Haaga-Helia
University of Applied Sciences Ltd.

Extending IT governance with Azure cloud governance

Tony Mikkola

Master’s thesis

Information Systems Management

2021

HAAGA-HELIA
University of Applied Sciences

Abstract

Author(s)
Tony Mikkola

Specialisation
Master’s Program in Information Systems Management

Thesis title	**Number of pages + number of appendices**
Extending IT governance with Azure cloud governance	76 + 1

The use of public cloud services plays a significant role in this modern era of digital transformations and disruptions boosted by cloudification. This thesis delves into the most common hurdles and blockers for adopting public cloud services, which is a deficient or a completely missing Cloud Governance Model.

The purpose of this thesis is to clarify the role of public cloud governance model, its importance when deploying public cloud services and to introduce a model on how to incorporate cloud governance into existing governance models. The goal is to provide tangible guidance for organizations embarking on their cloud journey and iteratively evolving their cloud maturity to support digital transformation.

A key focus of the thesis is on Microsoft Azure cloud services and the utilization of the Microsoft Adoption Framework for a tested and proven guidance on cloud adoption for organizations. The thesis provides a useful aid for organization IT department and IT management on expanding the usage of public cloud services in a controlled and secure manner. The thesis covers the elements needed for building an effective governance model for Microsoft Azure cloud services. The presented process and guidance for creating a cloud governance model helps building an iterative model with logical phases for improvements.

Research approach used in the thesis is based on case study research, together with literature review and document analysis. The research questions the thesis answers are: 1. What is cloud governance? 2. Why do we need a cloud governance model? 3. How do we create a cloud governance model and integrate it to existing IT governance? 4. When (at what stage during cloud journey) should we create a cloud governance model?

An actionable outcome of the thesis provides organizations guidance on how they can get clarity on making the complexity of cloud governance topic into a clear, structured, and understandable process while continuing their cloud transformation journey.

Keywords
Cloud governance, Cloud services, Digitalization, IT Governance framework

Contents

Abbreviations

AI	Artificial Intelligence
BTS	Business Technology Standard
CapEx	Capital Expenditures (Capital Expenses)
CEO	Chief Executive Officer
CIO	Chief Information Officer
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technologies
CRM	Customer Relationship Management
ERP	Enterprise Resource Planning
IaaS	Infrastructure as a Service
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
ITG	IT Governance
ITIL	IT Infrastructure Library
ITSM	Information Technology Service Management
MVP	Minimum Viable Product
NIST	National Institute of Science and Technology
OpEx	Operational Expenditures (Operational Expenses)
PaaS	Platform as a Service
RACI	Responsible, Accountable, Consulted, and Informed
ROI	Return on Investment

SaaS	Software as a Service
SLA	Service Level Agreement
TEI	Total Economic Impact

1 Introduction

The use of public cloud services plays a significant role in digital transformations, at least to a certain extent. This thesis delves into the most common hurdle, or even a blocker for deploying public cloud services, which is a completely missing or a deficient Cloud Governance Model. Enterprises often start the planning and designing a cloud governance model only after some portion of cloud services are already deployed and the first issues related to this has already emerged. At the same time, the business units in the organization demands cost efficient and modern services faster and more agile by the IT department. To be able to respond to this demand, and to be able to take advantage of the promises by cloud computing, the IT teams needs to be ready and have the knowledge and resources for adopting new cloud services. Some example themes of the requirements that cloud services produces are IT service management (ITSM) processes, cloud skills of the employees, information security and corporate culture.

The purpose of this thesis is to clarify the role of public cloud governance model, its importance in the implementation of cloud services and introduce a model on how to incorporate cloud governance into existing governance model. The model proposed in this thesis builds on an existing framework, the Microsoft Cloud Adoption Framework (CAF) for Azure. The presented model is a simplified and actionable adaption of the framework, based on the thesis author extensive experience on guiding customers in their digital transformation and cloud adoption journeys.

The result of the thesis is guidance, recommendations, and introduction of a general agile model that can be used to build and align the management model within the company's existing management model. This provides the companies IT departments a useful aid when preparing or evolving the digital transformation and expanding the usage of public cloud services in a controlled and secure manner. Some examples of the IT roles benefiting of the thesis results: service owner and service manager, cloud architect, IT manager, security manager. Naturally, the roles are not limited to these as the topics covered in the thesis are beneficial for any role involved in cloud computing services.

1.1 Thesis objectives

Any size of organization, with an existing IT function, also has an IT governance model in use, at least on some level. The IT governance in use can be based on an existing and well-known standard, framework, or methodology, such as COBIT, Business Technology Standard or TOGAF, or as in many cases when looking at smaller organizations, the IT governance model can be a set of customized practices evolved over time, either as documented or undocumented.

The objectives for this thesis are to solve a very common problem organizations face today; A cloud governance model needs to be created, or updated, and migrated to organizations existing IT governance model.

The objectives for this thesis include the introduction of the most important areas of cloud governance and a best practices model for an organization how to merge these areas of cloud governance to their existing IT governance model.

The guidance and recommendations introduced in this thesis can be used by an organization to ensure the following topics are covered and considered:

- The most important elements of Microsoft Azure cloud services governance are observed.
- The cloud governance model is built as an iterative model with ability to evolve to further improve.
- The new or modified cloud governance model can be migrated to existing IT governance model in a controlled way.

1.2 Research questions

As described in the thesis objectives in the previous chapter, a cloud governance model plays a pivotal role in cloud services adoption. The creation of, and further evolving a cloud governance model requires resources that often needs justification for the management.

This thesis supports organizations building a process for a controlled cloud adoption governance, setting the focus of the thesis on the following research questions related to cloud governance:

- What?
    - What is cloud governance, what should it include and at what extent?
- Why?
    - Why do we need a cloud governance model?
- How?
    - How do we create a cloud governance model and migrate it to an existing IT governance model?
- When?
    - At what stage during the cloud services adoption should we define and start using a cloud governance model?

Once we have the answers to these questions, organizations can see how to make the complexity of cloud governance topic into a clear, structured, and understandable process while continuing their cloud transformation journey.

1.3 Thesis scope

The public cloud services landscape is very broad, with a lot of various cloud service providers and a wide range of diverse cloud services, therefore the scope of this thesis has been scoped purely on Microsoft Azure cloud services. This thesis will not evaluate the different cloud service providers or recommend a cloud service provider over another, however the results and recommendations introduced in this thesis can be applied on most parts for public cloud services provided by any cloud service provider.

The three biggest public cloud providers currently in the market are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). While going through a tough and never-ending battle of customers, all of these three providers have their own strengths and target group of customers.

The adoption and deployment of cloud services includes several phases and topics. This thesis will use the Microsoft Cloud Adoption Framework (CAF) for Azure as a basis, which divides the cloud adoption phases to following methodologies:

- Strategy
- Plan
- Ready
- Migrate
- Innovate
- Govern
- Manage
- Organize

Regarding the above methodologies related to cloud adoption, this thesis will focus on the Governance methodology, which is the Microsoft Cloud Adoption Framework vision and recommendation on cloud governance. All cloud migration and cloud development activities are scoped out of this thesis. Although the other methodologies listed above are scoped outside this thesis, they will be introduced and their relations and relevance to cloud governance will be described.

1.4 Thesis structure

The structure of the thesis is formed out of 9 chapters. The **first** chapter introduces the thesis and its objectives, the research problem, and the research methods. The **second** chapter describes the background of cloud computing services. The **third** chapter is the result of a literature review that outlines the theoretical background for the thesis on organization governance layers. The **fourth** chapter presents the most common and well-known IT governance frameworks and standards. The **fifth** chapter presents cloud governance and its impact on IT governance. The **sixth** chapter introduces the Microsoft Azure cloud platform. The **seventh** chapter introduces the Microsoft Cloud Adoption Framework. The **eight** chapter presents the model for creating a cloud governance model. The **ninth** chapter concludes the thesis and presents the conclusions, further development ideas and reflections on own learnings throughout the thesis creation process.

1.5 Research methods

For being able to define a research approach and the research methods for a development work, more accurate development tasks and scoped development targets are needed. These are achieved by the background information and research data gathered of the target environment (Ojasalo, Moilanen & Ritalahti 2015, 26). Similarly stated by Robert Yin (2018, 3), a clear methodological path should be followed. This can be reached by starting with a literature review and the research questions. Or through conducting some fieldwork, before defining any concerns or doing the literature research.

The focus on the theoretical part, which is conducted through a literature review, is on governance layers, common and well-known governance models, frameworks, and best practices. The focus of the literature review is mainly on the following topics:

- Public cloud computing services
- Organization governance
- IT governance models
- IT management Frameworks, methodologies, best practices

The research approach used for this thesis is case study research. As presented by Yin (2018, 2), case study research is recommended if these apply (1) the main research questions are “how” or “why” questions, (2) you have little or no control over behavioral events, (3) your focus of study is a contemporary phenomenon – a “case”.

The case study process is described by Yin (2018, 1) as a linear but iterative process. The process includes six phases, as illustrated in figure 1.

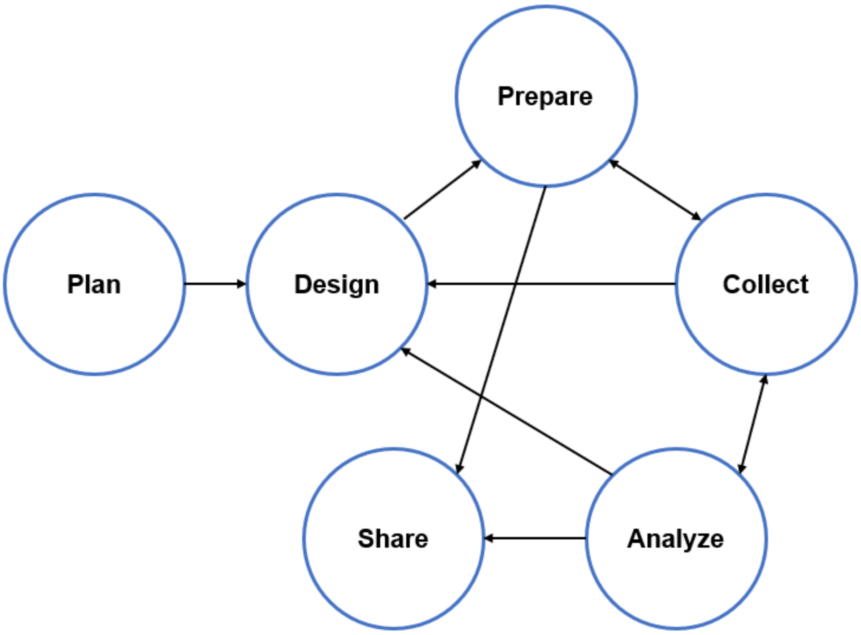


Figure 1. A linear but iterative process (adapted from Yin 2018, 1)

Ojasalo et al. (2015, 54) introduces a view on case study process with four phases. Figure 2 illustrates their view on the phases and progress of a case study.

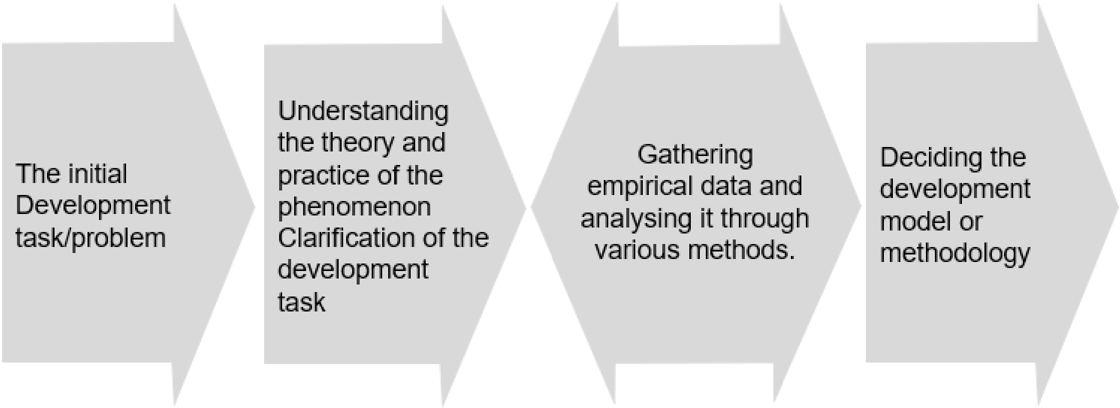

The initial Development task/problem
Understanding the theory and practice of the phenomenon Clarification of the development task
Gathering empirical data and analysing it through various methods.
Deciding the development model or methodology

Figure 2. Phases of case study (adapted from Ojasalo et al. 2015, 54).

When comparing these two different case study processes, presented by Ojasalo et al. (2015) and Yin (2018), it is obvious they have a lot of similarities. However, the process by Yin has somewhat more focus on the plan, design and prepare stages, and they have all been defined as own separate phases.

The case study research method and processes used in this thesis follows more closely the process introduced by Yin (2018,1), however in an adapted manner. The thesis research questions were defined in the **design** phase, the actions in **prepare** and **collect** phases have been literature reviews and document analysis. During the **analyze** phase the initial cloud governance model was created, and the **share** phase consist of the thesis documentation.

Yin (2018, 113-114) introduces the “six sources of evidence” concept in the collect phase, meaning the common sources used in case study research. The six sources are: documentation, archival records, interviews, direct observations, participant-observation, and physical artifacts. This should not be seen as a complete list, as there are a lot of additional sources available.

Document analysis will be used in this thesis as a method for qualitative research. According to Ojasalo et al (2015, 137), document analysis is a method where conclusions are made from written material. The reviewed documents can be interviews in writing, web pages, articles, annual reports, marketing materials, memos, diaries, photographs, drawings, speeches, reports, and other written materials.

For this thesis, much of the theory, its recommendations and guidance are based on publicly published guidance and frameworks by Microsoft, focusing on Azure cloud services. These publications have been created based on years of experience and a significant amount of executed real-life cloud adoptions, providing knowledge related to cloud guidance, best practices, governance models, and cloud deployments. The materials have been used by diverse organizations in numerous industries around the globe to successfully adopt Azure as their cloud service platform.

The thesis will also introduce a tool and method with guidance for identifying an organization cloud governance baseline, for identifying the gaps in organizations governance key areas that will be described in the cloud governance section of this thesis.

2 Public cloud computing services

For more than a decade already, the concept of public cloud computing has been revolutionizing the way modern information technology offers and delivers its services. In addition to being a technical innovation, it is also seen as a new economic model, making it possible to use IT services without massive investments upfront. This is because of the public cloud delivery model converting the capital expenditures (CapEx), e.g., owning servers and other datacenter infrastructure, to operational expenditure (OpEx) (Wikipedia 2021a). More often cloud services has become a core element of organization IT strategy. On the strategic and foundational level, cloud computing is presented as a secure, agile, and cost-effective use of IT services. This is nowadays the expectation, when planning for cloudification and the digital transformation.

A massive accelerator for cloud computing and cloud services took place in 2020, as the Covid-19 pandemic hit the whole world. Satya Nadella, the CEO of Microsoft highlighted in a Microsoft Earnings Release call: “What we have witnessed over the past year is the dawn of a second wave of digital transformation sweeping every company and every industry” (Microsoft 2021e). Remote work has become the new normal in many organizations, making the intelligent tools and platforms imperative for enabling work anytime and anywhere, which is the expectation of current digital workforce.

Throughout its existence, cloud computing as a concept has a lot of different definitions and descriptions. The basic idea of cloud computing is that instead of buying and maintaining your own hardware, you rent resources from a cloud provider and only pay for what you use. The term cloud computing is widely used to describe geographically distributed datacenters, providing on-demand availability of computing resources without the direct active management by the users, and available to users through the Internet (Wikipedia, 2021a). Some common definitions of cloud computing based on existing literature on the subject:

> “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” (NIST 2011)

> "Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand." (ISO/IEC 17788)

> “Cloud computing is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies.” (Gartner 2021a)

> “Due to newly developed IT technologies (such as virtualization) and availability of high speed, reliable internet connection, consumers do not need to have their own IT system; they can use IT as a service. This model is called ‘cloud computing’.” (Fuzes 2018)

> "A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers.” (Buyya et al. 2009)

The cloud computing market has been growing huge steps for a while already, even before the Covid-19 pandemic started early 2020. Gartner says worldwide IaaS public cloud services market grew 37,3% in 2019 (Gartner 2020). Flexera 2020 State of the Cloud Report shows cloud adoption continues to accelerate, as shown in figure 3, respondents reported their current cloud usage was over budget by an average of 23% and the expectation was that their cloud usage would further increase by 47% in the next 12 months (Flexera 2020).

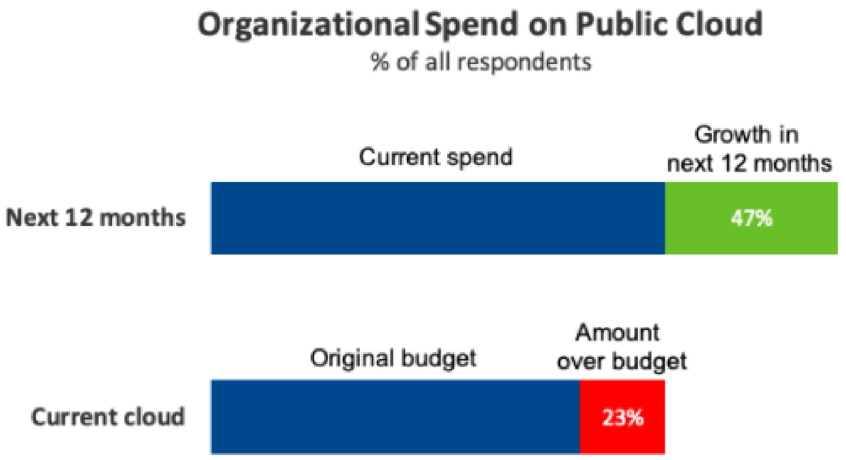


Figure 3. Organizational spend on public cloud (Flexera 2020).

According to IDC, spending of public cloud IT infrastructure increased 34,4% year over year and surpassed spending on traditional IT infrastructure for the first time in the second quarter of 2020 (IDC 2021). These calculations include IT vendor revenue from sales of IT infrastructure products (server, storage, and networking devices) for cloud environments, including public cloud and private cloud. In long term, IDC expects spending on cloud IT infrastructure to grow at a five-year compound annual growth rate of 10.4%, as shown in figure 4, reaching $109,3 billion in 2024 and accounting for 63,6% of total IT infrastructure spend (IDC 2021).

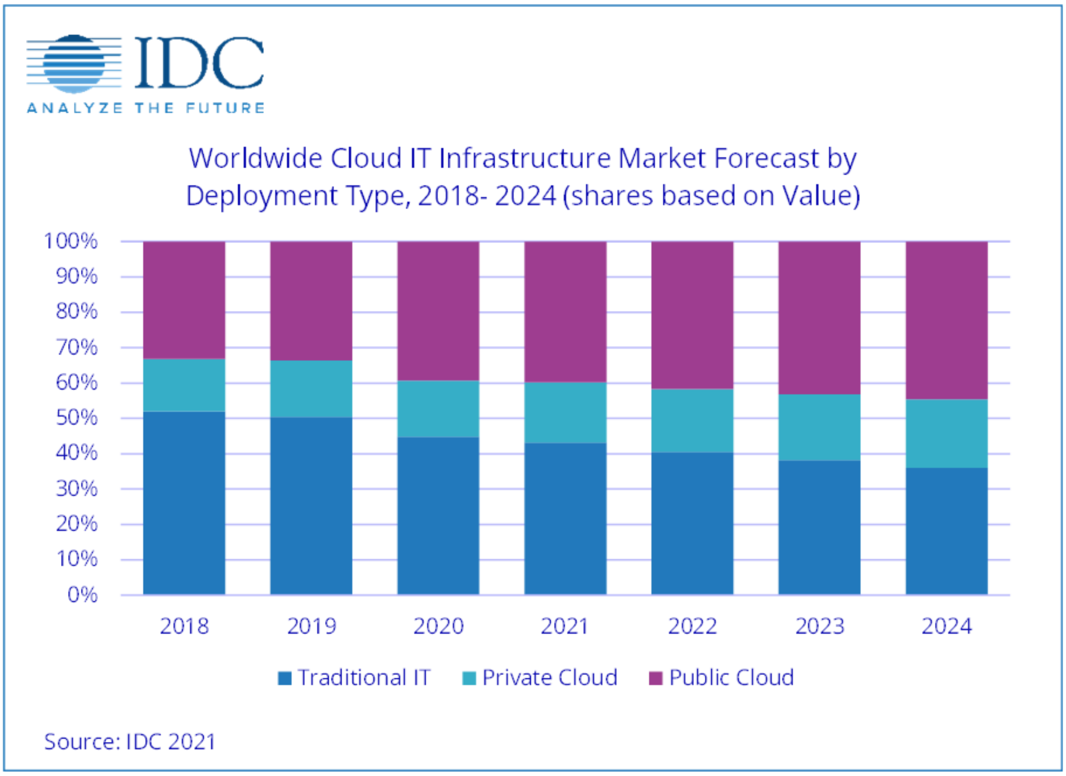


Figure 4. Cloud IT infrastructure market forecast by deployment (IDC 2021).

2.1 Cloud computing Deployment Models

The three most popular and commonly known deployment models for cloud computing are private cloud, public cloud, and hybrid cloud.

Private cloud is a model where the cloud infrastructure is operated exclusively for a single organization. The infrastructure can be owned, managed, and operated internally or by a third party, or a combination of them. The infrastructure can be hosted on-premises or externally (NIST 2011). A reason to choose private cloud can be security concerns or needs, as it is easier to isolate environments.

In **Public cloud** the infrastructure is provisioned for open use by the general public, and it can be owned, managed and operated by a cloud service provider. The infrastructure is hosted on the premises of the cloud provider (NIST 2011).

Hybrid cloud is a composition of two or more cloud infrastructures, for example private cloud and public cloud, that remain unique entities, but are bound together and offering the benefits of selected deployment models (NIST 2011). Hybrid cloud scenarios can be chosen for a variety of reasons, e.g., some applications are running on legacy platform and migration is too expensive and time consuming, or there might be policies to keep certain applications and their data on-premises.

In addition to these three models, the NIST (2011) definition of cloud computing defines a fourth deployment model: community cloud. Some additional cloud computing deployment models used commonly are government cloud, distributed cloud, multi cloud, poly cloud, big data cloud and HPC (High Performance Cloud) cloud.

2.2 Cloud Computing Service Models

When classifying cloud computing, the most common approaches for using cloud computing offered by the cloud providers, are called as service models. NIST (2011) defines the following three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Infrastructure as a Service (IaaS) is a model where the cloud service provider hosts and maintains core infrastructure, including hardware, software, servers, and storage on behalf of a customer. The cloud service consumer is renting server hardware and software for running virtual machines (VM) that consist of an operating system and the applications. Figure 5 illustrates a cloud server, where many operating systems and applications can coexist. A hypervisor runs and manages the virtual machines and the boxes highlighted in blue are operated and maintained by the consumer of the service.

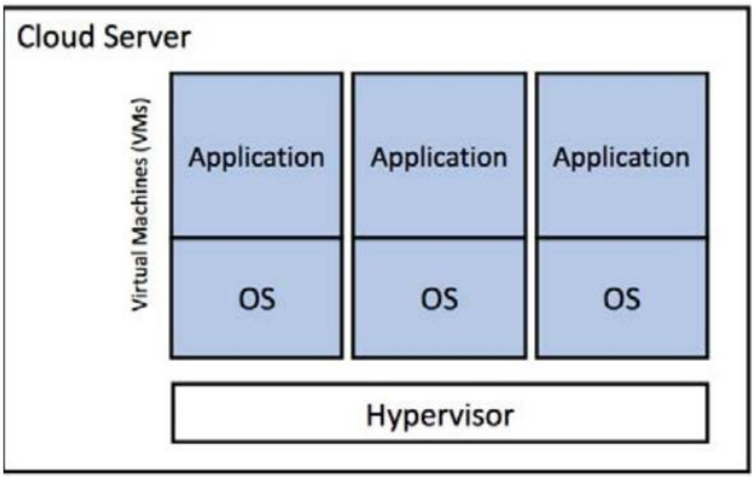


Figure 5. Infrastructure as a Service (Briggs 2019).

The definition for Infrastructure as a Service is described by NIST definition of cloud computing as:

> The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) (NIST 2011).

In **Platform as a Service (PaaS)** service model the maintenance of the system software is the cloud service provider responsibility, as shown in figure 6. This includes as an example the operating system upgrades and patches, so the consumer can focus on deploying its codes and applications on the servers.

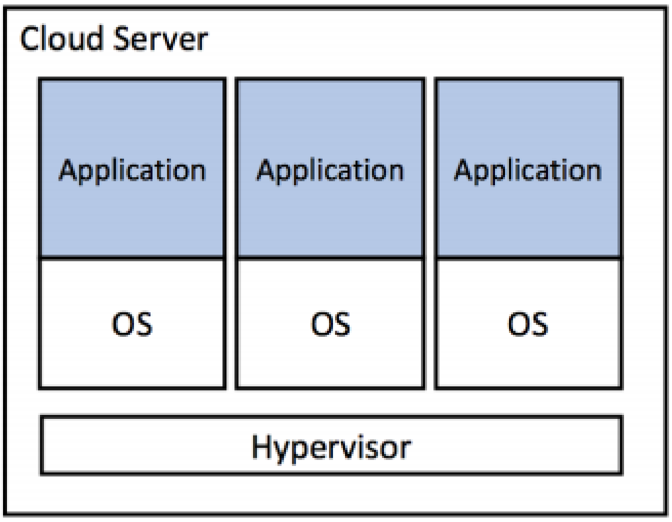


Figure 6. Platform as a Service (Briggs 2019).

Platform as a Service is defined in NIST's definition of cloud computing as:

> The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment (NIST 2011).

In **Software as a Service (SaaS)** it is the cloud service provider who manages the infrastructure and platforms where the applications are running. The consumer uses the application usually with a per-user pricing model or a subscription-based model. Well known Software as a Service applications are Microsoft Office 365 for email and productivity tools and Salesforce CRM platform called Salesforce Customer 360.

Software as a Service is defined by NIST's definition of cloud computing as:

> The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings (NIST 2011).

Figure 7 shows a comparison of a traditional on-premises datacenter and the cloud computing service models and their capabilities. The diagram highlights services managed by the customer in blue, and the service managed by the cloud service provider in orange.

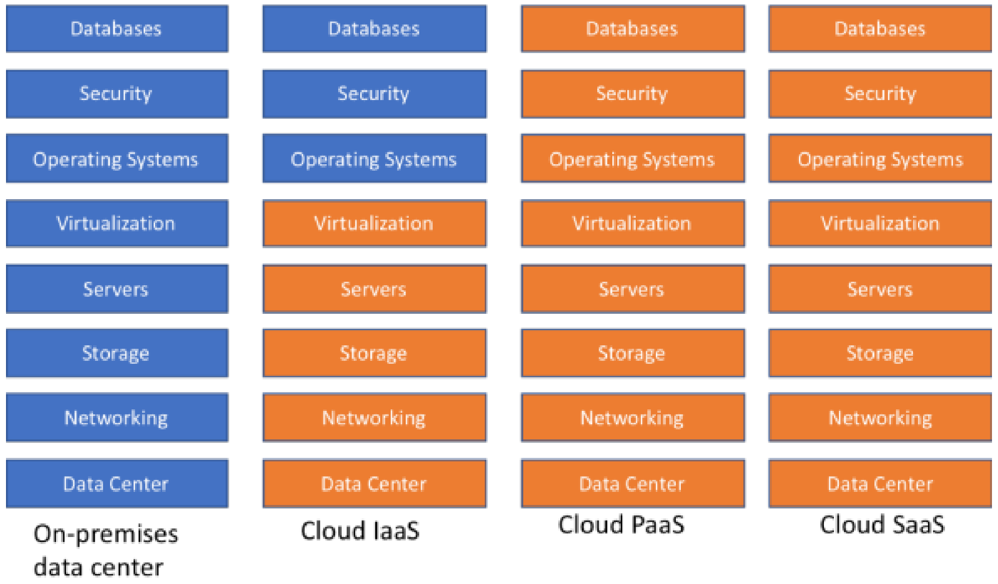


Figure 7. “As a Service”-management compared (Briggs 2019).

The distinctions between these cloud computing service models have been defined quite sharp in the past, but in recent years the lines have begun to blur. Today IaaS applications can take advantage of the cloud’s ability to scale up in response to high demand and scale down as the load decreases (Briggs 2019).

2.3 Benefits of Cloud Computing

There are a lot of studies available on cloud computing benefits, most commonly they are measuring the financial benefits and the potential Return-On-Investment (ROI). When looking at the benefits, one approach by Microsoft (Microsoft 2021e) is to categorize the benefits in two larger categories. One is the technical benefits, and the other is the financial benefits, which is reliant on the technical benefits.

Technical benefits – elasticity and on-demand are a huge shift in the transformation when moving to cloud, improving the management and provisioning of resources more dynamically. Key technical benefits:

- **Scalability** – ability to scale out resources depending on usage, utilization, and demand.
- **Availability** – it’s less costly to build highly available infrastructure on the cloud, compared to on-premises.

- **Security and compliance** – security infrastructure and toolsets are added and updated with respect to security threats on the worldwide datacenter networks.
- **Capacity optimization** – as only the resources in use are being charged, the capacity can be scaled by demand, meaning the capacity does not consume constantly the high load demand resources as it can be deprovisioned dynamically (Microsoft 2021e).

Financial benefits – making IT cost structure more flexible to minimize market changes risks and taking advantage of new business opportunities quickly. Financial benefits:

- **OpEx pricing models** – transforming overall budget allocation from CapEx investments to OpEx type pricing models where capacity or utilization of the cloud environment plays a bigger role.
- **Reduced datacenter footprint** – no more expensive facilities, co-location or hosting agreements required.
- **Staff productivity** – DevOps type of concepts brings more focus on automation and automating operations.
- **Sustainability** – Datacenters hosting cloud services, such as Azure, are provided at a scale where the environmental impact is the least (Microsoft 2021e).

There are a lot of market research and studies performed on the financial benefits of cloud services. Armbrust et al (2010, 52-54) research shows cost benefits was a key factor when moving to cloud services. The financial benefits are often compared to traditional on-premises infrastructure models.

Looking at Microsoft Azure cloud platform, a recent study on Azure IaaS services financial benefits was conducted by Forrester, a leading analysis firm. The report conclusions, which measured a three-year investment period, stated that with cloud services you could get e.g., a three-year 478 % return on investment, $10,3 million savings in infrastructure and staff costs, easier access to new technologies, accelerated developer and tester processes, and migration flexibility with hybrid capabilities (Forrester 2019). Figure 8 shows the benefits that could be achieved according to the Forrester report.

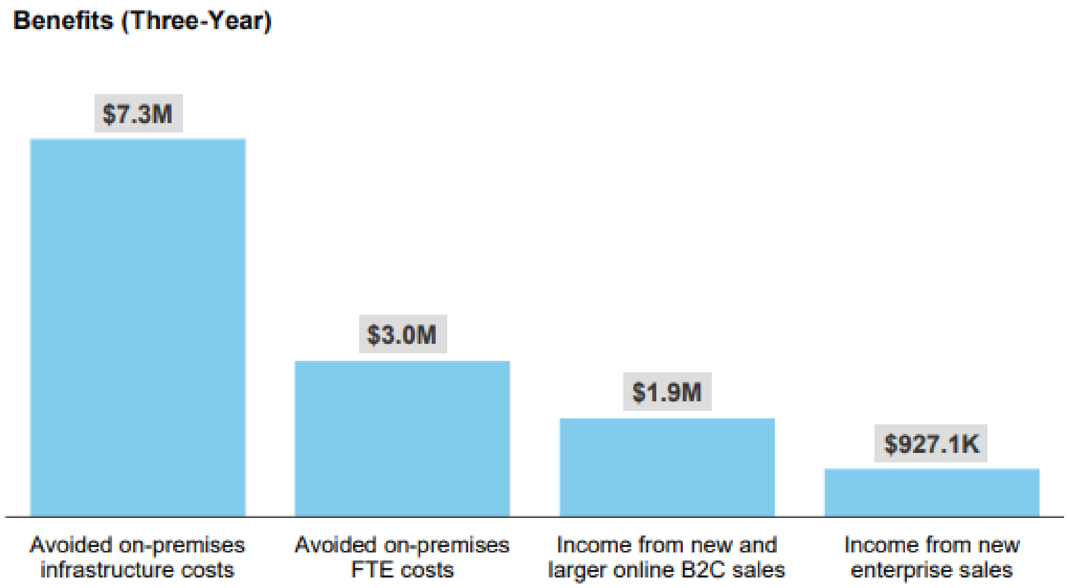


Figure 8. Azure IaaS benefits (Forrester 2019).

The benefits of cloud computing presented in this chapter has been focusing on Azure and it is good to note that majority of the used sources are impacted by Microsoft. Therefore, the numbers shown regarding savings should be considered directive. Nevertheless, similar results and findings occurs widely across literature on cloud computing.

Undoubtedly, also disadvantages exists for cloud computing. Some of the most commonly listed disadvantages throughout literature is the lack of self-control, rearchitecture needs on application design, compliance and security concerns, internet connectivity dependency, and available support options. However, many of the stated disadvantages can even turn into benefits when comparing on-premises to cloud, since the modern public cloud services has turned out to be more reliable and more secure compared to privately and on-premises hosted environments.

3 Background on governance

A wide range of governance models, various IT governance frameworks, and IT management models have been used already for decades. However, the speed of ongoing cloudification and technology innovations has changed the landscape and established new requirements and needs for governance and IT management. This has also impacted the governance and structures in organizations. In many industries, the role of IT department has become crucial in supporting the enterprise digital transformation and growth.

A major share of literature on governance in organizations defines governance processes in three groups, or governance layers, which are: Enterprise Governance, Corporate Governance, and IT Governance (Gheorghe 2010).

This chapter will focus on the governance layers and some of the most popular and well-known frameworks and models, their purpose for organizations, and their maturity for digital innovations and cloud services.

3.1 Enterprise governance

IT Governance Institute (ITGI) defines Enterprise governance as “a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise’s resources are used responsibly” (ITGI 2003).

Wilson (2009) defines Enterprise governance as “the structure and relationships which control, direct, or regulate performance of an enterprise, projects, portfolios, infrastructure, processes.” (Wilson 2009). On this definition, MITRE introduces the view of three different, interconnected levels in organizations: program lever, portfolio level, and enterprise level (MITRE 2021a). The use of these levels of governance varies significantly based on the organization and its industry.

Enterprise governance can be seen as a balance between Performance and Conformity (CIGREF 2005). Figure 9 illustrates the dependencies of enterprise governance, which is seen as the entire accountability framework of an organization. The conformance dimension takes an historic view, while the performance view is looking forward. This shows corporate governance also needs the strategy part (IFAC 2003).

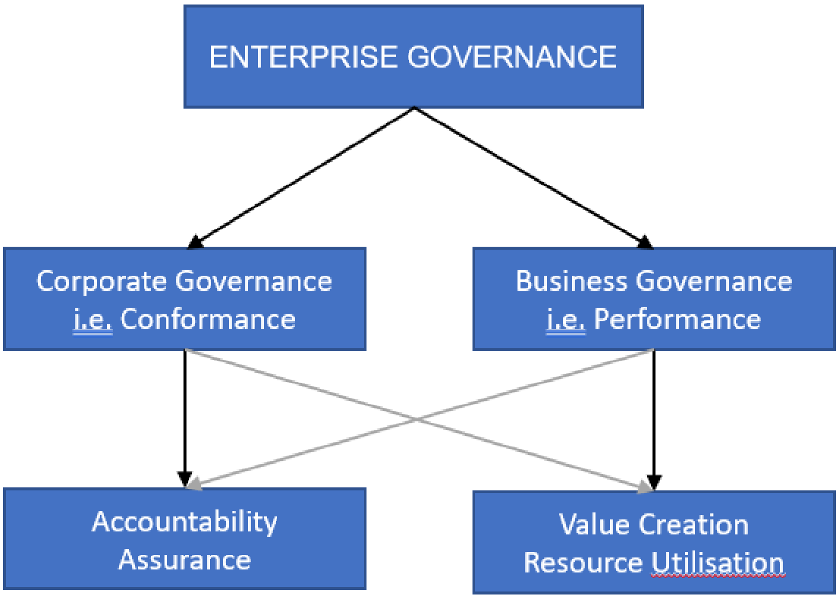


Figure 9. The enterprise governance framework (adapted from IFAC 2003).

3.2 Corporate Governance

Corporate Governance steers the organization management and defines the tasks and responsibilities of the top management. ICSA defines corporate governance as the system of rules, practices, and processes by which organizations are directed and controlled. Corporate governance defines the decision makers and who has the power and accountability. It ensures the needed decision-making processes and controls are in place, for all stakeholders interests to be covered (ICSA s.a.).

De Leusse et al (2009) defines Corporate governance as “The set of processes, customs, policies, laws and institutions affecting the way in which a corporation is directed, administered or controlled” (de Leusse, Dimitrakos, & Brossard 2009).

The G20/OECD Principles of Corporate Governance is recognized as the international benchmark in corporate governance. The purpose of the Principles is to help policy makers evaluate and improve the legal, regulatory, and institutional framework for corporate governance. The Principles defines the responsibilities of the board as "The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board’s accountability to the company and the shareholders" (OECD 2015).

According to the G20/OECD Principles of Corporate Governance, the key functions the board should fulfill includes:

- Reviewing and guiding corporate strategy, major plans of action, risk policy, annual budgets, and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions, and divestitures.
- Selecting, compensating, monitoring and, when necessary, replacing key executives and overseeing succession planning.
- Reviewing key executive and board remuneration and ensuring a formal and transparent board nomination process.
- Monitoring and managing potential conflicts of interest of management, board members and shareholders, including misuse of corporate assets and abuse in related party transactions.
- Ensuring the integrity of the corporation’s accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for monitoring risk, financial control, and compliance with the law.
- Monitoring the effectiveness of the governance practices under which it operates and making changes as needed.
- Overseeing the process of disclosure and communications.
  (OECD 2015)

3.3 IT governance

IT governance is the management process for organization IT function, which defines the management principles for information systems, IT development, steering and responsibilities. IT Governance Ltd. in UK sees IT Governance as an element of corporate governance, which is aimed at improving overall management of IT and improving the value of IT based on investments (IT Governance 2021). According to Gartner glossary, IT Governance is the processes that ensures effective and efficient use of IT, enabling an organization to achieve its goals (Gartner 2021b).

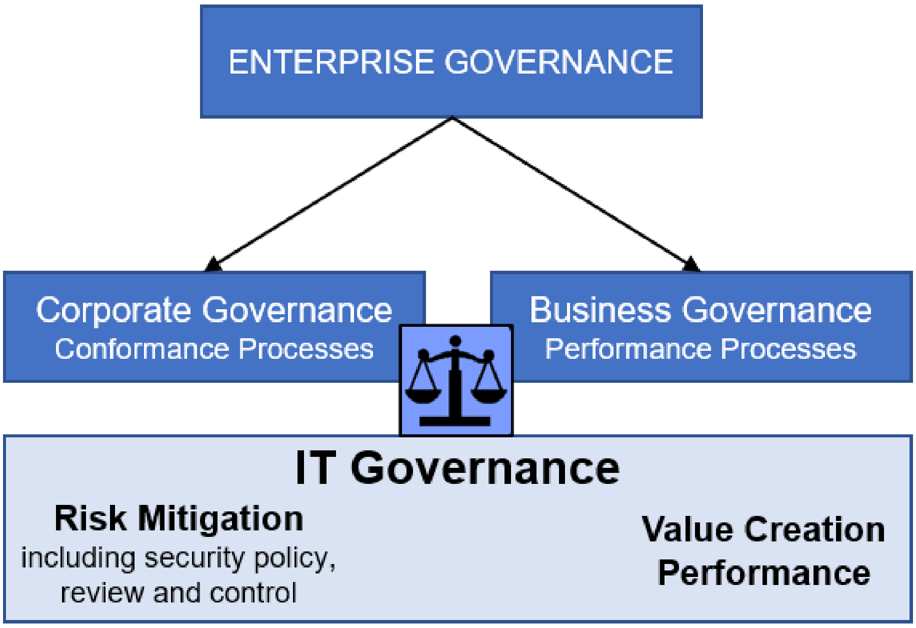


Figure 10. Positioning IT Governance (adopted from CIGREF 2005).

IT Governance positioning in figure 10. IT governance supports both Corporate and Business Governance inside Enterprise Governance (CIGREF 2005). According to CIGREF, IT Governance is a management process to drive IT function to support its value creation goals, improve IT process performance, manage the financial aspects of IT, develop IT solutions and employee competencies, and to ensure IT-related risks are managed (CIGREF 2005).

Some of the most common and widely referenced IT governance definitions available:

> IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and con-sists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives (IT Governance Institute 2003).

> Information technology (IT) governance consists of the leadership, structures, and processes that enable an organization to make decisions to ensure that its IT sustains and extends its strategies and objectives (MITRE 2021b).

> The processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. IT demand governance (ITDG—what IT should work on) is the process by which organizations ensure the effective evaluation, selection, prioritization, and funding of competing IT investments; oversee their implementation; and extract (measurable) business benefits. ITDG is a business investment decision-making and oversight process, and it is a business management responsibility. IT supply-side governance (ITSG—how IT should do

> what it does) is concerned with ensuring that the IT organization operates in an effective, efficient and compliant fashion, and it is primarily a CIO responsibility (Gartner 2021b).

In an IT environment, doing the right thing can be summarized in what the IT team decides to focus on to achieve the business aims. This is IT governance. When this has been decided, the IT team will focus on doing things right. In practical terms, this translates to how the IT team will carry out this task. This is IT service management (Vyas 2019).

While examining the governance topic, it can be confusing to do distinguish the concepts of IT governance (ITG) and IT service management (ITSM). Vyas (2019) clarifies this by stating work can be done in a way where we are doing the right thing or doing things right. IT governance tries to do the right thing, which is set by the focus to achieve business goals. When this has been agreed, the IT team will focus on doing things right. This is IT service management, the concrete work and how it is done (Vyas 2019).

Another similar confusion regarding terms comes with IT governance and IT management. Vyas (2019) continues with these terms clarifying IT governance works together with IT management. IT governance ensures that IT activities and processes are aligned with the overall objective, such as enterprise priorities. IT management is the methods used by IT teams to meet these objectives (Vyas 2019).

3.4 Findings on governance

So why do we need governance and what is the impact of governance? Reviewing the literature confirms there is a consensus that a correlation between corporate governance, performance and economic growth exists. Maher & Andersson (1999) highlighted there is no single model for good corporate governance, and the effectiveness of governance is influenced by differences based on country regulations and laws, culture, and the structure of product and factor markets. Also, the industry sector and the type of productive activity affects the corporate governance impact on performance.

A research made by Deloitte and Nyenrode (2016) had similar results, supporting the assumption that good governance improves corporate performance. Their research presented specific governance variables, that had a positive impact on performance However, the conclusions of their research highlighted also that there is no one size fits all approach in applying the specified governance variables in practice.

Organizations with a clearly defined and well-communicated governance on all layers, enterprise, corporate, and IT governance, sets a culture for the entire company on ways of working and making decisions. There are many alternative ways of establishing and managing governance within an organization and the governance model in use varies a lot. The used governance model is affected by several factors, for example organization size, industry, countries they operate in, history and age. Each acquisition and merger made in an organization can have a big impact on governance, as it can be slow and time consuming to change the culture for a large number of employees.

4 IT Governance frameworks and standards

The layers of governance have been introduced in earlier chapters to provide an overview on them and their role and impact in an organization. In this chapter the focus is on the most common and widely used IT governance models, frameworks, and standards. One of the most important aspect to note is the version of the framework or standard that is reviewed, as many of them have been updated within the recent years to cover the modern world where public cloud services and digitalization are used and has introduced a new set of requirements.

IT governance frameworks enables organizations to manage their IT risks effectively and ensures that the activities associated with information and technology are aligned with their overall business objectives (IT Governance 2021).

In the next sections, some of the most common and well-known standards and frameworks for IT governance will be introduced. These are the ISO/IEC 38500 standard, Information Technology Information Library (ITIL), the Business Technology Standard (BT Standard), Control Objectives for Information and related Technology (COBIT).

4.1 ISO/IEC 38500

The ISO/IEC 38500 standard (ISO/IEC 38500:2015 ”Information technology - Governance of IT for the organization”) is an international standard for corporate governance of information technology, first published back in 2008 under the name of “Corporate Governance of Information Technology” (ISO 2015).

The ISO/IEC 38500 standard was prepared by Joint Technical Committee ISO/IEC JTC1, Information technology, SC40, IT Service Management and IT Governance. The current version of the standard is ISO/IEC 38500:2015, updated in February 2015. The next reviewed version, ISO/IEC WD 38500, is under development and it will replace the current standard (ISO 2021).

The objective of the standard is to provide the organization management principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring Information Technology usage within the organization.

This international standard also provides guidance for stakeholders informing, advising, or assisting corporate management. These could be for example: executive managers, members of groups monitoring the resources within the organization, external business, or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies, internal and external service providers (including consultants), and auditors (ISO 2015).

The standard promotes effective and efficient use of IT in an organization by:

- assuring stakeholders that, if the principles and practices proposed by the standard are followed, they can have confidence in the organization's governance of IT
- informing and guiding governing bodies in governing the use of IT in their organization, and
- establishing a vocabulary for the governance of IT
(ISO 2015)

It is good to recognize this standard only defines the governance of IT, which is part of an existing corporate governance. The standard can be used for all organizations, both private and public companies, non-profit organizations, and government entities. The standard is also very versatile when it comes to the size of the organization, as it can be used for both small and large corporations. It will be interesting to see how the new version, ISO/IEC WD 38500, will support the governance of cloud services.

4.2 ITIL

The Information Technology Infrastructure Library (ITIL) is a well-known and widely used IT service management framework based on service management best practices and guidelines. The framework provides a structure that helps an organization to deliver and maintain IT and digital services, obtaining optimal value for all stakeholders, including the customers. The ITIL framework allows a service provider to tailor its services to an organization’s vision, mission, strategy, and goals. ITIL is supported by a certification system that allows ITIL professionals to demonstrate their expertise in the framework (Axelos 2020)

ITIL was originally developed in UK, by governments Central Computer and Telecommunications Agency (CCTA) back in 1980’s to help improve IT Service Management in UK central government. ITIL Version 2 was published in 2006, and ITIL Version 3 (also known as ITIL 2007 Edition) was released the next year, in 2007 with an update published in 2011. The current version of ITIL, ITIL 4 was published in February 2019 (Wikipedia 2021c).

ITIL is owned by Axelos Limited, a joint venture between the Cabinet Office and Capita, which was created in 2013 to manage, develop and grow the Global Best Practice portfolio. Axelos manages also PRINCE2, MSP and several other best practice frameworks and methodologies (Axelos 2021).

A study to understand the ITIL framework in relation to IT Governance was made by Gërvalla et.al. (2018). The study states IT service management focus is on operational excellence of IT related services, whereas IT governance focuses on enabling, controlling, and assisting with the decision making at the strategic level. IT and Business alignment have an important role on the strategic level. IT Governance can contribute to a better business environment by improving the business performance focused on managing and controlling IT services. ITIL framework provides a holistic approach in the context of IT Governance. ITIL application contributes to many aspects of organization sustainability, by controlling and managing technological changes to improve the usage of IT services and increase the stability of the organization (Gërvalla et.al. 2018).

ITIL 4, the latest version of ITIL, introduced several improvements to the best practice framework, expanding its adoption also for non-IT services. Among other updates, ITIL 4 brings help on ITSM practices for digital transformation and the new ways of working. One major benefit is the support for integrating IT management practices such as Agile, DevOps, and Lean. ITIL 4 has been updated to work seamlessly with emerging technologies such as AI and intelligent automation, cloud, and advanced analytics (Axelos 2021).

A key component in ITIL 4 is the service value system (ITIL SVS) shown in figure 11. The service value system is formed of the following core components:

- ITIL service value chain
- ITIL guiding principles
- Governance
- Continual improvement
- 34 management practices
  (Axelos 2021)

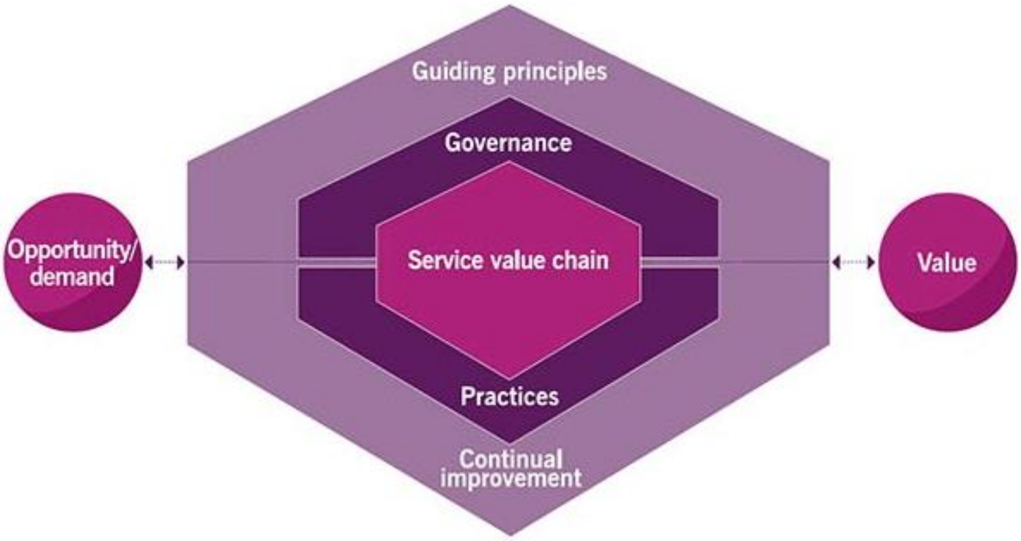


Figure 11. ITIL service value system, SVS (Axelos 2021)

The service value system (SVS) can be adapted for cloud services. Regarding the service value system components, O'Loughlin (2019) highlights the service value system provides a valuable structure for consuming the cloud service in the right way and aligned to the needs of all required stakeholders. On the ITIL Guiding principles O'Loughlin continues that they can be adapted for cloud services. Regarding the Governance component, the governance activities for cloud-based services are covered but it is critical to agree how the cloud services are managed, as parts of the service are not accessible by the organization (O'Loughlin 2019).

4.3 Business Technology Standard

The Business Technology Standard (BT Standard) is an open-source management framework to plan, build and run information technology. The standard is provided by a non-profit community, called the Business Technology Forum, and it is used by hundreds global companies and public organizations and seen as one of the leading best practices in Nordic countries (BT Forum 2020).

Figure 12 illustrates the development stages and the evolving versions of the Business Technology Standard. The standard was introduced in 2009 by Business Technology Forum and the first edition was called ICT Standard for Management. The focus of the first version was to align IT with business. The second edition was released 2012 and the focus was to run IT like a business. The third edition came out 2015, with and updated scope and title. The standard was now called "IT Standard for Business" and the focus was developing business capabilities. The fourth and latest edition, which is a completely rewritten and upgraded version, was published in 2019 and the scope was extended from information technology to business technology (BT Forum 2020).

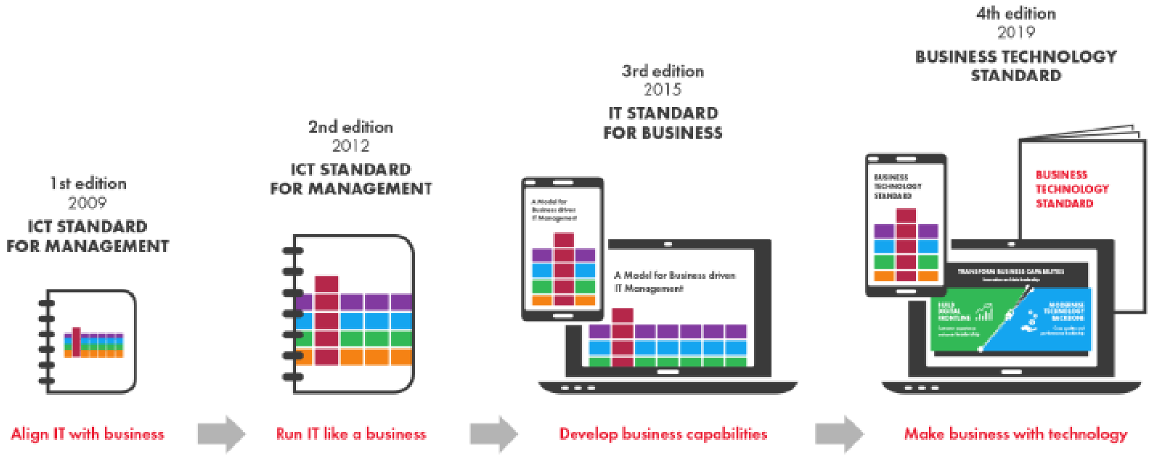

1st edition
2009
ICT STANDARD FOR MANAGEMENT
Align IT with business
2nd edition
2012
ICT STANDARD FOR MANAGEMENT
Run IT like a business
3rd edition
2015
IT STANDARD FOR BUSINESS
A Model for Business driven IT Management
Develop business capabilities
4th edition
2019
BUSINESS TECHNOLOGY STANDARD
BUSINESS TECHNOLOGY STANDARD
TRANSFORM BUSINESS CAPABILITIES
BUILD DIGITAL FRONTLINE
MODERNISE TECHNOLOGY BACKBONE
Make business with technology

Figure 12. Business Technology Standard development stages (BT Forum 2020).

The definition of business technology according to BT Forum (2020): “a strategy for organising and coordinating technology management across the entire enterprise”.

The business technology introduces three core elements:

- Transform business capabilities
- Build digital frontline
- Modernise technology backbone

The Business Technology Standard (BT Standard) is a framework for managing technology to bring value to business. The standard provides guidance on how to fit together traditional information technology operations and new digital development. The Business Technology Standard works very well together with other models and frameworks, as an example SAFe and DevOps for agile development, and ITIL for service management.

The Business Technology Standard consist of three models for unified information and digitalisation management:

- Operating model
- Capability model
- Roles and responsibilities model

The Business Technology Standard operating model has five disciplines: demand, development, and services, with two overarching disciplines: strategy and governance, and sourcing and optimisation.

The strategy and governance discipline in BT Standard defines the guidelines, rules, and framework for the business technology function. Figure 13 illustrates the governance and steering bodies in BT Standard.

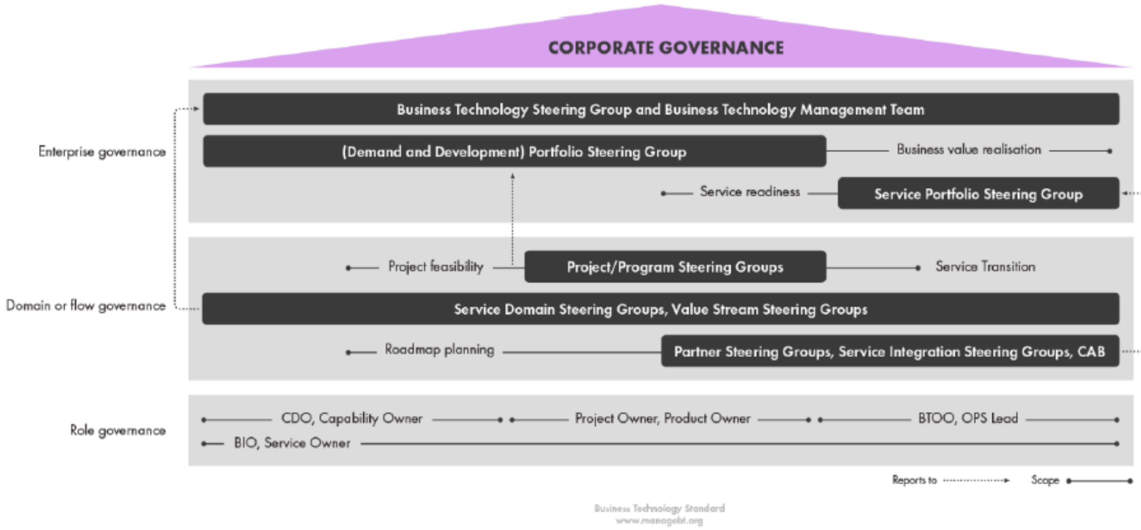

CORPORATE GOVERNANCE
Enterprise governance
Business Technology Steering Group and Business Technology Management Team
(Demand and Development) Portfolio Steering Group
Business value realisation
Service readiness
Service Portfolio Steering Group
Domain or flow governance
Project feasibility
Project/Program Steering Groups
Service Transition
Service Domain Steering Groups, Value Stream Steering Groups
Roadmap planning
Partner Steering Groups, Service Integration Steering Groups, CAB
Role governance
CDO, Capability Owner
Project Owner, Product Owner
BTOO, OPS Lead
BIO, Service Owner
Reports to
Scope
Business Technology Standard
www.managebt.org

Figure 13. Governance and steering bodies in BT Standard (BT Forum 2020).

The purpose of the model is that prioritisation and decision making is performed in roles as far as possible. The portfolios presented by the BT Standard is Demand Portfolio, Development Portfolio, and Service Portfolio.

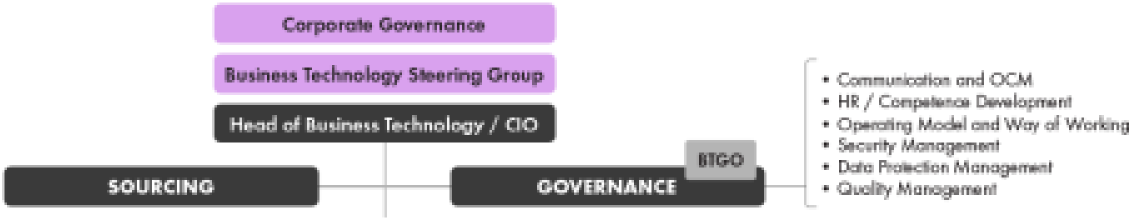

Corporate Governance
Business Technology Steering Group
Head of Business Technology / CIO
SOURCING
GOVERNANCE
BTGO
• Communication and OCM
• HR / Competence Development
• Operating Model and Way of Working
• Security Management
• Data Protection Management
• Quality Management

Figure 14. Business technology organization (adapted from BT Forum 2020).

The BT Standard proposes a couple of alternative ways to organize the business technology structure. Figure 14 illustrates the same top-level structure for the alternatives and presenting the role and responsibilities of governance. The term BTGO stands for the Business Technology Governance Officer, who leads the governance functions.

4.4 COBIT

COBIT (Control Objectives for Information and related Technology) is an IT governance framework owned and managed by ISACA. The purpose of the framework is to combine good IT governance, technology management, and managing business risks.

ISACA defines COBIT as a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise. COBIT defines the components and design factors to build and sustain a best-fit governance system (ISACA 2018).

The latest version of the framework is COBIT 2019, which was released in late 2018. The previous version, COBIT 5 was published back in 2012. Due to lack of support for new technology and business trends in IT, and several other limitations in COBIT 5, there was a huge demand to get the framework updated and to support the modern digital era.

According to the ISACA, COBIT 2019 was updated to include or improve:

- Flexibility and openness
  - The definition and use of design factors allow COBIT to be tailored for better alignment with a user's particular context. The COBIT open architecture enables adding new focus areas or modifying existing ones, without direct implications for the structure and content of the COBIT core model.

- Currency and relevance
  - The COBIT model supports referencing and alignment to concepts originating in other sources (e.g., the latest IT standards and compliance regulations).

- Prescriptive application
  - Models such as COBIT can be descriptive and prescriptive. The COBIT conceptual model is constructed and presented such that its instantiation (i.e., the application of tailored COBIT governance components) is perceived as a prescription for a tailored IT governance system.

- Performance management of IT
  - The structure of the COBIT performance management model is integrated into the conceptual model. The maturity and capability concepts are introduced for better alignment with CMMI.

(ISACA 2018)

Harisaiprasad (2020) compared COBIT 2019 to COBIT 5 and highlighted some of the most valuable changes, among an extensive list of updates. These included that COBIT

2019 now includes new technology and business trends in IT. Additionally it can now easier integrate with other international standards, guidelines, regulations, and best practices and provide an effective EGIT (Enterprise Governance of Information & Technology) framework (Harisaiprasad 2020).

COBIT 2019 is based on two sets of principles:

- Principles that describe the core requirements of a **governance system** for enterprise information and technology.
- Principles for a **governance framework** that can be used to build a governance system for the enterprise.

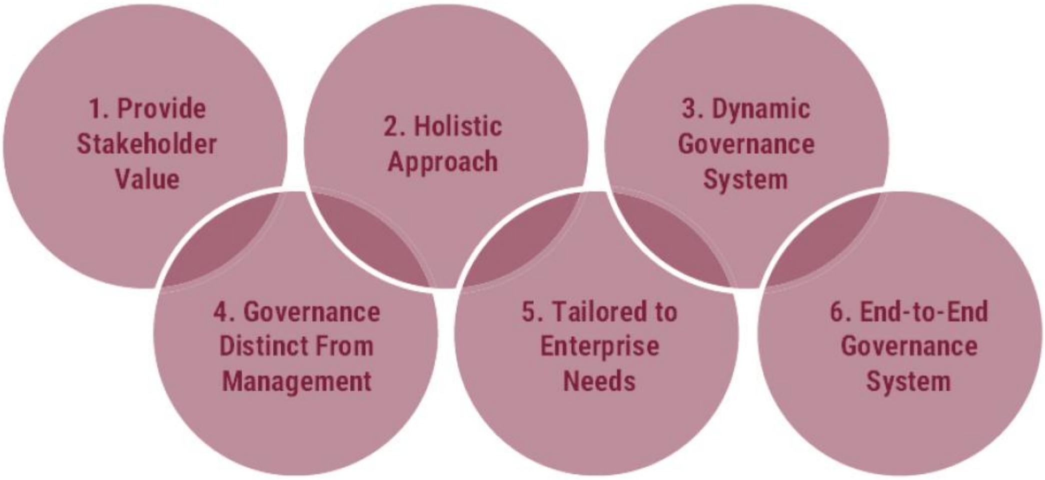

1. Provide Stakeholder Value
2. Holistic Approach
3. Dynamic Governance System
4. Governance Distinct From Management
5. Tailored to Enterprise Needs
6. End-to-End Governance System

Figure 15. Governance system principles (ISACA 2018).

Figure 15 illustrates the COBIT **Governance system principles** – which is a core requirement for an enterprise information and technology governance system. The principles are:

1. **Provide Stakeholder Value** - Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T.
2. **Holistic Approach** - A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.
3. **Dynamic Governance System** - A governance system should be dynamic. This means that each time one or more of the design factors are changed the impact of these changes on the EGIT system must be considered.
4. **Governance Distinct from Management** - A governance system should clearly distinguish between governance and management activities and structures.

5. **Tailored to Enterprise Needs** - A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.

6. **End-to-End Governance System** - A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals.
(ISACA 2018)

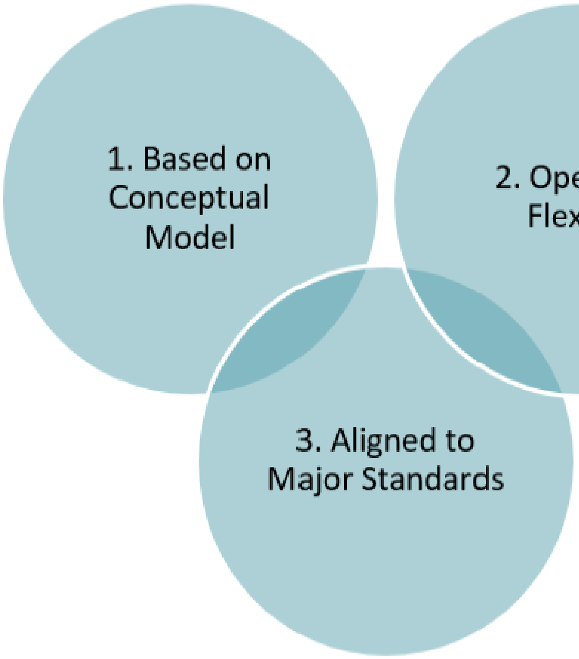


Figure 16. Governance framework principles (ISACA 2018).

Figure 16 illustrates the COBIT **Governance framework principles** – which identifies the underlying principles for a governance framework that can be used to build a governance system for the enterprise. The principles are:

1. **Based on Conceptual Model** - A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation.

2. **Open and Flexible** - A governance framework should be open and flexible. It should allow the addition of new content and the ability to address new issues in the most flexible way, while maintaining integrity and consistency.

3. **Aligned to Major Standards** - A governance framework should align to relevant major related standards, frameworks, and regulations.
(ISACA 2018)

The COBIT core model for governance and management includes 40 core objectives, where each objective relates to one process and several components. Figure 17 illustrates the components, which are factors that contribute to the IT governance.

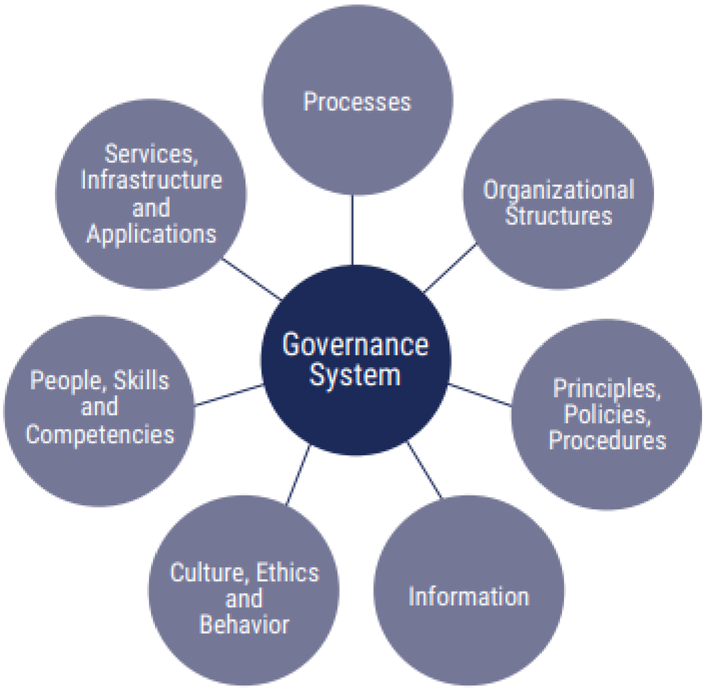

Processes
Services, Infrastructure and Applications
Organizational Structures
Governance System
People, Skills and Competencies
Principles, Policies, Procedures
Culture, Ethics and Behavior
Information

Figure 17. Components of a Governance System (ISACA 2018).

COBIT 2019 framework is built to support flexibility and customization for creating a tailored and unique governance system. The framework provides plenty of documentation and guidance. The latest version of the framework includes:

- **Introduction and Methodology** – introduces key concepts of COBIT.
- **Governance and Management Objectives** – describes the 40 core governance and management objectives. References also other standards and frameworks.
- **Designing an Information and Technology Governance Solution** – includes a workflow for planning a customized governance model for enterprise IT.
- **Implementing and Optimizing an Information and Technology Governance Solution** – implementation guide and model for continuous governance improvement.
  (ISACA 2018)

COBIT has clearly recognized the importance of governance expectations for digitalization and the fast pace on technology evolution. COBIT is also actively collaborating with its user community on a continuous basis to keep COBIT up to date with the latest trends and insights.

4.5 Summary of IT governance models and frameworks

What comes to governance methodologies and frameworks, many organizations use parts of multiple frameworks and methodologies. ITIL for service delivery, CMMI for application development, PMBOK for Project Management, TOGAF for enterprise architecture, COBIT for IT governance etc. The organization, including its various departments, might be satisfied with their own management framework. The problem in these cases can be the difficulties in IT governance for senior management, for making strategic decisions targeting a wide reach (Vyas et.al. 2016).

Andenmatten (2019) did mapping between COBIT 2019 and ITIL 4 and confirmed that both frameworks complement each other with their specific focus. Many COBIT 2019 governance management practices are not addressed in any ways ITIL 4. He also highlighted that because the new technologies, such as cloud services, AI, IoT, etc., have changed the way information is processed and services are delivered, the previous versions on both frameworks were considered outdated and therefore obsolete (Andenmatten 2019).

The older versions of these IT governance frameworks (e.g., ITIL 3, COBIT 5, TOGAF 9.1.) are also referred to as “traditional non-cloud computing governance frameworks” (The Open Group, 2016) as they do not provide governance for cloud solutions.

Many of these standards and frameworks, especially the latest versions, can be applied to work smoothly together in an organization. As an example, Vyas compared COBIT 2019 and ITIL 4, and how they support and complement each other. Vyas conclusion was that COBIT 2019 can work in harmony with ITIL 4 in any complex IT environment. And ITIL 4 practices will significantly support the implementation of a COBIT governance system in an IT environment (Vyas 2019). Figure 18 by Karttaavi (2014) shows an overview of IT governance frameworks and their main focus areas. The figure helps visualizing the use of multiple frameworks within an organization.

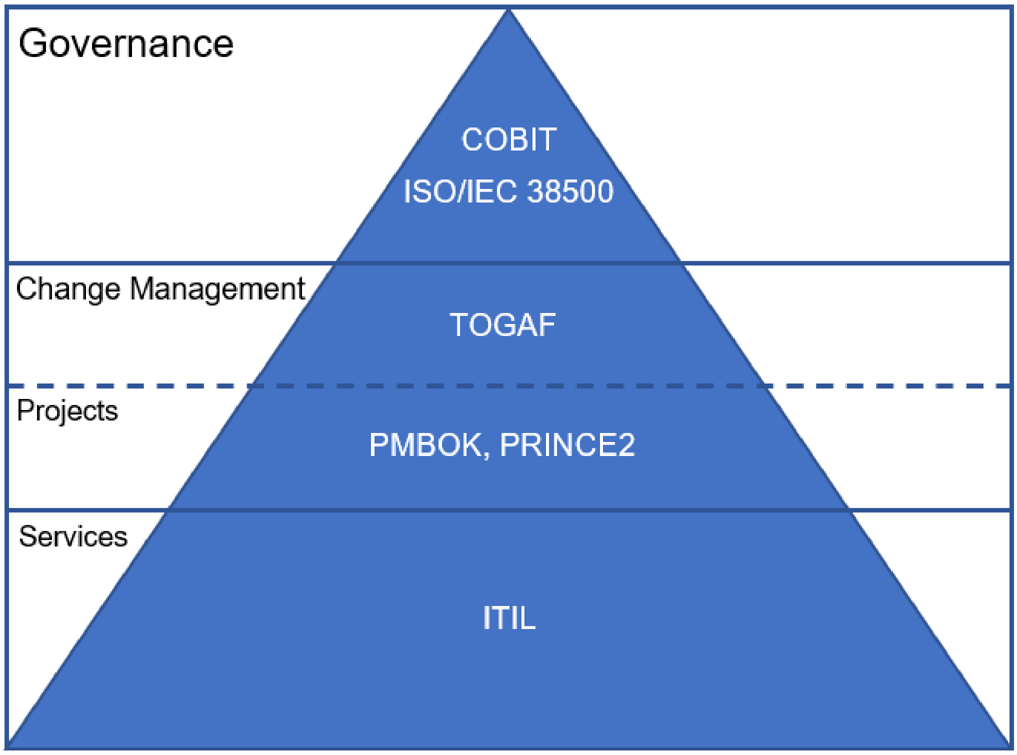


Figure 18. IT Governance Frameworks (adapted from Karttaavi 2014)

When planning and starting the task to add or migrate a new cloud governance model on top of these existing frameworks and models, it is crucial to understand what models are already in use, which versions and in what extent. There can be business units or development teams using their own model, or a modified implementation of an existing framework.

5 Cloud governance

The role of the company's IT department is changing due to the growing use of cloud computing services, and this change could positively impact some of the problematic areas of business-IT alignment. IT department has an important role to coordinate and integrate between various on-premises and cloud-based solutions. By outsourcing basic tasks to cloud providers and reassigning roles, IT department has better possibility to focus on higher level business solutions and to become the strategic partner of the business (Fuzes 2018).

To be able to effectively govern new cutting-edge cloud services, new disciplines, policies, and processes must be deployed. Cloud governance refers to the decision-making process and policies used for planning, deployment, operating and managing cloud services. Cloud governance should not be considered as a new function, rather like a governance activity that extends existing IT governance activities.

The Open Group (2016) defines cloud computing governance as:

> A view of IT governance focused on accountability, defining decision rights and balancing benefit or value, risk, and resources in an environment embracing cloud computing.

To evaluate the cloud computing governance maturity of an organization, The Open Group has developed a set of metrics that can be tracked across cloud governance processes. The metrics for cloud computing governance are:

- Level of Cloud Adoption
  - Percentage of projects that are not part of cloud transformation
  - Percentage of enterprise cloud services subscribed
  - Average number of subscribers per service
  - Actual against expected consumption
  - Percentage of consumption patterns
  - Rate of change to subscriber count
- Level of Cloud Computing Governance
  - Percentage of cloud-ability reviews exercised
  - Percentage of service compatibility reviews exercised
  - Percentage of service provider usage reviews exercised
  - Ratio of planned versus actual cloud services
  - Frequency of exceptions
- Operational Efficiency
  - Percentage of incidents reported
  - Average time to deploy
  - Average time to onboard
- Cost Reduction
  - Percentage of budget allocated to IT
- Business Value Alignment

    - Percentage of idle services decreased
    - Percentage of business service-level requirements met
    - Ratio of number of subscriptions/number of unsubscriptions
    - Number of consumer/provider combinations impacted by exceptions
- Service-Drive Integration
    - Percentage of service provider exceptions/service provider integrations
    - Percentage of enterprise services subscribed
    - Number of SLAs impacted by exceptions
- Risk Mitigation
    - Percentage of compliance with security policies
    - Percentage variance in schedule
    - Number of incidents related to unsubscribe
    - Severity of exceptions

(The Open Group 2016)

Regarding the maturity metrics, especially the Level of Cloud Computing Governance metrics are interesting as they relate to the primary focus of this thesis.

Extending IT Governance with Cloud Governance

There's a lot of academic and professional literature on cloud adoption, focusing on the benefits of cloud computing and guidance for implementation. What often gets less attention, is the impact of cloud adoption for IT governance. And when there is a study or research on this topic, most likely the impact has been evaluated against a five or more years old IT governance framework, which hasn't been updated to reflect the needs raised by the current era of digitalization. This makes many of the existing research and case studies to expire very fast, as the technology is progressing with an enormous speed, and the guidance and methodologies must keep up with it.

As introduced in the previous chapters, some of the latest versions of IT management models and standards already covers cloud governance as part of IT governance. If an organization has one of these modern versions already onboarded, it's rarely justified to add a new framework only for cloud governance.

When establishing a new cloud governance for an organization, the first task is always to understand where the organization is now, where it wants to be, how to get there and why it wants to go there. For this task the governance models and frameworks plays a big role, as they guide through the process by providing best practices, guidance, instructions and documentation. This makes it crucial that the existing governance frameworks and their versions are up to date and can support the modern requirements for governance.

One viewpoint on adding new cloud governance into existing IT governance is the new skills required by the IT staff members. Generally, the cloud services brings a lot of new resources and services that needs to be deployed, managed, and monitored. Developing new necessary skills require a comprehensive plan and relevant learning resources for the IT teams.

Additional review on cloud governance literature proposes several models and frameworks for launching a successful cloud governance. One example of such model is the proposed cloud governance reference model by Karkošková & Feuerlicht which reflects SOA governance and an older version of COBIT, the COBIT 5 back in 2017 (Karkošková & Feuerlicht 2017). The challenge with these proposed approaches for cloud governance is that they are designed and created against models and frameworks available at that time. The risk of outdated processes and guidance grows when implementing several separate governance models using different frameworks or reference models.

McGarth (2014) did a research on the impact of cloud computing on IT governance and especially when ITIL framework is already in place in the organization for traditional IT service management. McGarth found out that because the target company was focusing only on the cloud solution, instead of the company and its IT governance framework, there was several gaps identified in the existing IT governance framework. This again presented different levels of risk to the business (McGarth 2014).

Anggrainin et al. did a study on designing architecture framework to help adopting cloud solution based on ROCCA and TOGAF 9.2. The conclusion of the

Bailey & Becker (2014) presented the Cloud Governance Dial, which consists of the steps needed for implementing an appropriate IT governance for a cloud environment. The processes and components of Cloud Governance Dial is shown in figure 19.

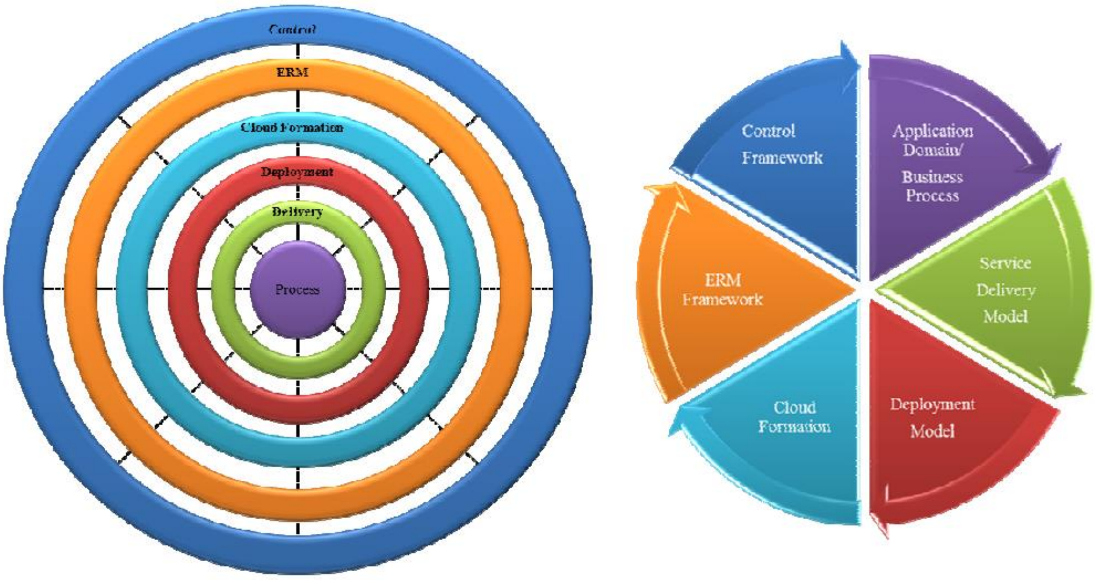


Figure 19. Cloud Governance Dial (Bailey & Becker, 2014).

The six components can be viewed as the following dials:

1. Process
    - What is moving to the cloud?
2. Delivery
    - How will it be delivered (SaaS, PaaS, IaaS)?
3. Deployment
    - How will it be deployed (Public, Private, Hybrid)?
4. Cloud Formation
    - Internal/External, Proprietary/Open, Parameterized/De-parameterized, In-sourced/Outsourced
5. ERM (Enterprise Risk Management)
    - What unique risk factors arise from steps 1-4?
6. Control
    - What are the control modifications necessary for this cloud solution?

According to Bailey and Becker (2014), the IT Cloud Governance Dial is designed to not only meet IT governance goals, but also achieves alignment with corporate governance. The process is seen as an iterative evolution, continuing to expand the Governance model together with the cloud adoption journey (Bailey & Becker, 2014).

Looking at this model today, I think it could be useful it the organization is using a legacy IT governance framework version and need to find out the required IT governance models. Bailey and Becker also states it is often not needed to replace an effective, existing well-designed IT governance framework, but the cloud governance model needs to be aligned with corporate governance.

6 Microsoft Azure

Microsoft Azure is a public cloud computing platform provided by Microsoft. Azure infrastructure is available through a continually expanding network of datacenters in global regions. There are now over 60 Azure regions globally, containing more than 160 physical datacenters linked by interconnected networks (Microsoft 2021b), which strengthens Azure's competitive global position against its competitors.

Microsoft Azure initial introduction was made with the name “Windows Azure” back in October 2008 in the Professional Developers Conference (PDC) when Microsoft announced a Community Technology Preview of Windows Azure (Microsoft 2008). The formal release was made in February 2010, when Microsoft announced the general availability of the Windows Azure platform in 21 countries (Microsoft 2010). The renaming of Windows Azure to Microsoft was announced in 2014, to reflect Microsoft's strategy and focus on Azure as a public cloud platform for both internal services and external customers (Microsoft 2014).

Microsoft Azure cloud platform runs on virtualization technology, like most of the other public cloud platforms. The range of Azure services is broad, from a simple web service up to hosting fully virtualized server architecture running custom applications and solutions. Among the wide range of services provided by Microsoft Azure, a few of them are centralized account management, database hosting, remote storage, Internet of Things (IoT), and AI services (Microsoft 2021a).

Azure market growth has been following the cloud computing market trends and the most recent Microsoft earning release, fiscal year 2021 Q2, highlighted the revenue in Intelligent Cloud was $14,6 billion with an increase of 23%. This included the server products and cloud services revenue increase of 26% driven by Azure revenue growth of 50% (Microsoft 2021e).

Microsoft Azure cloud platform is recognized as one of the top three cloud solution providers, according to Gartner's Magic Quadrant report on public cloud providers. The other two are Amazon Web Services (AWS) and Google Cloud Platform (GCP). Among enterprises customers, Microsoft benefits from their strong software-as-a-service (SaaS) footprint, which includes Office 365 and Dynamics 365 (CRM and ERP provided from cloud services). This is seen as an advantage when choosing the cloud service provider for other cloud services (ZDNet 2021).

Azure cost saving benefits

As described in previous chapter, one significant reasoning for organizations moving to public cloud services is the financial benefit. All cloud service providers have their unique strengths and advantages. According to Microsoft, some of the cost-savings options especially available for Microsoft Azure cloud services are listed below.

- **Azure Hybrid Benefit** – This is a licensing benefit where you can take benefit of existing on-premises licenses. In addition to Windows Server and SQL Server licenses, applies also to RedHat and SUSE Linux subscriptions.

- **Spot virtual machines –** Discounted pricing for unused Azure compute capacity. This is ideal for workloads that can be interrupted, such as batch processing jobs, dev and test environments, large-scale stateless applications, or visual rendering applications.

- **Reservations –** Significant discounts can apply when reserving resources in advance. With the options for one-year or three-year reservations, Azure services gets visibility on resource needs and due to being more efficient, it passes the savings to customers.

- **Azure dev and test pricing** – Discounted rates are available for development and testing purposes. As an example, there are no software charges on Azure Virtual Machines.

- **Extended security updates –** For SQL Server 2008 and SQL Server 2008 R2, which are already out of support, you can get continued support in Azure. When migrating the servers to an Azure Virtual Machine, customers receive free extended security patches.
  (Microsoft 2021d)

An important topic related to cloud financial benefits is the Cost Management function within cloud governance. The Cost Management discipline will be covered later in this thesis when describing the cloud governance methodology. For many organization consuming cloud services, the cost management is an area needing improvement. There is a risk the financial benefits presented in this chapter are not reached due to missing cost management processes. It is not sufficient to only plan and design cloud environments and solutions cost efficient, iterative, and ongoing cost optimization tasks and assessments are needed as an iterative process.

7 Microsoft Cloud Adoption Framework for Azure

The current generation of IT, where cloud computing is a new normal and businesses are embracing digital transformation, requires a new operating model for being able to take advantage of the new technologies. As we have moved to a digital world, where “digital” is no longer something distinct, the requirement for an updated Operating Model has emerged. As a result of this, a concept of Digital Operating Model has been evolved. The Cloud Adoption Framework for Azure, created by Microsoft and evolved from their Cloud Operating Model (COM), builds on Microsoft’s proven view on how to deliver a Digital Operating Model (Scarfe et.al. 2019).

An adoption framework is a common way for cloud providers to assist and guide customers on their cloud transformation journey. All three major public cloud providers, Amazon, Google, and Microsoft, have their own adoption frameworks. These adoption frameworks have a lot of similarities, but in this case study the focus is purely on Microsoft Cloud Adoption Framework for Azure.

Microsoft Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools designed to help organizations in their cloud adoption journey. The framework is built on best practices from Microsoft employees, partners, and customers who have already undertaken the cloud journey.

The Microsoft Cloud Adoption Framework is in a key role in this case study, as the cloud governance model used is based on the framework and observes the recommendations and guidance provided by the framework. The Cloud Adoption Framework is available through a web site and as a downloadable PDF-file. To give a perspective on the magnitude of the content, when downloaded as a PDF-file the document includes nearly 2000 pages.

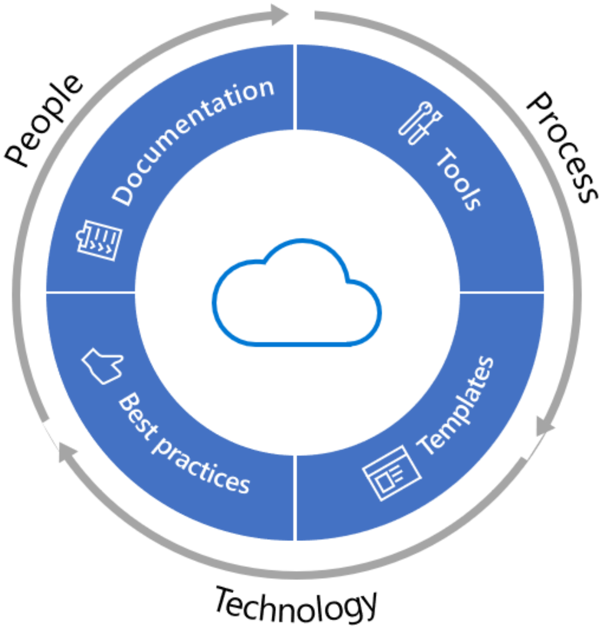


Figure 20. Cloud Adoption Framework - People, Process, Technology (Microsoft 2021f).

The Cloud Adoption Framework focuses on people, process, and technology. Figure 20 shows a high-level overview of the framework that is aligned on business, people, and technology strategy to achieve business goals with actionable, efficient, and comprehensive guidance.

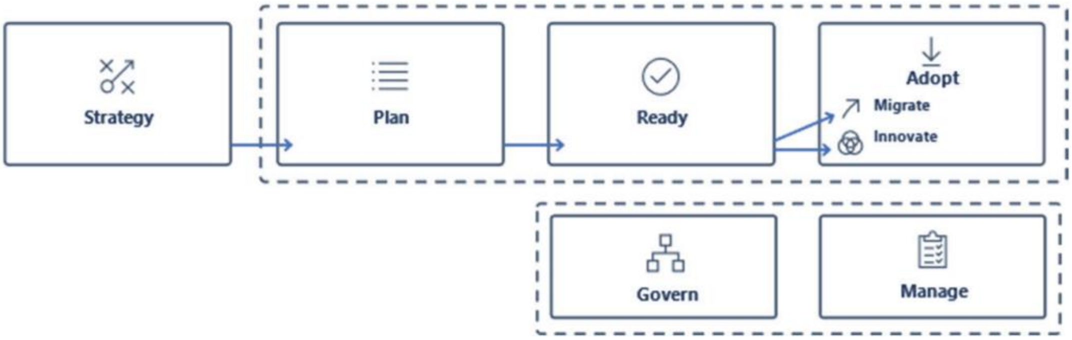


Figure 21. Cloud Adoption Framework (Microsoft 2021f).

The Cloud Adoption Framework for Azure helps organizations with their cloud journey in three main stages: Plan, Ready and Adopt. This is preceded by a business strategy phase and surrounded by an Operate phase expanding through the cloud adoption journey as shown in figure 21. The framework covers end-to-end guidance on each of these adoption journey phases:

- Strategy
    - Understand motivations to move to cloud
    - Documenting business outcomes
    - Business justification
- Plan

    - Understanding on current state of digital assets
    - Initial organization alignment
    - Skills readiness plan
    - Cloud adoption plan based on current digital estate
- Ready
    - Azure setup guide
    - First landing zone in cloud environment
    - Expand the blueprint
    - Best practice validation
- Govern
    - Basic understanding on methodology
    - Benchmark current state and future state
    - Initial best practice (MVP)
- Manage
    - Define business commitments
    - Establish an operations management baseline
    - Adapt to changing business needs
- Adopt
    - Migrate
        - First workload migration
        - Expanded scenarios
        - Best practice validation
        - Process improvements
    - Innovate
        - Innovation guide
        - Expanded scenarios
        - Best practice validation
        - Process improvements (Microsoft 2021f)

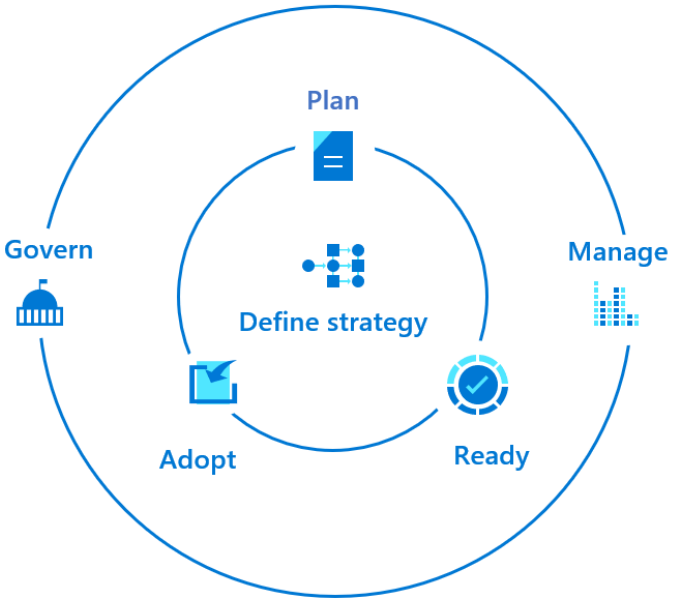


Figure 22. Cloud Adoption Framework is an iterative process (Microsoft 2021).

The cloud adoption journey using Microsoft Cloud Adoption Framework is designed as an iterative process. Figure 22 illustrates the iterative planning and how the journey starts with a vision, where the strategy is defined. With an Agile approach, the framework considers security, governance, cost-optimization, and hybrid-cloud awareness by default. Organizations change, and the processes and frameworks in use needs to support this.

7.1 Governance in Cloud Adoption Framework

For cloud governance, the Cloud Adoption Framework provides guidance by examples of actionable governance guides and helps creating customer specific governance models covering the needs for cloud governance. The guidance helps building a cloud governance strategy in parallel with cloud implementation, and supports in developing customized corporate policies, processes, and tooling.

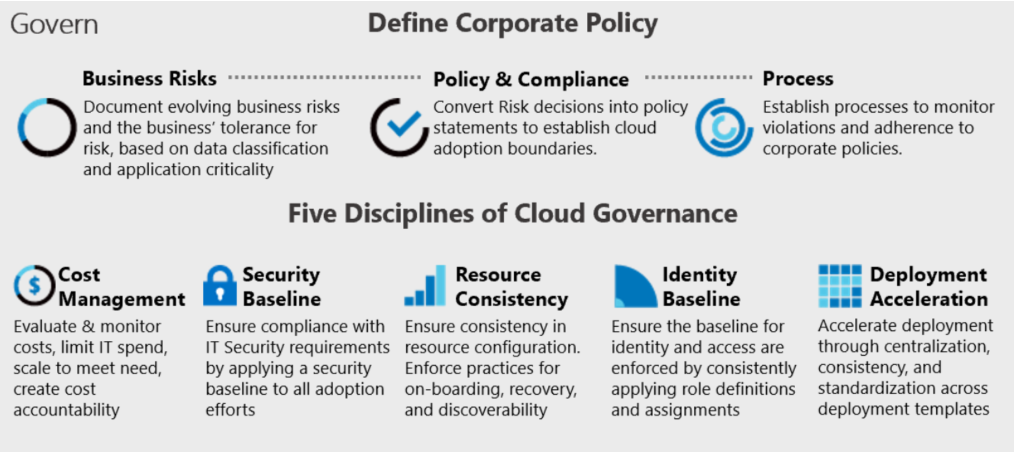
The Cloud Adoption Framework approach to cloud governance is an iterative process, where cloud governance processes and policies continually changes because of evolvement of cloud footprint and the balance of used cloud and on-premises services.

The Cloud Adoption Framework guidance steps on starting an initial governance foundation:

- Methodology
    - For a basic understanding of the methodology that drives cloud governance in the Cloud Adoption Framework to begin thinking through the end state solution.
- Benchmark
    - To assess the current state and future state for a vision for applying the framework.
- Initial governance foundation
    - Guidance to get easily started with the governance journey, helping to create an initial governance foundation, a minimum viable product (MVP).
- Improve the initial governance foundation
    - Throughout the cloud adoption and implementation, additional governance controls need to be iteratively added to support the journey.
      (Microsoft 2021f)

Governance methodology for Azure

The first step in the cloud adoption journey is to build a vision of the end state. This is normally derived from organization Digital Transformation strategy or IT strategy, which enables the Business to meet its goals. Figure 23 shows a reference for the cloud governance end state, the destination.



Govern

Define Corporate Policy

Business Risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Policy & Compliance

Convert Risk decisions into policy statements to establish cloud adoption boundaries.

Process

Establish processes to monitor violations and adherence to corporate policies.

Five Disciplines of Cloud Governance

Cost Management

Evaluate & monitor costs, limit IT spend, scale to meet need, create cost accountability

Security Baseline

Ensure compliance with IT Security requirements by applying a security baseline to all adoption efforts

Resource Consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity Baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment Acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

Figure 23. Frame of reference for adoption end state (Microsoft 2021f).

Each of these key areas in figure 23 relates to different types of risks an organization needs to address while adopting new cloud services. The governance guide steers the cloud governance team towards required actions related to the key areas in the framework. The principles of the Cloud Adoption Framework include:

Corporate policies: Corporate policies drive the cloud governance. The governance methodology focuses on following aspects:

- Business risks
    - Identifying and understanding corporate risks.
- Policy and compliance
    - Converting risks into policy statements that support any compliance requirements.
- Processes
    - Ensuring adherence to the stated policies.

Five Disciplines of Cloud Governance: These disciplines support the corporate policies. Each discipline protects the company from potential pitfalls:

- Cost Management
- Security Baseline
- Resource Consistency
- Identity Baseline
- Deployment Acceleration

A typical case in cloud adoption journeys is that cloud services are already deployed before a proper cloud governance is established. Often the business needs and expectations on operational agility and modern services raises the risk of shadow it. This has been one of the drivers for a different approach for IT governance. An *incremental govern-*

ance approach is evolved to speed up the ability to incorporate governance into implementations at any stage of the cloud journey. In the Cloud Adoption Framework this approach is called a minimum viable product (MVP).

An MVP can be created at any point in the cloud journey, but the recommendation is to adopt an MVP as early as possible. An MVP is a small set of corporate policies, processes, and tools helping with setting up the foundation for governance. The cloud governance team can work with cloud strategy teams to add new policies and guardrails to manage risks with adoption plans. With the help of these just-in-time governance layers, also known as *governance iterations*, the governance is incorporated into deployments and migrations. Figure 24 shows a governance MVP with three governance iterations. In each iteration, new corporate policies are added to remediate risks. The changes are then applied across each deployment by the Deployment Acceleration discipline.

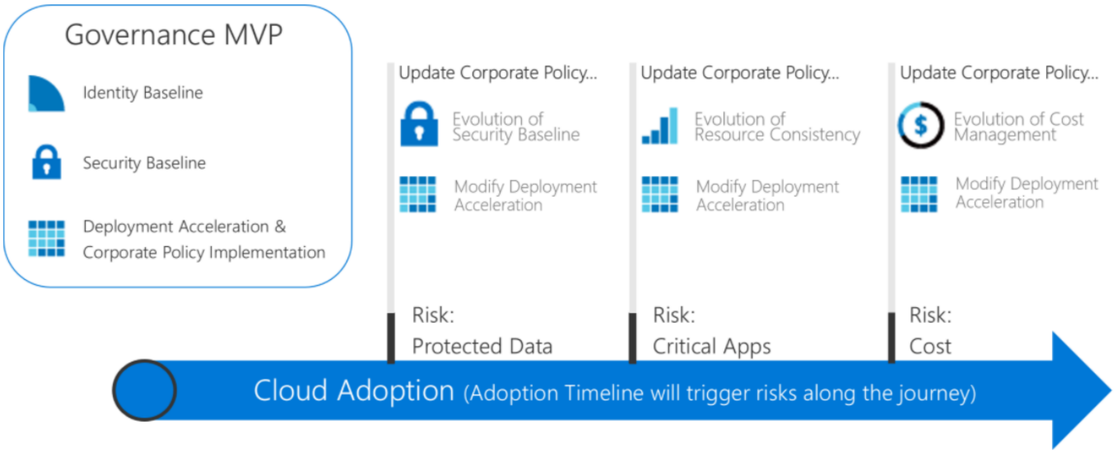

Governance MVP
Identity Baseline
Security Baseline
Deployment Acceleration & Corporate Policy Implementation
Update Corporate Policy...
Evolution of Security Baseline
Modify Deployment Acceleration
Update Corporate Policy...
Evolution of Resource Consistency
Modify Deployment Acceleration
Update Corporate Policy...
Evolution of Cost Management
Modify Deployment Acceleration
Risk: Protected Data
Risk: Critical Apps
Risk: Cost
Cloud Adoption (Adoption Timeline will trigger risks along the journey)

Figure 24. MVP with three governance iterations (Microsoft 2021f).

7.2 Updates in the framework

Microsoft builds the Cloud Adoption Framework together with its customers, partners, and internal Microsoft teams. New content is being added regularly and existing content is updated often. Microsoft actively encourages new customers and partners to join building the Cloud Adoption Framework.

8 Creating a cloud governance model

In this section the objective is to create a cloud governance model for Azure cloud services. The model is created based on guidance from the Cloud Adoption Framework for Azure. The Cloud Adoption Framework for Azure was introduced in previous chapter, and the focus in this chapter is on starting the creation of cloud governance and building a model for iterative improvement on cloud governance.

The downloaded version of Cloud Adoption Framework contains nearly 2000 pages of guidance, templates, and recommendations, whereof the governance section is almost 300 pages. The model presented in this section is an adapted, simplified, and aggregated version based on hands-on experience and years of real-life cloud adoptions.

One of the research questions defined for this thesis is: “When – At what stage during the cloud services adoption should we define and start using a cloud governance model?” This is a question that repeatedly raises up among organizations evaluating whether or not there’s a need for a defined and documented cloud governance model. A common question related to this is: ”what if we have been using cloud for some time already?”. Especially for organizations where a “cloud-first” strategy is in place and a history of several years of cloud service usage, the mindset might be that there is no need to define governance or that it is already too late for it.

The Cloud Adoption Framework Governance methodology can be added at any stage of adoption. In many organizations the cloud adoptions start with some business units using cloud service. This creates the shadow IT effect, as this has no support form the company IT. At some point there is a requirement to do integrations, add security or support to the service and here IT can have the right control and compliance, helping business units using services they require with risks mitigated. There is no end point in governance, it is a continuous cycle of evaluating risk and defining or optimizing policies to address the risk.

The concept of a minimum viable product (MVP) in the Cloud Adoption Framework was introduced in the previous chapter. Implementing an MVP is one of the first things to implement when starting the cloud adoption journey. Based on the environment complexity, there are different guides available in the Cloud Adoption Framework for standard and complex enterprises.

Figure 25 illustrates the adapted model and simplified process of creating a cloud governance model. The process is adapted, simplified, and actionable version of the guidance and recommendations provided by the Cloud Adoption Framework.

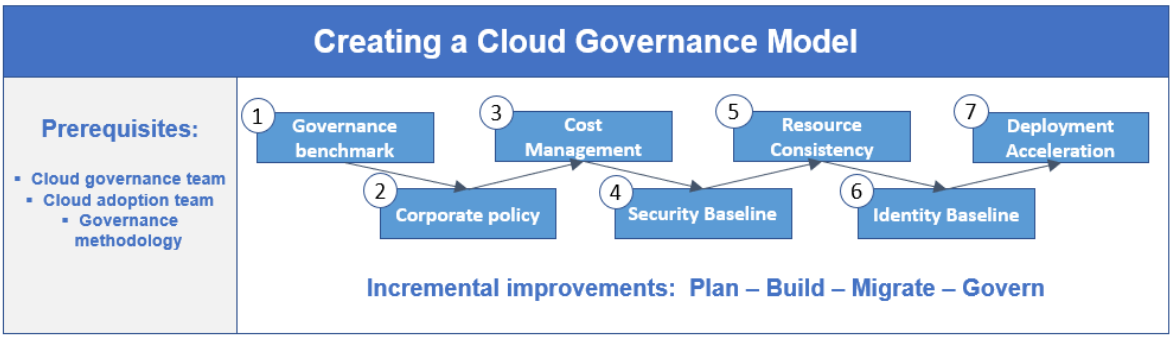


Figure 25. Creating a Cloud Governance Model.

Before starting the creation of an MVP, a basic understanding of the Cloud Adoption Framework governance methodology needs to be present. This is seen as a prerequisite, together with establishing teams within the organization for cloud governance and adoption. The next step is to establish an updated view on the current state of organization IT and cloud operations. The knowledge of current state is required to be able to envision the end state that will be used in our initial governance foundation, the MVP. For this action (1), the governance benchmark tool will be used, which is a tool provided by the Cloud Adoption Framework. Next actionable steps are: (2) Creation of Corporate policy, (3) Cost Management, (4) Security Baseline, (5) Resource Consistency, (6) Identity Baseline, and (7) Deployment Acceleration.

8.1 Cloud governance team – Prerequisites for governance

There are many options to build the teams in an organization for cloud adoption. Microsoft recommendation is to have at least two teams taking responsibility throughout the cloud adoption journey.

- **Cloud adoption team** – accountable for technical solutions, business alignment, project management, and operations for solutions that are adopted.
- **Cloud governance team** – balancing the cloud adoption team, accountable for platform maturity, platform operations, governance, and automation.

Cloud Adoption Framework describes this ‘two team’ -model as the: “Best practice, MVP”. The model is seen as an MVP because it might not be sufficient in many organizations and may need to be expanded over time.

Figure 26 illustrates the steps for establishing a cloud governance team. The cloud governance team is responsible for evaluating and managing the cloud adoption risks.

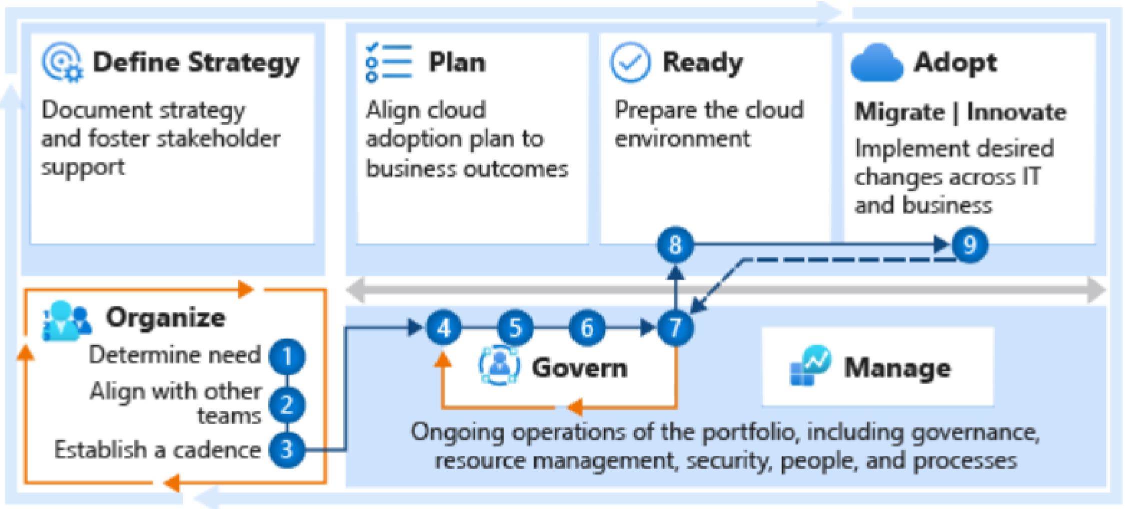

Define Strategy
Document strategy and foster stakeholder support
Plan
Align cloud adoption plan to business outcomes
Ready
Prepare the cloud environment
Adopt
Migrate | Innovate
Implement desired changes across IT and business
Organize
Determine need
1
Align with other teams
2
Establish a cadence
3
4
5
6
7
8
9
Govern
Manage
Ongoing operations of the portfolio, including governance, resource management, security, people, and processes

Figure 26. Steps for building a cloud governance team (Microsoft 2021f).

Steps for building a cloud governance team as illustrated in figure 26:

- Step 1: Determine whether a cloud governance team is needed.
  - The best practice is to always create a cloud governance team.
- Step 2: Align with other teams.
  - The cloud governance team ensures critical topics are aligned with other teams. A RACI template can be used to identify the stakeholders.
- Step 3: Establish a cadence with other teams.
  - Regular cadence with supporting teams, to stay engaged with strategy, adoption, and operations teams.
- Step 4: Review the methodology.
  - To ensure the end state vision for governance is clear and a working approach to that vision exists.
- Step 5: Complete the governance benchmark.
  - The governance benchmark assessment helps assessing governance needs and priorities.
- Step 6: Implement the initial governance best practice and configuration.
  - Implementation of the initial governance (MVP), starting with the basic tools and configurations.
- Step 7: Continuously improve governance maturity.
  - Improve the existing governance based on changes and ongoing adoption plans.
- Step 8: Evaluate landing zone changes.
  - Ensure landing zones configurations comply with governance policies.
- Step 9: Adoption handoffs.
  - Regular reviews on new adoptions to ensure proper documentations and policy alignment.
    (Microsoft 2021f)

Organizations have different needs on governance, it can be depending on the size of the organization, industry, phase on their cloud journey, or the already existing teams. The level of cloud governance maturity changes over time, as continuous cloud adoption efforts are completed.

When creating the initial governance model (MVP), the focus will be on steps 5, 6 and 7 from the cloud governance team creation steps.

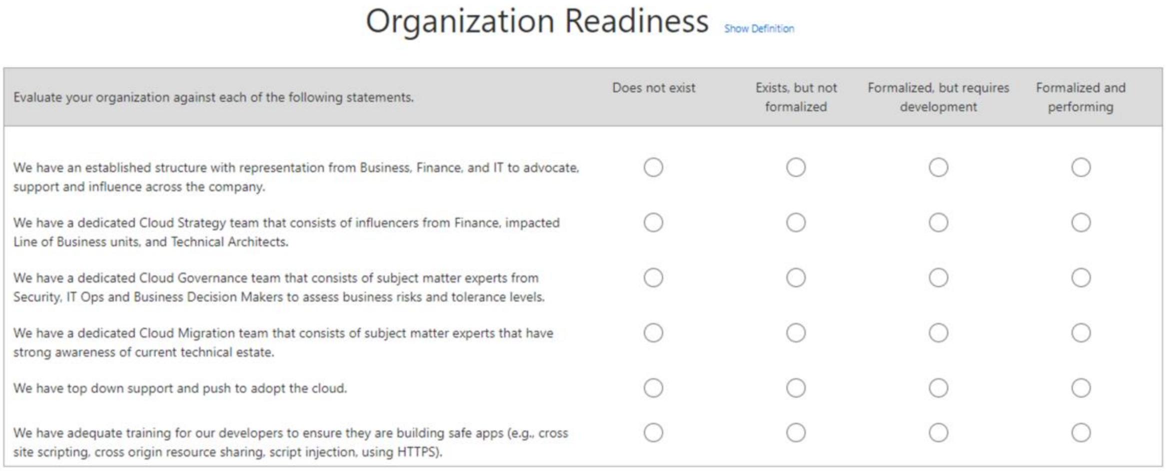
8.2 Governance benchmark tool

To be able to implement governance in a way where control and agility is balanced, it is necessary to understand the risks associated with our cloud transformation journey plans. Governance benchmark tool was designed to help understanding the gaps between current state and the desired state of governance, and the current state of relationships between business and technical teams.

The governance benchmark tool is an online experience, with three sections:

- Defining your business vision
    - Captures business objectives and goals.
- Setting your business priorities
    - Questions for understanding the end state vision for proper governance.
- Evaluating current state
    - Questions on current environment and its state of governance.

The result of the assessment shows the gaps needed to focus on to reach the vision of end state for governance. Figure 27 shows some of the assessment questions related to organization readiness.



Organization Readiness Show Definition

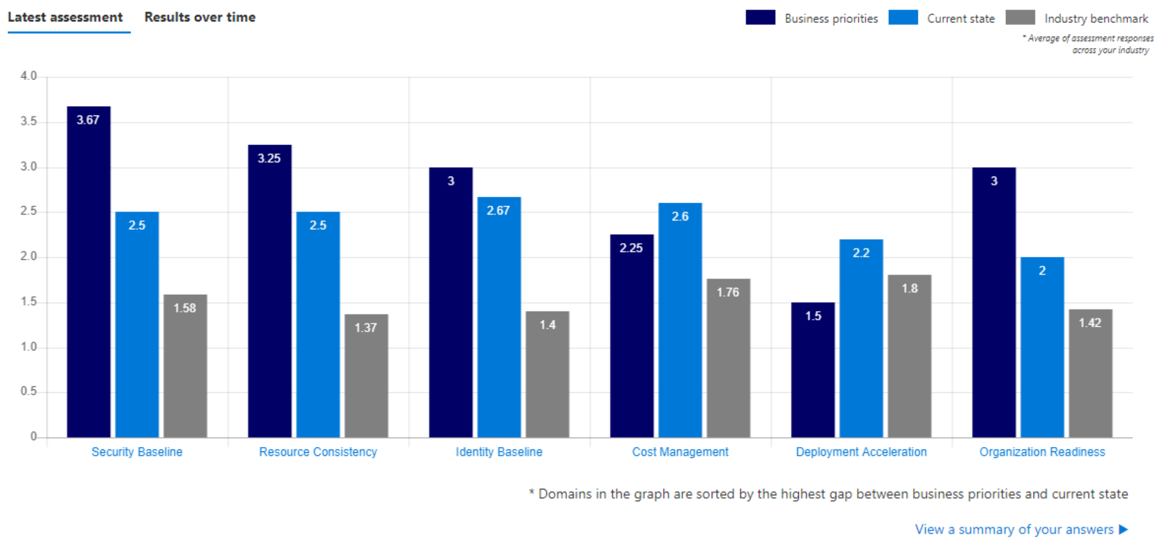
Evaluate your organization against each of the following statements.	Does not exist	Exists, but not formalized	Formalized, but requires development	Formalized and performing
We have an established structure with representation from Business, Finance, and IT to advocate, support and influence across the company.	○	○	○	○
We have a dedicated Cloud Strategy team that consists of influencers from Finance, impacted Line of Business units, and Technical Architects.	○	○	○	○
We have a dedicated Cloud Governance team that consists of subject matter experts from Security, IT Ops and Business Decision Makers to assess business risks and tolerance levels.	○	○	○	○
We have a dedicated Cloud Migration team that consists of subject matter experts that have strong awareness of current technical estate.	○	○	○	○
We have top down support and push to adopt the cloud.	○	○	○	○
We have adequate training for our developers to ensure they are building safe apps (e.g., cross site scripting, cross origin resource sharing, script injection, using HTTPS).	○	○	○	○

Figure 27. Governance Benchmark tool questions.

Figure 27 shows the results of an example assessment. The domains available for the assessment includes the *Five Disciplines of Cloud Governance* described in earlier chapter and added with organization readiness. In the analysis the following domains are included:

- Security Baseline
- Resource Consistency
- Identity Baseline
- Cost Management
- Deployment Acceleration
- Organization Readiness

In the results the organization can compare its current state to industry benchmarks, as shown in figure 28. The analysis visualizes the gap between current state and future state for the included domains. This gap should then be used for a starting point to achieve the desired state.



* Domains in the graph are sorted by the highest gap between business priorities and current state

Figure 28. Governance Benchmark tool example results.

The results can be emailed or downloaded in pdf-format for sharing and documenting purposes. If the assessment is made while signed in with an Azure account, the assessment answers can be updated, and the analysis cart will be updated accordingly.

Once the gaps are identified, the creation of an initial governance foundation, the MVP, can continue.

8.3 Initial governance foundation

When creating the initial governance foundation, or MVP (Minimum Viable Product), it is important to keep the goal in organizing Azure to reflect your company, not organizing your company to reflect Azure. The Cloud Governance team might not be familiar with the full range of Azure services available, in this case it’s recommended to start with an initial set of core services and locations, which can then be expanded over time.

In this initial governance foundation, the first step is to start with describing the initial corporate policy and create some examples. This is followed up with going through the Cloud Adoption Framework governance model five disciplines (cost management, security baseline, resource consistency, identity baseline and deployment acceleration), and create sample policies for each discipline.

8.3.1 Corporate policy

In the governance methodology the corporate policy aspects, as introduced in an earlier chapter, are business risks, policy and compliance, and processes. The MVP for corporate policy is dependent on the workloads and solutions planned or already migrated to cloud. Some organizations might start with a couple of none-critical virtual machines in the cloud, where another organization starts by moving a business-critical ERP system to the cloud. The business risks in the latter cloud adoption example are exponentially greater.

When planning for business risk, an MVP approach is often a good way to start. Defining an initial starting point and a set of assumptions that cover all, or at least the most common assets. Some of the most common risks with cloud transformations are data breach, service disruptions and budget control. Examples of business risks could be: “assets are at risk of generating too much costs” or “assets are at risk of being deleted through misconfiguration”. The business risk MVP can be updated later depending on the changes in cloud assets and new risks can be added.

A good approach in defining business risks and their tolerance is to go through a list of questions. Three question sets and examples of questions to determine the risk tolerances:

- Loss impact:
  - Could this risk cause customer loss?
  - Could this risk stop business operations?
  - Could this risk violate corporate policies?
  - Could this risk create new legal liability?
- Risk remediation cost:
  - What is needed from the business to validate the costs?
  - Is there a clear solution and what does it cost?
  - Are there options for preventing or minimizing the risk?
- Probability of loss:
  - Has any research been done regarding the likelihood of this risk being realized?
  - Are there other companies that have been hit with this risk?
  - Is this risk unique to something this company has done poorly?

Based on these questions, grouping of probability could be for example:

- No indication
- Low risk
- Medium risk
- High risk

The risk tolerance can help when discussing funding and investments. If the risk and probability is low, and remediation cost high, most likely it is difficult to get funding. If the risk and probability is high, it is much more likely to get the needed funding.

Once the risk factors are determined, the policy statements can be documented which would mitigate the risks and draw boundaries for cloud adoption. The final step in defining corporate policy is to have a clear statement on how to monitor, enforce, and remediate against any violations of those policies.

With the corporate policy defined, the next step is to begin defining policies around the governance methodology five key disciplines.

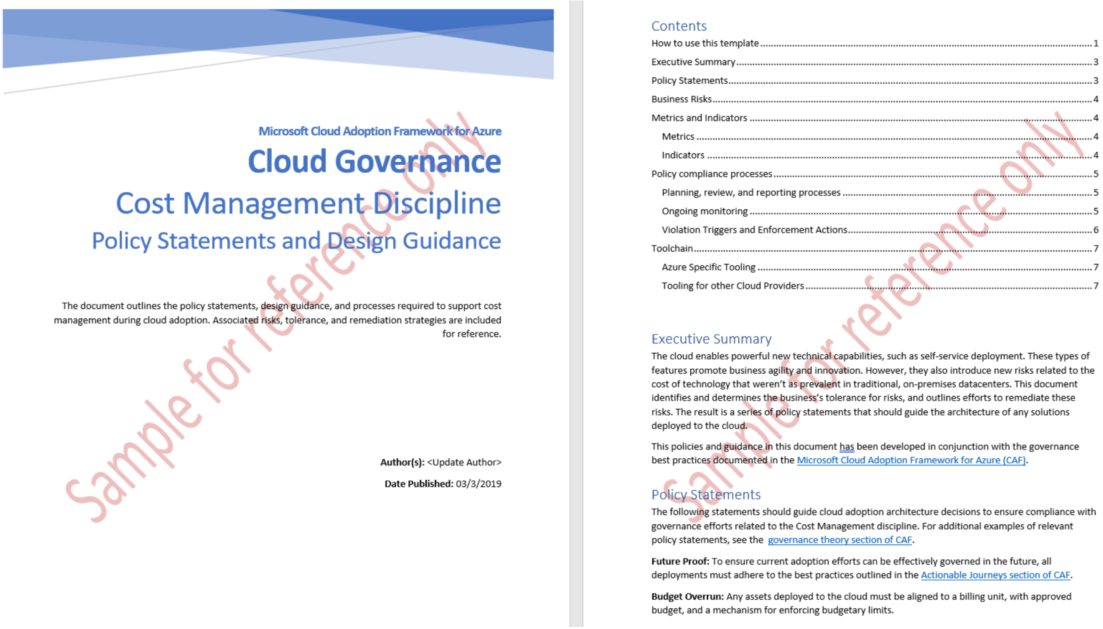
8.3.2 Cost Management

Cost management, one of the biggest concerns for many organizations, is the process to effectively plan and control the costs. The tasks related to cost management are normally carried out by finance, management, and application teams. Cost management helps to analyze costs effectively and to take actions in cloud optimization. One of the benefits in having cost management in the Azure Portal is that you can take advantage of the already existing integrations to several Azure services. You can use Azure policy to tag resources and do better cost analysis. You can implement notifications through action groups, to monitor the budgets.

The purpose of Cost Management is to identify and mitigate any Azure related risks related to IT spending, and to help business and IT teams in using cloud resources. The discipline is not replacing existing practices or procedures related to organization’s IT financing.

The goal of Cost Management discipline is to create and maintain a planned cost cycle. Once initial version of Cost Management is created, there are potential tasks that are recommended perform during different governance maturity phases, to further improve the Cost Management discipline.

Cloud Adoption Framework provides a template (figure 29) for the Cost Management discipline, which can be used as the starting point for documenting the cost management related policy statements for an organization. Another option is to use the general discipline template presented in appendix 1. Before using the template, you should make sure the planned policies align to you cloud governance strategy. The primary roles working with the template are cloud architects and the cloud governance team.



Microsoft Cloud Adoption Framework for Azure

Cloud Governance

Cost Management Discipline

Policy Statements and Design Guidance

The document outlines the policy statements, design guidance, and processes required to support cost management during cloud adoption. Associated risks, tolerance, and remediation strategies are included for reference.

Author(s): <Update Author>

Date Published: 03/3/2019

Contents

Executive Summary

The cloud enables powerful new technical capabilities, such as self-service deployment. These types of features promote business agility and innovation. However, they also introduce new risks related to the cost of technology that weren't as prevalent in traditional, on-premises datacenters. This document identifies and determines the business's tolerance for risks, and outlines efforts to remediate these risks. The result is a series of policy statements that should guide the architecture of any solutions deployed to the cloud.

This policies and guidance in this document has been developed in conjunction with the governance best practices documented in the Microsoft Cloud Adoption Framework for Azure (CAF).

Policy Statements

The following statements should guide cloud adoption architecture decisions to ensure compliance with governance efforts related to the Cost Management discipline. For additional examples of relevant policy statements, see the governance theory section of CAF.

Future Proof: To ensure current adoption efforts can be effectively governed in the future, all deployments must adhere to the best practices outlined in the Actionable Journeys section of CAF.

Budget Overrun: Any assets deployed to the cloud must be aligned to a billing unit, with approved budget, and a mechanism for enforcing budgetary limits.

Figure 29. Cost Management template (Microsoft 2021f).

For Cost Management policy statements each statement definition should include the following piece of information:

- Business risk
  - A summary of the risk this policy will address.
- Policy statement
  - A clear summary explanation of the policy requirements.
- Design options
  - Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

Sample policy for Cost Management – Over optimization:

- Business risk:
  - Effective cost management creates new risks. Optimization of spending is inverse to system performance. When reducing costs, there is a risk of overtightening spending and producing poor user experiences.
- Policy statement:
  - Any asset that directly affects customer experiences must be identified through grouping or tagging. Before optimizing any asset that affects customer experience, the cloud governance team must adjust optimization based on at least 90 days of utilization trends. Document any seasonal or event-driven bursts considered when optimizing assets.
- Design options:

    - In Azure, “Azure Monitor's insights features” can help with analysis of system utilization.
    - There are several options for grouping and tagging resources based on roles. In Azure, you should choose a resource consistency model in conjunction with the governance team and apply this to all assets.

Additional samples:

- For tracking purposes, all assets must be assigned to an application owner within one of the core business functions.
- When cost concerns arise, additional governance requirements will be established with the finance team.
- Allowed Azure Region for Resources and Resource Groups.
- Allowed Azure Virtual Machines sizes (SKUs).
  (Microsoft 2021f)

8.3.3 Security Baseline

The primary purpose of Security Baseline discipline in Cloud Adoption Framework is to identify and mitigate any risks and concerns related to cloud security. Each organization, regardless of its size and industry, needs to understand the core security related business risks and their impact. The risks vary a lot based on organization’s industry, regulatory requirements, needs for sensitive data, demanding workloads, etc.

The recommendation is to use template provided by the Cloud Adoption Framework for the Security Baseline discipline, or the general discipline template presented in appendix 1. The template can be used as a starting point for documenting the organization’s policy statements related to cloud security. Before using the template, you should make sure the planned policies align to you cloud governance strategy.

For Security Baseline policy statements, each statement definition should include the following piece of information:

- Technical risk
    - A summary of the risk this policy will address.
- Policy statement
    - A clear summary explanation of the policy requirements.
- Technical options
    - Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

Sample policy for Security Baseline – Security review:

- Technical risk:

    - Effective cost management creates new risks. Optimization of spending is inverse to system performance. When reducing costs, there is a risk of overtightening spending and producing poor user experiences.
- Policy statement:
    - Trends and potential exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tools used in the cloud.
- Potential design option:
    - Establish a regular security review meeting that includes relevant IT and governance team members. Review existing security data and metrics to establish gaps in current policy and Security Baseline tools, and update policy to remediate any new risks. Use Azure Advisor and Azure Security Center to gain actionable insights on emerging threats specific to your deployments.

Additional samples:

- All deployed assets must be categorized by criticality and data classification.
- All protected data must be encrypted when at rest.
- Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.
- All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.
- No public facing web site backed by IaaS should be exposed to the internet without DDoS.
- Governance tooling must audit and enforce network configuration requirements defined by the Security Baseline team.
  (Microsoft 2021f)

8.3.4 Resource Consistency

The Resource Consistency discipline identifies potential business risks when managing cloud resources and provides mitigation guidance teams managing and operating the resources. Resource management, delivered by cloud operations teams, includes monitoring, automation, scaling and remediation activities and the Resource Consistency discipline ensures these are designed as repeatable processes.

Examples of common business risks related to core operations of resources, that should be considered in Resource Consistency discipline planning and documented:

- Unnecessary operational cost
- Underprovisioned resources
- Management inefficiencies
- Business interruption

In addition to the general discipline template presented in appendix 1, the Cloud Adoption Framework provides a template also for the Security Baseline discipline. The template can be used as a starting point for creating the policy statements related to resource consistency.

For Resource Consistency policy statements, each statement definition should include the following piece of information:

- Technical risk
  - A summary of the risk this policy will address.
- Policy statement
  - A clear summary explanation of the policy requirements.
- Technical options
  - Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

Sample policy for Resource Consistency – Disaster recovery:

- Technical risk:
  - Resource failure, deletions, or corruption can result in disruption of mission-critical applications or services and the loss of sensitive data.
- Policy statement:
  - All mission-critical applications and protected data must have backup and recovery solutions implemented to minimize business impact of outages or system failures.
- Potential design option:
  - The Azure Site Recovery service provides backup, recovery, and replication capabilities that minimize outage duration in business continuity and disaster recovery (BCDR) scenarios.

Additional samples:

- All deployed assets must be categorized by criticality and data classification.
- Subnets containing mission-critical applications must be protected by a firewall solution capable of detecting intrusions and responding to attacks.
- Governance tooling must audit and enforce network configuration requirements defined by the Security Management team.
- Governance tooling must validate that all assets related to mission-critical apps or protected data are included in monitoring for resource depletion and optimization.
- Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.
  (Microsoft 2021f)

8.3.5 Identity Baseline

Identity Baseline discipline identifies business risks related to identities and provides mitigation guidance for teams implementing, managing, and operating organization identity management services. In traditional IT, with on-premises directories, securing infrastructure and application environments was normally done by controlling access on the networking level, granting access only for use within internal networks. Modern cloud identity sets new requirements for securing the identity, where the authentication and access controls have been expanded to the internet.

One of the first, and most crucial, questions to ask when starting with the public cloud is "who should have access to resources?" and "how do I control this access?"

Common business risks related to identity services, that should be considered in Identity Baseline planning and documented are for example:

- Unauthorized access
- Multiple identity solutions and systems
- Sharing resources to external users
- Dependencies with on-premises resources

The Cloud Adoption Framework provides a template also for the Identity Baseline discipline. The template helps creating the organization’s policy statements related to cloud identity.

For Identity Baseline policy statements, each statement definition should include the following piece of information:

- Technical risk
    - A summary of the risk this policy will address.
- Policy statement
    - A clear summary explanation of the policy requirements.
- Technical options
    - Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

Sample policy for Identity Baseline – Weak authentication mechanism:

- Technical risk:
    - Identity management systems with insufficiently secure user authentication methods, such as basic user/password combinations, can lead to compromised or hacked passwords, providing a major risk of unauthorized access to secure cloud systems.
- Policy statement:
    - All accounts are required to sign in to secured resources using a multi-factor authentication method.
- Potential design option:
    - For Azure Active Directory, implement Azure Multi-Factor Authentication as part of your user authorization process.

Additional samples:

- All assets deployed to the cloud should be controlled using identities and roles approved by current governance policies.
- A least-privilege access model will be applied to any resources involved in mission-critical applications or protected data.
- Elevated permissions should be an exception, and any such exceptions must be recorded with the cloud governance team. Exceptions will be audited regularly.
- All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved RBAC role.
- Deployment of any applications that require customer authentication must use an approved identity provider that is compatible with the primary identity provider for internal users.
  (Microsoft 2021f)

8.3.6 Deployment Acceleration

The purpose of Deployment Acceleration discipline is to identify risks and provide mitigation guidance to the teams responsible for managing cloud resources. Activities included in the Deployment Acceleration discipline would be deployments, scaling and failover tasks, and automating disaster recovery. DevOps or DevSecOps are nowadays seen as an efficient way to manage deployments, as automation plays a big role in provisioning and configurating cloud resources. Looking at the maturity of organizations using cloud providers, the level of automation is one of the differentiators.

Common business risks associated to Deployment Acceleration that should be addressed during cloud adoption:

- Service disruption
  - Lack of predictable repeatable deployment processes or unmanaged changes to system configurations can disrupt normal operations and can result in lost productivity or lost business.
- Cost overruns
  - Unexpected changes in configuration of system resources can make identifying root cause of issues more difficult, raising the costs of development, operations, and maintenance.
- Organizational inefficiencies
  - Barriers between development, operations, and security teams can cause numerous challenges to effective adoption of cloud technologies and the development of a unified cloud governance model.

To be able to quantify business risk for Deployment Acceleration discipline, it is recommended to define metrics and indicators for the risk. Common examples for this:

- Deployment failures
  - Percentage of deployments that fail or result in misconfigured resources.
- Time to deployment

    - The amount of time needed to deploy updates to an existing system.
- Assets out-of-compliance
    - The number or percentage of resources that are out of compliance with defined policies.

For Deployment Acceleration policy statements, each statement definition should include the following piece of information:

- Technical risk
    - A summary of the risk this policy will address.
- Policy statement
    - A clear summary explanation of the policy requirements.
- Design options
    - Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The Deployment Acceleration discipline policy statements, related to cloud configuration and deployment issues, can be documented using one of the templates provided by the Cloud Adoption Framework.

Sample policy for Deployment Acceleration – Automation on deployment and configuration:

- Technical risk:
    - Relying on human intervention during deployment or configuration increases the likelihood of human error and reduces the repeatability and predictability of system deployments and configuration. It also typically leads to slower deployment of system resources.
- Policy statement:
    - All assets deployed to the cloud should be deployed using templates or automation scripts whenever possible.
- Design options:
    - Azure Resource Manager templates enable using infrastructure as code to deploy your resources to Azure. You could also use Terraform as a consistent on-premises and cloud-based deployment tool.

Additional samples:

- Key metrics and diagnostics measures will be identified for all production systems and components.
- Operations will consider using monitoring and diagnostic tools in nonproduction environments such as Staging and QA to identify system issues before they occur in the production environment.
- Cloud governance processes must include monthly review with configuration management teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.
  (Microsoft 2021f)

8.4 Governance model incremental improvements

Once the initial version of governance model is created, there are many recommended tasks to be performed during the various governance maturity phases. The purpose is to further improve the existing governance model and each of its key discipline.

Figure 30 shows the phases in a cloud solution implementation, which are planning, building, adopting (migrating) and operating (govern) phases. For improving the initial governance foundation, through an incremental approach, several activities are recommended to be engaged for each phase.

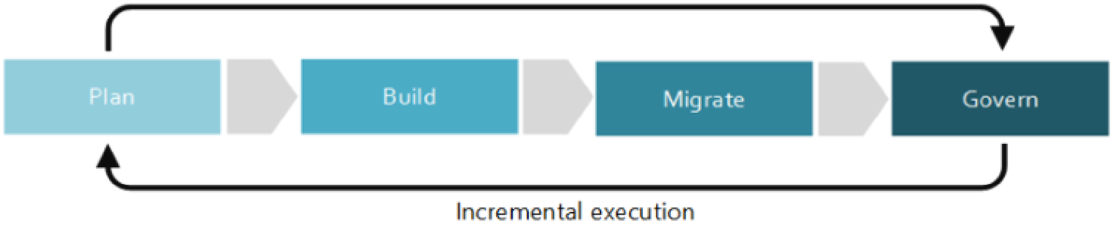


Figure 30. Phases of and incremental approach to cloud governance (Microsoft 2021f).

The adoption phases and the suggested activities by the Cloud Adoption Framework for different key disciplines:

- Planning and readiness
  - The phase where leadership team defines specific metrics, and the deployments are planned.
  - Examples of recommended and potential activities for the phase:
    - Evaluate the management tools available and the benefits they introduce to this phase.
    - In migrations, create initial architecture guidelines document.
    - Perform knowledge transfer regarding architecture guidelines and share information within teams.
    - Understand the cloud accounting model and how costs are allocated.
    - Adjust budgets and align them with business goals.
- Build and predeployment
  - The focus in this phase is on activities before a migration or deployment, e.g., readiness and decisions.
  - Examples of recommended activities:
    - Deploy the chosen management tools during predeployment.
    - Update any design documents and architecture guidelines and share to impacting teams.
    - Create documentation and other materials to help drive user adoption.

        - Align purchase requirements with existing budgets.
        - Revise any cost discrepancies that affects migration plans.

- Adopt and migrate
    - The phase when applications or workloads are deployed and adopted to cloud.

    - Examples of recommended activities:
        - Make sure Cost Management tools are migrated from dev/test to production.
        - Update any design documents and architecture guidelines and share to impacting teams.
        - Create documentation and other materials to help drive user adoption.
        - Implement a cloud accounting model.
        - Monitor budgets and validate changes.

- Operate and post-implementation
    - In this governance maturity phase, when migration is complete, the focus is on activities coming after implementation and the transformation cycle stabilizes.
    - Examples of recommended activities:
        - Review recent updates in available Cost Management tools and evaluate current requirements.
        - Enhance reports, monitoring and notifications on Azure spending.
        - Validate need of resources and their efficient usage.
        - Perform analysis on value and cost reporting methods on a periodic basis.

As with the governance model, also cloud teams and their responsibilities are often created and defined by following the MVP-mindset, meaning starting with a minimum structure. Improving team skills and expanding the structure of the cloud governance team is often needed as the maturity of cloud governance increases. Reviewing this need and documenting the progress is recommended on regular basis.

One common and well-known tool used for defining the responsibilities across different teams is the RACI (responsible, accountable, consulted, informed) chart. If an organization has created a RACI matrix for cloud operations, it should be aligned also during the cloud governance iterations.

9 Conclusions

The purpose of this thesis was to (1) clarify the role of a cloud governance model, (2) raise the awareness of cloud governance importance in the adoption of cloud services, (3) and to introduce a simplified process for creating a cloud governance model, and (4) guidance to incorporate cloud governance into existing IT governance model. The goal was to provide tangible guidance for organizations embarking or evolving their cloud journey supporting digital transformation.

This chapter reviews the research questions and how well the objectives of the thesis have been achieved. My thoughts on further development of the research, and a reflection on my learnings during the thesis will conclude the chapter and the thesis.

The objective of introducing a simplified process for cloud governance model creation was presented in chapter eight, in figure 25. The process consists of defined prerequisites, six steps to build the governance model, and a four-phase iterative process for the incremental improvements.

The research questions identified for this thesis was the: “What, Why, How and When”.

1. What is cloud governance, what should it include and at what extent?
2. Why do we need a cloud governance model?
3. How do we create a cloud governance model and migrate it to an existing IT governance model?
4. When (at what stage during the cloud journey) should we define and start using a cloud governance model?

The first question regarding what cloud governance is and what it should include was described in the literature review part of the thesis, in chapters three (Background on governance) and five (Cloud governance). It was first clarified what the role of governance is within organizations, how different governance layers are related to each other, and how the academic and professional literature defines them. This background clarification of governance layers set the scope and understanding of cloud governance positioning within an organization governance landscape. Additionally, it gave clarification on the aspects and topics that governance generally contains. It was shown cloud governance is part of IT governance by extending it, not replacing it. Chapter five described also in more detail the topics a valuable governance model should include.

The second question, why we need a cloud governance model, was answered through a literature review in chapter five, Cloud governance. To be effectively governed, the new and modern cloud services require new policies and processes to be deployed. In the same chapter, it was also presented metrics how to evaluate the current level of organization's cloud governance maturity. These metrics of maturity can help justifying the question why a cloud governance model is needed. Common control needs for organizations are related to regulatory compliance, cost control, security, and consistency in design.

The third question, how do we create a cloud governance model and migrate it to an existing IT governance model, was answered with the help of Microsoft Cloud Adoption Framework and its methodologies and guidance on cloud governance. In chapter eight the creation of an initial cloud governance model was described with tangible examples, templates and guidance. The prerequisites for cloud governance were also introduced in chapter eight and this provided guidance on how to build a cloud governance team within an existing IT organization. Clear and actionable steps were provided to build a cloud governance team together with RACI model to identify stakeholders and responsibilities within the organization.

The fourth and last question was the question regarding the timing for the creation of a cloud governance model. This was described before and during the creation of the initial cloud governance model in chapter eight. It was identified that many organizations incorporate cloud governance only after business units or development teams already been using the cloud offerings for some time and it is revealed risks need to be mitigated. During the process of creating the initial cloud governance model, it was identified in each step how to proceed if there already is an existing culture or process for the task. It was also advised by examples and guidance how to incorporate a culture of an iterative process for continuous improvement and evolvement of cloud governance. There is no end point in governance, but the recommendation is to address it early to ensure the successful usage of cloud services within and organization.

My favorable view is that this thesis has reached its objectives and I feel confident organizations preparing, embarking, or evolving their cloud adoption journey would benefit of the results this thesis provides.

9.1 Further development

It has been very rewarding to deepen my knowledge on governance models and frameworks, and to do research on the topics covered in this thesis. A lot of new findings and interesting themes has arrived during the process of the case study research. There are many aspects worth additional investigation and research regarding cloud computing and cloud governance.

For further development, one of the most interesting activity would be to set the newly created model of creating the initial cloud governance model into real-life action. To establish cloud governance team and build a governance model with a real and existing company. The model created and proposed in this thesis was created based on one experienced person view and experience on cloud adoptions within organizations, and a natural next step for the model would be to get it assessed by other experienced experts in cloud architecture, governance, and adoption area. It would also be valuable to get feedback by cloud experts on other than Microsoft platform, perhaps AWS or Google cloud experts.

Another path for further development would be to analyze how the created model would work together with ITIL and/or COBIT frameworks.

9.2 Reflecting on my learnings

I have been working in IT field in many roles for more than twenty years and with organizations using public cloud services for more than ten years. Even though cloud services are part of my daily work, I felt cloud governance is something I need to get more perspectives on. I've seen customers struggle with missing cloud governance models and management processes, and by having a holistic view on governance in general would help me framing the discussions with them. The document analysis and literature reviews provided me a lot of tools and knowledge on the topic.

One personal goal I had for this thesis was to deepen my knowledge on Azure Cloud Adoption Framework and especially the Governance area of the framework. This goal was successfully achieved, and this will have a positive impact on my everyday work.

It was highly rewarding to find new perspectives on cloud computing and governance through numerous case studies, academic literature, and commercial articles. There is a significant amount of content and research literature available on digitalization and cloud related topics. I made a very important note already in the beginning of the thesis work, which was to always start by checking the release date of the publication. For most of the material and literal related to cloud services, more than five years old publish time meant it was outdated.

I was fortunate to have an experienced thesis supervisor who gave me valuable help and confidence throughout the process. I'm thankful for all the support and meaningful Teams meetings.

References

Andenmatten, M. 2019. ITIL4 – COBIT2019 MAPPING. Available on: https://blog.itil.org/2019/05/itil4-cobit2019-mapping/. Accessed: 22.4.2021.

Armbrust et al. (2010). A View of Cloud Computing. Communications of the ACM, 50-58. Available on: https://www.researchgate.net/publication/220422375_A_View_of_Cloud_Computing. Accessed: 21 April 2021.

Axelos, 2020. Building IT and digital excellence with ITIL 4 White Paper. Axelos Limited, London.

Bailey, E. & Becker, J. 2014. A Comparison of IT Governance and Control Frameworks in Cloud Computing. Twentieth Americas Conference on Information Systems. Savannah, USA.

Briggs, B. 2019. Enterprise Cloud Strategy. 3rd edition. Microsoft Corporation. Available on: https://azure.microsoft.com/mediahandler/files/resourcefiles/enterprise-cloud-strategy-third-edition/Enterprise_Cloud_Strategy_3rd_edition.pdf. Accessed: 25 April 2021.

BT Forum 2020. The Business Technology Standard, Version 4.0.1. The Business Technology Forum. Available on: https://www.managebt.org. Accessed: 25 April 2021.

CIGREF 2005. The place of IT Governance in the Enterprise Governance. Institut de la Gouvernance des Systemes d’Information. Available on: https://cigref.typepad.fr/itgifrance/files/place_IT_governance_in_enterprise_governance.pdf. Accessed: 22 March 2021.

Deloitte & Nyenrode 2016. Good Governance driving Corporate Performance? A meta-analysis of academic research & invitation to engage in the dialogue. The Netherlands. Available on: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-good-governance-driving-corporate-performance.pdf. Accessed: 12 May 2021.

Flexera 2020. Flexera State of the Cloud Report. Available on: https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020. Accessed: 25 April 2021.

Forrester 2019. The Total Economic Impact™ Of Microsoft Azure IaaS. Forrester Consulting. Available on: https://azure.microsoft.com/mediahandler/files/resourcefiles/b97e0ab9-3aff-49b4-af44-eaf1bef33085/Azure%20IaaS%20Total%20Economic%20Impact%20Report%20(TEI)%202017%20by%20Forrester.pdf. Accessed 25 April 2021.

Fuzes, P. 2018. “How Does Cloud Computing Change the Strategic Alignment Between Business and IT?” Proceedings of the Fifth International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC2018). pp. 1-6.

Gartner 2021a. Gartner Glossary, Cloud Computing. Available on: https://www.gartner.com/en/information-technology/glossary/cloud-computing. Accessed: 25 April 2021.

Gartner 2021b. Gartner Glossary, IT Governance. Available on: https://www.gartner.com/en/information-technology/glossary/it-governance. Accessed: 28 April 2021.

Gartner 2020. Gartner Says Worldwide IaaS Public Cloud Services Market Grew 37.3% in 2019. Gartner Newsroom. Available on: https://www.gartner.com/en/newsroom/press-releases/2020-08-10-gartner-says-worldwide-iaas-public-cloud-services-market-grew-37-point-3-percent-in-2019. Accessed: 25 April 2021.

Gheorghe, M. (2010). Audit Methodology for IT Governance. Informatica Economica, Academy of Economic Studies - Bucharest, Romania, vol. 14(1), pages 32-42. Available on: https://www.researchgate.net/publica-tion/43121541. Accessed: 23.4.2021.

Harisaiprasad, K. 2020. COBIT 2019 and COBIT 5 Comparison. Available on: https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison. Accessed: 22 April 2021.

IDC 2021. Public Cloud IT Infrastructure Revenue Growth Remained Strong in Third Quarter of 2020, According to IDC. Available on: https://www.idc.com/getdoc.jsp?containerId=prUS47279621. Accessed: 25 April 2021.

IFAC 2003. Enterprise Governance - Getting the Balance Right. Available on: https://www.ifac.org/system/files/publications/files/enterprise-governance-gett.pdf. Accessed: 12 April 2021.

ICSA s.a. The Chartered Governance Institute. Available on: https://www.icsa.org.uk/about-us/policy/what-is-corporate-governance. Accessed: 2 March 2021.

ISACA 2019. Introducing COBIT 2019. Available on: https://www.isaca.org/resources/news-and-trends/industry-news/2018/introducing-cobit-2019-the-motivation-for-the-update. Accessed: 22 March 2021.

ISACA 2018. COBIT 2019 Framework: Introduction & Methodology. ISACA. IL, USA.

ISO 2015. ISO/IEC 38500:2015, Information technology — Governance of IT for the organization, 2021. Available on: https://www.iso.org/standard/62816.html. Accessed: 25 April 2021.

ISO 2021. ISO/IEC WD 38500, Information technology — Governance of IT for the organization, 2021. Available on: https://www.iso.org/standard/81684.html. Accessed: 25 April 2021.

ISO 2014. ISO/IEC 17788. Information technology – Cloud computing – Overview and vocabulary. Available on: https://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip. Accessed: 25 April 2021.

IT governance 2021. What is IT governance. Align IT with your business strategy with best-practice IT governance models and frameworks. Available on: https://www.itgovernance.co.uk/it_governance. Accessed 1 March 2021.

IT Governance Institute (ITGI) 2003. Board Briefing on IT Governance, 2nd Edition. IT Governance Institute. USA.

Karkošková, S. & Feuerlicht, G., 2017. Cloud Computing Governance Reference Model for Cloud Service Consumers. Proceedings of the 29th International Business Information Management Association Conference-Education Excellence and Innovation Management through Vision 2020: From Regional Development Sustainability to Global Economic Growth.

Maher, M., Andersson, T. 1999. Corporate Governance: Effects on firm performance and economic growth. OECD. Eindhoven, the Netherlands. Available on: https://www.oecd.org/sti/ind/2090569.pdf. Accessed: 12 May 2021.

McGrath, D. 2014. Impact of Cloud Computing on IT Governance. EMC.

Mell, P., Grance, T. 2011. The NIST definition of cloud computing. National Institute of Standards and Technology. Available on: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Accessed: 25 April 2021.

Microsoft 2021a. Azure documentation. Available on: https://docs.microsoft.com/en-us/azure/?product=featured

Microsoft 2021b. Azure geographies. Available on: https://azure.microsoft.com/en-us/global-infrastructure/geographies/. Accessed: 25 April 2021.

Microsoft 2008. Introducing Windows Azure. Available on: https://azure.microsoft.com/en-us/blog/introducing-windows-azure/. Accessed: 25 April 2021.

Microsoft 2021c. Cloud Economics. Available on: https://azure.microsoft.com/en-us/overview/cloud-economics/. Accessed: 25 April 2021.

Microsoft 2021d. Demystifying cloud economics. Available on: https://azure.microsoft.com/en-us/blog/demystifying-cloud-economics/. Accessed: 25 April 2021.

Microsoft 2021e. Earnings Release FY21 Q2. Available on: https://www.microsoft.com/en-us/Investor/earnings/FY-2021-Q2/press-release-webcast. Accessed: 25 April 2021.

Microsoft 2021f. Microsoft Cloud Adoption Framework for Azure. Available on: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/. Accessed: 25 April 2021.

Microsoft 2014. Upcoming Name Change for Windows Azure. Available on: https://azure.microsoft.com/en-us/blog/upcoming-name-change-for-windows-azure. Accessed: 25 April 2021.

Microsoft 2010. Windows Azure Platform Now Generally Available in 21 Countries. Available on: https://azure.microsoft.com/en-us/blog/windows-azure-platform-now-generally-available-in-21-countries/. Accessed: 25 April 2021.

MITRE 2021a. Enterprise Governance. Available on: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/enterprise-governance. Accessed: 22 April 2021.

MITRE 2021b. IT Governance. Available on: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/enterprise-planning-and-management/it-governance%20/. Accessed: 8 February 2021.

Muhamet Gërvalla, Naim Preniqi,Peter Kopacek, 2018. IT Infrastructure Library (ITIL) framework approach to IT Governance. IFAC-PapersOnLine, Elsevier. https://www.sciencedirect.com/science/article/pii/S2405896318329562

OECD 2015. G20/OECD Principles of Corporate Governance, OECD Publishing, Paris. Available on: http://dx.doi.org/10.1787/9789264236882-en. Accessed: 8 May 2021.

O'Loughlin M. 2019. ITIL 4 and the Cloud. Axelos Limited. Available on: https://www.axelos.com/case-studies-and-white-papers/itil-4-and-the-cloud. Accessed: 25 April 2021.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 3.-4. painos. Helsinki: Sanoma Pro Oy.

Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. 2009. “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility.” Future Generation Computer Systems 25 (6): 599–616.

Scarfe D., Morris S., Bennett F., Bricknell R. 2019. Building a Digital Operating Model with the Microsoft Cloud Adoption Framework for Azure? 1visionOT Pty Ltd trading as Smart Questions. Australia. Available on: https://azure.microsoft.com/en-us/resources/building-a-digital-operating-model-with-microsoft-cloud-adoption-framework/. Accessed: 22 March 2021.

The Open Group, 2016. Cloud Computing Governance Framework. Published by The Open Group, December 2016. Available on: http://www.opengroup.org/cloud/gov_snap-shot/p1.htm. Accessed: 21 April 2021.

Karttaavi T. 2014. Tietohallinnon johtamisen ja suunnittelun viitekehykset. Presentation in FCG ICT-forum 12.2.2014. Available on: https://www.slideshare.net/tommikarttaavi/ict-foorumi20140212. Accessed: 8 February 2021.

Vyas V. 2019. ITIL 4 and COBIT White Paper. Axelos Limited, London.

Vyas V., GEIT, Al Ghaith J., Al Yaqoobi A., Hasan S. 2016. Dubai Customs COBIT 5 Implementation. ISACA Industry News. Available on: https://www.isaca.org/resources/news-and-trends/industry-news/2016/dubai-customs-cobit-5-implementation. Accessed: 25 April 2021.

Wikipedia 2021a. Cloud computing. Available on: https://en.wikipedia.org/wiki/Cloud_computing. Accessed: 7 March 2021.

Wikipedia 2021b. Microsoft Azure. Available on: https://en.wikipedia.org/wiki/Microsoft_Azure. Accessed: 25 April 2021.

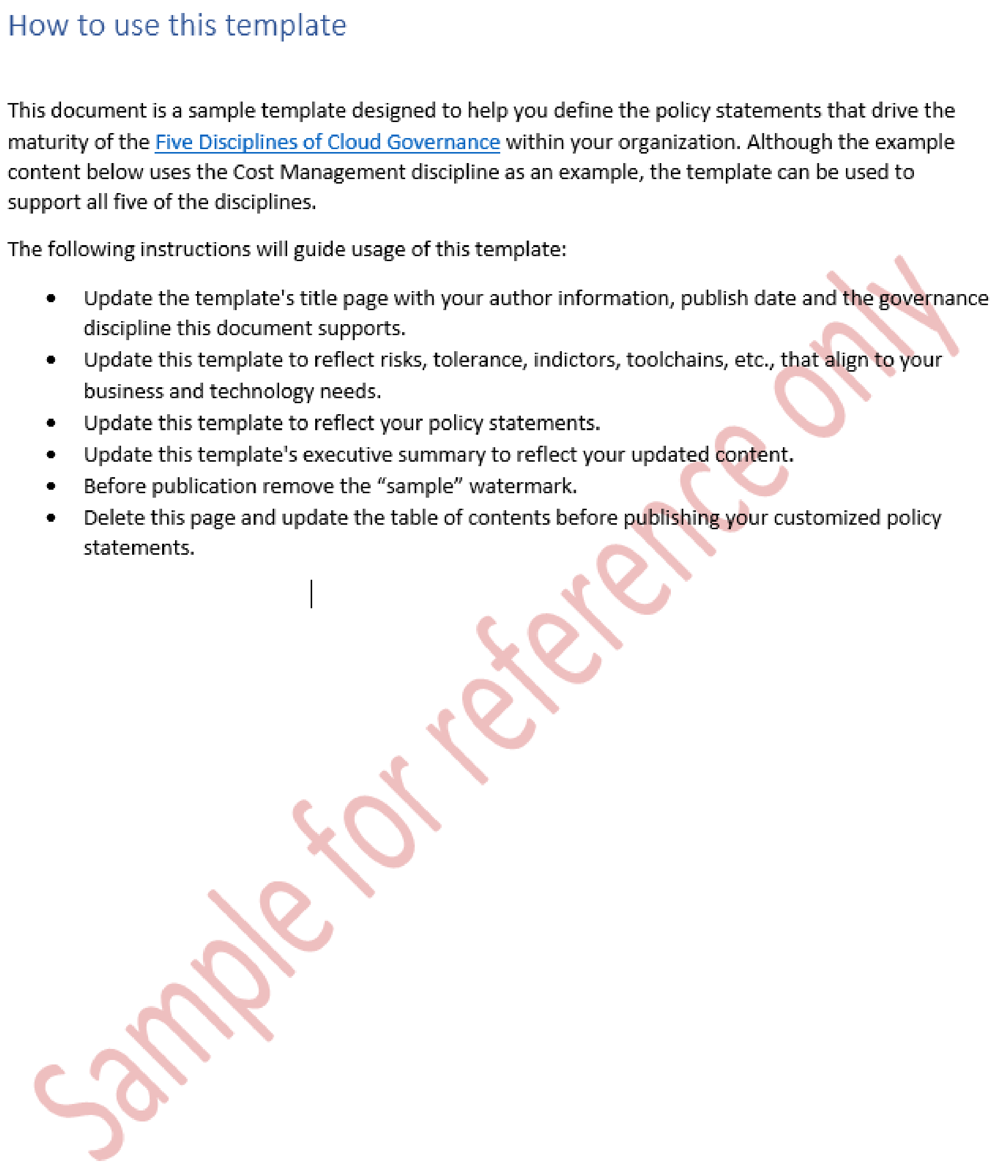
Wikipedia 2021c. ITIL. Available on: https://en.wikipedia.org/wiki/ITIL. Accessed: 25 April 2021.

Yin R. 2018. Case study research and applications: design and methods. Sixth edition. Los Angeles, US. SAGE.

ZDNet 2021. Top cloud providers in 2021: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players. Available on: https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/. Accessed: 8 February 2021.

Attachments

Appendix 1. Governance discipline -template

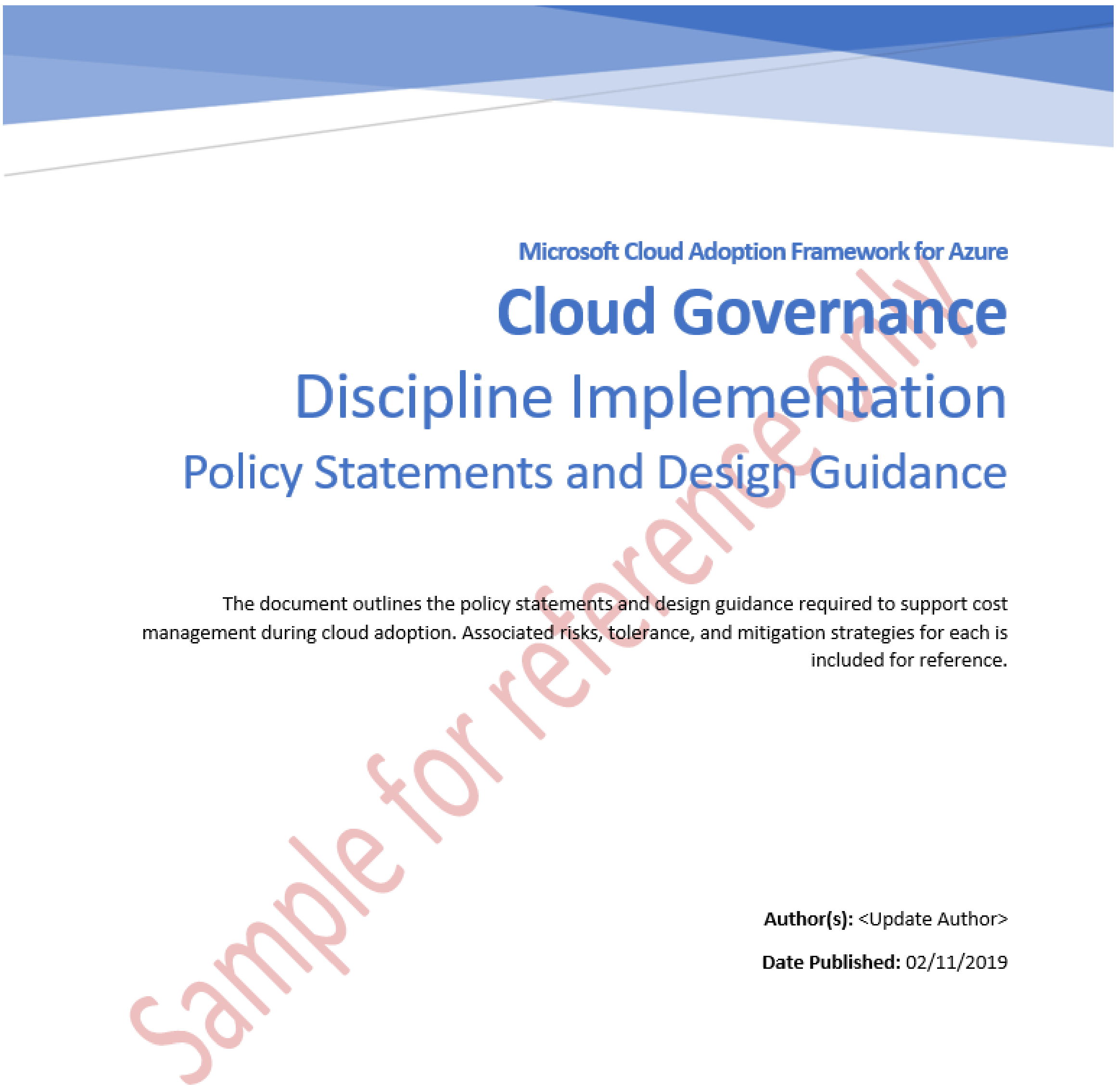


How to use this template

This document is a sample template designed to help you define the policy statements that drive the maturity of the Five Disciplines of Cloud Governance within your organization. Although the example content below uses the Cost Management discipline as an example, the template can be used to support all five of the disciplines.

The following instructions will guide usage of this template:

- Update the template's title page with your author information, publish date and the governance discipline this document supports.
- Update this template to reflect risks, tolerance, indictors, toolchains, etc., that align to your business and technology needs.
- Update this template to reflect your policy statements.
- Update this template's executive summary to reflect your updated content.
- Before publication remove the “sample” watermark.
- Delete this page and update the table of contents before publishing your customized policy statements.



Microsoft Cloud Adoption Framework for Azure

Cloud Governance

Discipline Implementation

Policy Statements and Design Guidance

The document outlines the policy statements and design guidance required to support cost management during cloud adoption. Associated risks, tolerance, and mitigation strategies for each is included for reference.

Author(s): <Update Author>

Date Published: 02/11/2019

Contents

Executive Summary

The cloud enables powerful new technical capabilities, such as Self-Service Deployment. These types of features promote business agility and innovation. However, they also introduce new risks related to the cost of technology that weren't as prevalent in traditional, on-premises datacenters. This document identifies these risks, along with the business's tolerance for said risks. It also outlines efforts to mitigate said risks. The result is a series of policy statements that should guide the architecture of any solutions deployed to the cloud.

This document has been developed in conjunction with the governance best practices documented in the Microsoft Cloud Adoption Framework for Azure (CAF).

Policy Statements

The following statements should guide your cloud adoption architecture decisions to ensure compliance with governance efforts related to this management discipline. For additional examples of relevant policy statements, see the governance theory section of CAF.

Future Proof: To ensure current adoption efforts can be effectively governed in the future, all deployments must adhere to the best practices outlined in the Actionable Journeys section of CAF.

Budget Overrun: Any assets deployed to the cloud must be aligned to a billing unit, with approved budget, and a mechanism for enforcing budgetary limits.

Over Provisioned Assets: All deployed assets must be registered with a solution that can monitor usage and report on any over provisioned resources.

Business Risks

The following cost related business risks have been identified as concerns based on the current plans for cloud adoption. For additional examples of relevant business risks, see the governance theory section of CAF.

Risk	Description	Indicators	Resolution
Future Proof	Lack of standards will hinder future governance.	Current	Policy Statement enforced
Budget Overrun	Budget overruns are a potential risk in the future.	Next Major Release	Policy Statement drafted but not enforced
Over Allocation	Paying too much for unused resources is a potential future risk.	Monthly spend exceeds $1M USD	Policy Statement drafted but not enforced

Metrics and Indicators

The following are key metrics and indicators that will guide the resolution or mitigation of business risks. For additional examples of relevant metrics or indicators, see the governance theory section of CAF.

Metrics

This governance discipline attempts to govern and improve the following key metrics.

- Annual Spend: The total annual cost for services provided by a cloud provider.
- Monthly Spend: The total monthly cost for services provided by a cloud provider.
- Forecast vs Actuals Ratio: The ratio comparing forecasted and actual spend (Monthly or Annual).
- Pace of adoption (MOM) Ratio: The percentage of the delta in cloud costs from month to month.

Indicators

The following indicators will trigger changes in policy statements based on changes in metrics and other conditions.

- Current: Current state of metrics. Any policy statements listed as current should be actively enforced.
- Release based indicator: Upon the next major release, there will be a sufficient risk of budget overrun to warrant budget controls.
- Monthly spend: When monthly spend exceeds $1M USD, new policy statements will go into effect to better control spending.

Processes

The following section outlines the process for monitoring the metrics governed by this discipline. It also identifies situational triggers that would suggest deviation from current policy statement. For each, the actions to be taken to enforce policy are documented as well. For additional examples of relevant monitoring and enforcement processes, see the governance theory section of CAF.

Primary Process for Monitoring

Deployment Planning: Prior to deployment of any asset, establish a forecasted budget based on expected cloud allocation.

Annual Planning: On an annual basis, perform a roll up analysis on all deployed and to be deployed assets. Align budgets by business units, teams, or other appropriate divisions to empower self-service adoption. Ensure the leader of each billing unit is aware of the budget and how to track spend.

This could be a good point in time to make a pre-commitment or pre-purchase to maximize discounting. It could be wise to align annual budgeting with the cloud vendor's fiscal year to further capitalize on year end discount options.

Quarterly Planning: On a quarterly basis, review budgets with each billing unit leader to align forecast and actual spend. If there are changes to the plan or unexpected spending patterns, align and reallocate the budget.

Monthly Reporting: On a monthly basis, report actual spending against forecast.

Violation Triggers and Enforcement Actions

Monthly Budget Deviations: Any deviations in monthly spend exceeding 20% Forecast vs Actuals ratio will be discussed with billing unit leader. Resolutions or changes in forecast will be recorded.

Pace of Adoption: Any deviation at a subscription level exceeding 20% will trigger a review with billing unit leader. Resolutions or changes in forecast will be recorded.

Toolchain

The following cloud provider specific tools will be implemented to automate the policy statements in this document. For additional examples of relevant tooling specific to Azure, see the governance theory section of CAF.

Azure Specific Tooling

Budget Control: Azure Cost Management

Enforce spend controls across subscriptions: Azure Policy

Detect Over Provisioning: Azure Advisor

Tooling for other Cloud Providers

List similar tools for other cloud providers, as needed.