring and event management practice ensures that cloud services and their health can be monitored end to end. From a value co-creation perspective, this is an extremely important practice because there are multiple dependencies in cloud service delivery, such as:

- CSP or partner infrastructure monitoring end points
- in-house infrastructure
- supporting services.

When an issue occurs or performance suffers, monitoring can isolate the issue so that the correct team can take corrective actions. The CSP or partner should provide relevant monitoring end points to give insight into the CSP's or provider's service health.

Table 7.8 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of monitoring and event management and the operational excellence driver.

Table 7.8 High-level responsibilities for monitoring and event management

Consumer organization	CSP/partner
Define an end-to-end service monitoring plan, highlighting all cloud configuration items to be monitored, along with their monitoring mode, monitoring thresholds, alert actions, tools for monitoring, and so on	Provide appropriate application programming interfaces (APIs) for cloud service monitoring
Define and manage correlation analysis, and artificial intelligence or machine learning capabilities, for the effective management of alerts for end-to-end service monitoring	Provide tools and dashboards for cloud service monitoring
Define monitoring dashboards and internal alerts	
Configure, manage, and maintain all monitoring and event management tools	
Define a monitoring strategy	

7.4.3.4 Change enablement

The change enablement practice ensures that changes and the associated risks to cloud services are identified, evaluated, and managed throughout their lifecycle. This practice can create friction in the context of value co-creation, because changes (such as service retirements, new features, and updates from CSPs or partners) are often deployed in real time. Organizations cannot always reject a change such as the degradation of a service or feature, but they should expect an appropriate notice period (although some new features and updates may have an opt-in or -out option).

In a co-creation model, the CSP or partner should publish roadmaps and schedules of upcoming changes, thereby providing an opportunity for the consumer organization to provide feedback. The consumer organization may need to identify required actions based on upcoming changes, such as infrastructure or user training changes.

Table 7.9 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of change enablement and the operational excellence driver.

Table 7.9 High-level responsibilities for change enablement

Consumer organization	CSP/partner
Identify and align to the CSP's roadmap and its communication channels for updates	Establish communication channels for new features and updates, including appropriate information for planning
Review, triage, log, and categorize all communicated planned features and updates	Provide feedback mechanisms for consumer organizations
Ensure that appropriate change categories and models have been defined to cater for the streamlined 'push' nature of deployments of cloud features and updates	Deploy changes and updates in a phased and coordinated way
Identify use cases for new cloud features, to realize maximum value and enable innovation	Provide timely access to new features for piloting and early testing
Assess the readiness of architecture, processes, people, and support for new features or updates, and for improvements where needed	
Establish a phased deployment model (aligned with the CSP's model)	
Manage changes throughout their lifecycle	
Establish internal feedback channels for cloud consumers	
Define relevant release policies and strategies for the release of cloud changes, including understanding the impact of cloud changes on in-house applications and how they can accommodate the changes	
Establish deployment pipelines and scripts for continual integration and deployment	

7.4.4 Reliability, resilience, and continuity

The reliability, resilience, and continuity driver is about ensuring stable, robust service availability and performance. This driver is usually associated with core backbone systems that do not necessarily need to be optimized for cost or performance, but which do need to be highly stable.

In the context of value co-creation, the CSP's or partner's SLAs and contractual commitments to continuity and reliability need to be clearly defined. The consumer organization should also assess the CSP's or provider's architecture best practices and design patterns with regard to service warranty. Many CSPs have publicly available cloud adoption frameworks or well-architected frameworks that provide detailed guidance.

The following four examples of ITIL practices illustrate what value co-creation in the context of such drivers might look like:

- availability management
- capacity and performance management
- architecture management
- continuity management.

7.4.4.1 Availability management

The availability management practice is about maintaining the overall availability of a service, even if some of its components should fail. It is important for mission-critical systems that cannot tolerate service interruptions, where downtime may result in damage or financial loss.

Highly available cloud services guarantee a certain percentage of uptime, such as 99.9%. Three other elements of high availability are:

- **Redundancy** Any critical system elements have a redundant component that can take over if a failure occurs.
- **Monitoring** Data is collected from a running system to detect when a component stops responding or fails.
- **Failover** A mechanism that causes the system to switch automatically from an active component to a redundant component when a failure is detected.

Three technical components also enable high availability:

- **Data backup and recovery** The system will automatically back up data to a secondary location and recover back to the source. By doing this, redundancy and failover can be set up.
- **Load balancing** A load balancer manages traffic, routing it between systems that can serve that traffic. It can avoid systems that have failed, thus enabling monitoring and failover.
- **Clustering** A cluster is made up of several nodes, each of which serves a similar purpose. Each node in the cluster is able to failover to another node. By replicating within the cluster, the organization can create redundancy between nodes.

Table 7.10 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of availability management and the reliability, resilience, and continuity driver.

Table 7.10 High-level responsibilities for availability management

Consumer organization	CSP/partner
Define availability requirements based on selected metrics Plan for high-availability architecture and identify the types of failure that can be experienced, then implement recovery strategies Ensure that systems can fail safely and restore operations without service disruption Define and implement a data redundancy strategy Perform realistic load testing until a system fails, then observe how failure mechanisms behave Conduct a planned or unplanned experiment in which systems fail and the team must implement the disaster recovery plan Periodically check data from monitoring systems to ensure that it is accurate Consider availability in release and deployment practices. Achieve rolling updates that do not require critical component downtime	Implement and offer reporting in terms of high-availability metrics, such as percentage of uptime, mean time to recovery, and mean time between failures Implement failure mode analysis and indicate single points of failure Isolate critical resources to ensure that if a component fails, operations can continue Provide tools and guidance that allow consumers to implement data replication in support of redundancy strategies and recovery time objectives and recovery point objectives Provide tools and guidance that allow consumers to identify failures under load Implement disaster recovery mechanisms and run disaster recovery exercises for those parts of the cloud environment that they are responsible for Automate and make continuous monitoring available to consumers Provide tools and guidance so that consumers can design release and deployment mechanisms that enable updates with minimum service disruption

7.4.4.2 Capacity and performance management

The capacity and performance management practice is about service performance and the performance of the resources that support services, such as infrastructure, applications, and third-party services.

Table 7.11 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of capacity and performance management and the reliability, resilience, and continuity driver.

Table 7.11 High-level responsibilities for capacity and performance management

Consumer organization	CSP/partner
Identify requirements for service capacity and performance Measure, assess, and report on service capacity and performance Document and manage service capacity and performance risks Define metrics for service capacity and performance	Provide tools and guidance that allow consumers to: ● design and implement an approach to capacity planning, monitoring, and performance analysis ● design and implement capacity reporting and dashboarding features ● design and implement a mechanism for capacity logging and risk threshold triggering ● design and implement an approach to capacity measurement

7.4.4.3 Architecture management

A comprehensive architecture management practice applies to all levels of an organization's architecture.

Table 7.12 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of architecture management and the reliability, resilience, and continuity driver.

Table 7.12 High-level responsibilities for architecture management

Consumer organization	CSP/partner
Ensure that the organization's strategy is supported by the: ● target business architecture ● target product and service architecture ● target information systems architecture ● target technology architecture ● target environmental architecture	Support the following by registering component interactions, depicting interdependencies, and modelling structure templates for information, operational, and communication technologies: ● business architecture ● product and service architectures adopted by customers ● information systems architectures adopted by customers ● technology architectures adopted by customers ● environmental architectures adopted by customers

7.4.4.4 Continuity management

The continuity management practice is about the proportion of time that a service is functional, which is one of the areas of software quality.

Table 7.13 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of continuity management and the reliability, resilience, and continuity driver.

Table 7.13 High-level responsibilities for continuity management

Consumer organization	CSP/partner
Identify and resolve any single point of failure	Define and provide access to components, services, resources, and compute instances that can be deployed to prevent a single point of failure
Define and break down workloads by service level objective	Design applications to be configurable to use multiple instances, and to automatically detect failures and redirect requests to non-failed instances
Understand and minimize service dependencies. In particular, understand the overall impact of failure or reduced performance for each dependency	Design and implement service composition of critical and less-critical workloads to specify the service features and number of instances to meet availability requirements
Ensure that tasks and messages are idempotent. This may mean detecting duplicated messages or ensuring consistency by using an optimistic approach to handling conflicts	Define the number of different services used, and ensure that all features and service dependencies are known and visible
Ensure that applied timeouts are appropriate for each service or resource and for the users accessing them. In some cases, a longer timeout can be allowed for a particular instance of a user, depending on the context and other actions that the user is performing. Plan throttling periods for certain users to avoid blocking	Implement idempotent operations that can be repeated multiple times and produce the same result. Ensure that duplicated requests do not cause problems
Plan scaling to mitigate graceful degradation. Ensure that there is sufficient performance and capacity available under non-burst conditions	Configure request timeouts. Services and resources may become unavailable, causing requests to fail. Provide throttling for high-volume users to avoid excessive load
Design to fail back to multiple components and different services or workflows	Design applications to gracefully degrade (autoscaling can help handle the load)
	Design and implement components to use multiple instances without affecting operation and existing connections, where possible

7.4.5 Governance and control

The governance and control driver is about ensuring that cloud services are trustworthy, and that consumers can safely use them without being exposed to unnecessary risks and costs.

A common misconception in the context of value co-creation is that the CSP or partner is responsible for ensuring that cloud services are effectively governed and secured. Unless this is contractually agreed as a managed service from a partner, the CSP or partner will be accountable only for the governance of its infrastructure. It should, however, provide features to help the consumer organization to implement effective governance and controls.

Four example ITIL practices can illustrate what value co-creation in the context of this driver might look like:

- service financial management
- supplier management
- information security management
- risk management.

7.4.5.1 Service financial management

The service financial management practice ensures that cloud service costs are transparent, optimized according to the value they provide, and appropriately owned. It also helps to ensure that unoptimized costs are addressed.

In the context of value co-creation, the consumer organization is accountable for understanding and optimizing its cloud consumption. The CSP or partner will ensure that appropriate tools and controls are provided to enable the organization to manage its cloud consumption and the associated costs.

Table 7.14 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of service financial management and the governance and control driver.

Table 7.14 High-level responsibilities for service financial management

Consumer organization	CSP/partner
Identify and map the costs associated with all cloud service components	Provide cost calculators or licensing costs for cloud services
Define, negotiate, and agree cloud service cost models	Provide access to detailed cloud component consumption, service, or licensing costs
Identify and appoint cost ownership for scoped cloud services	Provide a monthly consolidated billing statement for all cloud components, services, and licensing costs
Define cloud service consumption budgets and thresholds	Provide consumption and licensing cost features and tools to assist with the tagging, budgeting, reporting on, and optimization of consumption and licence usage
Establish cost monitoring across all cloud service components, and integrate with the CSP's consumption and licensing cost data sources	
Establish consolidated consumption and cost dashboards for reporting	
Track cloud service consumption, licence usage, and the associated costs. Identify deviations and anomalies, and action them with the relevant cost owners	
Configure the CSP's cost features and tools to manage and optimize cloud consumption, licence usage, and the associated costs	
Identify cost risks and manage them through their lifecycle	

7.4.5.2 Supplier management

The supplier management practice ensures that all of the suppliers involved in delivering the organization's cloud services are aligned, deliver contractually, and deliver the expected value.

From a value co-creation perspective, this practice ensures that the roles of the consumer organization and the CSP or partner are clearly defined, understood, and agreed.

Table 7.15 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of supplier management and the governance and control driver.

Table 7.15 High-level responsibilities for supplier management

Consumer organization	CSP/partner
Work with architecture teams and the wider business to source appropriate CSPs or partners based on business requirements, readiness assessments, and an organizational sourcing strategy	Understand the consumer organization's needs, and negotiate enterprise or partner agreements if appropriate
Negotiate and agree on CSP or partner enterprise agreements	Provide proofs of concept where applicable
Ensure that the supplier meets internal and external regulations	Publish all security, regulatory, and compliance audit results
Ensure that the cloud customer journey is followed	Publish detailed SLA information for cloud services
Ensure that the expected ROI is received	Publish historical SLA statistics on request
Ensure that the CSP or partner is integrated through ongoing service reviews	
Manage contracts or legal disputes throughout their lifecycle	
Manage supplier risks throughout their lifecycle	

7.4.5.3 Information security management

The information security management practice ensures that cloud services are safe, trustworthy, and secure.

The CSP or partner usually only provides security for its internal infrastructure and services, unless contracted to provide more through a managed service agreement. However, it does provide features and controls that the consumer organization can use to align the cloud service to its security and compliance requirements.

Table 7.16 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of information security management and the governance and control driver, as defined by the Center for Internet Security.

Table 7.16 High-level responsibilities for information security management

Consumer organization	CSP/partner
Establish primary service agreement	Service agreements must incorporate mutually agreed provisions and/or terms, including the: ● scope, characteristics, and location of the business relationships and services offered ● information security requirements ● change management process ● logging and monitoring capability ● incident management and communication procedures ● right to audit and third-party assessment ● service termination process ● interoperability and portability requirements ● data privacy requirements
Ensure adherence to the security management policy and procedures	Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for the management of security incidents. Review and update the policies and procedures at least annually
Establish and monitor relevant security metrics	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations
Review internal compliance testing	Define and implement a process for internal assessments to confirm the conformance with and effectiveness of standards, policies, procedures, and SLA activities at least annually
Define and implement a system development lifecycle process for cloud service design, development, deployment, and operation in accordance with security requirements	Update the end-to-end cloud-servicing lifecycle capabilities for design, development, deployment, and operation in accordance with security requirements
Review secure automated testing and implement a testing strategy, including criteria for the acceptance of new information systems. Automate when applicable and possible	Upgrade automated testing capabilities
Ensure secure automated deployment	Establish and implement strategies and capabilities for secure, standardized, and compliant cloud service enablement, automating where possible
Conduct vulnerability remediation reviews	Define and implement a process to mitigate security vulnerabilities, automating where possible
Ensure that security incident response plans are defined and reviewed	Establish, document, approve, communicate, apply, evaluate, and maintain a security incident response plan, which includes relevant internal departments and other business-critical relationships (such as supply chain) that may be impacted
Ensure that security incident response testing is performed	Test and update incident response plans at planned intervals or upon significant organizational or environmental changes
Ensure that the event triage process is calibrated for cloud services	Define, implement, and evaluate processes, procedures, and technical measures to triage security-related events
Establish and review a security breach notification process	Define and implement processes, procedures, and technical measures for security breach notifications. Report security breaches and assumed security breaches, including any relevant supply chain breaches, as per applicable SLAs, laws, and regulations
Ensure that points of contact are up to date	Maintain points of contact with applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities

A prerequisite of digital transformation is handling large amounts of data. Related technologies, such as data lakes, data warehouses, data hubs, and data marts, are crucial. Data privacy has become an integral part of managing the end-to-end lifecycle of large amounts of data.

Table 7.17 shows roles and responsibilities linked to data privacy in the cloud, as defined by the Center for Internet Security.

Table 7.17 High-level responsibilities for data privacy

Consumer organization	CSP/partner
Ensure data inventory is in place	Create and maintain a data inventory, especially for sensitive and personal data
Ensure data classification is respected for all data types	Classify data according to its type and sensitivity
Review data flow documentation	Create data flow documentation to identify how data is processed, stored, or transmitted. Review data flow documentation at defined intervals, at least annually, and after any change
Establish data ownership and ensure stewardship is in place	Document ownership and stewardship of all relevant documented personal and sensitive data, and review at least annually
Ensure principles of data privacy by design are embedded in organizational practices, systems, and products	Develop systems, products, and practices based on privacy by design and industry best practices. Ensure that systems' privacy settings are configured according to applicable laws and regulations by default
Review data protection impact assessment	Conduct a data protection impact assessment to evaluate the origin, nature, particularity, and severity of risks in the processing of personal data according to applicable laws, regulations, and industry best practices
Evaluate and review sensitive data transfer procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and processed only within scope as permitted by laws and regulations	Define, implement, and evaluate processes, procedures, and technical measures: ● to ensure any transfer of personal or sensitive data is protected from unauthorized access, and is processed only within scope as permitted by applicable laws and regulations ● to enable data subjects to request access to, modify, or delete their data ● to ensure that personal data is processed according to applicable laws and regulations, and for the purposes declared to the data subject ● for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations ● to disclose the details of personal or sensitive data access by sub-processors to the data owner before the access occurs
Ensure procedures for access to, and reversal, rectification, and deletion of, personal data are in place	
Communicate limitation of purpose in personal data processing	
Ensure personal data sub-processing procedures are in place	
Review disclosure of data sub-processors	
Review limitation of production data use	Obtain authorization from data owners, and manage associated risk, before replicating or using production data in a non-production environment
Review data retention and deletion procedures	Manage data retention, archiving, and deletion in accordance with business requirements and applicable laws and regulations
Review sensitive data protection procedures	Define and implement processes, procedures, and technical measures to protect sensitive data throughout its lifecycle
Manage and respond to requests for disclosure of personal data by law enforcement authorities and data subjects, according to applicable laws and regulations	Manage and respond to requests for disclosure of personal data by law enforcement authorities according to applicable laws and regulations
Review data locations of classified data types	Define and implement processes, procedures, and technical measures to specify and document the physical locations of data, including any locations where data is processed or backed up

7.4.5.4 Risk management

The risk management practice ensures that the risks associated with cloud services are effectively managed so that negative impacts are avoided.

From a value co-creation perspective, the CSP or partner should provide tools to assist in highlighting cloud service risks so that the consumer organization can effectively monitor and plan their mitigation. However, risk management is predominantly the consumer organization's responsibility.

Table 7.18 outlines the high-level responsibilities of the consumer organization and the CSP/partner when co-creating value in the context of risk management and the governance and control driver, as defined by the Center for Internet Security.

Table 7.18 High-level responsibilities for risk management

Consumer organization	CSP/partner
Ensure risk, compliance, audit, and assurance processes and teams have baseline requirements	Establish, document, and maintain baseline requirements for securing different cloud services
Ensure metrics for risk, compliance, audit, and assurance are monitored and have assigned, actionable continual improvement items	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations
Ensure adherence to secure and compliant design and development	Define and implement a software development lifecycle process for cloud service design, development, deployment, and operation in accordance with the organization's security requirements
Ensure adherence to secure and compliant automated testing	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades, and new versions, which provides assurance of cloud service security and maintains compliance, while enabling speed-of-delivery goals to be met, automating where possible
Ensure adherence to secure and compliant automated deployment	
Conduct vulnerability remediation reviews	Establish and implement strategies and capabilities for secure, standardized, and compliant cloud service enablement, automating where possible
	Define and implement a process to mitigate security vulnerabilities, automating where possible

7.5 Managing the optimization of cloud service consumption

7.5.1 The dynamics of cloud service consumption

Cloud service consumption is directly correlated to cost generation and, if the service is well designed, to service value realization. Cloud consumption is also highly dynamic, whereas organizational budgets and traditional accounting practices are not. Organizations therefore need to balance the use of cloud services to obtain value with controlling costs.

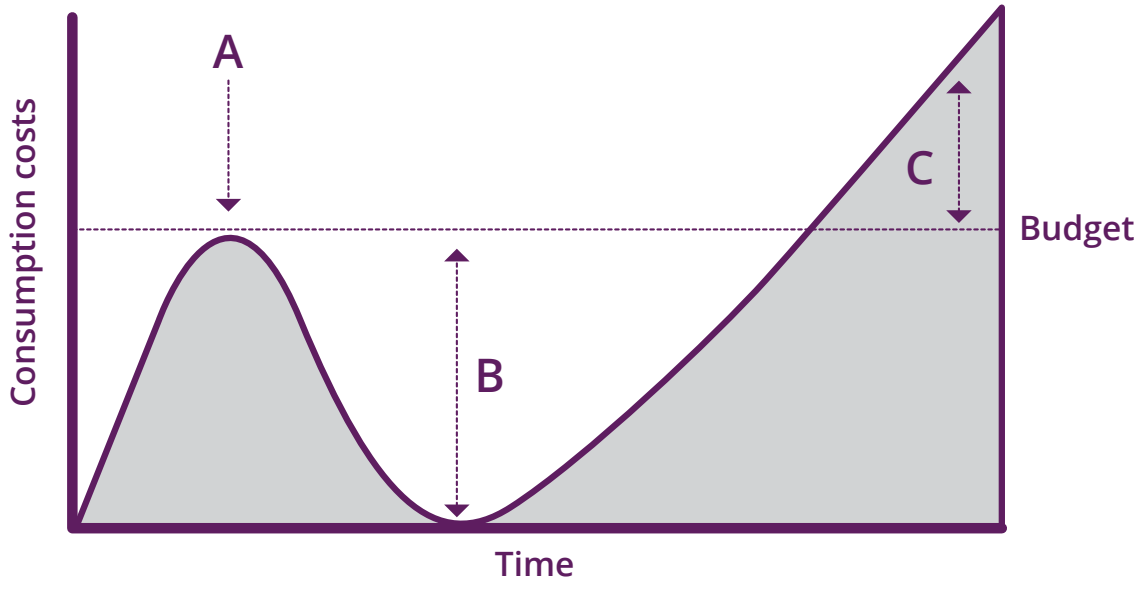

Figure 7.3 Cloud consumption dynamics

Figure 7.3 illustrates an organization that experiences three common scenarios associated with cloud service consumption over time:

- **Scenario A** An optimal scenario in which consumption aligns with the organization's budget. However, in most cases the value of cloud services will lead to increased adoption, which should result in a natural month-on-month increase in consumption costs until usage stabilizes.
- **Scenario B** A scenario where there are blockers or a lack of interest in cloud service adoption; the budget is available but the value is not consumed. In pay-per-use models, this scenario may be acceptable. However, in enterprise agreements or bulk purchase commitment contracts, this scenario represents wasted capital.
- **Scenario C** A scenario with trending over-budget consumption costs. This may be the result of:
  - poorly managed or unoptimized cloud resources or licences, resulting in increasing consumption costs for inactive resources or licences
  - poorly designed cloud architecture standards, resulting in cloud solutions that do not optimize cloud resource usage, leading to growing debt because of over-provisioned, under-utilized cloud resources
  - mass migration of applications and services into the cloud, or significant usage of licensing across the entire organization for solutions based on software-as-a-service (SaaS).

Finance teams need to understand how to optimize real-time cloud consumption costs. Controlling costs too heavily results in stifling of adoption and innovation. Publicizing the open use of cloud without any controls will lead to uncontrolled cloud consumption.

Organizations must understand that:

- **Unless they are licensed, most cloud services are pay-per-use and charged in real time** Most cloud resources are charged according to usage, which can result in variable consumption costs.
- **Most cloud services allow on-demand self-service with no blockers to deployment** Anyone (if access controls are not implemented) can provision cloud resources or allocate licences to use cloud services, without any approval. Controls need to be implemented to control consumption costs.

Given the dynamic nature of cloud services, organizations cannot rely on traditional yearly budget cycles. Cloud services do not fit into the capex model, and should instead be provisioned through opex.

7.5.2 Optimizing cloud service consumption

Cloud service optimization means balancing cloud demand and consumption costs. This balance is unique to every organization.

Methods for preventing over-consumption include:

- Identify accountable people and owners for cloud service consumption spend, such as application owners or business unit owners.
- Implement chargeback models so that cloud consumers within the organization account for and pay for their usage. This incentivizes them to optimize their own usage.
- Use CSP or partner controls or features to control consumption at the source. Examples of typical controls are:
  - **Policies** To whitelist the usage of standard resources (as opposed to premium resources) within certain environments.

- **Automatic start, shutdown, and deallocation of virtual machines** If compute resources are running constantly when being used only during working hours, this contributes significantly to consumption costs.
- **Use of budgets** Some CSPs provide soft- or hard-capped budgets that either provide an alert when a spend threshold is met or halt consumption beyond a given cost threshold.
- **Role-based access control** Only authorized staff should be allowed to provide and maintain cloud resources.
- **Autoscale up or out** This feature allows for automatic allocation of resources, but can be configured so that it can be allocated only manually, or to provide a prior notification that allows the consumer to decide.

- Implement cloud architecture standards, and review them against the CSP's or partner's best practices to ensure optimal allocation and usage of resources.
- Deallocate licences for SaaS solutions when not in use. This could be automated as part of the offboarding process.

A process for preventing under-consumption could be:

- Understand current blockers to consumption. Common blockers include:
  - lack of interest or awareness of cloud services and how they can provide value
  - lack of budget or approval
  - security and compliance concerns
  - lack of skills and resources to make effective use of the cloud.
- When blockers are identified, investigate them further to understand the full context.
- When the blockers have been assessed, work with the CSP or partner to address them.

7.6 Managing cloud service quality

Organizations often base their primary measure of quality on SLAs, focusing on availability and performance. However, this is only a small portion of true service quality. The dimensions of service quality are outlined in Table 7.19.

Table 7.19 Dimensions of service quality

Service quality dimension	Description
Responsiveness	The readiness and performance of the service and support staff
Assurance	The knowledge and courtesy of employees, including their ability to inspire trust and confidence
Tangibles	The elements of the service that a user can see and interact with, such as the aesthetics, ease of use, and accessibility of cloud service portals
Empathy	The caring and individualized attention that the organization provides to consumers
Reliability	The ability to provide the service dependably and accurately

These quality dimensions are usually used in surveys to understand consumers' expectations for and current perceptions of service quality.

When designing cloud services, consumers should consider interviewing customers to understand their quality expectations, as part of defining service requirements. It should use proofs of concept, demonstrations, and samples to help articulate and assess the consumer expectations in each dimension.

For example, when designing a new cloud service, the organization should list the tangibles, such as portals, knowledge articles, and reports. Then a sample or proof of concept should be shared with the consumer organization to help gauge whether its expectations can be met. This information should be used as part of the final design of the cloud service.

Where possible and practical, key metrics and thresholds should be used to determine whether the elements provide the expected quality.

When the service has been designed and is being delivered, the organization should create a service quality survey. It should define a set of questions for each quality dimension to help rate the consumers' perceptions about the service quality, and the results can then be benchmarked against the expectations. The survey should include both quantitative and qualitative methods. If, for example, the perceived quality of a dimension is lower than expected, the organization needs enough information to identify why that is the case.

7.6.1 Co-creating quality

Although several aspects of the quality dimensions are not easily defined in a contractual agreement, they should still be evaluated and reviewed with the CSP or partner to ensure that the overall service quality is being delivered as expected.

7.6.1.1 Responsiveness

This dimension focuses on how responsive the CSP or partner is with regard to addressing incidents and providing information about outages and changes. Contractual commitments can be implemented for these elements, such as response times to incidents.

Outside of contractual obligations, the consumer organization will have a general perception (right or wrong) about the CSP's or partner's responsiveness. It should evaluate and discuss this responsiveness with the CSP or partner to ensure that it is effectively managed, including the CSP or partner educating the consumer organization and adjusting its expectations regarding responsiveness.

7.6.1.2 Assurance

This dimension focuses on how the CSP or partner provides knowledgeable and courteous employees who inspire confidence and trust in the consumer organization. This includes how the CSP or partner understands and uses best-practice guidance, architect design patterns, and knowledge articles.

If an organization has a support contract in place, it should experience the assurance dimension when interacting with account managers and support staff. This dimension is difficult to contractually enforce, but it can be used to highlight any gaps between expectations and perceived quality.

7.6.1.3 Tangibles

This dimension focuses on the cloud portals, documentation, training, assessments, reports, and so on that are provided by the CSP or partner, along with their perceived effectiveness in delivering value. For example, if documentation has spelling errors, outdated content, or mistakes, this will negatively impact the perceived quality of the tangible aspect of the overall service.

Where practical, tangibles should be listed and reviewed frequently to ensure alignment between expectation and reality. CSPs or partners usually provide feedback mechanisms that allow the organization to provide feedback about improvements.

7.6.1.4 Empathy

This dimension focuses on the caring and personalized attention the organization gives its customers. It is usually measured across interactions with personnel from the CSP or partner, or it can be experienced based on the CSP or partner showing significant interest in the organization's success, such as by providing free assessments and resources or inviting the organization's representatives to relevant conferences.

Although this dimension is difficult to capture in a contract, it is important to review it and provide feedback to the CSP or partner to highlight issues that need to be addressed.

7.6.1.5 Reliability

This dimension focuses on the CSP's or partner's ability to deliver dependable and robust cloud services. This is often clearly defined in the SLA, and is represented by the service's availability and response times.

The elements of reliability are often clearly defined and easy to report on. These measures need to be continually reviewed to determine the overall quality of the service and to ensure issues can be addressed.

The reliability of the cloud service also requires the organization to design and implement it correctly. CSPs or partners often provide architecture reference documentation, design patterns, and best practices to help organizations design cloud services that will deliver the expected reliability.

7.7 Using cloud tools for value co-creation

CSPs and providers provide a range of tools to help organizations optimize their cloud service experience and ensure that they can deliver the expected value. Each CSP and provider has its own proprietary toolsets and offerings, but a general overview of the nature of these tools is outlined in Table 7.20.

Table 7.20 Cloud tools for value co-creation

Co-creation driver	Cloud tools
Strategic adaptability	**Service roadmaps** Provide information about upcoming features and releases, which may indicate new available functionalities
Consumer experience	**Feedback channels** Allow cloud service consumers to provide feedback about functionalities and features, which the CSP can use to improve services and align them to consumers' expectations
Operational excellence	**Service health dashboards and communication APIs** Provide insights into the current health of cloud services and notify the consumer organization about potential outages **Message centres** Provide notifications about changes to and planned maintenance on cloud services provided by the CSP **Service roadmaps** Provide extended insights into new features and updates that the consumer organization should prepare for **Assessment tools** Help the organization to determine whether there are issues with its current technical or operational deployments **Advisory dashboards** Outline the overall health of resources within the cloud and provide advice about optimizations

Co-creation driver	Cloud tools
Reliability, resilience, and continuity	**Reference architecture, design patterns, and best practices** **Advisory dashboards** CSPs and partners typically provide document libraries on how to best architect and deploy their cloud services
Governance and control	**Policy controls** Can be used to enforce certain behaviours. These need to align to the consumer organization's policies, to ensure that the cloud service is governed and controlled as expected **Management tools** Help to effectively manage cloud resources, such as resource tagging and grouping access controls **Cost management tools** Help to manage cloud service costs, such as APIs that report on consumption costs in close-to-real time, budgets that set thresholds of spend across groups of resources, and cost dashboards that evaluate costs at a high level **Security and compliance centres** Make the application and management of security and compliance controls, and the reporting of threats and compliance, easier to manage **Monitoring** Can be used to get transparency about the operating health of cloud services

7.8 Summary

The co-created value and quality potential of delivered and consumed services can be examined through five key drivers: strategic adaptability; consumer experience; operational excellence; reliability, resilience, and continuity; and governance and control. Strategic adaptability ensures that cloud service opportunities continue to be identified and defined in alignment with strategic objectives. Consumer experience ensures that the cloud service lifecycle is consumer-focused. Operational excellence aims to optimize cloud services to achieve and maintain high performance. Reliability, resilience, and continuity focus on achieving stability, availability, and performance. Governance and control verify that cloud services are trustworthy and compliant at acceptable levels of cost and risk. These drivers should be reviewed against the consumer organization's defined strategic objectives, and enabled by applying the corresponding ITIL practices.

CHAPTER 8

REALIZE: MEASURING AND IMPROVING

8 Realize: Measuring and improving

8.1 About the realize step

Once the cloud services have been onboarded and are fully operational, it is possible to evaluate whether the anticipated value has been realized for all stakeholders.

The purpose of the realize step is to ensure that the organization is continually optimizing its cloud strategies and usage of cloud services to get the most value from its investments, and that the intended organizational benefits and goals are realized.

In this context, 'stakeholders' refers to:

- customers in the consumer organization who evaluate whether the cloud services have met the requirements specified and whether they have supported the activities and results anticipated
- users in the consumer organization who evaluate the extent to which the cloud services have met their expectations and enabled them to conduct the activities the service was designed for
- sponsors in the consumer organization who evaluate whether the expected return on investment has been achieved
- executives in the cloud service provider (CSP) or partner organizations who ensure that services have been delivered as agreed, and that they have been profitable
- support staff and managers in the CSP organization who identify improvements to the service and resolve any aspects where delivery has not been up to the agreed level
- customers of the consumer organization who will provide feedback (directly or indirectly) about the quality and performance of their services or products after the introduction of cloud services.

The realize step involves understanding:

- how to continually evaluate the services in the light of changes due to volatility, uncertainty, complexity, and ambiguity (VUCA) in the organization's internal and external contexts
- whether the cloud services have achieved the required results and, if not, determining what action needs to be taken (either to improve the service and the way it is used, or to move to a different solution)
- the impact on the organization's operating model, and especially the need to change it based on lessons learned from using the cloud services
- whether the cloud strategy needs to be adjusted

- whether the requirements for cloud services need to be changed, either to correct earlier assumptions made, or because the organization's needs have evolved
- how to calculate whether the intended return on investment has been achieved
- how to correct the situation if the return on investment has not been achieved.

Inputs to the realize step include:

- information about the organization's operating model
- ongoing assessments of the organization's internal and external contexts, which are done as part of a regular review of the cloud strategy
- a continual improvement methodology.

Outputs from the realize step include:

- adjustments to the organization's operating model
- review of the organization's cloud strategy
- short-term plans and measures for dealing with VUCA situations
- improvement plans and initiatives
- review of the achievement of strategic objectives.

8.2 Maintaining operating model alignment

As explored in Chapter 7, an organization's operating model needs to accommodate and encourage value co-creation to enable collaboration with the cloud service provider (CSP) or partner.

The consumer organization, the CSP, and partners are each exposed to socio-political, economic, and market-related risks and challenges. They also face unique demands and challenges from customers, their delivery partners, their employees, and sometimes their technology. These conditions can result in turbulent, dynamic, or chaotic environments. For a consumer organization to remain competitive and deliver its intended value, the strategy and operating model will need to evolve to address these challenges. Most of these evolutions will be independent, so each organization must ensure that its independent evolution does not negatively impact value co-creation.

The direction of a CSP's or partner's service portfolio may become less strategically aligned with that of the consumer organization over time. For example, a small consumer organization may move from an infrastructure-as-a-service (IaaS) focus to a platform-as-a-service (PaaS) or software-as-a-service (SaaS) focus. Its current CSP's or partner's portfolio and roadmap may not support that change, and so would probably not be the best fit for value co-creation in the future.

Another example is that a CSP or partner may evolve its technology platform, and therefore its design principles, reference architecture, and best practices too. Documentation, knowledge bases, services, and customer-facing processes, toolsets, and people will all evolve in turn. These changes may be subtle in the short term, but will significantly accumulate over time. If the consumer organization does not continually align its operating model to these changes, there will be negative impacts on the five drivers of value co-creation.

8.3 VUCA and the value co-creation map

VUCA stands for 'volatility, uncertainty, complexity, and ambiguity'. A VUCA environment is one that is turbulent or chaotic. In such an environment, organizational leaders must mitigate or otherwise address the risks associated with each letter in the acronym. Figure 8.1 shows the value co-creation map for cloud with a VUCA context.

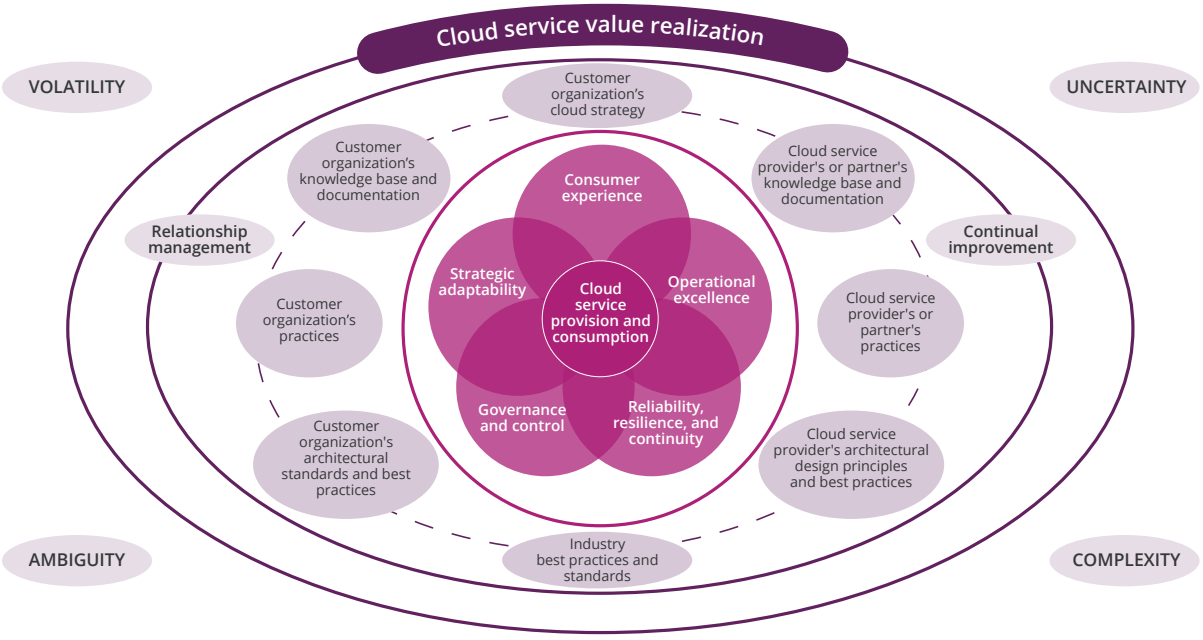

Figure 8.1 The value co-creation map for cloud with a VUCA context

Organizations must adapt their behaviour and thought patterns to accommodate the turbulent, chaotic environment. A VUCA environment leads to failures and losses, but these can be reduced, measured, and learned from.

Organizations need to understand and study VUCA to be able to predict, plan, and respond to VUCA environments. Table 8.1 provides definitions for each element of a VUCA environment.

Table 8.1 VUCA elements

VUCA element	Definition
Volatility	The speed of a change in an industry, market, or overall environment
Uncertainty	The lack of predictability in an environment
Complexity	The number of issues and amount of confusion that surround the organization
Ambiguity	The lack of clarity and potential for misreading situations

8.3.1 Strategic planning for a VUCA future

Defining a cloud strategy is difficult when the future is uncertain. In a VUCA environment, there are too many possibilities and risks for organizational leaders to map and consider. A consumer organization needs to enable individual teams, CSPs, and partners to help define the cloud strategy, accounting for the many challenges of a VUCA environment.

The organization should invest in people (stakeholders, CSPs, CSP partner networks, and so on) and involve them in the cloud strategy planning.

The cloud strategy plan should include:

- user- and community-centric business case
- high-level description of cloud service
- cloud vision
- cloud mission
- corporate values and purpose
- measured objectives with cloud adoption roadmap milestones and success criteria
- how each objective will transition to the next phase
- stakeholder list and requirements
- communication and feedback flow mechanism
- resources required
- a plan from each stakeholder group for its own department or function
- high-level risk and VUCA issues
- requirements for approval of cloud adoption roadmap
- assigned owner of cloud strategy and cloud adoption roadmap
- organizational structure: names of sponsors and management with list of all other stakeholders.

8.3.2 VUCA and the five drivers of value co-creation

Generic strategies used for addressing each element of VUCA are outlined in Table 8.2 and discussed in more detail in *ITIL® 4: Digital and IT Strategy.*

Table 8.2 Addressing VUCA elements

Characteristic	Recommendation
Volatility	Prepare for variations by investing in extra resources
Uncertainty	Improve knowledge management and the quality of information
Complexity	Restructure for self-organization and agility
Ambiguity	Experiment to explore available options

Tables 8.3, 8.4, 8.5, 8.6, and 8.7 provide examples of organizations addressing VUCA challenges within the context of the value co-creation map for cloud. These examples represent a small sample of the risks that could be identified.

Table 8.3 Addressing VUCA challenges in the context of strategic adaptability

Co-creation challenges	Approach
Volatility	
Aligning evolving service offerings to the consumer organization's cloud and business strategy For example, a partner's managed service may no longer provide value when the consumer organization's resources become able to deliver the service on their own	Follow CSPs' and partners' technology and offering roadmaps Invest in the relationship with the CSP or partner to ensure early insights into its future Include CSPs and partners in strategic planning to enhance alignment Shorten the strategic planning cycles
Uncertainty	
Strategic planning is difficult because of the rapidly changing technology landscape and offerings from CSPs or partners	Follow the same approach as for volatility Invest in research about industry and market trends
Complexity	
Evolving CSP and partner offerings and innovative technologies make it difficult for consumer organizations to know how to obtain the most value from cloud services	Follow the same approach as that for volatility Invest in research about industry and market trends
Ambiguity	
Defining a clear strategic plan is difficult because of the high number of competing offerings and the many proprietary best practices for the use of cloud services	Engage with CSPs and partners to understand their best practices, and work with them to align the consumer organization's strategic plan and operating model so that the optimal services are used to deliver the strategy

Table 8.4 Addressing VUCA challenges in the context of consumer experience

Co-creation challenges	Approach
Volatility	
It is hard to keep up with new technologies and feature updates, and trying to do so can cause change fatigue or sub-optimal adoption of cloud services	Ensure that there is a dynamic adoption and change process, develop a culture of change, and ensure ongoing readiness for new technologies and associated features Monitor CSPs' and partners' roadmaps to prepare for upcoming changes Communicate with CSPs and partners to learn about upcoming changes, including how the changes will impact the organization and how change practices can be enhanced
Uncertainty	
Rapidly changing consumer requirements may be difficult to fulfil For example, consumers can have very specific requirements that CSPs and partners cannot fulfil	Provide feedback to CSPs and/or partners to request new features and recommend improvements Monitor CSP and partner roadmaps to identify when upcoming features or services could fulfil requirements
Complexity	
Consumers expect simplicity, but IT systems are increasingly complex, so it is difficult for IT organizations to meet expectations	Use a service-oriented approach to simplify and package complex cloud architecture and solutions into cloud services that align to consumer requirements. These should be published and marketed in a service catalogue for easy consumption
Ambiguity	
Emerging cloud practices, patterns, or features may not be easy to use or intuitive	Use consumer personas to define consumer types, then pilot the new practice, pattern, or feature with different consumer types to clearly articulate use cases Develop instructions and adoption plans

Table 8.5 Addressing VUCA challenges in the context of operational excellence

Co-creation challenges	Approach
Volatility	
It can be difficult to incorporate the growing number of cloud service and feature changes with minimal risk	Establish cloud change triage teams to categorize changes based on their probable impact on the consumer organization Leverage automation and phased releases to reduce lead times and negative impacts
Uncertainty	
When an organization does not know what skills will be required for future cloud services, it is difficult to define training plans and skills development programmes	Develop a culture of continuous learning and growth Use online training for certifications, as well as informal online training
Complexity	
The organization may not have enough specialist skills to address the many possible cloud service issues and challenges	Staff skill sets should evolve from deep specialists to T-, Pi-, or comb-shaped generalists
Ambiguity	
Competing goals (speed versus control, security versus cost, and so on) make it difficult to find the right approach for the organization	Encourage autonomous decision-making Take a minimal viable product and iterative approach to governance Ensure there are strong customer feedback loops that are continually reviewed

Table 8.6 Addressing VUCA challenges in the context of reliability, resilience, and continuity

Co-creation challenges	Approach
Volatility	
The CSPs' services can have unexpected downtime	Use reference architectures and design principles to build for resilience and mitigated impacts of cloud service failure Design cloud solutions and architecture with expectations of failure and a backup plan
Uncertainty	
Cloud architecture evolves in uncertain ways, so there is no way to know how consumer organization architecture standards need to evolve	Follow and align to CSP and partner roadmaps Review CSP and partner cloud architecture references, design principles, and best practices every quarter, to ensure there is alignment
Complexity	
Because cloud service dependencies are very complex, it can be difficult to isolate the location of a point of failure and quickly fix the issue	Ensure the consumer organization has a clear end-to-end service monitoring plan that monitors the key configuration items involved in cloud service delivery, including using monitoring tools to monitor configuration items for an end-to-end view of the components' health Integrate the CSPs' service health communicators to ensure that all known issues from CSPs and partners are automatically logged at the service desk Consider self-healing automation, to ensure that outages or issues are addressed before they become incidents Review cloud advisory solutions, to identify underlying component or service performance issues, and address these before they become incidents
Ambiguity	
When an issue occurs with a CSP or partner, there may be little clarity about the full nature and impact of the issue or when it will be resolved	Ensure cloud systems are architected with resilience in mind, to attempt to counter any issues experienced by the CSP or partner Ensure partnership and collaboration between development and operations teams and cycles

Table 8.7 Addressing VUCA challenges in the context of governance and control

Co-creation challenges	Approach
Volatility	
Full cloud governance cannot necessarily be designed, developed, and implemented before the first service is introduced into the organization	Governance should follow Agile practices, including short sprints, incremental releases, and continuous feedback The consumer organization should focus on a minimal viable governance product to ensure basic, impactful controls are established first
Uncertainty	
Traditional governance can be a constraint; for example, by preventing innovation	Define an acceptable level of uncertainty in the consumer organization's governance model
Complexity	
As products and services continuously change, and increasing numbers of providers support the organization's value streams, governance becomes more complex	Implement a minimal viable governance model and, as new requirements develop, add governance controls
Ambiguity	
New cloud service feature releases are often ambiguous and therefore difficult to govern	Accept and embrace ambiguity by adapting governance through short sprints and fast feedback loops Organizations should use the information and documentation provided by the CSP or CSP partner Use early release and test channels for cloud features, in order to better understand the features and respond with the required governance

8.4 Continual improvement and the value co-creation map for cloud

To maintain a viable cloud strategy, an organization should continually improve its strategies and cloud services. In the context of the value co-creation map for cloud, continual improvement helps an organization to align to CSPs and their partners on an ongoing basis. It also ensures that the consumer organization's operating model is aligned with the cloud strategy, and that the cloud strategy itself is still viable.

The continual improvement practice guide provides detailed guidance on continual improvement, and the continual improvement model, shown in Figure 0.3 in the ITIL Foundation recap section at the beginning of this guide, can be discussed in the context of cloud services and the value co-creation map.

8.4.1 What is the vision? Defining and refining the cloud vision

Definition: Vision

A defined aspiration of what an organization would like to become in the future.

A cloud vision reflects the consumer organization's strategic objectives and mission. The organization should first define its cloud strategy in the explore and engage stages of the cloud customer journey. However, because cloud service offerings continually evolve, a consumer organization's cloud vision should be revised regularly (along with the cloud strategy and service requirements) to maximize value realization. As it uses more cloud services, its needs will mature and become more complex.

Important considerations when revising the cloud vision include:

- **Cloud usage trends** How are competitors or peer organizations using cloud solutions? What trends and patterns can be seen in cloud consumer requests and requirements?
- **CSP and partner roadmaps** What are the CSPs and partners working on? Are they moving away from or towards any particular area of cloud service provision?
- **Service feedback** What are cloud service consumers saying about the services?
- **The current vision** Does the current vision align to identified trends? Does it need to evolve and improve in order to ensure clear direction?
- **Other areas of alignment** How is the cloud strategy currently aligned with other organizational and IT strategies?

8.4.2 Where are we now? Reviewing the current state

When the cloud strategy and vision are reviewed and optimized, the next step is to determine how the organization is currently delivering against them.

In the engage step, the organization should perform a cloud readiness assessment to determine its operating model's ability to create, deliver, support, and govern cloud services in collaboration with CSPs or partners. It should assess its operating model thoroughly at first and after significant changes, and also should perform regular high-level assessments.

Important considerations when reviewing an organization's current state include:

- **Proficiency** Are there gaps in or sub-optimal levels of value co-creation across the current operating model? How effective are cloud solution architectures that get migrated or built in the cloud? Is the cloud service portfolio performing as expected?
- **Alignment** Do the consumer organization's architecture standards and design patterns align with the CSP or partner best practices? Does the cloud service portfolio align to the appropriate cloud strategy and vision?
- **Backlog** What is the current architecture technical backlog for cloud services?
- **Trending issues** What are the trending incidents and problems? What are the current security incident trends? What are the trending cloud risks in the risk register?
- **Costs** What is the current cost of the cloud services? What return on investment is being achieved? Are cloud usage costs predictable and optimized?
- **Service level** What are the current service level trends? What is the service level performance of each service that the CSP or partner provides?
- **Customer experience** What is the current customer experience level for cloud services? What customer feedback trends are there?
- **Deployments** Are deployments effective? How does the overall cloud real estate compare with the intended cloud architectural standards?
- **Roadmap** Is the organization delivering against its cloud roadmap on time? What work is in progress for cloud services and feature development?

- **Staffing** What is the ratio of cloud-trained employees to non-trained employees?
- **Accessibility** What is the accessibility level of the cloud services?
- **Changes** Are the service changes streamlined and integrated smoothly? Are the cloud services being adopted at a speed and cadence optimal for the organization?

8.4.3 Where do we want to be? Defining the future state

When an organization compares its current operating model against its cloud strategy and vision, gaps and alignment issues should become clear. These gaps and misalignments represent opportunities for improvement.

A new target operating model may be required to fulfil these opportunities. For example, if an organization has sub-optimal outcomes in several operational areas, it may need to define a more holistic approach in a target operating model.

A CSP, partner, or third-party consulting firm can help an organization to establish its target operating model; outside expertise can provide a blueprint for the future state that is aligned with industry best practice.

If the outcome of the comparison with the target operating model does not require a holistic change, a list of opportunities and risks relating to improving operational and strategic alignment should be defined and recorded in an improvement register.

Other considerations that need to be made when defining the future state include:

- **Culture** Does the current culture enable rapid change and continuous and adaptive learning?
- **Future roles** What skill sets and roles do we need to be more effective in the future? What do traditional cloud roles look like?
- **Structure** Do the organizational structure and governance structures foster autonomous decision-making?
- **Co-creation** What are the relationships with CSPs and partners like? Can a contract-driven mindset transition into a value co-creation approach?
- **Toolsets** How will the target operating model use and integrate CSP toolsets, such as service health dashboards, advisories, roadmaps, knowledge repositories, support procedures, and change models?
- **Improvements** Has the CSP or partner identified improvements or risks that can be addressed through an improvement programme?

8.4.4 How do we get there? Defining the roadmap to the future state

If the organization has defined one, the new target operating model should be carefully compared with the existing operating model to determine the gaps between the two. From this comparison, the organization can define a transitioning roadmap, which may include:

- new or amended processes
- upskilling and training plans
- organizational or committee restructuring
- hiring for new roles

- implementation or integration of technology and tools provided by the CSP or partner
- new CSP or partner agreements.

Some areas of the target operating model can be outsourced to a managed service provider. Organizations often choose to outsource because it can be cost effective and can increase proficiency. Questions that can help determine whether outsourcing is feasible include:

- Is this area of the operating model central to the business and to value realization?
- Would outsourcing be cost effective?
- Would outsourcing give the organization access to useful skills, expertise, and infrastructure?
- Would outsourcing help the organization to realize the cloud strategy and vision?

An organization should not outsource key strategic areas, as this could put it at significant risk of losing control of its value proposition or its ability to deliver value. When an organization outsources a part of its operating model, it is still accountable for the successful outcomes of that area.

If the organization has not defined a new target operating model, the cloud improvement opportunities registered in the improvement backlog should be prioritized.

The CSP or partner should be involved in enabling improvements.

8.4.4.1 Improvement initiatives

Organizations usually cannot afford to wait significant periods of time for their improvement initiatives to be implemented. Successful implementation requires a culture of continuous delivery, and all improvement initiatives should be placed into a continual improvement backlog. They should also be recorded as iterations that are small enough to work on as one project.

The initiative backlog can then be prioritized based on each initiative's anticipated value. There are many prioritization methods available, including:

- MoSCoW
- HiPPO
- return on investment
- cost of delay.

Profitability criteria include how much the initiative is expected to:

- increase or influence revenue, such as by increasing consumption of paid-for services
- protect revenue, such as by sustaining current service value against competing alternatives
- reduce costs, such as by optimizing existing costs
- avoid extra costs, such as by keeping current costs constant.

Another factor is how long it would take for all of the iterations of an improvement to be established and for the full anticipated value to be realized.

The cost of delay can be calculated as:

Increase revenue + Protect revenue + Decrease costs + Avoid costs = Contributors to profitability

Contributors to profitability / (52 × Length of time to realize value in weeks) = Cost of delay

This calculation provides a strong index that can help the organization to prioritize. However, it is not a tool for forecasting and should be used only as a guideline.

For non-profit or subsidized organizations, the revenue factors can be replaced with an alternative, such as a customer experience score.

An organization should establish a minimal viable product mindset when starting a large improvement initiative, aiming to refine and add to the initiative iteratively until it is a fully implemented improvement.

A consumer organization should include its CSP and partner in the prioritization discussions, so that it can highlight the amount of work needed for each initiative, point out potential pitfalls, and agree on the most effective way to deliver value.

8.4.5 Take action: Executing the adoption roadmap

If an organization has decided to outsource areas of its operating model, it needs to start at the engage step (to determine which CSP or partner will ensure the best results) and then continue on through the rest of the customer journey.

The improvements in the backlog, if prioritized correctly, can be accomplished through Agile frameworks or methods, such as Kanban or Scrum, which will help to achieve a continuous flow of improvement within the organization.

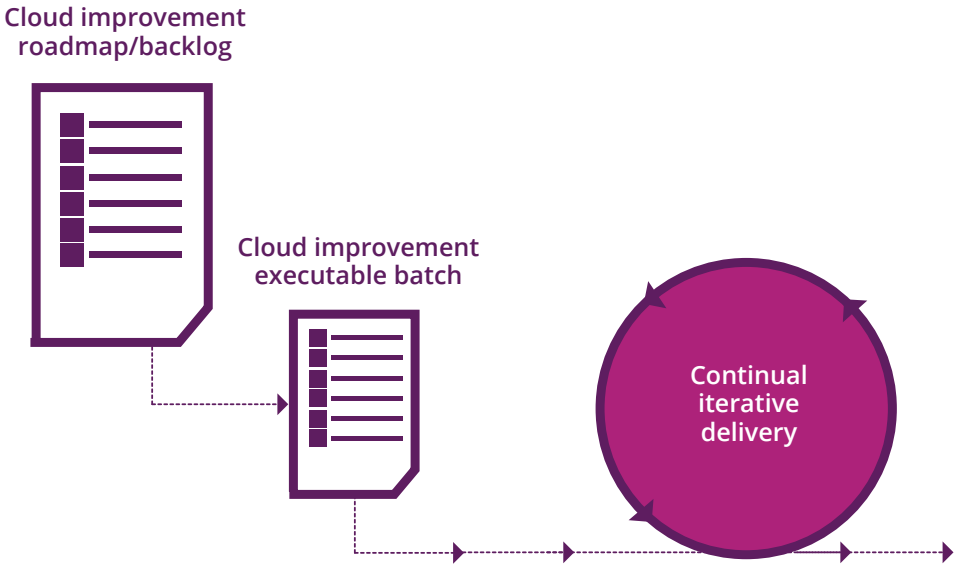

Figure 8.2 Delivery of cloud improvements

As shown in Figure 8.2, an organization can batch initiative iterations into sprints, based on priority. Metrics such as cumulative flow diagrams, cycle and lead times for Kanban, and burndown charts or sprint velocity for Scrum, can be used to measure the effectiveness of the ongoing delivery of the improvement backlog.

Important questions that can help assess whether the improvement delivery will be successful include:

- Does the organization include teams that are familiar with Agile delivery, and are there tools to support it? If the organization does not have this experience, teams should practise in Agile delivery techniques.
- Is the organization structured to enable continuous improvement delivery?
- Is there a culture of collaboration between development and operational teams?

- Are steering committees established to coordinate and direct multiple teams and enable Agile autonomous decision-making?
- Does the consumer organization currently deliver on initiatives with the CSP or partner using Agile methods?
- How will improvements be aligned with cloud standard architectures and best practices provided by both the organization and the CSP or partner?

8.4.6 Did we get there? Evaluating objectives and key results

An organization should define objectives and key results (OKRs) for each improvement initiative and iteration to determine how success will be measured. Key results should be associated with key metrics that will be continually reviewed.

A consumer organization should engage with its CSP or partner to understand what metrics and cloud solutions can be used to effectively measure and report back on its OKRs. Clear OKRs allow a consumer organization to objectively evaluate whether or not improvements have been effectively achieved.

Example

An organization wants to improve its cloud governance and control.

Objective 1: Ensure that cloud platforms and services are effectively governed so that they provide transparency and safety for cloud service consumers.

Key results:

1. Ensure 95% compliance for cloud asset tagging for ownership, application, environment, and cost centre.
2. Ensure that cloud budgets are established for all subscriptions and resource groups. There should not be more than a 10% breach of cloud budget spend.
3. Ensure that a role-based access control model is defined and automated.
4. Ensure that compliance with the defined cloud policy does not drop below 97%.
5. Ensure 0% configuration drift of estate.
6. Ensure that security compliance is maintained at 100% within production.

Objective 2: Streamline and improve the quality of the cloud support experience.

Key results:

1. Increase the first-call resolution percentage of cloud service incidents by 40%.
2. Achieve a customer net satisfaction level of 90%, and obtain 40% of customer feedback from surveys to identify improvement areas.
3. Identify and report on the top ten trending incidents and problems, and achieve a 10% reduction on the top ten reports every 2 months.
4. Ensure functional escalation of incidents is kept below three re-allocations on average.
5. Ensure 95% of incidents are resolved within the agreed time.

Important questions that can help an organization to evaluate its improvement achievement rate include:

- Who will own the improvement portfolio and review the improvement OKR results?
- Were the OKRs defined by the right audience, and do they correctly address the organization's anticipated cloud use?
- Are the metrics used to measure achievement of the OKRs appropriate?
- Has the organization defined what is 'good enough' for cloud? In other words, is it investing in improvements that have little or no actual value?

8.4.7 How do we keep the momentum going? Refine the approach and repeat

Continual improvement does not stop when one round of improvements has been made. Especially in the dynamic world of cloud services, when technologies and approaches continually change, organizations need to continually evolve and improve.

The OKRs for an improvement initiative, when they have been achieved, should form the baseline of the next improvement. This ensures that improvements do not regress. Further improvements can be built on top of this baseline, and then in turn become the new baseline, as shown in Figure 8.3.

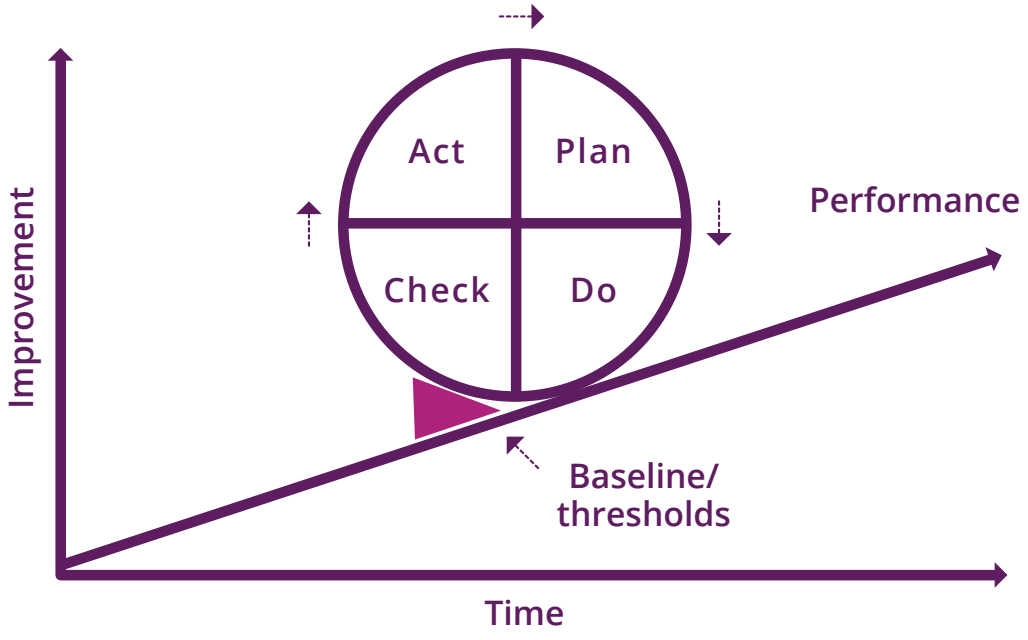

Figure 8.3 The Plan-Do-Check-Act (PDCA) cycle with baselining

An organization should also continually improve its continual improvement practice. This will help to ensure that a mechanism for rapid continual improvement is in place so that the organization can evolve. The practice should be continually reviewed to ensure that it is enabling the delivery of improvements at an acceptable speed, cost, and level of quality. The practice should have OKRs and key metrics to ensure that performance can be measured and baselined, and to ensure that performance does not regress.

Considerations that can help with improvement momentum include:

- There should be an initial deep assessment to report on the proficiency of the operating model, which should then be maintained through quick health and readiness checks.
- Several elements of continual improvement should be assessed, including:
  - the rate at which improvements need to be produced to meet demand
  - the time taken for improvements to be implemented
  - the average number of improvements being worked on per week or per month.
- Automation and cloud reference architectures and standards can be used to ensure that anything provisioned to the cloud is done so in a repeatable and standardized way. Infrastructure as a code (IaaC) and configuration as a code (CaaC) can be used to define declarative scripts that incorporate all cloud architecture standards and references.
- Cloud policy enforcement and other governance tools can help ensure that compliance with cloud reference architectures or standards can be reported on. Deployments can be obstructed if the code does not meet the standards.
- An organization should work with the CSP and partner to use governance tools to control the cloud estate, to prevent configuration drift and compliance regression.
- An organization can establish key thresholds to ensure that regression in improvements and performance can be identified and addressed.

In a VUCA environment, the PDCA cycle must be accelerated, lessons learned must be validated, and improvements must be made incrementally. This accelerated cycle is illustrated in Figure 8.4.

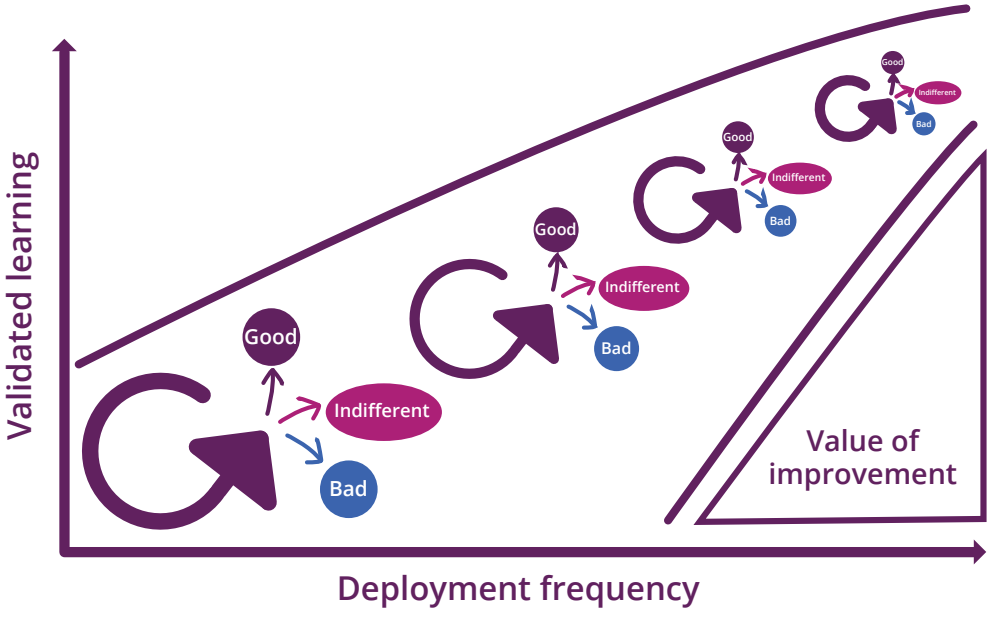

Figure 8.4 Continual improvement with purpose

In Figure 8.4 a plan, do, check, act cycle is performed. The intended and unintended consequences are analysed and compared with the purpose of the initiative (or strategy). Good aspects are retained as part of the next iteration. Indifferent or neutral aspects are analysed to determine whether they could be improved as part of the next cycle or whether they are unnecessary. Bad aspects (those that detract from the purpose or cause waste or unnecessary expense) need to be discarded or fixed in the next cycle.

The more each cycle teaches the organization, the faster it can move, the more it can improve, and the higher the value of those improvements.

8.5 Summary

Success should never be disputable; therefore, the facilitation of co-created value must be continually validated, reported, and communicated. These activities will inform potential modifications to the consumer organization's operating model and cloud strategy. The benefits of an ongoing analysis of value co-creation can be long term as well as short term; for example, lessons learned should become the basis for continual improvement. Continual evaluation and improvement actions also increase the consumer organization's capability to react and adapt to VUCA contexts.

CHAPTER 9

CONCLUSION

9 Conclusion

This publication has explored the key elements of an organization's acquisition and use of cloud services. It has examined the steps an organization will follow, including:

- deciding how cloud services will help it to meet its strategic and operational objectives
- engaging with one or more cloud service providers (CSPs)
- selecting the most appropriate services and service providers
- onboarding and using the selected services
- evaluating whether its use of cloud has enabled it to achieve its objectives and identify ways to improve the way they acquire, use, and manage cloud services.

Cloud services are delivered to consumer organizations by CSPs and their partners. Effectively selecting and using those services involves a complex process of exploration, evaluation, selection, and use that takes place within a specific type of consumer/provider relationship. The customer journey described in *ITIL® 4: Drive Stakeholder Value* is a good framework for managing this process.

This publication should be studied alongside the ITIL practice guides, which are available online and provide detailed practical recommendations for all 34 management practices. They include hands-on guidance that can be applied in the context of all ITIL 4 publications. Appendix A contains information about which practices are most relevant to the acquisition and use of cloud services.

All ITIL publications are holistic and focused on value. They address the four dimensions of service management and help to manage resources in a way that enables value creation for the organization, its customers, and other stakeholders.

ITIL® 4: Digital and IT Strategy provides guidance on how to influence and drive strategic decisions that enable an organization to provide value to its customers and to remain viable by adapting in an ever-changing environment characterized by the innovative use of digital technology.

ITIL® 4: Create, Deliver and Support provides guidance on the cultural and team management aspects of product and service management, and an overview of the various tools and technologies that support service management. It demonstrates how to integrate management practices into end-to-end value streams.

ITIL® 4: Direct, Plan and Improve provides guidance on aligning product and service management with today's business requirements, driving successful organizational transformation, and embedding continual improvement into an organization's culture at every level.

ITIL® 4: Drive Stakeholder Value contains guidance on establishing, maintaining, and developing effective service relationships. It leads organizations on a service journey in their roles as service provider and service consumer, helping them to interact and communicate effectively at every step.

ITIL® 4: High-velocity IT provides detailed guidance on comprehensive digital transformation and helps organizations to evolve towards a convergence of business and technology, or to establish a new digital organization.

APPENDIX A

ITIL PRACTICES AND THE CUSTOMER JOURNEY

Appendix A: ITIL practices and the customer journey

This appendix is a common mapping of ITIL practices against steps of the cloud customer journey, showing how involved or useful the practices are for each set of activities. Table A.1 shows each practice mapped against each step of the customer journey, where the darker shade indicates a more involved or useful practice.

The practices and most relevant steps of the customer journey are discussed in more detail in the sections that follow.

A.1 General management practices

A.1.1 Architecture management

The architecture management practice contributes to:

- **Explore** Provides the organization with an understanding of the current architecture and desirable future states that align with the organization's vision and strategy
- **Onboard** Provides the resources needed to transition key products, services, and operating model(s) to the desired cloud-oriented architecture(s) (may be responsible for updating policies, procedures, and other artefacts)
- **Co-create** Provides the resources needed to create, modify, and manage cloud product or service architecture
- **Realize** Provides the resources needed to analyse and assess whether the transition to and consumption of cloud services enabled the organization to meet its architectural objectives.

A.1.2 Continual improvement

The continual improvement practice contributes to:

- **Explore** Allows the organization to identify and highlight key tactical or operational activities or improvement opportunities
- **Onboard** Allows the organization to assess and incorporate new information so that onboarding efforts are executed more effectively and efficiently, or to improve
- **Co-create** Allows the organization to assess and incorporate new information to continue to improve
- **Realize** Allows the organization to assess data from the consumption of cloud services, and to identify and execute on opportunities to improve.

Table A.1 Heat map of practices against steps of the customer journey

	Explore	Engage	Offer	Agree	Onboard	Co-create	Realize
Architecture management	Useful				Most useful	Most useful	Useful
Continual improvement	Useful	Less useful	Less useful	Less useful	Useful	Most useful	Most useful
Information security management	Less useful	Less useful	Less useful		Most useful	Most useful	Most useful
Knowledge management	Useful				Most useful	Most useful	Less useful
Measurement and reporting	Less useful	Less useful	Less useful	Less useful	Useful	Most useful	Most useful
Organizational change management	Useful				Most useful	Less useful	Useful
Portfolio management	Useful		Less useful	Less useful	Useful	Most useful	Useful
Project management	Less useful	Less useful	Useful	Useful	Most useful	Useful	Less useful
Relationship management	Less useful	Useful	Useful	Most useful	Useful	Useful	Useful
Risk management	Less useful	Less useful	Less useful	Useful	Most useful	Useful	Most useful
Service financial management			Useful	Most useful	Useful	Useful	Most useful
Strategy management	Most useful	Useful	Useful	Less useful		Useful	Most useful
Supplier management	Less useful	Useful	Useful	Most useful	Useful	Less useful	Useful
Workforce and talent management	Less useful				Most useful	Most useful	Useful
Availability management	Less useful	Less useful	Less useful		Most useful	Most useful	Useful
Business analysis	Useful	Less useful	Most useful	Useful	Most useful	Useful	Most useful
Capacity and performance management	Less useful	Less useful	Less useful		Most useful	Most useful	Useful
Change enablement	Less useful		Less useful		Most useful	Most useful	Useful
Incident management	Less useful		Less useful		Useful	Most useful	Less useful
IT asset management	Less useful		Less useful		Useful	Less useful	Less useful
Monitoring and event management	Less useful		Less useful		Useful	Most useful	Less useful
Problem management	Less useful		Less useful		Useful	Most useful	Most useful
Release management	Less useful		Less useful		Most useful	Most useful	Less useful
Service catalogue management	Less useful		Less useful		Useful	Most useful	Less useful
Service configuration management	Less useful		Less useful		Most useful	Most useful	Less useful
Service continuity management	Less useful		Less useful		Useful	Most useful	Less useful
Service design	Less useful		Less useful		Useful	Useful	Less useful
Service desk	Less useful		Less useful		Useful	Most useful	Less useful
Service level management	Less useful		Less useful	Less useful	Useful	Most useful	Less useful
Service request management	Less useful		Less useful		Useful	Most useful	Less useful
Service validation and testing	Less useful		Less useful		Useful	Most useful	Less useful
Deployment management	Less useful		Less useful		Most useful	Most useful	Less useful
Infrastructure and platform management	Less useful	Less useful	Less useful		Useful	Most useful	Less useful
Software development and management	Less useful	Less useful	Less useful		Useful	Most useful	Less useful

- Most useful
- Useful
- Less useful
- Not applicable

A.1.3 Information security management

The information security management practice contributes to:

- **Onboard** Provides the resources needed to ensure that product and service management activities remain compliant with information security policies and controls (may also be responsible for updating policies, procedures, and other artefacts used when creating new products and services)
- **Co-create** Provides the resources needed to create, mitigate, and manage information security risks
- **Realize** Provides the resources needed to analyse and assess whether the transition to and consumption of cloud services enabled the organization to meet its information security objectives.

A.1.4 Knowledge management

The knowledge management practice contributes to:

- **Explore** Collects, maintains, and shares information about the current strengths and weaknesses present in the internal and external environments
- **Onboard** Provides the resources needed to collect, maintain, and share information about the chosen cloud solution and the changes made to the service value system during onboarding
- **Co-create** Provides the resources needed to collect, maintain, and share information about the usage of the cloud solution.

A.1.5 Measurement and reporting

The measurement and reporting practice contributes to:

- **Onboard** Collects data and reports on activities to introduce the cloud solution(s) into the organization and to retire incumbent solution(s)
- **Co-create** Collects data and reports on the service utilization
- **Realize** Enables data-driven decisions on the continued use of the service through service consumption reporting.

A.1.6 Organizational change management

The organizational change management practice contributes to:

- **Explore** Provides the resources needed to complete an organizational readiness assessment that can facilitate subsequent steps of the cloud customer journey
- **Onboard:**
  - Provides tools and approaches to design and manage the changes to roles and responsibilities, skills, team structures, and other human aspects of onboarding
  - Allows the organization to identify residual risks that may require longer-term plans or interventions when the onboarding/offboarding is complete
- **Realize** Provides data and information on the successes and failures of the organizational change.

A.1.7 Portfolio management

The portfolio management practice contributes to:

- **Explore** Provides information on the organization's current portfolios, upcoming changes, and the aspirational state of the portfolios
- **Onboard** Provides the tools needed to capture and share information about changes being made to certain products, services, projects, and programmes
- **Co-create** Provides the tools needed to ensure that the organization is investing in an optimal mix of products, services, projects, programmes, suppliers, and so on
- **Realize** Provides data and information on the successes and failures of cloud service adoption, enabling the organization to understand whether its strategic or tactical goals have been met.

A.1.8 Project management

The project management practice contributes to:

- **Offer** Provides the resources needed to define commercial and technical requirements
- **Agree** Provides the resources needed to negotiate and agree commercial terms with the cloud service provider (CSP)
- **Onboard:**
  - Provides the resources needed to migrate to the new platform
  - Enables the modification of processes, skills, templates, and other artefacts to support future projects
- **Co-create** Provides the resources needed to co-create value by organizing work around projects and programmes.

A.1.9 Relationship management

The relationship management practice contributes to:

- **Engage** Provides the skills and resources needed to build effective relationship with CSPs
- **Offer** Provides the skills and resources needed to consolidate key requirements across multiple stakeholder groups and to define the scope of future engagement and activities
- **Agree** Provides the skills and resources needed to negotiate and agree operational and commercial terms of engagement and contracts
- **Onboard** Provides the resources needed to manage important relationships within the organization and externally
- **Co-create** Provides the resources needed to manage important relationships and escalations within the organization and externally
- **Realize** Provides the resources needed to manage important relationships within the organization and externally; it analyses the usage of cloud solutions and manages the resulting divergences or alignments with the organizational strategy.

A.1.10 Risk management

The risk management practice contributes to:

- **Agree** Supports the organization with the resources needed to negotiate with the chosen CSPs to agree the commercial terms, and to understand how the organization's risk profile and appetite change as a result
- **Onboard** Enables the organization to identify changes to the organization's risk profile and appetite as it transitions to the use of the chosen CSPs
- **Co-create** Enables the organization to identify and manage risks at strategic, tactical, and operational levels as it consumes cloud services and solutions
- **Realize** Provides the resources needed to analyse and assess data from cloud service consumption, in order to understand if these services have enabled the organization to better manage organizational risks.

A.1.11 Service financial management

The service financial management practice contributes to:

- **Offer** Enables the organization to articulate its financial constraints and considerations
- **Agree** Enables the organization to negotiate and agree the optimal financial terms
- **Onboard** Enables the organization to track and manage the costs of transitioning to the chosen CSP, and modifies the processes, skills, templates, and other artefacts needed to support future budgeting and accounting activities
- **Co-create** Enables the organization to project, track, and manage the ongoing cloud consumption costs
- **Realize** Enables the organization to assess whether the transition to and ongoing consumption of cloud services have and continue to meet the organization's financial strategy and projected return on investment.

A.1.12 Strategy management

The strategy management practice contributes to:

- **Explore** Enables the organization to understand the role that cloud solutions could have in enabling desirable strategic outcomes and the likely impact on the organization's (or competitor's) strategies
- **Engage** Enables the organization to identify cloud solutions and providers that align with their vision, strategy, and objectives
- **Offer** Enables the organization to articulate its strategy and service requirements
- **Co-create** Enables the organization to maintain, manage, and update its strategy as the cloud solution is used to co-create value
- **Realize** Enables the organization to understand whether strategic objectives have been met and whether the cloud solutions remain a strategic fit (providing the resources needed to update the strategy as required).

A.1.13 Supplier management

The supplier management practice contributes to:

- **Engage** Enables the organization to begin discussions with CSPs
- **Offer** Enables the organization to consolidate and articulate technical and non-technical service requirements
- **Agree** Provides the resources needed to select CSPs and negotiate terms and conditions
- **Onboard** Provides the resources needed to manage onboarding
- **Realize** Enables the organization to determine whether the CSPs and contracts have allowed the organization to fulfil its service requirements.

A.1.14 Workforce and talent management

The workforce and talent management practice contributes to:

- **Onboard** Enables the organization to understand the skills needed to benefit from the cloud solutions
- **Co-create** Enables the organization to plan and manage staff skills and capabilities across multiple teams
- **Realize** Enables the organization to determine whether the changes to staff skills and capabilities have delivered the expected return on investment and to identify opportunities to develop talent based on historical data and organizational strategy.

A.2 Service management practices

A.2.1 Availability management

The availability management practice contributes to:

- **Onboard** Provides the resources needed to migrate key products and services, and updates goals, policies, KPIs, tools, and processes to enable the achievement of availability targets
- **Co-create** Enables the organization to monitor the availability of products and services and manage risks and breaches
- **Realize** Enables the analysis of data to determine whether availability goals have been met.

A.2.2 Business analysis

The business analysis practice contributes to:

- **Explore** Provides information about which strategic, tactical, and operational goals, KPIs, or metrics might be impacted by cloud service adoption

- **Offer** Supports the organization in consolidating requirements and assessing cloud solutions against them
- **Agree** Supports the organization in analysing contracts, terms, and conditions, and recommending solutions, as well as updating policies, KPIs, tools, and processes to reflect the impact of cloud services on the organization's activities
- **Onboard** Provides the resources needed to support onboarding by identifying and analysing requirements and helping to plan migration activities
- **Co-create** Enables the definition of requirements and recommends cloud solutions to fulfil them
- **Realize** Enables the analysis of data to determine whether strategic, tactical, and operational goals have been met.

A.2.3 Capacity and performance management

The capacity and performance management practice contributes to:

- **Onboard** Provides the resources needed to migrate key products and services to the chosen cloud solution and updates goals, policies, KPIs, tools, and processes
- **Co-create** Enables the monitoring of the capacity and performance of products and services, and manages any risks or breaches
- **Realize** Enables the analysis of data to determine whether capacity and performance goals have been met.

A.2.4 Change enablement

The change enablement management practice contributes to:

- **Onboard** Provides the resources needed to assess, authorize, schedule, and manage changes, and updates goals, policies, KPIs, tools, and processes to reflect changed cloud services
- **Co-create** Enables the organization to successfully assess, authorize, schedule, and manage changes to products and services that are reliant on cloud solutions.

A.2.5 Incident management

The incident management practice contributes to:

- **Onboard** Provides the resources needed to manage incidents impacting existing products and services during onboarding, and updates goals, policies, KPIs, tools, and processes to reflect the changed cloud services
- **Co-create** Enables the organization to successfully manage incidents in the cloud space.

A.2.6 IT asset management

The IT asset management practice contributes to:

- **Onboard** Provides the resources needed to manage IT assets being onboarded or decommissioned, and updates goals, policies, KPIs, tools, and processes to reflect the changed cloud services.

A.2.7 Monitoring and event management

The monitoring and event management practice contributes to:

- **Onboard** Provides the resources needed to monitor and manage events during onboarding, and updates goals, policies, KPIs, tools, and processes to reflect the changed cloud services
- **Co-create** Enables the organization to successfully monitor and manage events and build effective monitoring and event management solutions.

A.2.8 Problem management

The problem management practice contributes to:

- **Onboard** Provides the resources needed to identify and manage underlying problems, errors, and workarounds, and updates goals, policies, KPIs, tools, and processes
- **Co-create** Enables the organization to identify and manage problems, errors, and workarounds that impact product or service components which have been built with cloud technologies or solutions
- **Realize** Provides the resources needed to analyse historical data to identify problems, errors, and workarounds that need to be managed or mitigated, and shares historical data to enable the organization to determine whether operational and tactical goals are being met.

A.2.9 Release management

The release management practice contributes to:

- **Onboard:**
  - Provides the resources needed to release previously configured cloud platforms or solutions to internal users, as well as to release migrated products, services, or service components
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
  - May be involved in offboarding the organization from incumbent products, services, platforms, or solutions
- **Co-create** Enables the organization to successfully manage the release of products, services, and service components, as well as new or changed cloud solutions.

A.2.10 Service catalogue management

The service catalogue management practice contributes to:

- **Onboard** Provides the resources needed to update or create the service catalogue, and updates goals, policies, KPIs, tools, and processes
- **Co-create** Enables the organization to successfully manage and maintain its service catalogue to reflect the ongoing and evolving use of cloud services.

A.2.11 Service configuration management

The service configuration management practice contributes to:

- **Onboard:**
  - Provides the resources needed to define new configuration management databases, configuration item classes, and relationships
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
  - May be involved with offboarding the organization from incumbent products, services, platforms, or solutions
- **Co-create** Enables the organization to successfully manage service configuration data.

A.2.12 Service continuity management

The service continuity management practice contributes to:

- **Onboard:**
  - Provides the resources needed to evolve and transition existing service continuity plans to reflect the use of cloud services and retire continuity plans that are no longer needed
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
- **Co-create** Enables the organization to successfully manage the service continuity data of products, services, and service components.

A.2.13 Service design

The service design practice contributes to:

- **Onboard:**
  - Provides the resources needed to design the users' experience of consuming cloud services
  - Evolves the design of products, services, or service components that are migrated
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
  - Updates the users' experience of products, services, platforms, or solutions as they are retired and replaced by cloud solutions
- **Co-create** Enables the organization to design and manage the users' experience of products, services, and service components that leverage the cloud solutions.

A.2.14 Service desk

The service desk practice contributes to:

- **Onboard** Updates goals, policies, KPIs, tools, teams, and processes to reflect the organization's use of cloud services, and transitions tools, teams, value streams, and processes to leverage the new cloud solutions
- **Co-create** Enables the organization to leverage service desk resources to capture demand for incident resolution and service requests for products, services, and service components.

A.2.15 Service level management

The service level management practice contributes to:

- **Onboard:**
  - Provides the resources needed to update and manage existing service targets and service level targets attached to the products, services, and service components being migrated to the chosen cloud solutions
  - Updates policies, KPIs, tools, and processes to reflect the impact of cloud services and solutions on the organization's service level management activities
- **Co-create** Enables the organization to continue to define and manage service targets and service level agreements.

A.2.16 Service request management

The service request management practice contributes to:

- **Onboard:**
  - Provides the resources needed to define and manage new or impacted request models to reflect the use of the cloud services
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
  - Offboards the organization from incumbent products, services, platforms, or solutions
- **Co-create** Enables the organization to successfully manage service requests related to products, services, and service components.

A.2.17 Service validation and testing

The service validation and testing practice contributes to:

- **Onboard:**
  - Provides the resources needed to test and validate previously configured cloud platforms or solutions before they are released to internal users
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
  - Offboards the organization from incumbent products, services, platforms, or solutions
- **Co-create** Enables the organization to successfully manage the validation and testing of products, services, and service components, as well as of new or changed cloud solutions or features.

A.3 Technical management practices

A.3.1 Deployment management

The deployment management practice contributes to:

- **Onboard:**
  - Provides the resources needed to define new or changed deployment management processes, procedures, automation, roles, and responsibilities
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
  - Offboards the organization from incumbent products, services, platforms, or solutions
- **Co-create** Enables the organization to successfully manage the deployment of product or service components.

A.3.2 Infrastructure and platform management

The infrastructure and platform management practice contributes to:

- **Onboard:**
  - Provides the resources needed to define new or changed infrastructure and platform management processes, procedures, automation, roles, and responsibilities
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
  - Offboards the organization from incumbent infrastructure and platform products, tools, services, or solutions
- **Co-create** Enables the organization to successfully manage infrastructure and platforms.

A.3.3 Software development and management

The software development and management practice contributes to:

- **Onboard:**
  - Provides the resources needed to define new or changed software development and management processes, procedures, automation, roles, and responsibilities
  - Updates goals, policies, KPIs, tools, and processes to reflect the organization's use of cloud services
  - Offboards the organization from incumbent products, tools, services, or solutions
- **Co-create** Enables the organization to successfully manage software.

FURTHER RESEARCH

Further research

Axelos publications

ITIL® 4 practice guides are available through MyITIL: https://www.axelos.com/my-axelos/my-itil [accessed 06 September 2021].

Axelos (2021) *ITIL® 4: Sustainability in Digital and IT.* TSO, London.

Axelos (2021) *Management of Risk* (M_o_R). TSO, London.

Axelos (2020) *ITIL® 4: Create, Deliver and Support*. TSO, London.

Axelos (2020) *ITIL® 4: Digital and IT Strategy.* TSO, London.

Axelos (2020) *ITIL® 4: Direct, Plan and Improve*. TSO, London.

Axelos (2020) *ITIL® 4: Drive Stakeholder Value.* TSO, London.

Axelos (2020) *ITIL® 4: High-velocity IT.* TSO, London.

Axelos (2019) *ITIL® Foundation: ITIL 4 Edition.* TSO, London.

Axelos (2018) *A Guide to AgileSHIFT®.* TSO, London.

Axelos (2020) *Managing Successful Programmes.* TSO, London.

Axelos (2017) *Managing Successful Projects with PRINCE2®*. TSO, London.

Axelos (2015) *PRINCE2 Agile®.* TSO, London.

Axelos (2015) *RESILIA®: Cyber Resilience Best Practice.* TSO, London.

Office of Government Commerce (2010) *Management of Value.* TSO, London.

Other publications

Bakshi, V. (2017) *The Forward-Looking Manager in a VUCA World.* Sage Publications Pvt. Ltd.

Campbell, A., Gutierrez, M. and Lancelott, M. (2017) *Operating Model Canvas: Aligning Operations and Organization with Strategy.* Van Haren Publishing.

Hubbard, D. W. (2014) *How to Measure Anything: Finding the Value of Intangibles in Business*. 3rd edition, Wiley.

Mack, O., Khare, A., Kramer, A. and Burgartz, T. (2016) *Managing in a VUCA World.* Springer.

Wood, J.B., Hewlin, T. and Lah, T. (2011) *Consumption Economics: The New Rules of Tech.* Point B Inc.

Websites

Amazon web services. AWS Cloud Adoption Framework. Available at: https://aws.amazon.com/professional-services/CAF/ [accessed 06 September 2021].

Amazon web services. AWS Well Architected Framework. Available at: https://aws.amazon.com/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc [accessed 06 September 2021].

Amazon web services. What is Cloud Computing? Available at: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/what-is-cloud-computing.html [accessed 06 September 2021].

Australian Cyber Security Centre. Anatomy of a Cloud Assessment and Authorisation. Available at: www.cyber.gov.au/acsc/view-all-content/publications/anatomy-cloud-assessment-and-authorisation [accessed 06 September 2021].

CISPE. Buying cloud services in public sector handbook. https://cispe.cloud/website_cispe/wp-content/uploads/2019/05/Public-Policy-strategy-on-Procurement-Handbook-Final-190528.pdf

Center for Internet Security. CIS controls navigator. Available at: https://www.cisecurity.org/controls/cis-controls-navigator/ [accessed 06 September 2021].

Cloud Industry Forum (UK) (2014). Cloud Security Guidance: IaaS Consumer Guide. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/350981/Cloud_Security_Guidance_-_IaaS_Consumer_Guide.pdf [accessed 06 September 2021].

Cloud Industry Forum. 8 criteria to ensure you select the right cloud service provider. Available at: https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider [accessed 06 September 2021].

Cloud Security Alliance. How to share the security responsibility between the CSP and customer. Available at: https://cloudsecurityalliance.org/blog/2019/09/05/how-to-share-the-security-responsibility-between-the-csp-and-customer/ [accessed 06 September 2021].

CNIL. Recommendations for companies planning to use cloud computing service. Available at: www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles [accessed 06 September 2021].

EDUCAUSE. Cloud Computing and Services library of resources. Available at: https://library.educause.edu/topics/infrastructure-and-research-technologies/cloud-computing-and-services [accessed 06 September 2021].

European Data Protection Supervisor (2018). Guidelines on the use of cloud computing services by the European institutions and bodies. Available at: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf [accessed 06 September 2021].

Evrone (2020). Business and cloud computing – what to expect in 2020. Available at: https://vc.ru/evrone/107989-biznes-i-oblachnye-vychisleniya-chego-ozhidat-v-2020 [accessed 06 September 2021].

Government of Canada. Government of Canada Cloud Security Risk Management Approach and Procedures. Available at: www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-security-risk-management-approach-procedures.html [accessed 06 September 2021].

IBM, Wilson, M. (2018). Survey: Most companies use multicloud, but far less have tools for management. Available at: www.ibm.com/blogs/cloud-computing/2018/10/19/survey-multicloud-management-tools/ [accessed 06 September 2021].

IDC (2020). Spending on Public Cloud IT Infrastructure Surpasses Spending on Traditional IT Infrastructure for the First Time in the Second Quarter of 2020. Available at: www.idc.com/getdoc.jsp?containerId=prUS46895020 [accessed 06 September 2021].

Information Commissioner's Office (UK Government). Guidance on the use of cloud computing. Available at: https://ico.org.uk/media/fororganisations/documents/1540/cloud_computing_guidance_for_organisations.pdf [accessed 06 September 2021].

IT WORLD CANADA (2017). The cloud service broker – a necessary role? Available at: www.itworldcanada.com/blog/the-cloud-service-broker-a-necessary-role/390170 [accessed 06 September 2021].

KPMG (2016). Moving to the cloud – key considerations. Available at: https://assets.kpmg/content/dam/kpmg/pdf/2016/04/moving-to-the-cloud-key-risk-considerations.pdf [accessed 06 September 2021].

Microsoft, Lanfear T. (2021). Shared responsibility in the cloud. Available at: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility [accessed 06 September 2021].

Microsoft. Microsoft Azure Well-Architected Framework. Available at: https://docs.microsoft.com/en-us/azure/architecture/framework/ [accessed 06 September 2021].

Microsoft. Microsoft Cloud Adoption Framework for Azure. Available at: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ [accessed 06 September 2021].

Purdue University (2019). Cloud Computing Consumer Guidelines. Available at: www.purdue.edu/securepurdue/it-policies-standards/it-guidelines/cloud-computing-consumer-guidelines.php [accessed 06 September 2021].

R&A Enterprise Architecture. The many lies about reducing complexity part 2: Cloud. Available at: https://ea.rna.nl/2021/01/10/the-many-lies-about-reducing-complexity-part-2-cloud/amp/ [accessed 06 September 2021].

Vonya Global. Cloud Governance Counts: Understanding Cloud Governance and its Goals. Available at: www.vonyaglobal.com/internal-audit/knowledge/cloud-governance-counts/ [accessed 06 September 2021].

GLOSSARY

Glossary

aggregate CSP

Cloud service providers that offer a comprehensive blend of services using two or more cloud service models. *See also* infrastructure-as-a-service (IaaS); platform-as-a-service (PaaS); software-as-a-service (SaaS).

Agile

An umbrella term for a collection of frameworks and techniques that together enable teams and individuals to work in a way that is typified by collaboration, prioritization, iterative and incremental delivery, and timeboxing. There are several specific methods (or frameworks) that are classed as Agile, such as Scrum, Lean, and Kanban.

application programming interfaces (API)

A type of software interface that offers a service to other pieces of software, such as access to or transmission of data, according to predefined rules.

architecture

Architecture is the process of planning and designing how a solution, system, service, or organization are structured to meet a set of defined objectives. The product of architecture is a blueprint that shows which elements will be used, how they are related, and how they should be managed through their lifecycle.

artificial intelligence

Highly advanced automation that demonstrates capabilities of general reasoning, learning, and human-like intelligence; a branch of computer science and engineering focused on simulating intelligent behaviour in computer systems.

big-bang migrations

An approach to cloud migration that focuses on moving all identified components into the cloud as quickly as possible.

business case

A justification for the expenditure of organizational resources, providing information about costs, benefits, options, risks, and issues.

capital expenditure (capex)

The cost of purchasing something that will become a financial asset (e.g. computer equipment and buildings). The value of the asset depreciates over multiple accounting periods. *See also* operating expenditure (opex).

cloud migration

The process of moving applications, workloads, services, and/or data into, from, or between cloud environments.

cloud native

A solution that has been designed and built specifically to operate in the cloud.

cloud service

IT services (infrastructure, platforms, and software) that are hosted by third-party providers and made available on demand to users through the internet.

cloud service agreement (CSA)

A compilation of documents or agreements that contain the terms governing the relationship between the cloud customer and the cloud service provider (CSP). The CSA is the key output of the negotiation between a CSP and a service consumer.

cloud service provider (CSP)

An organization that offers private or public cloud-based infrastructure, platforms, or applications on an on-demand (or pay-per-use) basis.

cloud service provider (CSP) partner

An organization that is formally recognized by one or more CSPs, and which specializes in helping consumer organizations to plan for, prepare for, acquire, and use cloud services. Types of partner include resellers, brokers, consultancies, implementors, and solution developers.

cloud sprawl

Over-utilization of cloud services through duplication and failure to decommission services that are no longer used.

cloud strategy

The part of the digital strategy that refers to which cloud services will be used and how they will be acquired and used.

cloud, the

The provision of IT services that are available on demand, via the internet, from a pool of shared resources. These might be storage, processing facilities, operating systems, applications, functionality, development platforms, and/or IT management facilities.

continuous integration/continuous delivery

An integrated set of practices and tools used to merge developers' code, build and test the resulting software, and package it so that it is ready for deployment.

customer experience (CX)

The sum of functional and emotional interactions with a service and service provider as perceived by a customer.

customer journey

The complete end-to-end experience that service customers have with one or more service providers and/or their products through touchpoints and service interactions.

decision model

A way to break down and represent the steps and information required when making a complex business decision.

DevOps

DevOps is a combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity. DevOps focuses on culture, automation, Lean, measurement, and sharing (CALMS).

digital strategy

A business strategy that is based all or in part on using digital technology to achieve its goals and purpose.

digital transformation

The use of digital technology to enable a significant improvement in the realization of an organization's objectives that could not feasibly have been achieved by non-digital means.

disaster recovery

The formal plan and measures that enable an organization to restore key activities, systems, and facilities following a sudden unplanned event that causes great damage or serious loss. A disaster results in an organization failing to provide critical business functions for some predetermined minimum period of time.

disbenefit

A measurable decline resulting from an outcome perceived as negative by the investing organization(s) and which detracts from one or more organizational objectives.

elasticity

The extent to which capacity can be provided to services in order to match real-time demand and performance requirements.

failover

A mechanism that causes the system to switch automatically from an active to a redundant component when monitoring detects a failure.

feedback activity

The process of using the results and outputs of a step in the cloud customer journey to modify the next instance of an earlier step.

feedforward activity

The process of using the interim results and outputs of a step to modify a later step before the former step is complete.

framework agreement

A catalogue of agreements that have been negotiated and approved by an organization on behalf of multiple customers within the organization. Customers can select the service they need from a list of preferred service providers at rates, terms, and conditions that have been pre-negotiated.

governance

The means by which an organization is directed and controlled.

hybrid cloud

A combination of bespoke and standardized services from several internal and/or external service providers.

infrastructure-as-a-service (IaaS)

A service model that provides technology components, such as standardized infrastructure services on a pay-as-you-use or reserved-use basis. Using IaaS services abstracts the user from the hardware layer of the solution.

interoperability

The ability of computer systems or software from different vendors to operate together, and exchange and make use of information.

legacy system

An outdated IT system that is still in use.

middleware

Software that connects two or more software components or applications. Middleware is usually purchased from a supplier, rather than developed within the IT service provider.

minimal viable product

A product with just enough features to satisfy early customers, and to provide feedback for future product development.

multi-cloud

A deployment model in which a single workload can be spread across two or more cloud service providers.

multi-tenancy

A technology environment that is architected to support more than one customer at a time.

objectives and key results (OKR)

A framework for defining and tracking objectives and their outcomes.

operating expenditure (opex)

The cost resulting from running IT services, which often involves repeating payments such as staff costs, hardware maintenance, and electricity (also known as current expenditure or revenue expenditure). *See also* capital expenditure (capex).

operating model

A conceptual and/or visual representation of how an organization co-creates value with its customers and other stakeholders, as well as how the organization runs itself.

platform-as-a-service (PaaS)

A service model that provides an environment within which systems and solutions can be built. Using PaaS services abstracts the user from the infrastructure layer of the solution.

private cloud

A deployment model based on customized consumer requirements. A private cloud model is consumer centric, and each service is built specifically for individual consumers. This could be provided by an internal IT department or a service provider.

public cloud

A deployment model in which standard services using standardized components are delivered to a range of consumer organizations by a cloud service provider (CSP).

request for information

A technique used when requirements are unclear or incomplete and external assistance is needed to refine or add to them.

request for proposal

A formal document that provides background information and requirements to a short list of service providers, and invites them to submit a commercial proposal for products and services that meet or exceed the stated requirements.

return on investment

A measurement of the expected benefit of an investment. In the simplest sense, it is the profit of an investment divided by the costs invested. Most calculations will also include qualitative elements, such as the impact on culture and the perception of stakeholders.

scalability

The ability of an IT service, process, and so on to perform its agreed function when the workload or scope changes.

service catalogue

Structured information about all the services and service offerings of a service provider that are relevant for a specific target audience.

service level agreement (SLA)

A documented agreement between a service provider and a customer that identifies both the services required and the expected level of service.

shared responsibility model

A shared responsibility model defines the line between consumer and provider responsibilities. It should be tailored based on the service and the organizational context.

software-as-a-service (SaaS)

A service model that provides applications which can be used as they are, or with limited customization to suit a particular consumer. Using SaaS services abstracts the user from the underlying platform and infrastructure layers of the solution.

sustainability

A business approach focused on creating long-term value for society and other stakeholders by addressing the risks and opportunities associated with economic, environmental, and social developments.

technical debt

The total rework backlog accumulated by choosing workarounds instead of system solutions that would take longer.

utility

The functionality offered by a product or service to meet a particular need. Utility can be summarized as 'what the service does' and can be used to determine whether a service is 'fit for purpose'. To have utility, a service must either support the performance of the consumer or remove constraints from the consumer. Many services do both.

vendor lock-in

The dependency on a cloud service provider for services and the inability to use another vendor without substantial switching costs.

vision

A defined aspiration of what an organization would like to become in the future.

warranty

Assurance that a product or service will meet agreed requirements. Warranty can be summarized as 'how the service performs' and can be used to determine whether a service is 'fit for use'. Warranty often relates to service levels aligned with the needs of service consumers. This may be based on a formal agreement, or it may be a marketing message or brand image. Warranty typically addresses such areas as the availability of the service, its capacity, levels of security, and continuity. A service may be said to provide acceptable assurance, or 'warranty', if all defined and agreed conditions are met.

well-architected framework

Best-practice framework that has been created and adapted by major cloud service providers (CSPs) aiming to enable a secure, high-performing, and resilient infrastructure.

ACKNOWLEDGEMENTS

Acknowledgements

Axelos Ltd is grateful to everyone who has contributed to the development of this guidance and in particular would like to thank the following people.

Lead editor

David Cannon

David has been a service management practitioner and consultant for more than three decades. During that time he has seen the industry go through at least four technology-enabled shifts. David focused on understanding the core management disciplines that enabled organizations to successfully navigate each shift. He has contributed to ITIL by reviewing books in v2, co-authoring *Service Operation* (2007) and authoring *Service Strategy* (2011), and acting as joint lead editor on *ITIL® 4: Digital and IT Strategy* (2020). David has led consulting practices at Hewlett-Packard, BMC Software, and Forrester Research, supporting the definition and implementation of strategy at all levels in more than 250 organizations. David is a co-founder of *it*SMF International, and recipient of the *it*SMF Lifetime Achievement award.

Authoring team

Akshay Anand

Akshay is a veteran ITSM professional and keynote speaker with a wealth of experience from working with Fortune 100 companies in the US, UK, and India. He has had multiple roles in the industry, from leading complex ITSM tool implementation projects, to organizational transformations. Akshay is the product ambassador for ITIL, and has contributed to ITIL 4 as a lead architect, author, and reviewer, launching the Axelos podcast in 2020. He is passionate about modernizing and humanizing IT service management, and instilling empathy and ethics into teams and behaviours. He occasionally tweets as @ bloreboy.

Adam Griffith

Adam is an IT best-practice consultant at Axelos. Before 2021, he worked as a global technical trainer at New Horizons, specializing in all things ITIL and helping professionals to embrace best practice. He used practical experience from his previous role as a CIO to emphasize the importance of good service management, and was the top technical trainer in the US for the five years that he worked there. Adam is a master trainer for ITIL 4, a keen proponent of the ITIL guiding principles in all aspects of life, and a frequent contributor to digital publications on the Axelos site.

Richard de Kock

Richard is an award-winning business and IT strategy and management consultant who has worked across the world with organizations of all sizes and industry verticals. Richard has an MSc degree in service management and multiple certifications in governance, Lean, Agile, and organizational change management. He is an industry author and has contributed to several bodies of knowledge in the IT management domain, as well as formal research on digital transformation. Richard currently works for Microsoft®, specializing in the modernization of organizational strategies, operating models, and cloud capabilities using innovative technology to ensure a sustained competitive advantage.

Krikor Maroukian

Krikor is a principal service management consultant at Microsoft® and the international representative of *it*SMF Hellas. His past experience was in project management and information security management. Krikor is also a researcher at Henley Business School (UK) where he focuses on topics such as Agile software development, Lean IT, and high-performance service management. Krikor has authored academic papers on leadership, service management, DevOps, project management, and model-driven business process engineering. He was awarded the Emerald Literati Network Award for Excellence in 2017.

Alexey Petrov

Alexey is an IT adviser and freelance consultant. Based in Latin America and then in Moscow, Alexey has more than 13 years' experience with IBM technologies such as storage software, backup and archive solutions, cloud, and the IBM Maximo application suite. Alexey's previous position at Hewlett Packard Enterprise required him to lead teams of technical and process consultants, as well as project managers and software sales collaborators. Alexey has been involved in many service management projects, including IT4IT, ITIL 4, MoC, cloud, and DevOps initiatives.

Mark Smalley

Mark Smalley, also known as the IT Paradigmologist, is a writer, speaker and bridge builder at Smalley.IT. He helps people discover where they are and to visualize where they want to be. Mark's main area of interest is the management of IT systems and services. He has contributed to many bodies of industry knowledge and was lead editor of *ITIL® 4: High-velocity IT.*

Architect team

Laura Jones

Laura joined Amazon Web Services (AWS) in 2018 and is currently principal of Global Business Development and Solutions. Laura is a leading cloud acquisition expert with 13 years' experience in global business development and programme management. She has guided both governments and private-sector organizations in IT modernization and procurement strategy. In her current role, she designed and launched the cloud industry's first training course dedicated to helping customers acquire cloud. Prior to this, she was AWS's Capture & Deal Management lead for the One Government Value Agreement (OGVA), an agreement between AWS and the UK government to accelerate cloud adoption and innovation in the public sector.

Anthony Kelly

Anthony joined Amazon Web Services (AWS) in 2014 and is currently the senior manager for Global Business Development and Solutions. He is a leading industry expert in cloud acquisition, cloud policy, and public-sector digital transformation, with more than a decade of experience in helping governments plan and execute successful IT modernization initiatives. Anthony's publications include *Unpicking Vendor Lock-in – A guide to understanding and mitigating switching costs when changing your cloud services provider; 10 considerations for a cloud procurement;* and *Cloud Procurement: Best Practices for Public Sector Customers.*

Axelos ITIL 4 architect team

Akshay Anand	Product ambassador ITSM
Adam Griffith	Consultant, IT best practice
Philip Hearsum	ITIL portfolio manager
Vicky Hunter	Product manager
Roman Jouravlev	ITIL portfolio development manager
Margo Leach	Chief product officer

ITIL 4 lead editors

Dinara Adyrbayeva	ITIL 4 practice library
David Cannon	*ITIL® 4: Digital and IT Strategy*
Erika Flora	*ITIL® 4: Digital and IT Strategy*
Lou Hunnebeck	*ITIL® 4: Direct, Plan and Improve*
Antonina Klentsova	*ITIL® 4: Sustainability in Digital and IT*
Christian F. Nissen	*ITIL® 4: Drive Stakeholder Value*
Barclay Rae	*ITIL® 4: Create, Deliver and Support*
Stuart Rance	ITIL 4 examinations
Mark Smalley	*ITIL® 4: High-velocity IT*

Project team

David Atkins	Content delivery and production manager
Nicola Carrol	Project manager
Rachida Chekaf	Head of translations
Sarah Conner	Senior production editor
Adrian Crago-Graham	Head of PMO
Ricky Elizabeth	Brand and design manager
Joanna Fejklowicz	Project manager
James Lord	Senior qualifications and assessment specialist
Amy Metcalfe	Project editor
Oleksandra Spiegler	Qualifications and assessment specialist
Tom Young	Commissioning editor: ITIL core content

Contributors

Romuald Boutault, Dirk Brinkmann, Sean Burkinshaw, Alexander Dmitriev, Gabriela Feijoo Carrillo, Birgit Fiddelke, Leandro Frasso, Harold Groothedde, Jessica Hinkal, Kashyap Kompella, James Monek, Ryan Moodley, Jon Morley, Milton Nucci, Mark O'Loughlin, Mitch Pautz, Nicola Reeves, Minor Rojas, Gary Roos, Hilary Rosenfeld, Greg Sanker, Beti Simeonova.

INDEX

Index

A

acceptable use policies 72, 119
acquisition channels 89–90
aggregate CSPs 65, 67, 68
agree step of customer journey 116–125
anything-as-a-service (XaaS) 7
API vulnerability 50
application portfolios 41
application/workload-specific readiness checks 87
architecture management practice 160–161, 192
ARTS (Association for Retail Technology Standards) 71
Association for Retail Technology Standards (ARTS) 71
assurance 169
automation of security policies 141
availability management practice 159–160, 197

B

backup and data recovery 58
benefits of cloud services 10–12
big-bang migrations 37
billing 83, 105
'born in the cloud' scenario 36
BPaaS (business-process-as-a-service) 7
brokers 68, 123
business analysis practice 197
business cases 110–114
business-process-as-a-service (BPaaS) 7

C

capacity and performance management practice 160, 198
CCIF (Cloud Computing Interoperability Forum) 70
change enablement practice 158, 198
change management 75, 154–155
charging models 124–125
CISPE (Cloud Infrastructure Services Providers in Europe) 70
cloud
  adoption 26
  benefits 10–12
  commoditization 4–5
  definition 3
  disbenefits 10–12
  and innovation 5
  origins 3–6
  risks 12
  solutions 6–10
  strategic decisions 10–12
  utilization 26–30, 47
Cloud Computing Interoperability Forum (CCIF) 70
cloud consumer journey *see* customer journey
Cloud Infrastructure Services Providers in Europe (CISPE) 70
cloud management offices 74
cloud readiness assessments 84–87
Cloud Security Alliance 70
cloud service agreements (CSAs) 119–120
cloud service consumption 166–168
cloud service deployment models 66
cloud service integrators 67
cloud service model specialists 65–66, 68
cloud service models 7–8
cloud service providers (CSPs)
  aggregates 65, 67, 68
  definition 2–3
  engaging with 87–91
  implementation 69–70
  industry and regulatory organizations 70–71
  migrations 69–70
  migrations between 137–139
  partners 68–70, 124
  regulatory organizations 70–71
  requirements 82–83, 104
  responsibilities 17–19, 88, 121–122, 123
  services 65–68
  types of 9–10, 65–68
cloud service quality 6, 168–170
cloud service requirements 92
cloud strategies 35–36, 92
  abstraction levels 57–58
  elements 55–57
  formulation 55–58
  initial 53–61
  multiple 57
cloud tools 170–171
cloud usage strategy spectrum 27–29
cloud vision 180–181
cloud-compatibility 6
co-create step of customer journey 146–171
co-creation *see also* value co-creation
  costs 46–47
  models 151
  quality 169–170
commoditized digital solutions 4–5
communication channels for onboarding 132
compliance 141

consumer experience driver 153–155, 178
consumer responsibilities 19, 88, 122, 123
continual improvement xiv, 180–188
continual improvement practice 192
continuity management 161
cost management 5
cost reporting 83, 105
costs 44–47, 59, 79
CSAs (cloud service agreements) 119–120
CSP partners 68–70, 124
CSPs *see* cloud service providers
current state reviews 181–182
customer agreements 72, 119
customer enablement services 69
customer expectations 39
customer experience (CX) 76–77
customer impact 77–78
customer journey
  agree step 116–125
  co-create step 146–171
  cyclical activities in 22–23
  engage step 64–92
  explore step 32–61
  governance 16–17
  and ITIL practices 192–202
  offer step 94–113
  onboard step 128–143
  progress through 26
  realize step 174–188
  steps 20–21
customer requirements 39
customer responsibilities 19, 88, 122, 123
CX (customer experience) 76–77

D

data governance 60
data privacy 165
data recovery 58
data requirements 80–81, 103
delivery models 7–8
deployment management practice 202
deployment models 8–9
development methods 142
digital strategy 12–13, 33–35
digital transformation 13–14
disbenefits of cloud services 10–12
disputes 120
Distributed Management Task Force (DMTF) 70

E

elevating mutual capabilities 133
empathy 170
employee development 74
engage step of customer journey 64–92
event management 157–158
evolutionary migrations 37
exit strategies 139
explore step of customer journey 32–61
exploring cloud services costs 45
external factors 38–40

F

financial management 162, 196
flexibility of services 6, 60–61
four dimensions of service management xv
framework agreements 100–101
future state definition 182
future state roadmaps 182–185

G

general management practices 192–197
general service requirements 80
governance xiv, 6, 15–19, 59–60
governance and control driver 162–166, 180
greenfield scenario 36

H

HiPaaS (hybrid integration platform-as-a-service) 67
hub-and-spoke model 28
hybrid cloud 9
hybrid integration platform-as-a-service (HiPaaS) 67
hybrid IT 142

I

IaaS (infrastructure-as-a-service) 7–8, 66
implementation 69–70
improvement initiatives 183–185
improvement momentum 186–188
incident management practice 156, 198
industry and market opportunities and threats 39–40
industry and regulatory organizations 70–71
information security management practice 163–165, 194
infrastructure 5
infrastructure and platform management practice 202
infrastructure-as-a-service (IaaS) 7–8, 66
in-house solutions 58–62
initial cloud strategy 53–61
integration platform-as-a-service (iPaaS) 67
internal factors 40–42
iPaaS (integration platform-as-a-service) 67

IT asset management practice 198
ITIL guiding principles xiii, 133
ITIL practices xiii
  architecture management 160–161, 192
  availability management 159–160, 197
  business analysis 197
  capacity and performance management 160, 198
  change enablement 158, 198
  continual improvement 192
  deployment management 202
  general management practices 192–197
  incident management 156, 198
  information security management 163–165, 194
  infrastructure and platform management 202
  IT asset management 198
  knowledge management 194
  measurement and reporting 194
  monitoring and event management 157–158, 199
  organizational change management 154–155, 194
  portfolio management 153, 195
  problem management 157, 199
  project management 195
  relationship management 195
  release management 199
  risk management 165–166, 196
  service catalogue management 199
  service configuration management 200
  service continuity management 200
  service design 200
  service desk 200
  service financial management 162, 196
  service level management 154, 201
  service management practices 197–201
  service request management 201
  service validation and testing 201
  software development and management 202
  strategy management 152–153, 196
  supplier management 163, 197
  technical management practices 201–202
  workforce and talent management 197
ITIL service value chain xii
ITIL service value system xi

K

knowledge management practice 194

M

management control 6, 59–60
management offices 74
market opportunities and threats 39–40
market surveys 84
master service agreements 72
measurement and reporting practice 194
migration monitoring 73–74
migration services 73
migrations
  data governance 60
  existing services 36–37
  and onboarding 134–139
  risks 53
  SaaS (software-as-a-service) 139
  between service providers 137–139
monitoring and event management practice 157–158, 199
multi-cloud 9

N

National Institute of Standards and Technology (NIST) 70
negotiation 118
new services 37
NIST (National Institute of Standards and Technology) 70
non-standard services 8, 73–75

O

Object Management Group (OMG) 71
objectives and key results (OKRs) 54–55, 185–186
OCC (Open Commons Consortium) 70
offboarding 133–134
offboarding costs 46
offer step of customer journey 94–113
OGF (Open Grid Forum) 71
OKRs (objectives and key results) 54–55, 185–186
OMG (Object Management Group) 71
onboard step of customer journey 128–143
onboarding
  communication channels 132
  costs 45–46
  ITIL guiding principles 133
  and migrations 134–139
  planning 129–131
  and security 140–141
  SLAs (service level agreements) 142–143
  user involvement 131
  user preparation 132
one-off migrations 37
Open Commons Consortium (OCC) 70
Open Grid Forum (OGF) 71
operating models 41–42, 147–149, 175
operational excellence driver 155–158, 179
operational impact 78
opportunities and threats 39–40
organizational change management 75

organizational change management practice 154–155, 194
outages 47
outcomes 44, 78–79
over-utilization 47

P

PaaS (platform-as-a-service) 7–8, 66
packaged groups of services 118
packaged solutions 6
payment requirements 83, 105
people-related requirements 82, 104
performance management 160
Plan-Do-Check-Act cycle 186–187
planning for onboarding 129–131
platform-as-a-service (PaaS) 7–8, 66
portfolio management practice 153, 195
portfolio reviews 41
practice improvements 151–152
privacy policies 72
private cloud 9
problem management practice 157, 199
professional services 66
project management practice 195
project portfolios 41
proof of concept 84
proposal reviews 101–105
public cloud 9

R

raw resources 6
readiness assessments 84–87
realize step of customer journey 174–188
regulations and standards 38–39
regulatory compliance 141
regulatory organizations 70–71, 124
relationship management practice 195
release management practice 199
reliability, resilience, and continuity driver 159–161, 179
reliability of services 170
requests for information 84
requests for proposals (RFPs) 96–101
requirements, definition 75–83
responsibilities maps 122–124
responsiveness 169
return on investment (ROI) 95–96, 105–110
RFPs (requests for proposals) 96–101
risk management practice 165–166, 196
risks of using cloud services 12, 47–50, 79
roadmaps 182–185
ROI (return on investment) 95–96, 105–110
roles and responsibilities 48
roles and responsibilities maps 122–124

S

SaaS (software-as-a-service) 7–8, 66, 139
scalability of services 6, 60–61
security
  of cloud services 49–50
  and development 142
  and onboarding 140–141
security management 6, 60
security policies 141
security requirements 81, 103
separation between tenants 51
service availability 91
service catalogue management practice 199
service changes 6
service configuration management practice 200
service consumption 166–168
service continuity management practice 200
service deployment models 66
service design practice 200
service desk practice 200
service financial management practice 162, 196
service integrators 67
service level agreements (SLAs) 72, 119, 142–143
service level management practice 154, 201
service management practices 197–201
service migrations 36–37
service model specialists 65–66, 68
service models 7–8
service packages 118
service providers
  definition 2–3
  engaging with 87–91
  implementation 69–70
  industry and regulatory organizations 70–71
  migrations 69–70
  migrations between 137–139
  partners 68–70, 124
  regulatory organizations 70–71
  requirements 82–83, 104
  responsibilities 17–19, 88, 121–122, 123
  services 65–68
  types of 9–10, 65–68
service quality 6, 168–170
service relationships 117
service reliability 170
service request management practice 201
service requirements 92
service scalability 6, 60–61
service usage, visibility of 140–141

service validation and testing practice 201
shared responsibility model 17–19, 120–122
SLAs (service level agreements) 72, 119, 142–143
SNIA (Storage Networking Industry Association) 71
software development and management practice 202
software-as-a-service (SaaS) 7–8, 66, 139
standard services 8, 71–73
standards 38–39
Storage Networking Industry Association (SNIA) 71
strategic adaptability driver 152–153, 178
strategic impact 77
strategic objectives and plans 40–41, 54–55, 151
strategic planning 176–177
strategic positioning 38–43
strategic scope 36–37
strategy management practice 152–153, 196
subscription services 72–73
supplier management practice 163, 197
sustainability 14
systems management and control 59–60

T

tangibles 169–170
technical management practices 201–202
technology management 5–6
Telemanagement Forum (TM Forum) 71
third-party contracting 52
TM Forum (Telemanagement Forum) 71
tools 170–171
training 74
typical requirements 79–83

U

unauthorized procurement/use of cloud services 48–49
under-utilization 47
usage strategy spectrum 27–29
user experience 6
utility 76

V

value co-creation
  agreeing and planning 117
  cloud tools 170–171
  drivers
    consumer experience 153–155, 178
    governance and control 162–166, 180
    operational excellence 155–158, 179
    reliability, resilience, and continuity 159–161, 179
    strategic adaptability 152–153, 178
  maps 22–23, 149–152, 177–188
value: outcomes, costs, and risks (VOCR) 43–53, 78
vendor lock-in 51–52
visibility of service usage 140–141
vision 180–181
VOCR (value: outcomes, costs, and risks) 43–53, 78
VUCA (volatility, uncertainty, complexity, and ambiguity) 176–180

W

warranties 76
workforce and talent management practice 197

X

XaaS (anything-as-a-service) 7