UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE

Cloud for Official Statistics

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

This publication is issued in English.

Photocopies and reproductions of excerpts are allowed with proper credits.

This publication is issued in English.

Preface

In recent years, numerous official statistics organisations have embarked on a journey to adopt cloud computing. It brings many opportunities to make organisations more efficient and responsive to policy and user needs. Organisations are at very different stages in their cloud adoption: some are considering cloud computing; some are implementing it; some have already executed important production processes in this environment; and, others are already maintaining their cloud environment, including a new round of procurement round.

The UNECE High-Level Group on the Modernisation of Official Statistics (HLG-MOS) recognized the importance of cloud computing and the varying level of maturity among organisations. The latter was not perceived as an issue, but rather as an opportunity to initiate a collaborative project. While organisations must respect country-specific laws and regulations to protect the privacy and security of citizens, they also face similar types of challenges. It is in this context that IT experts from several organisations got together to share and learn from their experiences, successes and challenges.

This publication is the result of the collaboration from the HLG-MOS Cloud for Official Statistics Project. It shares with the broad official statistical community a base of knowledge and experiences on which managers can make sound informed decisions along their statistical organisation’s cloud adoption journey.

Acknowledgements

We would like to acknowledge the significant effort and contribution from all the project participants. To complete a high quality document while managing the day to day work of individual workloads is a significant challenge and the effort and enthusiasm shown is acknowledged.

This publication is prepared based on the reports from the UNECE HLG-MOS Cloud for Official Statistics Project:

- Chapter 1 - Background: Authors - Claude Julien (UNECE Project Manager) and Keith Scanlon (Ireland)
- Chapter 2 - Cloud Service and Deployment Models: Theme leader - Branko Josipovic (Serbia); Main author - Roger Schuncken (Netherlands)
- Chapter 3 - Cloud Procurement: Main author - Mihai Cosma (Eurostat); Theme leader: Neville DeMendonca (United Kingdom); Theme experts - Andrew Sinkinson (Canada), Ken Rennoldson (United Kingdom) and Karl MacKenzie (United Kingdom)
- Chapter 4 - Cloud Adoption: Theme leader and main author - Keith Scanlon (Ireland); Theme experts and authors - Anne-Marte Krogsrud (Norway), Blair Cardno (New Zealand) and Nemanja Trbojevic (Serbia)
- Chapter 5 - Cloud by Security and Privacy: Theme leader and main author - Anton Örn Karlsson (Iceland); theme experts and authors - Timo Rauta (Finland), Toni Räikkönen (Finland) and Nebojsa Tolic (Serbia)
- Chapter 6 - Cloud Capacity and Competencies: Theme leaders and authors - Ian Bale (Canada) and Andrew Sinkinson (Canada); Theme experts: Adam Rumbold (Australia), Chris Penner (United Kingdom) and Trygve Falch (Norway)
- Chapter 7 – Conclusion and Recommendations: Project leader - John Conway (Ireland)

A big thanks to John Conway for his leadership and direction, Claude Julien for his energy and passion, and Amilina Kipkeeva for her professional support and innovation in bringing the project to deliver this publication on time and to a high standard.

TABLE OF CONTENTS

1. Background

Cloud computing, or simply cloud, is growing very rapidly. It is “the on-demand availability of computing resources (such as storage and infrastructure), as services over the internet. It eliminates the need for individuals and businesses to self-manage physical resources themselves, and only pay for what they use”[1]. In 2023, “Gartner forecasts worldwide public cloud end-user spending to reach nearly $600 billion in 2023” and “that by 2026, 75% of organisations will adopt a digital transformation model predicated on cloud as the fundamental underlying platform”[2]. Over the years, cloud adoption strategies have ranged between cloud-only, cloud-first and, more recently, cloud-smart[3]. While cloud technology offers many advantages, many organisations have very good reasons to retain some parts of their legacy on-premises IT infrastructure[4].

Cloud Adoption in Government

Cloud adoption has become a prominent strategic initiative for government entities worldwide, as they recognise the transformative potential of cloud computing in enhancing operational efficiency, scalability, and service delivery. Embracing cloud technology allows governments to optimise resource utilisation, improve data accessibility, and foster innovation across various sectors.

Government agencies have traditionally deployed and delivered IT systems on-premises. The adoption of cloud computing by the government is also recognised at the European level, confirming cloud computing as a critical enabler for the European Commission Digital Strategy 2018, which sets out a vision for a digitally transformed and user-focused administration. Likewise, the United Nations Department for Economic and Social Affairs reports that governments now realise the necessity of adopting cloud computing environments. In Canada, the Government of Canada renewed its cloud strategy in 2018 in-line with a Cloud-First policy and updated its strategy in 2023 based on the principle of a cloud smart[5]. In New Zealand, the Government instituted a Cloud First Policy in 2016, and this has recently been refreshed[6]. In the Netherlands the national government issued in

[1] https://cloud.google.com/learn/what-is-cloud-computing

[2] https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

[3] https://silk.us/blog/why-you-should-go-cloud-smart-not-cloud-first/

[4] https://www.spiceworks.com/tech/cloud/articles/cloud-vs-on-premise-comparison-key-differences-and-similarities/

[5] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[6] https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/about/cabinet-requirement/

2022 an implementation framework for risk assessment cloud usage[7] which describes for which cases the use of public cloud services is permitted and what are the obligations when public cloud services are being used.

Cloud Adoption in Statistical Organisations

National Statistical Organisations (NSOs), as vital components of government organisations, are also embarking on this journey to leverage the benefits of cloud adoption. Chiefs Statisticians and senior management recognise its immense strategic importance for the continued success of statistical bodies. By embracing cloud technology, NSOs are better positioned to produce relevant, timely and accurate information that supports evidence-based decision-making. The drivers for cloud adoption encompass the following aspects:

- There is a growing demand from government, businesses, citizens, and researchers for statistics and insights. Cloud adoption enables statistical agencies to meet this demand by providing scalable and efficient infrastructure for data storage, processing, and analysis.

- The use of administrative data is increasing, leading to significant volumes of data being stored and processed. Cloud solutions offer the necessary scalability and storage capacity to handle large datasets effectively, enabling efficient data management and analysis.

- The emergence of new administrative big data sources, such as web scraping, scanner data, mobile phone data, and shipping data, necessitates the ability to handle larger and richer datasets. Cloud technologies provide the computational power and storage capabilities required for processing and deriving insights from these vast and diverse data sources.

- The increasing procurement and implementation difficulties arise as new products are designed to work specifically in a cloud environment. Adapting these technologies to on-premises situations becomes necessary, but it can pose challenges as they are primarily optimised for cloud usage.

- There is a growing concern for ensuring the highest level of security for critical systems and data. Cloud adoption offers advanced security measures, including encryption, access controls, and robust data protection protocols, to safeguard sensitive information and mitigate security risks.

- The requirement for large-scale, temporary infrastructure arises in various scenarios such as conducting a population census. Cloud computing provides a feasible solution to meet these needs efficiently, as it offers flexible and scalable resources that can be provisioned and deprovisioned as required.

[7] https://www.rijksoverheid.nl/documenten/rapporten/2023/01/05/implementatiekader-risicoafweging-cloudgebruik

- The use of cloud computing is identified as a critical enabling factor in several governmental strategies, emphasising the importance of leveraging cloud technologies to achieve digital transformation and enhance service delivery.

- There is a desire to ensure that cloud adoption maximises value and enhances the customer experience while upholding trust and confidentiality. Cloud solutions can offer cost-effectiveness, scalability, and improved service delivery, enabling organisations to achieve these objectives while maintaining data privacy and security.

Cloud for Official Statistics Project

The transition to cloud-based solutions in organisations comes with numerous challenges, considerations and, on some occasions, barriers that are well documented. It also brings issues that are unique or more prominent in NSOs. Unlike traditional businesses, statistical bodies have distinct requirements, such as data confidentiality, security, and compliance with statistical standards. Chiefs Statisticians and senior management need to be aware of these specific considerations and understand the potential benefits and risks associated with cloud adoption in the statistical context.

With this in mind, the UNECE High-Level Group for the Modernisation of Official Statistics (HLG-MOS) launched a cloud for Official Statistics Project in March 2023 to inform NSOs on the opportunities and challenges in cloud adoption. The project aimed to bring together IT experts to share their knowledge and experiences in cloud adoption; collaborate in gathering good practices; and share them with the official statistics community. The project was developed by the HLG-MOS Blue-Sky Thinking Network and at the time it was launched, five main themes were identified: **Models**; **Cloud Procurement**; **Cloud Adoption**; **Cloud Security and Privacy**; and **Cloud Capacity and Competencies**.

The Project brought together 17 experts from 10 NSOs under the leadership of the Ireland CSO with support from the UNECE Secretariat. The experts shared and collaborated from March to December 2023. They were divided into subgroups to address each cloud adoption theme. They met virtually to collaborate on their respective theme and share the fruits of this collaboration with the whole group of experts. One in-person meeting hosted by the Statistical Office of the Republic of Serbia took place in September in Belgrade. This meeting included a webinar at which the early developments of the project were shared and input from attendees were sollicited. The project concluded with the delivery of a webinar in November and the publication of this document.

Objectives of the publication

This publication aims to explore the specific barriers and challenges faced by NSOs in adopting cloud technology, while also highlighting the experiences and lessons learned from official statistics organisations. By addressing these challenges and leveraging best practices, NSOs can effectively navigate the cloud adoption landscape and drive meaningful transformation in their operations. Hereafter, NSOs include both national and international bodies whose main mission is to produce and deliver official statistics.

This publication shares the work of experts drawn from research on cloud adoption in organisational contexts. It analyses relevant experiences and experimentations from theoretical frameworks, providing a practical understanding of how cloud adoption has been addressed and is currently being researched within the official statistics community. Through the extraction of guidelines, recommendations, and key decision points, the publication provides actionable insights tailored to the production of official statistics.

It is important to note that it also serves as a valuable starting point, providing a first version based on current knowledge and experiences. Cloud adoption is an evolving field, and NSOs need to continuously explore, experiment, and reflect on their cloud strategies. It is crucial to acknowledge that the publication is a foundation that can be improved through ongoing cloud experimentation, development, and use in NSOs. Collaboration and knowledge sharing among statistical bodies will be essential for further advancements in cloud adoption.

In conclusion, cloud adoption in statistical organisations is of utmost importance. This publication aims to equip NSOs with the necessary knowledge and insights to make informed decisions and guide their organisations on a successful cloud adoption journey. By addressing the unique challenges and opportunities in cloud adoption for statistical bodies, the publication aims to empower statistical organisations to produce more relevant and high-quality information, enabling better decision-making.

Structure of the publication

The remainder of this publication consists of the knowledge, experiences and practices gathered on each cloud adoption theme. Chapter 2 describes cloud service and deployment models, as well as their key advantages and considerations relevant to organisations in various contexts. A common set of considerations needed in the procurement of cloud services, from key legalities to exit strategies, are layed out in Chapter 3. Chapter 4 explores elements focused around understanding the behaviours that support NSOs adoption of cloud technologies. The elements include perspectives or perceptions from internal (staff, senior management) and external stakeholders (public, indigenous/minority people, data sovereignty). The security and privacy considerations relating to the use of cloud which may enhance or inhibit its adoption across statistical organisations are described in Chapter 5. Chapter 6 follows with the capacity and competencies needed for the adoption and utilisation of cloud. Topics reviewed include staff skills development, acquisition, retention and culture. The publication concludes with selected recommendations on each theme and the need to continue collaboration within your organisation, with partner organisations and peer organisations.

The project identified early in its work the importance of clearly defining key concepts to enable readers to best understand the opportunities and challenges in adopting cloud. Many of these concepts are relevant to most themes addressed in this publication. Again, in order to avoid repetition, key concepts are defined once as much as possible. To avoid having readers searching the internet for some of these concepts, many are defined in Annex 1 for quick reference.

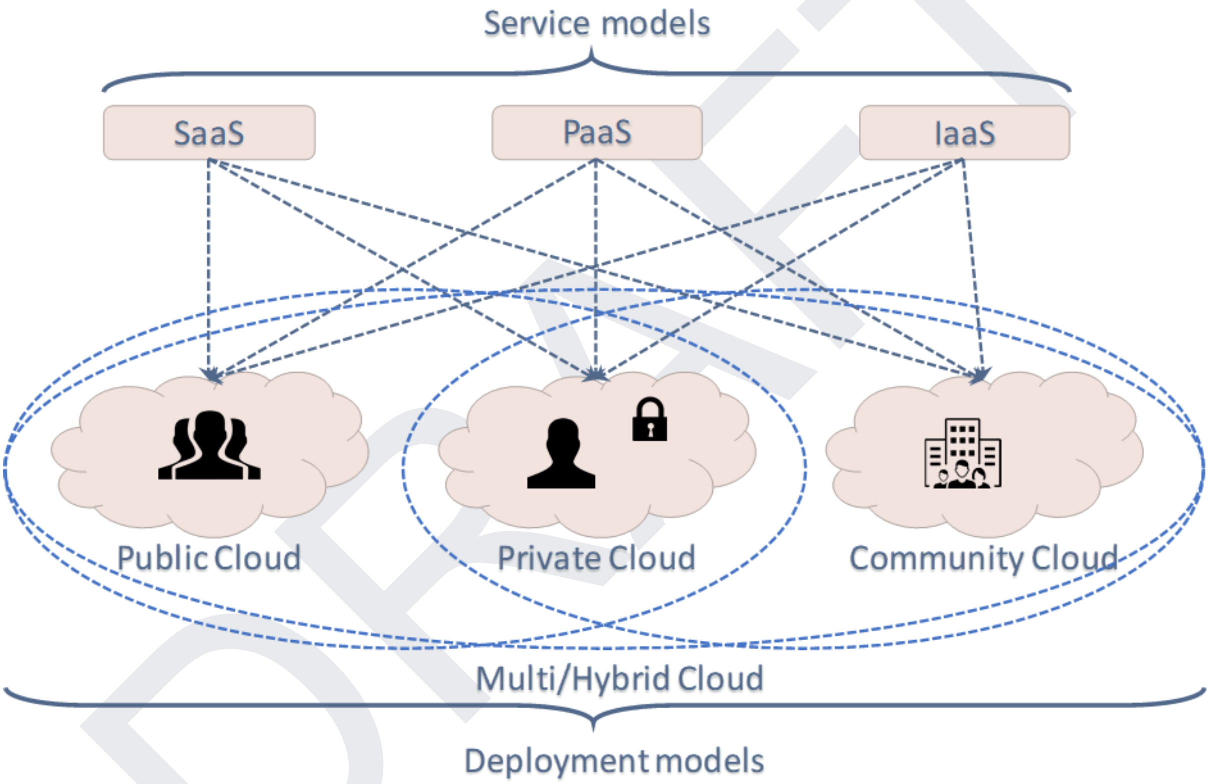
During their collaboration, project experts shared concrete experiences on cloud adoption practices and the use of cloud computing. Some of these experiences are presented in Annex 2. Finally, as with many other new technologies, cloud migration harbours a lot of myths, fears, and perceptions. This publication attempted to demystify the main ones listed in Annex 3.

It is important to note that all five cloud adoption themes are highly interrelated. The cloud service and deployment models selected have an impact on all the other themes. Security and privacy are key enablers or limitations to cloud adoption. The required capacity and competencies depend highly on the decisions and strategies used on the other themes. For this reason, the reader will come across some repetitions between the chapters that were written by different subgroups. This publication was edited to avoid as much overlap as possible, but some remain to ensure that each theme is covered adequately.

2. Cloud Service and Deployment Models

Cloud computing has revolutionised the way organisations operate, providing flexible and scalable solutions to meet their IT needs. Key aspects of cloud computing are self-service by the customer and automated execution of the self-service requests. Another advantage, maybe even a challenge, is that there are now multiple possibilities of how a solution can be used, from a service and deployment perspective. This chapter will explore these service and deployment models (Figure 2.1) and help you make an informed decision for your organisation as each option has its advantages and considerations.

Figure 2.1 Service and deployment models



The cloud computing service model defines the type of services provided by the cloud provider. There are three main types of cloud computing service models (Figure 2.2): **Software as a Service** (SaaS); **Platform as a Service** (PaaS); and, **Infrastructure as a Service** (IaaS).

On the other hand, the cloud deployment model defines how the cloud infrastructure is deployed and managed. There are four main types of cloud deployment models: **Public cloud**; **Private cloud**; **Community cloud**; and, **Multi / Hybrid cloud**.

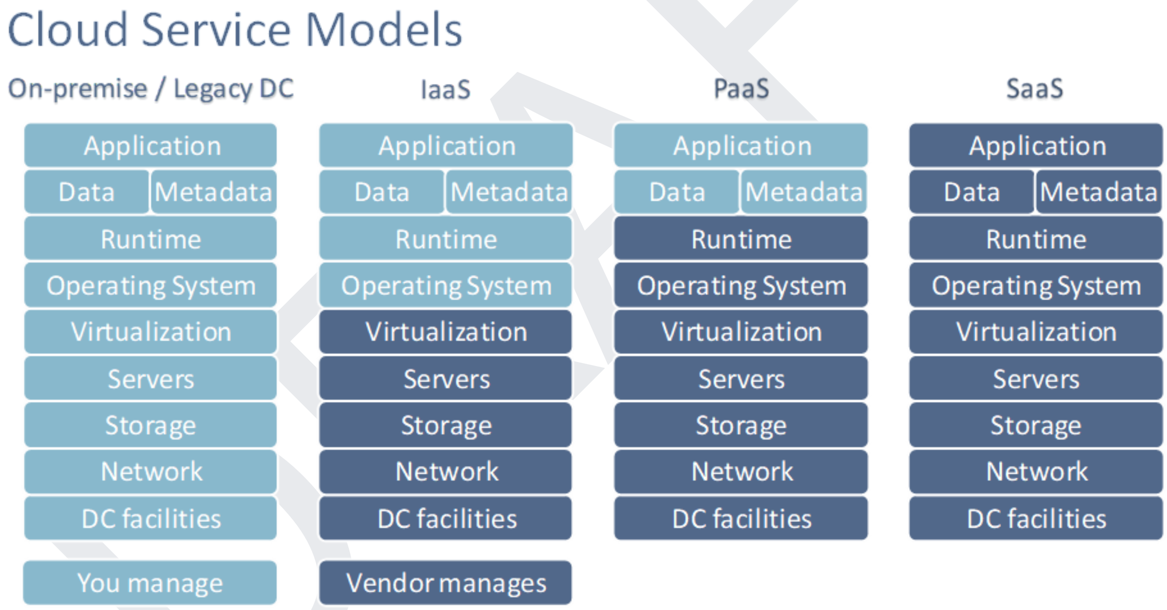
In summary, the difference between the two models is that the service model defines **what** services are provided by the cloud provider, while the deployment model defines **how** these services are deployed and managed. See also the picture below.

Another dimension is **where** the cloud resides. It does not define the cloud model, but is crucial to data sovereignty presented in the Cloud Procurement and Cloud Security and Privacy chapters.

Cloud computing service models

Figure 2.2 provides an overview of the differences between the three main types of cloud computing service models and the traditional on-premises IT infrastructure model for the different technical components which are managed by the own organisation or by the cloud vendor.

Figure 2.2 Cloud Service Models



Cloud Service Models

On-premise / Legacy DC	IaaS	PaaS	SaaS
Application	Application	Application	Application
Data | Metadata	Data | Metadata	Data | Metadata	Data | Metadata
Runtime	Runtime	Runtime	Runtime
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Network	Network	Network	Network
DC facilities	DC facilities	DC facilities	DC facilities

You manage

Vendor manages

On-premise / Legacy DC (On-prem)

On-premises computing refers to setting up and maintaining IT infrastructure within an organisation's own physical premises to have more control on IT assets by monitoring performance, security, upkeep, and their physical location. It is important to note an organisation can rent “rack space” in an external data centre. In that case DC facilities are being managed by the vendor who, in some setups, may also manage network components. Thus, in some IT setups, the DC facilities box under the On-premise model in the figure above can be partly light blue and partly dark blue.

Infrastructure as a Service (IaaS)

IaaS is a cloud computing model that provides virtualized computing resources over the internet. It offers organisations on-demand access to virtual machines, storage, networking, and other essential infrastructure components. With IaaS, organisations can scale their resources up or down based on demand, paying only for what they use. IaaS provides a cost-effective alternative to maintaining and managing physical hardware. It offers flexibility, allowing organisations to deploy and manage their chosen applications, databases, and operating systems. IaaS is suitable for organisations with complex infrastructure requirements, offering them scalability, security, and control over their IT environment. Drawback is that the organisation still has a large responsibility, i.e. cost, in delivering and maintaining business solutions.

Platform as a Service (PaaS)

PaaS is a cloud computing model that provides a platform and environment for developers to build, deploy, and manage applications. With PaaS, developers can leverage pre-configured frameworks, tools, and resources to streamline the application development process. PaaS eliminates the need for managing underlying infrastructure and allows developers to focus on coding and application logic. It offers flexibility and scalability, enabling rapid application deployment. PaaS is ideal for organisations seeking efficient development environments and supports various programming languages and databases. Examples of PaaS include hosting platforms, database management systems, and application development frameworks.

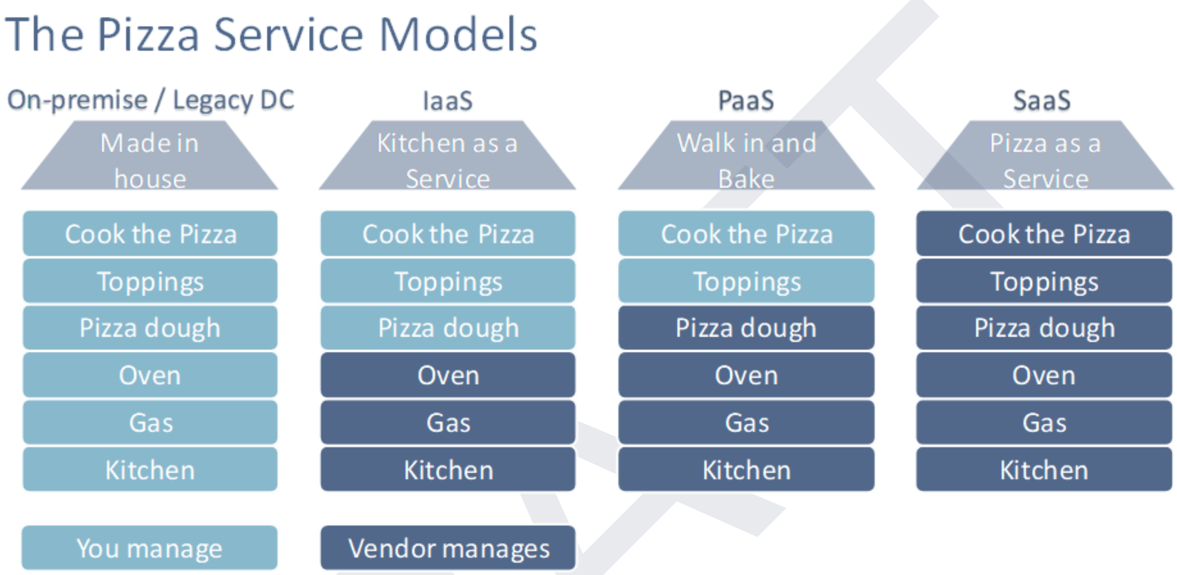
Software as a Service (SaaS)

SaaS is a cloud computing model that delivers software applications over the internet. With SaaS, organisations can access and use applications hosted by third-party providers without the need for installation or maintenance on the client's side. gUsers can conveniently access SaaS applications through a web browser, enabling seamless collaboration and accessibility from any device. Popular SaaS examples include customer relationship management (CRM) systems, project management tools, email services, and data production software. SaaS eliminates the hassle of technical and operational support of the application and the organisation can focus more on its core task. It can also provide a cost-effective and scalable solution for organisations.

Within the SaaS cloud computing model there are also some distinctive differences in how the offered system is being set up and managed by the SaaS supplier. This can range from a true Multi-tenant setup, where all software components like application and database are being shared across multiple users, up to a dedicated setup for a single customer. The latter option could also be in the essence a managed hosted solution. And although a managed hosted solution could offer some flexibility in for instance customization of the solution to the customer, it doesn’t necessarily offer the same scalability, reliability or functionality as a true SaaS model.

To provide an applied analogy for the non-technical world, Figure 2.3 illustrates the service different models in the context of making a pizza. In the on-premises model, the organisation is totally responsible for the acquisition and management of the whole pizza-making process, from the appliances to the ingredients to baking the pizza. On the other end, in the Saas model, the organisation simply specifies the type of pizza it wants from the vendor.

Figure 2.3 Pizza Service Models



The Pizza Service Models

On-premise / Legacy DC	IaaS	PaaS	SaaS
Made in house	Kitchen as a Service	Walk in and Bake	Pizza as a Service
Cook the Pizza	Cook the Pizza	Cook the Pizza	Cook the Pizza
Toppings	Toppings	Toppings	Toppings
Pizza dough	Pizza dough	Pizza dough	Pizza dough
Oven	Oven	Oven	Oven
Gas	Gas	Gas	Gas
Kitchen	Kitchen	Kitchen	Kitchen

You manage

Vendor manages

Cloud computing deployment models

The different cloud computing deployment models have their own key benefits and challenges. Depending on specific use cases (corporate support or data production), legal situation in a country / organisation etc. a certain deployment model might favour another one or not be allowed at all.

Public cloud Infrastructure

Public cloud infrastructure is provided by third-party service providers and accessible to the general public over the Internet. Organisations share the same pool of resources, making it a cost-effective option for organisations of all sizes.

Key benefits:

- Cost Efficiency: Public cloud services follow a pay-as-you-go model, allowing organisations to pay only for the resources they use.

- Scalability: Public clouds offer virtually unlimited scalability. Organisations can easily scale up or down their resources based on demand, ensuring optimal performance without the need for significant investments.

- Global Availability: Large public cloud providers can have data centres located worldwide, providing global access to applications and data but still it always needs to be assessed if the desired service is being offered in a specific country or region.

Challenges:

- *Limited Control*: With public cloud infrastructure, you have limited control over the underlying hardware, network, and security configurations. Since the infrastructure is shared among multiple users, you have little influence over the decisions made by the cloud provider regarding software updates, security protocols, and hardware upgrades. This lack of control can be a concern for organisations with specific compliance requirements or the need for custom configurations.

- *Security and Privacy Risks*: Storing sensitive data or running critical applications on a public cloud infrastructure introduces potential security and privacy risks. While cloud providers implement strong security measures, there is still a level of uncertainty regarding the safety of your data. A cloud provider's system breach or unauthorised access to your account could lead to data loss, leakage, or even malicious activities. Compliance with (inter)national regulations such as General Data Protection Regulation[8] (GDPR) or Health Insurance Portability and Accountability Act (HIPAA) may also be challenging due to the shared infrastructure nature of the public cloud.

- *Legal and regulatory requirements*: Failure to comply with legal and regulatory requirements can result in penalties, legal disputes, reputational damage, and loss of customer trust. Therefore, organisations considering public cloud infrastructure need to thoroughly assess the regulatory landscape and ensure that the chosen cloud provider offers the necessary compliance mechanisms and support to meet their obligations.

- *Performance and Reliability Dependence*: Public cloud infrastructure relies on the provider's network and hardware infrastructure, which means that your performance and reliability are dependent on their systems. If the cloud provider experiences outages, network congestion, or hardware failures, it can impact the availability and performance of your applications and services. Additionally, since resources are shared among multiple users, the performance of your applications may be affected by the activities of other users on the same infrastructure, leading to potential

[8] https://gdpr.eu/what-is-gdpr/

performance fluctuations. It must be noted that especially the larger cloud service providers can offer very competitive performance and reliability SLA's.

Private cloud Infrastructure

Private cloud infrastructure is solely dedicated to a single organisation. It can be hosted by the organisation itself or by a third-party provider. Private clouds offer enhanced security and control, making them suitable for organisations with stringent compliance requirements. A private cloud in an organisation's own data centre differs from an on-premises IT infrastructure as it uses more generic compute and storage hardware which can be easily replaced and extended. Managing (up- and down scaling) of the services on top of the hardware is being realised by using cloud technologies.

Key benefits:

- *Security and Compliance*: Private clouds offer greater control over data security and compliance. Organisations can implement customised security measures and adhere to specific regulatory standards.

- *Performance and Customization*: Private clouds allow organisations to tailor the infrastructure to their unique requirements, optimising performance and ensuring efficient resource allocation.

- *Data Privacy*: With a private cloud, organisations have complete control over access to their data, reducing concerns about data leakage or unauthorised access.

Challenges:

- *Higher Initial Costs*: Setting up a private cloud infrastructure typically requires a significant upfront investment in hardware, software, and network infrastructure. Organisations must purchase and maintain their servers, storage devices, networking equipment, and virtualization software. This initial cost can be substantial, making private cloud infrastructure less financially feasible for small or budget-constrained organisations.

- *Increased Maintenance and Management Responsibility*: In case the organisation hosts the private cloud by themselves, the organisation is responsible for the maintenance, management, and upkeep of the entire infrastructure. This includes tasks such as hardware maintenance, software updates, security patches, and troubleshooting. The organisation needs to have skilled IT personnel or teams dedicated to managing the private cloud environment. This additional management burden can be time-consuming and resource-intensive, diverting focus and resources from other business initiatives. However private clouds can also be maintained and managed by third parties reducing this burden.

- *Limited Scalability and Elasticity*: Private cloud infrastructure can have a finite capacity based on the organisation's hardware resources. Scaling up the infrastructure to meet increased demand requires additional investment in hardware and may take time to deploy and configure. Unlike public cloud services that offer elastic scalability, where resources can be provisioned on-demand, private clouds have limitations on scaling due to their fixed hardware infrastructure. This can be a drawback for organisations with fluctuating workloads or seasonal peaks in demand, as they may struggle to rapidly adjust resources to match the changing needs

Community cloud Infrastructure

Community cloud infrastructure is a shared computing environment tailored to meet the needs of a specific community or industry. It enables organisations within the community to collaborate, share resources, and achieve cost savings and operational efficiencies. Community clouds can offer industry-specific compliance, specialised services, enhanced data governance, and shared costs. An example of a community cloud is a government data centre.

Key benefits:

- *Collaboration and Resource Sharing*: Community clouds foster collaboration and resource sharing among community members, leading to cost savings and operational efficiencies.

- *Industry-Specific Compliance and specialised Services*: Community clouds can be customised to meet industry-specific compliance requirements and provide specialised services that cater to the unique needs of community members.

- *Enhanced Data Governance and Shared Costs*: Community clouds enable community members to define and enforce common policies, ensuring consistent data governance. They also allow for shared infrastructure costs, making it a cost-effective solution for organisations within the community.

Challenges:

- *Strong community governance is needed*: In order to keep up with new developments, on-going effort is needed to keep up-to-date. This requires a strong governance and funding model.

Multi / Hybrid cloud Infrastructure

Both "multi-cloud" and "hybrid cloud" refer to cloud deployments that integrate more than one cloud. They differ in the kinds of cloud infrastructure they include. A hybrid cloud infrastructure blends two or more different types of clouds, while multi-cloud blends different clouds of the same type[9]. They offer a flexible and versatile solution and allow organisations to leverage the benefits of different models or different vendors while addressing specific workload requirements and risk management.

Key benefits

- *Flexibility and Scalability*: Multi / Hybrid clouds enable organisations to scale their resources dynamically. They can run critical applications on a private cloud while utilising public clouds for non-sensitive workloads, ensuring cost-effectiveness and optimal performance.

- *Disaster Recovery and Backup*: Multi / Hybrid clouds can provide robust disaster recovery capabilities. Organisations can replicate critical data and applications to a private cloud for enhanced security and backup while utilising public cloud resources for redundancy.

- *Cost optimisation*: Multi / Hybrid clouds allow organisations to balance cost and performance. They can leverage public clouds for peak demand and seasonal workloads, minimising infrastructure costs.

Key disadvantages

- *Complexity*: Implementing and managing a multi / hybrid cloud infrastructure can be complex and challenging. It requires integrating and orchestrating resources and applications across multiple cloud environments, including both private and public clouds. This complexity arises from the need to ensure compatibility, connectivity, and data synchronisation between different cloud platforms. It often requires specialised expertise and ongoing maintenance to keep the hybrid cloud environment running smoothly.

- *Security and Compliance Risks*: Hybrid cloud environments introduce additional security and compliance risks. Organisations must carefully manage data protection, access controls, and encryption mechanisms across both the private and public cloud components. Data movement and integration between different cloud environments may increase the attack surface and introduce potential vulnerabilities. Ensuring consistent security policies and compliance with (inter)national regulations across multiple cloud platforms can be a daunting task. A breach or misconfiguration in one cloud environment can have repercussions on the overall security and compliance posture of the hybrid cloud infrastructure.

- *Cost and Resource optimisation*: While hybrid cloud infrastructure offers flexibility and scalability, optimising costs and resource allocation can be a challenge.

[9] https://www.cloudflare.com/learning/cloud/multicloud-vs-hybrid-cloud/

> Organisations need to carefully analyse and balance resource utilisation between the private and public cloud components. If not managed effectively, it can lead to underutilised resources in one environment or unexpected costs in another. Determining the most cost-effective and efficient deployment model for each workload and application requires careful planning, monitoring, and resource management practices.

Choosing the optimal cloud infrastructure model depends on factors such as data sensitivity, compliance requirements, scalability needs, and budget considerations. Conduct a thorough assessment of your organisation's unique requirements before making a decision. Consider consulting with cloud experts and leveraging proof-of-concept trials to evaluate the suitability of each model. It is also important to note that the cloud model(s) chosen will usually have to be connected to remaining core components of the legacy on-premises IT infrastructure.

In conclusion, the right cloud infrastructure model is pivotal for maximising efficiency and unlocking the full potential of your organisation's IT capabilities. By carefully evaluating the advantages and considerations of public, private, hybrid, and community clouds, you can make an informed decision that aligns with your business goals and delivers optimal results. Each model has its strengths and weaknesses compared to the others. For example, a public cloud is more scalable, a private cloud is more secure and a hybrid cloud can achieve scalability and security where most needed, but be more complex and costly. What is of utmost importance is to first work out your organisation's long term strategy on which to base your choice for the best deployment model.

3. Cloud Procurement

This chapter aims to provide a set of recommendations relevant to cloud procurement and possible alternatives for each of the topics. While many procurement aspects are addressed in dedicated sections, a small number of recommendations stand out and deserve to be evidentiated from the start.

Legal and data sovereignty issues need to be considered and addressed first. This will create a boundary on what can be implemented in the cloud. Creating this boundary will be specific to a statistical institute, as potentially sensitive data is at the core of statistical production and this data is a lot of the times gathered under domain specific legislations. As a result, there is little reuse potential of conclusions and practices created for other organisations or business domains.

The statistical institute should aim at defining a long term strategy to realise identified business benefits. Given the fast paced development of the data science domain, heavily supported by cloud technologies, there is an increased potential for statistical institutes to receive tangible added value and a real competitive advantage from transitioning to cloud technologies, on top of benefits traditionally identified across IT departments. This may result in multiple work streams with differing objectives and timelines. Also at strategic level an initial assessment will have to be made to understand if the organisation will benefit from having a multi-cloud or hybrid cloud strategy (refer to Cloud Service and Deployment Models chapter).

Procurement strategy

The procurement strategy needs to be clarified upfront. An organisation can negotiate better deals with the cloud service providers depending on the quantity of services being consumed and length of commitment. The latter needs to be thoroughly analysed as long term contracts may have the effect of restricting competition. If feasible, framework contracts with multiple cloud providers should be foreseen. While this introduces administrative overhead, it will conserve negotiating power over the whole duration of the contract and will bring flexibility for the technical teams.

For national organisations it would be recommended to try to have a framework contract covering the entire government. While this gives significant negotiating power with the cloud providers, it introduces an extra layer of complexity to coordinate departments' needs both prior to procurement and while running the contracts. A similar approach can be applied for international organisations, by trying to have global contracts or associating with similar organisations.

The cloud market is evolving constantly, cloud providers proposing new services at a high pace. This state of fact makes the procurement to such service challenging and cumbersome, and puts small and medium size customers such as statistical institutes in a weak situation in front of providers whose size is considerable. If possible implement an internal cloud broker capability to avoid technical teams having to deal with the complexity of the contractual relationships.

Full Lifecycle management including removing a service from operation in the cloud needs to be considered and resourced. Please see more information in the Vendor lock-in and exit strategy and the Budget management and cost optimisation sections in this chapter.

All of the cloud providers operate in a shared responsibility model. While estimating cloud consumption, a certain level of technical expertise is required to ensure that all business needs are met and that the organisation gets satisfactory levels of services. For example, to meet business continuity and disaster recovery needs an organisation might want to make use of multi region/data centre deployments. This can double the volume for certain categories of cloud services. There will always be complementary services (e.g. specific database PaaS) that the cloud provider will not provide. They will provide guidance or recommend partners, but the accountability stays with the client. This can result in the need for purchasing of extra external services or might increase the need for internal human resources.

A good practice for shaping the procurement strategy and cloud strategy in general is to engage with the cloud service providers well before launching any procurement actions. Experience shows that hyperscalers are open to investing considerable amounts of resources towards clarifying their offerings towards relevant organisations.

Legal considerations

When launching large scale procurement initiatives you should always seek specialised legal advice. Specific national or regional legal constraints might exist. As a non-exhaustive list, tenders must comply with applicable data protection, environmental, social and labour law obligations established by regional and national legislation, collective agreements or the international environmental, social and labour conventions.

When it comes to **service terms and conditions**, cloud service providers will most probably insist that their terms and conditions take precedence over the statistical institute’s terms and conditions. However the standard terms and conditions can be customised and extended to an extent, the degree of which is usually proportional to the scale of the investment being considered or to the image gains that come from working with public organisations. While terms and conditions related to technical matters or to general service levels are less likely to be flexible, there are areas where specific terms and conditions might be paramount among which we can mention data sovereignty and data protection or legal jurisdiction as described below. If specific terms and conditions are being put in place for the statistical institute, a key aspect is to make these available and to actively advertise these in the organisation. This will allow technical teams to make informed decisions about the services they use.

A key issue for statistical institutes is **data sovereignty**. There may not be a data centre within the country of the statistical institute, hence the use of certain cloud providers would require data to move outside of the national boundaries. This may limit what these services can be used for. It is essential that these constraints are determined before developing a cloud strategy to ensure that the expected value can be gained from these investments, especially when there are multiple data providers to a statistical institute. Each of these data providers are likely to have their own expectations, standards or legal constraints for the use of their data and whose agreement will be required before their data can be used in the cloud. The contractual provisions must assure complete transparency and control over the location of data at rest. Exceptions must be clearly accounted for and fully documented. For example, cloud providers might manage certain configuration or administrative data centrally, not being able to give control over where this data is stored, even if they have a data centre in the statistical institute's country.

Another key aspect is **data protection**, covering both personal data and other categories of legally defined sensitive data. It is recommended that contractual provisions mention that these data are protected by default, i.e. no dedicated requests need to be made per data set and most importantly data protection cannot be waived by the consumer of the service by punctually accepting specific terms and conditions.

When it comes to **legal jurisdictions**, it is paramount to have the dispute resolution process clearly defined. It is recommended that all legal disputes are resolved in the statistical institute's country.

Closely linked to all three topics above we have **intellectual property**. The statistical institute must have a good understanding of any specific needs to protect intellectual property that it may own and address these needs through specific contractual provisions. In the context of SaaS, special attention needs to be given to the ownership of any customisations performed by the statistical institute on top of the service. While cloud services development is often driven by open source technologies, most cloud service providers also have strong offerings based on licensed software which limits the further distribution of the software. While these offerings will most probably include a pay as you go option, some will also include a bring your own licence model. Statistical institutes might want to benefit from previously concluded licensing agreements. These agreements will have to be potentially reviewed to include the cloud services context.

Cloud adoption considerations

While cloud adoption is extensively discussed in its dedicated theme, this section will highlight specific topics that influence procurement.

A key aspect that will impact procurement is understanding the impact and benefits of using vendor specific or vendor agnostic technologies. Most organisations will reach a balance using a combination of these technologies. Using vendor specific technologies will heavily impact the exit strategy (elaborated below), while using vendor agnostic technologies will impact the type and quantity of complementary service that will have to be procured from other IT service providers as well as the size and structure of human resources in the technical teams of the statistical institute.

A well implemented organisational change and upskilling process is paramount for a successful cloud adoption. While the statistical institute might have some specialised organisational change competences internally, procurement of specific consultancy services might be desirable. Upskilling needs have to be well understood and a comprehensive training strategy needs to be devised (more details in the chapter on Cloud Capacity and Competencies). To implement the training strategy, at least in the early stages of cloud adoption it is recommended to negotiate training packages from the cloud provider included in the onboarding process. When it comes to upskilling, the need for specialised profiles needs to be acknowledged in the overall organisational strategy. These profiles are often difficult to attract across the labour market and potentially more so for public administration organisations. Some of these profiles will have to be covered through external contracting. This contracting needs to be foreseen in the procurement strategy. Security and privacy provisions.

Security and privacy provisions

While cloud service providers will generally offer state of the art security and privacy capabilities, these will not be implemented by default and will not be available to the same extent for all the services in the provider's portofolio. Under the shared responsibility model the national statistical institute will have to implement its own security and privacy measures (refer to Cloud Security and Privacy chapter) to reach the targeted security level. When it comes to procurement these implemented measures will greatly influence the volumes of cloud services contracts and operational budgets.

When procuring cloud services your organisation will probably request a set of **security certifications** or, in cases where standard accreditation schemes do not exist, **proof of compliance** with certain security and privacy requirements. It is important to put in place a process that monitors the various certifications across the duration of the contract with a cloud services provider. At least two aspects need to be monitored: validity of the certification and evolution of the certification scheme. While for the more common certifications the risk of a big cloud services provider not renewing them is relatively small, for more specific or regional level certifications the validity needs to be monitored in a proactive way. At the same time, certain certification schemes might evolve in time. A careful consideration of the potential evolution of the various certification schemes needs to be made at procurement time and contractual provisions need to be made according to the statistical institute's needs. When it comes to proof of compliance with certain security and privacy requirements a good practice would be to reserve the right to audit the cloud services provider, either directly or through a third party. Besides the contractual arrangements the organisation needs to take into account that conducting such audits will require considerable amounts of resources and specialised expertise.

Some of the technical aspects that might have significant impact on procurement are **logging and reporting**, **encryption key management** and **authentication and authorisation**. For independent security monitoring and auditing, aggregating logs and building reporting capabilities outside the cloud service provider's environment can be seen as good practice, more so in hybrid and multi cloud environments. For keeping full control of encryption and sensitive data access, specific services could be foreseen on premises or from a different service provider. For most organisations having centralised identity and access management would be desirable, usually based on an already existing setup. This would imply specific integrations between the cloud environment and the central identity and access management platform. All these technical aspects might lead to procurement of extra services from third parties and could have an impact on internal human resources profile needs.

Vendor lock-in and exit strategy

When entering a migration to a cloud provider it is essential to also consider an exit strategy to ensure that all the dependencies and capabilities are in place to ensure a clean transition should it become necessary in the future. This can become a very expensive operation if left until the end of a relationship where the customer has very little leverage for negotiation.

One of the most important items is the data migration strategy which needs to identify not only how information assets are moved securely into a cloud vendor but also how they can be copied out, while any remaining copies and the environments that hold them are destroyed or deleted in a manner that all parties are satisfied with. Any costs and licences involved need to be identified and agreed before the signature of the contracts.

While most organisations will use a mix of vendor specific services and vendor agnostic services, the share of each of these types of services will have to be carefully analysed to fully understand the impact of moving to a new cloud provider. Heavily using vendor specific technologies will mean rearchitecting and even redevelopment of information systems, while using mostly vendor agnostic technologies would most probably mean just reconfiguring existing information systems and integrating existing architectures in the new environment. As this will greatly influence the schedule, effort and types of services needed for a migration, it is recommended to aim for clear directions on this topic when defining any cloud services procurement strategy and early in the cloud adoption.

When onboarding with a new cloud services provider there will be significant additional costs on top of the actual cloud service consumption. As services from different cloud providers have their own specificities, there will be significant impact on the profiles and skills required to consume these services (refer to chapter on Cloud Capacity and Competencies). Both the actual cost of procuring training and human resources time allocation for these trainings should be considered. Any contracts for third party service providers should be reviewed in the context of the new cloud provider. As a result of this review the need for purchasing different third party services, the need to rebalance the team composition or the need to work with the service provider to reskill the existing profiles might show up. When working on the knowledge transfers as the information systems move from one platform to another it is essential to capture details that cannot be directly migrated, but would need to be addressed specifically in the new cloud provider environment. Maintaining a register of residual risks that the statistical institute will need to manage is recommended.

When changing cloud service providers there is always the option to negotiate with the new vendor to support at least in part migration fees and to cover most of the initial training needs.

When considering migrating out of a cloud provider it is important to always analyse the opportunity of a change in strategy. More specifically based on gained experience, the advantages of a hybrid or/and multi cloud setup might become more evident.

Budget management and cost optimisation

Cloud adoption goes hand in hand with a financial transformation. The main driver for this transformation is the adoption of pay as you go models and making the shift from capital expenditure (CAPEX) to operational expenditure (OPEX) to cover IT infrastructure costs. To stay in control during this financial transformation it is recommended to implement FinOps practices as early as possible.

FinOps is an evolving cloud financial management discipline and cultural practice that enables organisations to get maximum business value by helping engineering, finance, technology and business teams to collaborate on data-driven spending decisions. At its core, FinOps is a cultural practice. It's the way for teams to manage their cloud costs, where everyone takes ownership of their cloud usage supported by a central best-practices group. Cross-functional teams in engineering, finance and product work together to enable faster product delivery, while at the same time gaining more financial control and predictability.[10]

When using the cloud, the transformation is most evident for technical profiles that get the ability to order services generating expenses. This was not the case in a local data centre setup, where all expenditure was in principle accounted for before the technical profiles got access to the purchased computing resources. This means technical profiles need to transition from managing a capped set of computing resources to managing virtually limitless computing resources and the cost associated with resources being used. Raising awareness about these important changes and pushing cost accountability across IT departments is key for a successful cloud adoption.

In general taking a lift and shift approach when migrating to cloud services will result in higher costs compared to a data centre setup. To get the most value out of the usage of cloud services, specific cost optimisation measures need to be taken. A non-exhaustive list of measures that can be taken includes:

- *Long term reservation of resources:* Cloud providers offer better pricing for resources that are reserved in advance for a certain period of time. The pricing reduction is proportional with the length of the reservation. Generally any organisation could estimate a minimal amount of services that would be needed to operate business processes and should aim to reserve these computing resources.

- *Usage of spot capacity:* Cloud providers need to have an excess of computing resources, to be able to reply to sudden demand or to peak periods of consumption. It is in the cloud provider's interest to try to get some value out of this capacity. Because of this they will offer services at very attractive prices, but with no

[10] The paragraph content is cited from https://www.finops.org/

guarantee on the availability of these resources. This means that clients can take advantage of this spot capacity for activities that are not time sensitive, can be interrupted at any time and continued when the pricing conditions are again favourable. This approach usually makes sense in use cases requiring significant computing resources and where mechanisms to save the state at a given moment can be implemented.

- *Rightsizing and auto-scaling clusters, servers or containers:* In a local data centre context oversizing infrastructure resources is common practice, to be able to accommodate fluctuating needs in an environment where procuring extra resources in short time frames is not an option. This is not the case in a cloud environment. Resource allocation needs to be strictly matching the computing needs at a given moment. To address changes in demand, automated scaling of resources should be put in place. Policies to scale up resources need to be matched by policies to scale down when demand goes down. While cloud providers offer powerful tools for managing scalability, strict discipline needs to be observed also from the technical profiles managing the cloud services. Needless to say that any unused resources need to be decommissioned. For large organisations even resources that might seem trivial for a deployment or project, like for example public IP addresses, can add up to cost considerable amounts.

- *Usage of tiered storage:* In a cloud provider's portofolio an extensive list of storage services will be available, grouping different technical characteristics like storage technology, performance and transfer speeds, availability and backup. These services will vary greatly in price. The challenge is to match the right service to the right type of data. For example, cloud providers will have competitively priced offerings for backup data. Meaning that the price per unit of storage will be relatively low, but the cost of accessing the data will be higher and there might be a significant time delay between the moment the data access is requested and the moment the data is available to the customer. This perfectly matches the data backup use case, where data quantities are usually significant and the probability to need access to the data is low.

- *Usage of serverless technologies:* These technologies enable the use of shared infrastructure resources very high in the development stack of an information system or service. This means that little to no computing resources are wasted or remain idle on the cloud provider side, allowing for competitive time based computing pricing.

FinOps activities should be coordinated centrally in the organisation, ideally by a dedicated team. Even simple measures like requiring a budget estimate and setting corresponding alarms when provisioning new cloud accounts can provide a significant level of control on the cloud consumption. This being said specific tooling is needed to be able to put in place robust FinOps activities.

Cloud providers offer tools for budgeting and managing consumption and costs. On top of this the market of specific tools is quite mature at the moment, offering strong alternatives that might be preferred by statistical institutes, especially when aiming for a hybrid and/or multi cloud approach. A rigorous analysis of the options should be made early in the cloud adoption process.

FinOps tools allow for budgeting at various levels, present dashboards that allow cost tracking and trend visualisations, provide cost estimates for the future, allow the definition of alerts at various thresholds, allow cost breakdowns based on categories predefined by the cloud provider or defined by the customer.

An important aspect that may seem trivial initially is having a well defined tagging strategy. Cloud providers allow adding tags to provisioned resources. These tags can be added in an automated way and tag enforcement and validation policies can be implemented. Tags can have multiple uses, but in the FinOps context will allow splitting and monitoring costs on various breakdowns relevant for the customer. For example, tags defining the information system name, project or type of environment might be useful.

Payment terms need to be clarified from a strategic point of view and negotiated accordingly. Since in most organisations budgets will be allocated to business use cases, that will generate IT activities and cloud consumption, a form of periodic chargeback or budget transfer will have to be foreseen. The process of distributing costs and making internal transfers can potentially run longer than the payment deadlines defined in the payment terms. Appropriate buffers need to be foreseen in the process to accommodate these challenges.

Environmental considerations

While greening IT services can be complex and can imply multiple aspects, a couple of recommendations stand out when it comes to procurement.

First and foremost the environmental goals of your organisation must be clear to the procurement team and any impact of cloud services must be accounted for. Based on this specific service requirements need to be defined, so that providers having the right capabilities are identified.

Once it is clear what services would contribute to the statistical institute’s environmental goal (e.g. services with a reduced carbon footprint), the overall budget estimations and contract volumes need to be adapted, as greener services are usually optional and more expensive.

Another aspect to analyse at procurement is the availability of appropriate tools in the provider’s portofolio to monitor and manage sustainability information related to the consumed services.

Cloud models’ impact

Most organisations are likely to have a mix of different needs which range from core business support and data production systems through to ad hoc analytical processes. The different needs can be met by the different types of service offerings that the cloud providers can host. Procurement will be impacted by the mix of cloud service models considered.

Most procurement initiatives should cover together services that can be identified as **IaaS and PaaS**, under the same contract. While these services can have different value propositions and bring different levels of flexibility, it should be relatively straightforward to cover them with the same generic description as part of a contract.

When it comes to **SaaS** it is unlikely that services could be contracted in a generic way together with IaaS and PaaS or even that multiple SaaS offerings could be grouped under the same contract. A SaaS contract should aim to describe service requirements in detail, with specific performance indicators and as much as possible focused on business needs and use cases. If a larger number of SaaS contracts are foreseen, good practice would be to centrally build knowledge and provide guidance when it comes to nonfunctional requirements, like security, data protection, encryption, data migrations and integrations or identity and access management.

A topic that requires special attention covers **marketplace services**. Hyperscalers in particular have extensive marketplaces where third parties offer specific services, usually in the form of PaaS or SaaS. For these services the cloud provider acts like an intermediary, so covering the marketplace in a framework contract concluded with the cloud service provider might be challenging. As good practice, procurement of marketplace services should be done through dedicated contracts, similar to any SaaS contract. Special attention needs to be given and monitoring needs to be put in place to avoid consumption of marketplace services without having a contract with the provider.

Another set of services that needs to be taken into account are **connectivity** services, both while seeking to connect the statistical institute's offices to cloud environments and more so when hybrid and multi cloud environments are foreseen. These services are usually purchased from a small set of global providers, through a dedicated contract not linked to the cloud service providers.

4. Cloud Adoption

In the theme of cloud adoption, we explore various elements focused around understanding the behaviours that support NSOs adoption of cloud technologies. Adoption of cloud technology needs to consider critical elements beyond those of technical implementation by IT teams (whether that be internal IT teams, and/or vendors). Many of these critical elements should be addressed before and during the early stages of cloud technology adoption as they will enable a smoother transition.

There are many push and pull factors that move NSO's towards decisions to adopt cloud, such as legislation, government policy, and the increasing demands for insights and analysis that require processing power, scalability of data environments, and new tools to handle larger volumes of data from a range of different sources. However, there are many other factors that need to be addressed for NSO cloud adoption to be successful, such as sovereignty risks (both real and perceived), transparency and engagement with the public on how their data is kept secure, confidential and accessible. A well-managed organisation change process is also very important to ensure an ongoing sustainable adoption of cloud technologies.

We explore the challenges, look at current adoption strategies, the organisational change considerations, and stakeholder engagement. We conclude with the future outlook and recommendations for NSO's. The information presented comes from discussions and information supplied from multiple NSO's. The intended audience are those with governance and decision-making responsibilities in NSO's, such as Chief Statisticians and senior leaders.

Barriers and Challenges

As seen, the successful adoption of cloud technology in NSOs is crucial for leveraging its benefits. However, several barriers and challenges need to be addressed to facilitate a smooth transition. This section explores the key barriers and challenges associated with cloud adoption in statistical organisations, with specific considerations for Serbia, New Zealand, Canada, and Ireland.

Legislation and Data Sovereignty

- In Serbia, the legal regulation on data storage within the country represents a major barrier to cloud adoption. The current framework allows data to be stored only within the country, limiting the use of offshore cloud services. Addressing this regulatory constraint and establishing frameworks for secure cross-border data transfers would support cloud adoption in Serbia.

- In New Zealand, the adoption of cloud services is influenced by the need to work through the rights and interests of Indigenous populations and ensure data sovereignty. Efforts are underway to engage with Māori communities and develop a cloud toolkit for engagement on the use of cloud services. Respecting Indigenous perspectives and governance expectations is crucial in addressing this barrier.

- In Canada, considerations of data sovereignty and cybersecurity pose challenges to cloud adoption. Concerns about the jurisdiction of data and compliance with data protection laws are key factors that statistical organisations must navigate. Ensuring compliance with government policies, implementing robust security measures, and establishing governance frameworks can help address these challenges.

- In Ireland, the legal framework and data protection regulations play a significant role in the adoption of cloud services. Ensuring compliance with EU GDPR guidelines and addressing concerns related to data location and storage within the European Economic Area (EEA) are critical. Collaborating with central government bodies and establishing clear guidelines for data classification and handling can facilitate cloud adoption.

Lack of Social Licence and Public Perception

Building trust and confidence among the public, politicians, and stakeholders is a common challenge across all countries.

- In Ireland, there are concerns about the perception of cloud services, highlighting the need to address public perception issues through effective communication and education on the benefits and security measures of cloud adoption.

- In New Zealand, social licence and public trust are significant factors in cloud adoption. Engaging with Māori communities and addressing their expectations and interests in the use of cloud services is crucial for maintaining trust and building a social licence for cloud adoption.

Perception of cloud adoption poses a significant challenge for statistical organisations worldwide. The shift from traditional on-premises infrastructure to cloud-based solutions raises concerns among the public, politicians, and stakeholders regarding data security, privacy, and control. The perception that sensitive data might be at risk or subject to unauthorised access can hinder the adoption of cloud technology. While businesses deal with clients who provide information to obtain direct services, statistical organisations deal with respondents (persons or businesses) who provide information often on a mandatory basis with no direct or individual benefit. Thus, building trust and confidence in the security measures, data governance frameworks, and compliance standards implemented by cloud service providers becomes essential.

Effective communication strategies, education campaigns, and transparency in data handling practices are necessary to address the public's perception. By emphasising the rigorous security measures, data protection protocols, and benefits such as improved accessibility, scalability, and cost-efficiency, statistical organisations can work towards dispelling misconceptions and gaining broader acceptance and support for cloud adoption. This aspect is elaborated in Chapter X.

Capability and Skills Gap

Across all countries, a lack of capability and skills in understanding how to best access and use cloud technology poses a challenge. Upskilling the workforce and providing training programs can bridge the capability gap and empower statistical organisations to make informed decisions regarding cloud adoption. This aspect is elaborated in Chapter X.

Cost Considerations

While cost is not to be considered a driver for cloud adoption, it remains a crucial factor. Statistical organisations in all countries need to evaluate the financial implications of cloud adoption, specifically considerations such as the change from traditional cost models to cloud based consumption models (Capex vs. OpEx), integration costs, and long-term budget planning. This aspect was covered in Chapter X.

Government

In the context of cloud adoption, central government ambition and support play pivotal roles in orchestrating a cohesive and efficient transition to cloud technologies. One of the primary advantages of central government involvement is the standardisation and compliance it can bring to the process. This includes ensuring that data security, procurement rules and privacy regulations are consistently adhered to, particularly when migrating sensitive information to the cloud. By centralising support, the government can effectively allocate resources, eliminating redundancy and reducing costs. This shared approach to cloud adoption not only optimises financial investments but also streamlines the utilisation of expertise, making the migration more efficient and cost-effective.

Moreover, central government support is crucial in bolstering cybersecurity and data protection. As the cloud opens new avenues for data access and sharing, it's imperative that government agencies have robust cybersecurity frameworks in place. Central support can lead to the development of comprehensive security strategies that protect against emerging threats, enhancing the overall resilience of cloud services.

In summary, this chapter serves as a starting point, offering insights and recommendations to enable statistical organisations to make informed decisions and advance their cloud adoption journey. Cloud adoption presents statistical organisations with transformative opportunities to enhance their data management, operational efficiency, and service delivery. However, several barriers and challenges need to be overcome, including perception, legislative frameworks, data sovereignty concerns, and building IT capability. By addressing these challenges head-on, leveraging best practices, and drawing on the experiences of other statistical organisations, it is possible to embrace cloud technology while ensuring data security, privacy, and compliance. These aspects, that are particularly essential to NSOs, also apply to other government organisations. Thus, cloud adoption can be greatly facilitated by central government ambition and support offering a structured framework for navigating the cloud migration journey..

Best Practices and Case Studies

- *Collaboration with Stakeholders:* Foster collaboration and engagement with all relevant stakeholders, including indigenous communities or other groups with specific data governance considerations. This ensures that cloud adoption aligns with their expectations, interests, and regulatory requirements.

- *Low Risk Approach:* Begin with low-risk cloud solutions to build confidence and perception among stakeholders. Starting with manageable implementations allows for the accumulation of knowledge and experience, which can lead to increased acceptance and support for broader adoption.

- *Identify Easy Wins and Set Timeframes:* Identify applications that can be migrated to the cloud quickly and easily, based on their business benefits and suitability. This approach helps build confidence by demonstrating tangible outcomes and early wins. Start with solutions that require minimal changes and have reduced complexity to expedite deployment.

- *Agile Capability and Flexibility:* Consider an agile approach that allows for the flexibility to return to on-premises solutions if necessary. By starting small and evolving, organisations can establish solid foundations and practices that can be reused and scaled as cloud adoption progresses.

- *7Rs of cloud Migration:* utilise the 7Rs framework (Refactor, Rehost, Revise, Rebuild, Replace, Retire, Retain) to strategically assess applications and infrastructure for cloud migration. This framework facilitates decision-making by considering factors such as value for money, effort, cost, time, and security risks.

- *Cloud Centre of Excellence (CCoE):* Establish a cloud Centre of Excellence to drive and oversee cloud adoption initiatives. The CCoE helps capture and implement business requirements, accelerates adoption through the use of cloud-based solutions, maintains security and compliance standards, and approves the use of cloud-native tools. In 2018, Statistics Canada set up an Enterprise Cloud and Services division to enable, operationalize and support all cloud infrastructure requirements of the agency supporting the business as it transforms and creates new business models to better serve Canadians.

- *Upskilling and Training:* Develop a comprehensive training plan to enhance the skills and capabilities of the CCoE and organisation staff. This ensures that the necessary expertise is available to effectively manage and optimise cloud solutions.

- *Monitor Legal and Regulatory Developments:* Stay informed about legal and regulatory developments related to cloud computing. Work within the existing legal framework while actively advocating for better regulations to enable deeper cloud activities in the future.

- *Executive / Senior management support:* Development of a cloud adoption strategy and tactical implementation requires senior management support and commitment for funding, resourcing and prioritisation. This can take the form of an executive sponsor and/or senior management governance group.

By following these best practices, organisations can facilitate successful cloud adoption while addressing data governance, risk management, and stakeholder concerns.

Adoption Strategies and Roadmap

Cloud adoption in NSOs requires meticulous planning and execution to fully capitalise on cloud technologies while upholding security and privacy. To begin the process, NSOs must comprehensively assess their data and infrastructure requirements. This assessment will serve as the foundation for developing a well-defined roadmap, outlining the organisation's cloud adoption goals, priorities, and timeline. By adopting a systematic approach, the organisation can minimise risks and gradually migrate critical systems to the cloud, ensuring a smooth transition.

Additionally, NSOs must adapt their data governance policies to the cloud environment, establishing clear data access, sharing, and retention guidelines. Integrating cloud solutions with existing statistical systems requires careful planning and extensive testing to avoid disruptions. Moreover, investing in robust backup and disaster recovery solutions is critical to ensuring data resilience and reducing the risk of data loss. Leveraging cloud-native analytics tools empowers statistical organisations to process and analyse vast datasets efficiently, driving informed decision-making processes. Regular monitoring of cloud infrastructure performance and costs is essential for optimising resource utilisation and budget allocation. Compliance with data regulations and industry standards is also imperative to maintain the trust of citizens and stakeholders. Lastly, engaging in knowledge sharing and collaboration with other NSOs that have successfully adopted the cloud can offer valuable insights and best practices. Periodic reviews and assessments of the cloud adoption strategy enable organisations to adapt effectively to evolving technologies and changing needs.

Organisational Change and Stakeholder Engagement

Adoption of cloud capabilities will result in varying levels of organisational change for any NSO. Levels of change will be directly influenced by the pre-adoption state of the NSO, the objectives of the NSO from adopting cloud, and other factors such as, the availability of cloud technologies, legislation, government policy and directives, and public and organisational perceptions of cloud adoption. These factors may result in limitations to, or support increased, cloud adoption.

Adoption of cloud (like any considerable organisational change initiative) should follow an effective change management approach, such as the following:

1) Define the change

    a. Vision: a clear articulation of the "why" the NSO is adopting cloud for official statistics. For example, to support delivery of new strategic objectives. The vision should also cover "what" the change will be, and "when" and "how" it will be implemented.

b. Drivers of the change: articulate the key drivers that are either pushing the organisation towards adoption of cloud, or opportunities to generate new / improved value. For example, in 2019 the Irish government mandated agencies to adopt a cloud first approach that would underpin several critical government strategies.

c. Benefits of the change: what the benefits of adoption will be for the organisation, stakeholders, customers, and in the case of New Zealand, Māori (the indigenous population).

2) Prepare for the change

a. Stakeholders: working with stakeholders is explored in more depth in the following section.

b. Communications: thinking through what internal communications are needed to support organisational change (noting that external stakeholder engagement is covered in the following section).

c. Change impact: analysis of the change impact, including acknowledging where the changes will impact current organisation processes and resources, as well as the type of capacity and competencies required to manage, maintain, and generate value from cloud technologies.

d. Change readiness, planning & measurement: an assessment of how change ready organisation is for the adoption of cloud. Identification of processes, roles, capacity and competencies (as examples) that need to be in place. An assessment will determine if the organisation has the capacity and capability to engage in the change.

e. Learning: this covers what can the organisation learn from other NSO's (or other organisations) adoption of cloud. Can these experiences be leveraged? What learning is being generated as the adoption to the cloud is being implemented? Can these be applied to improve the implementation approaches?

3) Implement the change

a. Project management and delivery options: thinking through what implementation approach will work for the particular NSO.

b. Sustaining the change: putting appropriate activities in place to ensure the organisation has such elements as the capacity, capability, policies, processes, future plans, and change management plans to ensure the benefits from adoption of cloud are realised.

Stakeholder engagement has increasingly become an important aspect of data related decisions, such as use of cloud technologies. The public is becoming increasingly data savvy with growing awareness of data privacy, security, protections, ethics, and sovereignty over recent years. Legislation, such as the European General Data Protection Regulation (2018), and relevant government policies have also brought people's rights around their data into law and government directives. Therefore, engagement with stakeholders must take relevant legislation and government policies into account.

Recognising indigenous people's data rights and interests forms an important aspect of any stakeholder engagement and is increasingly driven by government policy and legislation. For example, the New Zealand government's cloud First Policy was recently refreshed to require agencies to consider accountability, ethics, transparency, and collaboration in relation to Māori data when making decisions about the adoption of cloud services. Te Kāhui Raraunga (a group representing multiple iwi (tribes)) released a paper regarding Māori data sovereignty and offshoring Māori data. One key recommendation is that Māori data sovereignty requirements must be central to decision making, particularly with regard to offshoring and procurement[11].

Alongside the New Zealand government's cloud First Policy, the Data & Statistics Act 2022 specifically requires Statistics NZ to "recognise and respect the Crown's (governments) responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi by recognising the interests of Māori in the way data is collected, managed and used for the production of official statistics and research"[12].

Regardless of the legal or policy environment, social licence considerations must also be considered. An NSO could have the legal support in place to utilise cloud technologies, but without transparency with the public on how their data is stored and protected a risk remains that cloud implementations could be viewed negatively and impact a NSO's ability to utilise cloud technologies. Transparency, engagement, education, and demonstrating the benefits of cloud technologies with the public on how data is stored, processed, and kept secure will help mitigate social licence issues. This engagement will result in reduction in perceived risks and support directly addressing any real risks (such as questions around data sovereignty).

Working with data suppliers (and this includes the public, both as responders to surveys and through administrative data) is also important when using cloud technologies. It may be prudent to engage in agreements, such as Memorandum of Understanding (MOUs), or legal agreements, to provide documented requirements to support cloud implementation.

Engagement with internal NSO teams is important to be able to drive any cloud implementation effort. Working with executive teams will support buy-in to any investment in cloud adoption. Executive (or internal governance / decision making) teams are likely to

[11] https://www.kahuiraraunga.io/_files/ugd/b8e45c_c035c550c8244c70a1025cd90a97298e.pdf

[12] https://www.legislation.govt.nz/act/public/2022/0039/latest/whole.html#LMS475214. Referring to Section 14 (a) (ii).

have to go through a similar journey as external stakeholders on the benefits, risks, and mitigations of cloud adoption. They will be driven by legislation and/or government and/or ministerial directives but will rely on expertise (either internal or externally sourced) to guide decision making and any implementation.

Other key internal teams to engage with include those engaged in statistical collection, analysis, processing, methodology work and production. These teams will need to understand the benefits and resulting business changes from any implementation. Getting buy-in and support from the key users of cloud technologies will be critical for the success of implementation of cloud. They will need to be supported with operational policies, training, and other change management activities to sustain the benefits of implementation.

Future Outlook and Recommendations

Several recommendations can be made to ensure a successful and sustainable NSO's transition to the cloud. Firstly, focusing on enhancing security and privacy measures in the cloud environment is essential. This can be achieved by continuously evaluating and updating security protocols, conducting regular audits, and implementing encryption techniques to protect sensitive statistical data. organisations should also consider leveraging multi-cloud or hybrid cloud strategies to diversify their cloud providers and mitigate the risk of vendor lock-in. This approach can offer additional flexibility, redundancy, and cost optimisation opportunities.

Additionally, statistical organisations should prioritise investing in data analytics and machine learning capabilities in the cloud. By embracing cloud-native analytics tools, they can harness the power of data-driven insights, enabling evidence-based decision-making processes. Exploring serverless computing and containerization can further enhance operational efficiency and resource utilisation in the cloud environment. As data volumes and analytical requirements grow, embracing cutting-edge technologies will be crucial for maintaining a competitive edge and staying at the forefront of statistical research and reporting.

Furthermore, ongoing staff training and upskilling initiatives should be integrated into the organisational culture. Cloud technology is continuously evolving, and a skilled workforce is essential for harnessing its full potential. By nurturing a cloud-first mindset within the organisation, employees can proactively contribute to the optimisation of cloud resources and the adoption of innovative cloud-based solutions. emphasising a culture of collaboration and knowledge sharing among statistical organisations can also facilitate the exchange of best practices and lessons learned during cloud adoption journeys. Regularly benchmarking progress and outcomes against industry standards and peer organisations will provide valuable insights for continuous improvement and help guide future cloud adoption strategies.

In conclusion, embracing cloud adoption in statistical organisations requires a thoughtful and holistic approach. By prioritising data security, exploring advanced analytics capabilities, and investing in employee skills, organisations can unlock the true potential of cloud technology and drive data-centric decision-making in a dynamic and rapidly evolving digital landscape.

5. Cloud Security and Privacy

NSOs are responsible for a vast array of data that are used for official statistical production and for that purpose only. The statistical business process depends on data about individuals, households, enterprises, municipalities, etc. and these different entities/statistical units trust the NSO to keep their data safe. There are also legal obligations, data protection, statistical act, etc. that NSOs must adhere to and are meant to further ensure the security and privacy of data used for official statistical production.

NSOs are, thus, quite sensitive and sensitised in matters of how and where data are kept.Due to these issues, they have traditionally been keen on keeping their data on site in dedicated data servers within the office. The thinking being that the NSO building being the most trusted and safe place for keeping sensitive data.

The cliché is that cloud computing has disrupted the global IT environment. There is of course some truth to the cliché and the IT environment of NSOs has been changed, although maybe not as drastically as has been the case for other sectors. Major issues with regards to implementing cloud solutions are security and privacy measures and if NSOs are legally allowed to store data in the cloud. This chapter provides guidelines on what needs to be taken into account from a security and privacy perspective when NSOs make decisions on moving data to the cloud. We provide interested managers and decision makers of NSOs with a checklist that can be followed when assessing if the security and privacy of a particular computer cloud solution is suitable for use from a perspective of official statistical production. The chapter is heavily indebted to the pioneering work of Statistics Finland in this area.

This chapter focuses on issues on privacy and security. While these terms are linked, there are also important differences between them. In this chapter cloud security are the measures that are in place to secure the NSOs infrastructure, processes and the data in the cloud. Examples are encryption protocols, access controls and data backup/recovery strategy. Privacy refers to how the data are kept in the cloud and to what extent the privacy of individual units are guarded, e.g. by disclosure control and what types of information are available. One example would be if direct identifiers are available in the data set or if sensitive information can be accessed by users of the data. Data security is generally more seen as a part of the IT work of an NSO.

Security and privacy issues

NSOs collect, process and disseminate vast amounts of data on various aspects of society that are then used by politicians, researchers, enterprises and the general public to make informed decisions. Trustworthiness and credibility are two vital factors for statistical agencies. If a statistical agency is not perceived as trustworthy, decision makers might be hesitant to use its data as a basis for decisions. NSOs with a poor reputation might also face issues in data collection. For example, individuals might be reluctant to participate and provide their information in voluntary surveys, if they view the collecting agency as not trustworthy. Integrity of the statistical data and processes is also important, as inaccurate or biassed statistics might lead to suboptimal decisions that can have a broad impact on society. Information security, privacy, and compliance are all important in ensuring the trustworthiness of a NSO.

Security, privacy and compliance concerns are typical blockers in adopting cloud services. In order to process and store data in the cloud, data must be transferred to a data centre of the third party, the cloud service provider. Some organisations are concerned about the possible risks involved in processing and storing data in the cloud services, and might prefer the traditional on-premises approach for more control of their data. Smaller organisations might also lack the relevant technical and legal capabilities to properly evaluate the actual risks associated with cloud computing, and decide to err on the side of caution.

On the other hand, major cloud service providers ("Hyperscalers") are much aware of the security, privacy and compliance concerns, and take them very seriously. Major cloud service providers are able to make investments in cybersecurity that smaller scale providers cannot match. Over time, the mindset of security being a weakness of cloud services has shifted to recognize it as a strength instead, mostly because of the major investments cloud service providers are able to make. It is important to note however, that security in the cloud does not rest solely on the service provider but is a shared responsibility between the customer and service provider. The responsibilities of customer and service provider are dependent on the service model (IaaS, PaaS, SaaS). The customer has most responsibility (and control) in the IaaS services, and less responsibility in the SaaS services. Regardless of the service model, the customer is always responsible for the data, devices (endpoints), accounts and access management.

Another issue that is important for NOAs is data sovereignty. Data sovereignty is a requirement that a cloud service provider guarantees that cloud services and underlying infrastructure is designed to provide data access in compliance with laws and regulations of the originating country of the data in question. One form of data sovereignty are legal restrictions regarding the geographical location of the location of data servers. This can limit the usefulness of a cloud environment. However, there are at least two possible alternatives. Firstly, the customer can set up his own on-premise private cloud. Secondly, many of the international firms providing cloud services have set up (or are setting up) data servers within different countries, allowing the users to choose in which physical location the data is kept.

Data sovereignty can be especially important for statistical agencies that might have to follow strict rules and regulations about where sensitive data can be hosted, for example in order to ensure that privacy frameworks of the country of origin are followed and third parties are not allowed access to the data. There can be some advantages to setting up an on-premise private cloud. For example, the owner can make his own policies and enact them on his cloud. Note that although a private cloud can be more secure, this puts an extra effort on the shoulders of the cloud consumer as it must keep up with the latest changes and know how to integrate the cloud with other systems and implement it without creating a security risk. There are other advantages like more control of data and therefore a clearer ownership. There is also the factor of having independence from commercial cloud providers. Although it is not as clear if this is a pro or a con.

The drawbacks of pushing towards complete data sovereignty is that compatibility with other cloud services might be compromised and also that the possibility of using the cloud as a hyperscaler (for example for machine learning or or complex processing of statistical data) could be more complex. These compatibility issues might not only decrease the processing power but they might also create their own security risk. Another issue is that unless the sovereign data cloud is operated by a commercial vendor (which I understand is rather rare) the adoption of new technologies in the cloud environment is slower. Which, again, can be a security risk in itself.

Experiences from other industries

Cloud computing has been making headway in other industries for quite some time now. It is interesting to see what lessons and/or experiences from other enterprises can be applied to security and privacy issues in statistical agencies where the adoption of cloud computing is less widespread.

The Shared Responsibility Model

Cloud service providers never and should not accept full responsibility for securing data. The contract with a cloud provider often limits their responsibility to hosting infrastructure, network controls, and physical server security. This arrangement is known as the shared responsibility model, where the provider assumes certain responsibilities, and the client (e.g. a statistical agency) agrees to handle the rest. Some of these factors are employee training and awareness, data encryption, establishing an access management policy, compliance with standards, penetration testing and creating a business continuity and disaster recovery (BCDR) Plan.

Employee Training and Awareness: Financial organisations, healthcare institutions, and other similar entities invest in employee training and awareness programs to educate their staff about security best practices and potential threats. Similarly statistical agencies should implement training programs to educate their personnel about cloud security, privacy, and data handling practices.

Data Encryption: It is essential to ensure that all data stored in the cloud is encrypted, both during transit and at rest. Encryption guarantees that even if unauthorised individuals gain access to the data, they won't be able to interpret or use it without the encryption keys. Financial institutions often encrypt sensitive customer data, such as bank account details and transaction information. NSOs can adopt a similar approach by encrypting official statistical data stored in the cloud, thereby protecting the data even in the event of unauthorised access. The management of encryption keys is an important factor and a nontrivial issue. Encryption is a basic mechanism for confidentiality of data and for guarding the privacy of data. A mismanagement of encryption keys can mean a significant loss of data – or at least worthless data that cannot be used. In order for the data to be useful a key management system can be set up where we can choose from at least four forms of key management forms ranging from a setup where the cloud provider manages the keys fully to the customer managing the keys and encryption themselves. The four forms are:

- Managed keys where the cloud provider manages the encryption and the keys.

- Bring your own key (BYOK) where the cloud provider provides the encryption but the client brings the key for the encryption.

- Hold your own key (HYOK) where the cloud provider manages the encryption while the client holds the key.

- Bring your own encryption (BYOE) where the client manages both the encryption and the key management.

Establish an Access Management Policy: Access management is solely in the hands of the client. A critical cloud security best practice is to develop an access management policy and consistently update it as the organisation changes and grows. The purpose of an access management policy is to:

- Define all users in the organisation

- Determine the appropriate access rights for each user, i.e. need-to-know basis

- Control the granting and revocation of access rights

Statistical agencies can implement strong access controls for their cloud environment, like healthcare organisations. This may involve employing multi-factor authentication for user logins, implementing role-based access control to restrict access and utilising privileged access management to monitor and control administrative access.

Compliance with Standards: When selecting a cloud service provider, it is crucial to choose one that complies with standards and regulations. For example, ISO 27001 for information security management and GDPR (General Data Protection Regulation) for data protection and privacy are important standards. It is important to verify that the provider holds appropriate certifications and undergoes regular audits. Healthcare organisations must comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Similarly, NSOs should identify relevant data protection and privacy regulations applicable to official statistics and ensure that their cloud service provider adheres to those regulations. At Statistics Canada, the cloud environment has enabled faster to market security implementation, notably for those solutions that are built upon cloud foundational or cloud native frameworks.

Perform Penetration Testing and Create a Business Continuity and Disaster Recovery (BCDR) Plan: Continuous monitoring and regular testing, such as penetration testing, are crucial activities for cloud security professionals. These activities help identify new vulnerabilities as they emerge and ensure that the highest-priority risks are addressed promptly. The information gathered from testing can also inform the creation and management of a Business Continuity and Disaster Recovery (BCDR) plan.

Differences between statistical agencies and other industries

The main differences between statistical agencies and other industries with regards to security and privacy issues in cloud computing are due to data volume and complexity, statistical methodology and software, and long term data preservation.

Concerns of data owners: As NSOs collect data from a variety of other institutions (governmental and non-governmental alike) the latter might have an interest in how their data is being handled within the cloud environment. Therefore there can be an increased requirement on the NSO from the data owners to show precisely how data security is ensured in the cloud. If the data are very sensitive to the data owner another solution might be to push computations out, where data data is not delivered to the NSO but only the results of the processes needed to be conducted for the production of statistics. That means that the data owner and the NSO join forces in implementing the necessary processes close to the data (i.e. within the data management system of the data owner) without ever moving the actual data.

Data Volume and Complexity: The data used for statistical production is of various types (enterprises, households, individuals, time series, etc.) and therefore the cloud environment must be able to handle them, without sacrificing neither privacy nor security. Statistical agencies often handle large volumes of complex data that require specialised processing and analysis techniques. Official statistical data can be intricate, necessitating unique methodologies and tools for data handling. NSOs must consider the scalability and performance of cloud services to efficiently handle the size and complexity of their datasets.

Statistical Methodologies and Software: Statistical agencies employ specific statistical methodologies, software packages and data processing tools tailored to their requirements, i.e. niche software and tools. Integrating these methodologies and tools with cloud services may require additional considerations, such as software compatibility, customization, and licensing agreements, to ensure seamless operations in the cloud environment.

Long-Term Data Preservation: NSOs frequently have long-term data preservation requirements to support historical research, policy analysis, and comparability over time. Ensuring the integrity, accessibility, and usability of official statistical data over extended periods becomes a critical concern.

Data stewardship: The move towards a more active role of NSOs as data stewards can both enable the move to a cloud based environment (e.g. for a more efficient data management and data sharing) or obstruct it (e.g. if data owners or governments are opposed to using a cloud environment for their data).

Statistics Finland’s cloud environment: A case study

Background

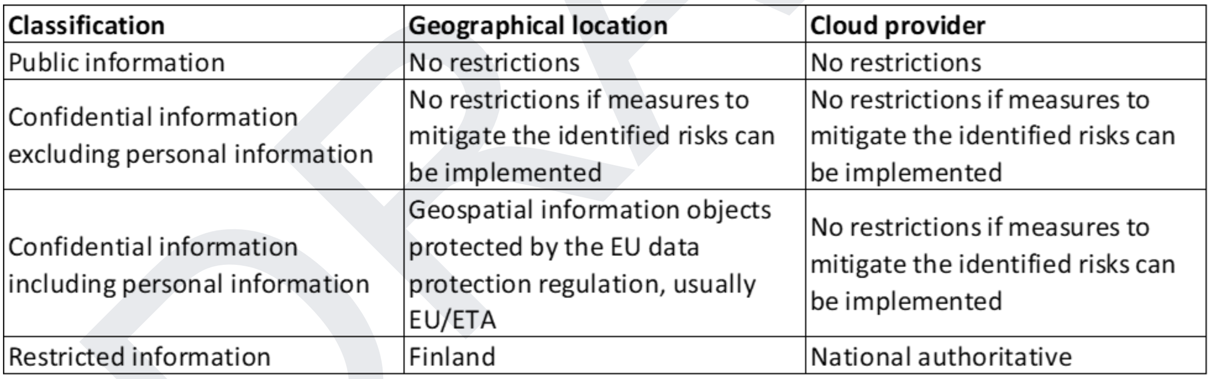
The principles for public cloud use in the Finnish government encourage a cloud-first approach whenever possible. However, if risk assessment outcomes, return-on-investment estimates, or architectural reasons prevent the use of public cloud services, alternative options should be explored. These principles were established by the Ministry of Finance in 2019 and are currently being updated in 2023.

Statistics Finland has its own cloud principles that are strongly based on the government cloud principles. While Statistics Finland's cloud principles may differ slightly, they are based on the same foundation of promoting a cloud-first approach whenever possible.

The government ICT operator, Valtori, provides public cloud services to government offices. These services are available through providers such as Microsoft Azure, Amazon Web Services, Google cloud Platform, and Oracle cloud Infrastructure. Offices can choose a single provider or use a multi-cloud approach. Regardless of the approach, all providers must meet government security requirements and other regulations.

In 2020, the National Cyber Security Centre in Finland published a set of criteria that can be used to evaluate the information security of cloud services. The criteria is designed to assess cloud services in eleven (11) different categories, each of which contains multiple requirements that must be met to achieve a satisfactory rating. Additionally, the criteria take into account the classification of information and how it impacts the use of cloud services (Table 5.1). This versatile evaluation method enables organisations to better understand the security of the cloud services they use and make informed decisions regarding their data and applications in the cloud.

Table 5.1



Classification	Geographical location	Cloud provider
Public information	No restrictions	No restrictions
Confidential information excluding personal information	No restrictions if measures to mitigate the identified risks can be implemented	No restrictions if measures to mitigate the identified risks can be implemented
Confidential information including personal information	Geospatial information objects protected by the EU data protection regulation, usually EU/ETA	No restrictions if measures to mitigate the identified risks can be implemented
Restricted information	Finland	National authoritative

Cloud in Statistics Finland

Statistics Finland has gradually adopted cloud services over the past several years, beginning with the deployment of Microsoft Dynamics 365 for production around 2015. From 2015 to 2017, we experimented with Microsoft Azure, focusing mainly on platform-as-a-service (PaaS) solutions. Between 2017 and 2018, Statistics Finland developed its first cloud principles and began working on cloud projects. By 2019, we had deployed the rest of the Microsoft 365 services for production. The cloud principles were also updated with data processing requirements and cloud governance documents for Microsoft Azure and Microsoft 365 were created. In 2020, the first cloud project was ready for production, and we began implementing Microsoft Azure cloud foundation. In 2021, we implemented an in-house machine learning platform and updated cloud principles to provide deeper coverage of regulations and legislative requirements. By 2022, we had finished implementing the cloud foundation, established a centralised logging architecture with cloud-based security information and event management (SIEM), and developed Zero Trust-based networking and identity and access management baselines. We also created cost management and business continuity principles and a legal framework for data processing in cloud services. In 2023 we are focusing on compliance requirements and will also introduce a 24/7 Security Operations centre (SOC).

Focus on legislative requirements

In 2022, we created a legal framework to support Statistics Finland's cloud journey. The legal framework encompasses all relevant national and EU-level legislation, as well as considers contradictory legislation and associated threats. It also covers regulations and other instructive documentation, along with control measures for achieving legislative compliance.

To create the framework, relevant legislation and regulations were resolved, including how the legislative requirements map to differently classified information. Existing instructive documentation from the Finnish government and Statistics Finland was also considered, and controls were described to fulfil compliance requirements.

In practice, the legal framework is used to classify data according to the classification system in use and select the appropriate category from the binding legislation documentation. For each defined section and subsection, the controls and measures implemented to fulfil requirements are described, with references to other relevant documentation as necessary. Any doubts about the sufficiency of a measure are noted for risk assessment purposes.

Box 5.1

An example of a legislative requirement

Legislation

Finnish Act on Public Administration Information Management (906/2019)

Requirement

16 § The authority responsible for the information system must define the access rights of the information system. Access rights must be defined according to the usage needs related to the user's tasks, and they must be kept up-to-date.

Implementation

The identity and access management is centralised using Azure Active Directory. The user is always required to use multi-factor authentication for accessing the requested resources. The resource access is based on role-based access control (RBAC) and the principle of the least privilege. The role of the user must be granted by the supervisor. The access roles are described in detail on the system documentation.

Summary

Information security and privacy are two pillars upon which official statistical production rests as they are integral for the trust which is necessary for statistical agencies to be able to collect, harvest, store and process data. Based on the work presented in this chapter on privacy and security for official statistics there are some general guidelines that are suggested when planning to move official statistics to a cloud based environment.

- Before moving to a cloud based environment, make sure that there are no hindrances in the legal environment of your country. Also, keep in mind data sovereignty and make sure that the geographical location of the data centres of the cloud provider.
- Document the process and all decisions made during it when moving to the cloud. This is especially important for all aspects concerning privacy and security.
- Decide and present how staff is supposed to work within the cloud environment. For example it must be clear how privacy issues will be tackled and what types of data can be processed in the cloud environment.
- Always be prepared to present how the SA is handling security issues within the cloud environment.
- All issues with regards with privacy and security have to be explicitly put forth in the agreement with the cloud provider, and the procurement.
- Key strategy for data encryption is important.
- Remember that encrypted data without an encryption key is useless.
- Keep an open dialog with your local data privacy authority.

6. Cloud Capacity and Competencies

When we think about learning for cloud it's all about people and building capabilities. To be successful you will need to invest in the following areas:

- **Fostering a learning culture:** cloud adoption requires a complete shift in both technical skills and organisational culture. Senior leadership needs to ensure that learning, upskilling and culture evolution are prioritised. Moreover, capacity planning needs to ensure that it allocates sufficient time and space for employees to focus on their growth and development.

- **Company Growth:** cloud adoption will ensure that technology and infrastructure can scale to meet evolving business needs. However, evolution of business processes are key to ensuring that cloud adoption is done effectively and efficiently. Employee growth, coupled with improved organisational performance and innovation through business process modernization will need to be foundational in your approach to cloud adoption.

We fundamentally believe that you need a culture founded in a growth mindset. It starts with a belief that everyone is empowered to grow and develop; that potential is nurtured, and that anyone can change their mindset. We need to be always learning and insatiably curious. We need to be willing to lean into uncertainty, take risks and move quickly when we make mistakes, recognizing failure happens along the way to mastery. The organisation in which we work must also be supportive of this approach, offering the psychological safety necessary to learn and develop as well as the structures to allow for agile delivery.

Leaders create clarity, generate energy, and deliver success.

- *Create clarity:* Leaders synthesise complex information, ensure shared understanding, and define a course of action that aligns with the organisation's vision and goals.

- *Generate energy:* Leaders inspire optimism, creativity, and growth within the organisation. They create an environment where everyone can do their best work and contribute to building organisations that are stronger tomorrow than today, all while keeping alignment with the organisation's values.

- *Deliver success:* Leaders drive innovation, seek solutions without boundaries, and tenaciously pursue the right outcomes that align with the organisation's vision and values.

By embodying these qualities, leaders inspire and empower their teams to align upskilling efforts with the organisation's vision and values. They provide the necessary clarity, energy, and focus to ensure that upskilling initiatives contribute to the organisation's success and growth while staying true to its core values.

Assumptions

The information provided in the chapter is based on the following assumptions:

- The **department or organisation** for which this chapter is presented has a specific **size** or number of employees. The exact size may vary, but it is considered a key factor in determining the requirements, resources, and strategies mentioned in this chapter.

- The organisation has decided to migrate or is considering migrating its infrastructure, applications, or data to a cloud environment. The specific **cloud migration approach**, such as lift-and-shift, re-platforming, or refactoring, may vary based on the organisation's goals and requirements.

- The organisation has an existing **IT infrastructure** in place, which includes hardware, networking components, servers, storage devices, and related systems. This infrastructure serves as the foundation for the cloud migration process.

- The organisation has a **portfolio of applications** or software systems that are currently running on its on-premises infrastructure or may already be partly located in the cloud. These applications may have different architectures, dependencies, and integration requirements, which need to be considered during the cloud migration process.

- The organisation has certain **security and compliance requirements** that must be addressed during the cloud migration. This includes data protection, access controls, regulatory compliance, and other relevant security measures.

- The organisation is considering migrating to a specific type of **cloud deployment model**, such as a public cloud or a private cloud environment. The choice of deployment model may depend on various factors, including the organisation's requirements, security considerations, data sensitivity, and regulatory compliance needs. The specific type of cloud deployment model will influence the cloud migration strategy and the tools and technologies involved in the process.

Upskilling for cloud

Cloud technology has revolutionised the way organisations deliver and consume services, including NSOs. Upskilling for cloud is essential to ensure that the workforce possesses the necessary knowledge, skills, and experience to effectively adopt, operate, and manage cloud services for Digital Government. It enables agencies to leverage the full potential of the cloud and drive innovation, efficiency, and agility in their operations.

Upskilling for the cloud encompasses more than just training. While training is an important component, upskilling for cloud also involves developing a comprehensive understanding of cloud concepts, architectures, and best practices. It includes acquiring hands-on experience with cloud platforms, developing problem-solving skills, and fostering a mindset of continuous learning and adaptation in the cloud environment.

Building a Cloud-Friendly Culture

Culture plays a crucial role in successful cloud adoption. A cloud-friendly culture embraces innovation, experimentation, and a willingness to explore new approaches. It encourages collaboration, knowledge sharing, and risk-taking. A culture that values learning and embraces change can facilitate the adoption of cloud technologies and drive digital transformation within the NSO.

Creating a culture of innovation and experimentation involves several key aspects:

- *Leadership support*: Leaders should champion cloud adoption, communicate the benefits, and provide resources to foster a culture of innovation.

- *Encouraging creativity*: Encouraging employees to think outside the box, propose new ideas, and experiment with cloud solutions fosters innovation and helps identify new opportunities.

- *Embracing failure as a learning opportunity*: Creating an environment where failures are viewed as valuable learning experiences promotes a culture of continuous improvement and risk-taking.

- *Empowering employees*: Providing employees with autonomy, decision-making authority, and opportunities to contribute to cloud initiatives helps create a sense of ownership and fosters innovation.

- *Engage and collaborate*: Ensure that both IT and subject matter experts are brought together to explore new ways of thinking, operating and exploring. Exploring opportunities jointly within multidisciplinary teams will enable greater growth and alignment between cloud platform offerings and business needs.

- *Iterative approach*: Reinforce the practice of building, refining, and improving solutions continuously. This approach will enable minimally impactful failures, maximising business value, all while driving learning along the way.

Alignment with Cloud Operating Models

Upskilling for cloud should align with the organisation's chosen cloud operating models (IaaS, PaaS or SaaS). The upskilling efforts should focus on the specific skills and competencies required to effectively operate and manage cloud services within the chosen operating model.

Open Source, Open Standards and Cloud-Based Technologies

Understanding and leveraging open-source software and its culture is extremely important in the context of cloud-based technologies. Cloud platforms often rely on open-source technologies as a foundation for their services. Open-source software promotes collaboration, transparency, flexibility, and cost efficiency. Upskilling initiatives should include educating employees on open-source principles, familiarising them with popular open-source projects[13] used in cloud environments, and providing training on open-source tools and technologies. Open standards are essential in the realm of technology, especially in the context of open-source and cloud-based technologies. They ensure compatibility, interoperability, and collaboration among different (parts of) systems. Upskilling initiatives should prioritise educating employees about open standards and their implementation in cloud environments, enabling organisations to leverage a wide array of compatible tools and technologies.

Approaches to building cloud capacity

Cloud transformation is complex due to the many ways in which people are impacted ranging from how they work, how they are organised, how they think and the new skills they need. Compounding these challenges is the ever evolving nature of cloud and its underlying technologies, which require that upskilling initiatives be evergreen.

Strategies to build cloud capability

- Conduct a training needs analysis. Assess gaps in capability/capacity including technology-based competencies, role-based competencies and cloud certification requirements

- Develop a comprehensive role-based training curriculum, leveraging open-source concepts and materials where possible.

- Develop training/knowledge transfer materials.

- Develop tailored communications materials to keep cloud experts informed of new upskilling opportunities, as well as changes in existing curriculums.

- Offer opportunities to experiment in the cloud, and collaborate broadly to expose external players to your cloud platform and business.

- Create learning champions that can create energy around upskilling and carry momentum continuously.

[13] Example Cloud Native Computing Foundation (https://www.cncf.io/)

One approach to build skills for cloud is to take a tiered approach:

- Tier 1
    - Designed for Specialists with a critical role in operating cloud services or delivering on cloud projects
    - Funded formal training at intermediate and advanced levels tailored for specialised roles or relevant services/technology with certifications as appropriate
- Tier 2
    - Designed for technical staff who may have some need to deliver solutions using cloud services
    - Funded formal training at Foundational level with intermediate level training provided as required.
- Tier 3
    - Designed for awareness and foundational skills, which can include members of both the IT and subject matter community.
    - Provision of free online training at foundational level, or self-paced learning options.

Example (AWS) capability uplift using formal learning alongside internal and informal approaches to build capability across specific roles.

Staffing Strategies

Many staffing strategies exist and you will need to combine multiple approaches such as hiring, training, staff augmentation and contracting throughout your cloud journey which will be influenced on your cloud adoption strategy, as well as availability of skilled capacity.

Ensuring your cloud implementation strategy leverages open source concepts will enable an organisation to attract a great range of tallent, while enabling that talent to become proficient more quickly when onboarded to an organisation.

Both attracting and retaining cloud tallent is challenging, and staffing strategies should ensure that both those elements are kept in consideration. Your staffing strategy should clearly indicate how new and existing resources will be upskilled and how those skills will be evergreen. Exposing this upskilling strategy can help further attract cloud talent. Some upskilling and staffing strategies include:

Training and Upskilling Curriculums

- Formal Training and Certification: Enrol in courses that provide formal training and certification in cloud technologies like Amazon Web Services (AWS), Microsoft Azure, or Google cloud Platform (GCP).
- Online Learning Platforms[14]: Use online learning platforms to access cloud computing courses and certifications.
- Hands-On Experience: Gain practical experience by working on cloud projects and experimenting with different cloud technologies. Participate in cloud related Open Source projects.
- Peer Learning: Join online communities like forums, discussion groups, or cloud user groups to learn from peers and experts in the field.
- Hackathons and Challenges: Participate in cloud-based hackathons, challenges, or contests to develop new skills and gain recognition.
- Conferences and Other Formative Events: Attend cloud computing conferences and events to learn about the latest trends, innovations, and best practices.
- Mentoring and Coaching: Seek out mentors or coaches who are experienced in cloud computing and can provide guidance, support, and feedback.
- Reading and Research: Keep up with the latest cloud computing trends and developments by reading articles, books, and research papers.
- Continuous Learning: Make upskilling in cloud computing a regular and ongoing part of your professional development, and leadership needs to ensure time is allocated to these activities.

Hiring

- Actively run selection processes, or hiring processes, to seek out the specific skills set that are gaps within your organisation and offer them permanent employment options.

[14] Examples include EdX (https://www.edx.org/), Pluralsight (https://www.pluralsight.com/), Cloud Native Computing Foundation (https://www.cncf.io/)

- Develop a robust apprenticeship or co-op programs with higher education institutions. Partnership with learning institutions provide an efficient and effective mechanism to continuously feed talent into your organisation, while offsetting any attrition and offering a continuous renewal of cloud talent.

- Continuously highlight your cloud journey or ambitions to ignite the imagination of potential talent.

Augment

Establish contracts to bring in contractors with the required skills. This is particularly effective when they are paired with employees that have the right skill set but lack experience**.** Moreover, this approach can also help accelerate the adoption of an emerging technology by exposing existing staff to expertise early on in the adoption process.

Procurement vehicles should also be established to match the agile and scaling needs of the cloud. Standing offers, or other procurement options, should be established before capacity is needed, to ensure such capacity can be leveraged if/when it's required.

Building cloud capacity requires investments in the people who will ultimately build and support your cloud platform. To build and maintain that capacity requires intentional strategies to attract talent, challenge and continuously upskill that talent, while providing them the time and space for both formal/structured learning and exploration and experimentation.

Key cloud Roles

As you mature in your cloud journey, foundational roles will be required to ensure your cloud platform is built and maintained efficiently and effectively. The size, number and types of roles required will depend on the size and needs of your organisation. Some key roles include:

- **Cloud architects** are responsible for designing and implementing cloud solutions that meet business and technical requirements. They have in-depth knowledge of cloud architecture and are skilled in designing scalable and secure cloud solutions. Having a cloud architect early on in cloud adoption will be critical to ensure your platform is built on a solid foundation.

- **Cloud engineers** are primarily responsible for cloud implementation, monitoring and maintenance. They set up and operate the cloud infrastructure designed by the architects. This requires engineers to possess detailed knowledge of a cloud's operation and be able to set up and configure resources, including servers, storage, networks and an array of cloud services. This may involve a significant amount of automation.

- **Cloud platform engineers** build and maintain one or more developer platforms that help software solutions run seamlessly. In collaboration with software development teams, the platform engineer ensures that the platform is reliable, scalable and capable of handling the needs of the solutions that are underpinned by the platform.

- **Cloud Developers** are responsible for building cloud-native applications that are optimised for cloud platforms. They have expertise in programming languages, cloud frameworks, and tools for building scalable and secure cloud applications. Often, working in CI/CD environments. Most cloud projects are typically focused on three goals: migrate an existing application to the cloud; modify an existing application for the cloud; or create an entirely new cloud-native application.

All of these use cases involve a team of professional cloud software developers responsible for designing, coding, testing, tuning and scaling applications intended for cloud deployment.

- **Cloud Security Engineers** are responsible for ensuring that cloud-based applications and infrastructure are secure and compliant with regulatory requirements. They have expertise in cloud security best practices, identity and access management, and data protection. A cloud security specialist sometimes oversees the architected infrastructure and software under development and ensures cloud accounts, resources, services and applications meet security standards. Security specialists also review activity logs, look for vulnerabilities, drive incident post-mortems and deliver recommendations for security improvements.

- **Cloud Operations Engineers** are responsible for ensuring that cloud infrastructure is highly available, scalable, and performs optimally. They have expertise in monitoring, troubleshooting, and automating cloud infrastructure.

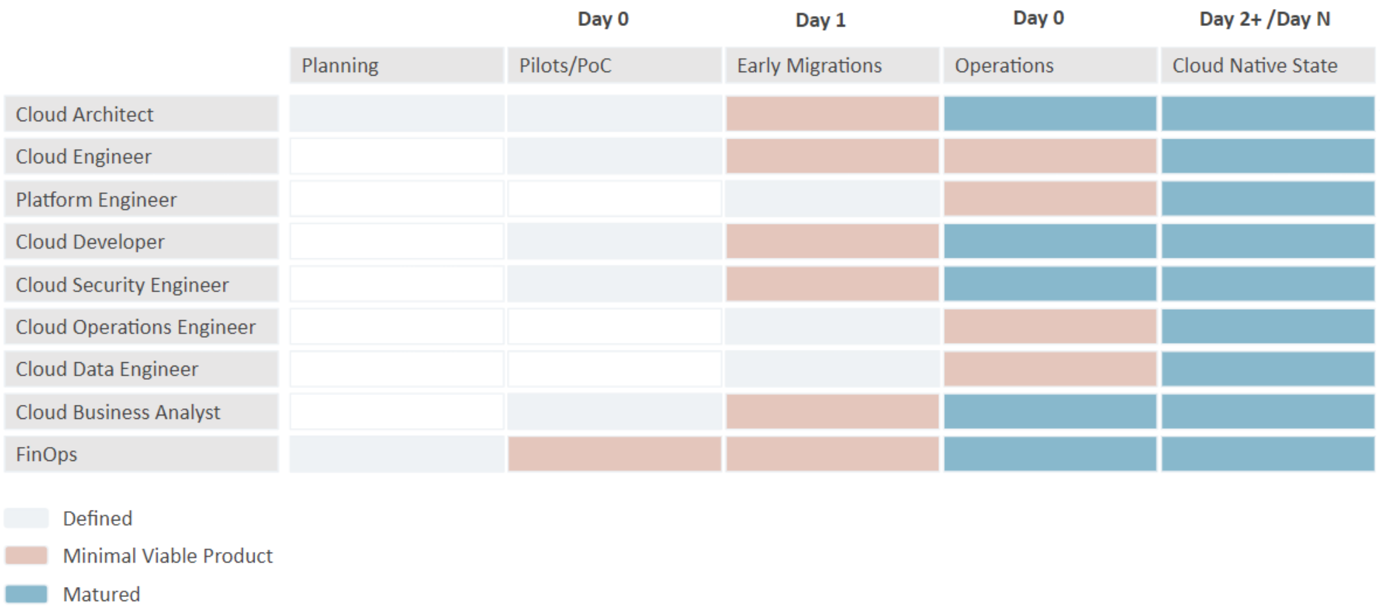
- **Cloud Data Engineers** are responsible for designing and implementing cloud-based data solutions that support analytics and machine learning. They have expertise in data storage, processing, and analysis technologies in the cloud. The cloud data engineer will work closely with an organisation's Information Management (IM) group to: design and implement data storage; design and develop data processing; design and implement data security; and, monitor and optimise data.

- **Cloud Business Analysts** are responsible for identifying and evaluating cloud solutions that meet business needs. They have expertise in cloud technologies and can analyse business requirements to recommend cloud solutions that align with business objectives.

- **FinOps**[15] is a new discipline that takes a strategic approach to managing and optimising cloud costs. It involves collaboration between finance, operations, and engineering teams to make the most of cloud investments. By adopting FinOps, organisations can improve cost transparency, enhance resource utilisation, and make more accurate budget forecasts, ultimately striking a balance between cost, performance, and business value. Implementing FinOps can help companies gain better control over their cloud expenditures and maximise the return on their cloud investments. To ensure cloud implementation is efficient and manageable within an organisation, it is recommended to have FinOps roles created early in the cloud adoption process.

Cloud roles should be established and mature along your cloud adoption journey. From initial planning stages, migrations (Day 1), operations (Day 2) to full cloud native state (beyond Day 2), roles should be intentionally established and refined. While they should be tailored to an organisation's particular cloud adoption plan, it is recommended to establish and mature your cloud roles to align to your organisation's cloud maturity as per the timelines in Table 6.1. The “Day” concept is defined in Annex 1.

Table 6.1



		Day 0	Day 1	Day 0	Day 2+ /Day N
	Planning	Pilots/PoC	Early Migrations	Operations	Cloud Native State
Cloud Architect	░	░	🟥	🟦	🟦
Cloud Engineer		░	🟥	🟥	🟦
Platform Engineer			░	🟥	🟦
Cloud Developer		░	🟥	🟦	🟦
Cloud Security Engineer		░	🟥	🟦	🟦
Cloud Operations Engineer			░	🟥	🟦
Cloud Data Engineer			░	🟥	🟦
Cloud Business Analyst		░	🟥	🟦	🟦
FinOps	░	🟥	🟥	🟦	🟦

░ Defined

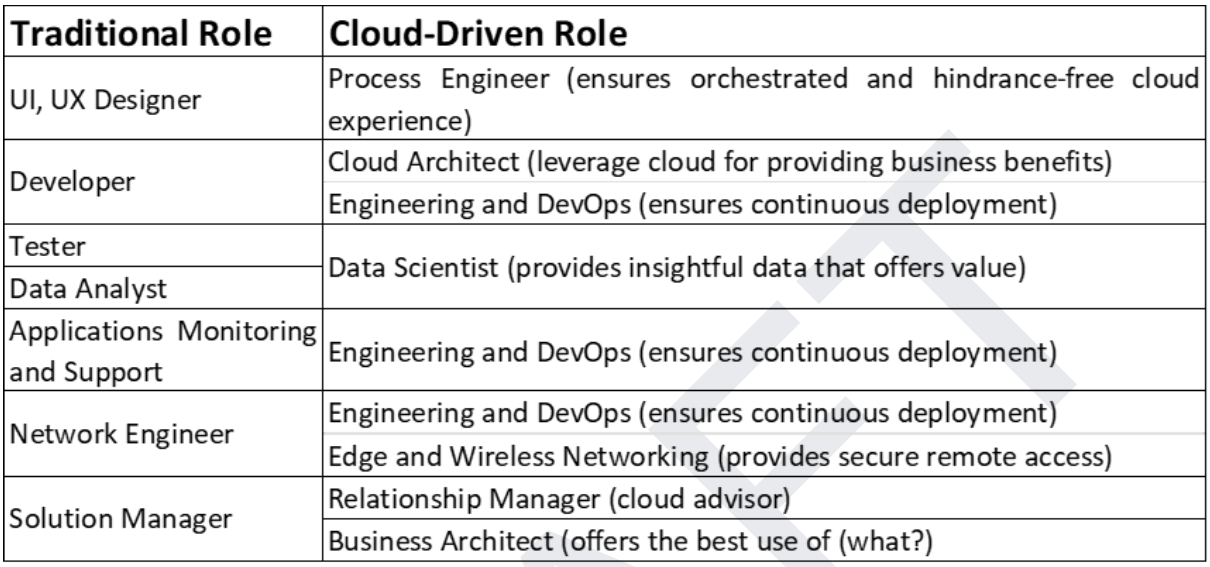
🟥 Minimal Viable Product

🟦 Matured

[15] Many of the FinOps concepts are defined through the FinOps Foundation (https://www.finops.org/)

To further assist in evolving and upskilling your organisation's cloud capacity, identifying the link between traditional IT roles with their evolved cloud-driven counterparts (Table 6.2) can aid in the development of targeted upskilling curriculums.

Table 6.2



Traditional Role	Cloud-Driven Role
UI, UX Designer	Process Engineer (ensures orchestrated and hindrance-free cloud experience)
Developer	Cloud Architect (leverage cloud for providing business benefits)
	Engineering and DevOps (ensures continuous deployment)
Tester	Data Scientist (provides insightful data that offers value)
Data Analyst	
Applications Monitoring and Support	Engineering and DevOps (ensures continuous deployment)
Network Engineer	Engineering and DevOps (ensures continuous deployment)
	Edge and Wireless Networking (provides secure remote access)
Solution Manager	Relationship Manager (cloud advisor)
	Business Architect (offers the best use of (what?)

These roles may overlap or have different titles in different organisations. However, having a team that covers these key areas can help ensure that your cloud infrastructure and applications are built, deployed, and maintained efficiently and effectively.

As part of your cloud journey, you must prepare, reskill, and upskill your staff to know their changing roles and responsibilities and train them for their future roles.

Change Management

In an organisation’s cloud journey, managing change is also a critical factor for success. Implementation of cloud is a fundamental shift in how an organisation delivers on its mandate, and ensuring that all key roles within that organisation, from top to bottom, are aligned on the journey is key to the success.

People need to be brought along on the journey to cloud and the new skills along with the new ways of working that it brings. The culture and approach to change is critical - highlighting that “change is done WITH you – NOT to you” and that collectively, we move people to new ways of thinking and working. The shift to cloud, and the changes it brings, is not a technology centric change; rather technology is the catalyst for foundation change.

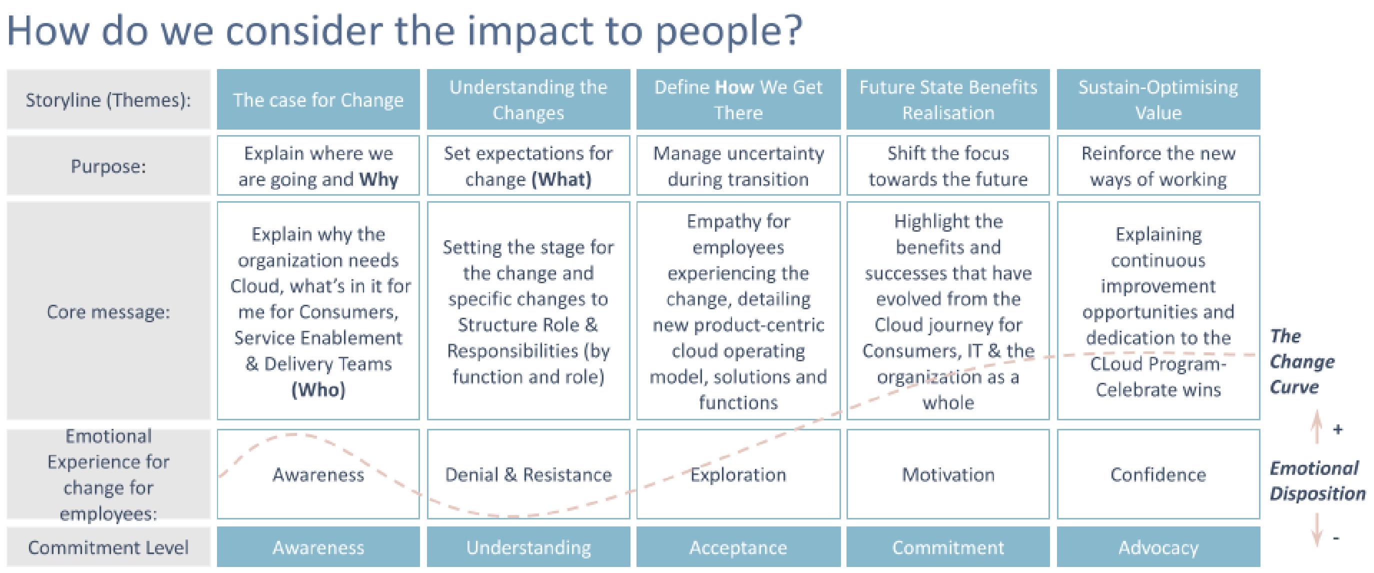
Elements of good change management practices should include:

- Explaining the change
    - What is the driver behind the change?

    - Why is the change beneficial to the organisation?
    - Who needs to be involved in building out the plan for change?
- Planning the change
    - Create a documented change strategy and vision
    - Coordinate stakeholder assessments and consultations
    - Document impact assessment
- Managing the change
    - Communicate often and regularly
    - Plan engagement sessions to both inform, but continuously seek input
    - Review any needed changes to organisational design and processes
    - Develop learning, capabilities, training and hands-on opportunities
- Reinforcing the change
    - Leadership and sponsorship, ensuring that all levels communicate the changes, champion its successes, and offer support and encouragement if any failures are encountered.
- Sustaining the change
    - Identify and document elements and capacity that is needed to sustain the change over the long term
    - Update process, align capacity and funding as required to ensure long-term sustainability.

Steps in managing change must be intentional and transparent to all. Throughout the change a focus on the behaviours and culture that is needed to operate successfully in the cloud is key (Figure 6.1).

Figure 6.1



How do we consider the impact to people?

Storyline (Themes):	The case for Change	Understanding the Changes	Define **How** We Get There	Future State Benefits Realisation	Sustain-Optimising Value
Purpose:	Explain where we are going and **Why**	Set expectations for change **(What)**	Manage uncertainty during transition	Shift the focus towards the future	Reinforce the new ways of working
Core message:	Explain why the organization needs Cloud, what's in it for me for Consumers, Service Enablement & Delivery Teams **(Who)**	Setting the stage for the change and specific changes to Structure Role & Responsibilities (by function and role)	Empathy for employees experiencing the change, detailing new product-centric cloud operating model, solutions and functions	Highlight the benefits and successes that have evolved from the Cloud journey for Consumers, IT & the organization as a whole	Explaining continuous improvement opportunities and dedication to the CLoud Program- Celebrate wins
Emotional Experience for change for employees:	Awareness	Denial & Resistance	Exploration	Motivation	Confidence
Commitment Level	Awareness	Understanding	Acceptance	Commitment	Advocacy

Upskilling and Change Management

Upskilling plays a crucial role in change management and overcoming resistance to change. By providing employees with the necessary skills and knowledge, they feel more confident and empowered to embrace the changes associated with cloud adoption. Upskilling programs should include change management elements, such as communication, training, and support, to address potential resistance and facilitate a smooth transition to the cloud.

By investing in upskilling initiatives, NSOs can build a workforce that is well-prepared for cloud adoption, create a culture that fosters innovation, embraces open-source principles, and successfully navigate the challenges associated with change management in the context of cloud technology. This comprehensive approach enables agencies to harness the full potential of the cloud and drive digital transformation in the pursuit of efficient and data-driven government services.

Challenges

Along your cloud journey, you'll encounter many upskilling and capacity challenges.

- Challenges in hiring and a lack of cloud competencies were top barriers to adoption.
- Concerns about the government's ability to offer competitive compensation.

- Worries about inadequate training opportunities and limited exposure to leading technologies for upskilling existing employees and attracting new talent.
- Budget constraints that may hinder investment in necessary resources and initiatives.

Strategies to Address Challenges

- Secure commitment from senior leadership to drive and support the cloud adoption and upskilling efforts.
- Invest (heavily) in upskilling the current workforce to bridge competency gaps.
- Identify key capability gaps and recruit individuals with the required skills.
- Establish a program and governance structure to oversee cloud adoption and upskilling initiatives.
- Align learning content with business objectives.
- Provide flexible learning options to accommodate different learning styles and preferences.
- Implement comprehensive and clear communications to ensure transparency and clarity.
- Maintain a two-way communication channel with employees to enhance retention.
- Incorporate recognition, reinforcement, gamification, and rewards to motivate and engage employees.
- Measure the success of the upskilling program through defined metrics.
- Implement organisational change management practices to facilitate smooth transitions.
- Allocate budgetary resources appropriately to support the necessary initiatives and investments.

By prioritising commitment from management as the top strategy, organisations can ensure that the necessary support, resources, and leadership are in place to drive the successful adoption of cloud technologies and upskilling initiatives.

Summary

Cloud adoption is a fundamental change to how an organisation thinks and operates. Such a foundational change requires a skilled and motivated workforce to ensure success. That motivation will be driven through a desire to learn, experiment, adapt and ultimately continuously strive to modernise for the betterment of all.

To ensure success in cloud adoption, an organisation must focus on supporting all stakeholders along the journey, by:

- Fostering a culture of learning:
    - The importance of a growth mindset where its both encouraged and expected that we should all become lifelong learners
    - Fostering an environment where there is time & space for learning and flexibility (i.e self-paced, instructors, access to labs etc)
    - Remove the fear of failure and encourage exploration, creativity and ideation
- Support upskilling and career development by allowing employees them the time to build new skills and support them in their professional development:
    - Developing strategies to both encourage and ensure employees remain skilled in the ever evolving cloud landscape
    - Be intentional with upskilling initiatives, to ensure operational needs are balanced with upskilling needs.
    - Make upskilling fun, engaging and valuable, while removing barriers to upskilling.
    - Ensure your organisation has the skills and roles needed to ensure cloud success.
- Continuously attract and retain talent:
    - Non-traditional recruiting/hiring – hire for potential and skills and rely less on academic background and experience, notably to eliminate bias and foster a more inclusive approach that opens doors to under-represented communities and underserved communities and ensures the workforce is representative of the population.
    - Prepare for the next generation of workers by partnering with industry, schools & higher education to position your organisation as an employer of choice for new careers and make it easier (and more fun) for younger generations to learn valuable skills such as AI, machine learning, and data science.

Cloud adoption is a revolution that will require an investment in people, process and technology. Only by including all three facets into your cloud upskilling and adoption plan will you achieve success and ensure that your organisation can leverage cloud in an efficient, effective and appropriate manner.

review how we want to capture the concepts here; at a minimum suggest we recreate this as a generic view without ABS/companies branding and copyright.

7. Conclusion and Recommendations

It is evident from this report that adoption of Cloud offers many opportunities and poses as many challenges for our statistical organisations. Each of the key themes explored provide a holistic view of the issues and capabilities of Cloud services. Furthermore, it is clearly apparent there is a desire to increase the utilisation of cloud capabilities, gaining benefits from factors such as scalability while also providing greater business value. We learned that enablement factors such as increased central government support and direction, can make a statistical organisation's cloud journey achievable.

The Cloud for Official Statistics Project offers, through this publication, aims to assist NSO managers in making sound informed decisions along their organisation's cloud adoption journey. It offers a broad review of what managers need to know and assess, and why these considerations are important. The project puts forward numerous recommendations on five key aspects in cloud adoption based on current experiences, some of which are provided as follows[16].

On service and deployment models, choosing the best one is very important. Each model offers benefits to organisations while presenting strengths and weaknesses compared to other models. From the onset, the decision must be centred on the organisation's business needs and strategic direction. National regulations will impose restrictions on the choice of models or the extent to which some can be used. Staying within these restrictions, undertaking proofs of concepts will inform this decision while leading to increased adoption of cloud over time. The concepts that underlie the different models may appear simple at first, but it is essential to understand their respective nuances as they greatly influence the other aspects addressed in this publication.

On procurement, legal and data sovereignty issues need to be considered and addressed first. This will create a boundary on what you can implement in the cloud. Many NSOs must keep their data kept in their country. NSOs should define early in the procurement process a long term cloud strategy centred on their mandate and business goals. Finally, NSOs should consider the full lifecycle of their cloud services, including the migration to a different cloud provider.

On adoption, enhancing security and privacy measures in the cloud environment is essential. This can be achieved by continuously evaluating the update and security protocols, conducting regular audits and implementing encryption techniques to protect sensitive statistical data. Organisations should also consider leveraging multi cloud or hybrid cloud strategies to diversify their cloud providers and mitigate the risk of vendor lock in this approach offers flexibility, anonymity and cost optimization opportunities. Finally, by embracing cloud native analytical tools, organisations can harness the power of data driven insights, enabling evidence based decision making processes, exploring cloud native technologies has served as computing, and containerization can further enhance operational efficiency, efficiencies and resource utilisation and increase resource utilisation in the cloud as data volumes and analytical requirements grow.

[16] The recommendations were highlighted at a webinar delivered on November 16 2023. (insert link)

On security and privacy, first and foremost, it is essential to conduct a thorough assessment of the legal environment in your country and clearly define what you can and can not do with your data. All agreements and procurement contracts should clearly state who is responsible and accountable for what according to a shared responsibility model. It's very important to document everything that concerns privacy and security along your cloud adoption journey. Thorough documentation will enable you to explain how security and privacy issues are being handled at any time, as well as keeping an open dialogue with local data privacy authorities. Upscaling staff competencies to set up and maintain the cloud environment is important. It is as important for all employees to be clearly informed and trained on how to work in this new environment to ensure strict security, privacy and cost efficiency.

On capacity and competencies, staff development and engagement must be anchored in a formalised cloud strategy. It is crucial that employees first understand why the organisation is adopting cloud and where it needs to grow with it. It is also important to refresh this strategy along the way and communicate changes in a continuous and transparent manner. Once you start to move into the cloud space, there will be a tendency to want to go quicker and do more, and that's fantastic. However, upskilling must be prioritised and planned intentionally. You need to make sure that you allocate enough space to ensure that everyone can learn and grow into that space to be effective, and to do it properly, you need to embrace an agile mindset. A strategy that includes an iterative approach, small steps and “fail and fail quickly” experimentations is foundational to build confidence and reduce risks of failure. Finally, you have to assume attrition is happening, that employees will move to the private sector, as well as, other government departments. It is important to have a continuous flow of talented employees to avoid having the weight of operating a cloud or migrating to a cloud fall on the shoulders of the few. Having a fleshed out cloud strategy allows you to have a vision as to where you're going and that quite often can offset the desire from somebody to leave because of seemingly greener pastures.

The project has attempted to explore many of the key issues experienced along a cloud adoption journey. It recognizes that there is no “one size fits all” approach to ensure an effective and efficient cloud adoption, for example, due to nuanced national legal requirements. It is also apparent that many NSOs do face many of the same challenges and opportunities. Therefore continued collaboration where knowledge and experiences are shared, can result in a net benefit for all. Cloud adoption is still relatively new among NSOs. There is much change in the cloud space, more change to come and, thus, there's so much to learn. Continued collaboration within your organisation, with partner organisations and peer organisations is important. The project benefited from the knowledge and experiences of organisations at very different stages along their cloud adoption journey and, as with all international collaborations, we believe that every organisation learned something.

Annex 1 - Concepts and definitions

The following are important concepts used in this publication. They are usually defined once to avoid reputation or incoherence. They are provided in this annex for quick reference in the order of the chapter where they first appear or mostly relate. The definitions are either taken from this publication or from a source on the Internet.

Background

Cloud computing
Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping you lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change.
https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/

Cloud-First Strategy
A cloud-first strategy is a business approach that emphasises the adoption of cloud computing technologies as the primary means of delivering IT services, in contrast to a strategy that relies on a more traditional IT architecture. The goal of this strategy is to reduce costs and improve the quality and speed of service delivery.
https://www.simplilearn.com/cloud-first-strategy-article

Cloud-Only Strategy
A cloud-only strategy is one where all IT resources are delivered from either public or private clouds, whereas no resources are delivered from traditional data centers operated by the company itself. The goal of this approach is to provide increased agility for business operations and improved cost efficiency for IT departments.
https://www.simplilearn.com/cloud-first-strategy-article

Cloud-smart strategy
Rather than migrating all applications to the cloud, a cloud-smart approach allows organisations to take a strategic look at what infrastructure will best serve each workload. Companies can better align their cloud strategy to meet their specific business goals and values.
https://silk.us/blog/why-you-should-go-cloud-smart-not-cloud-first/

Cloud Service and Deployment Models

Public cloud Infrastructure
Public cloud infrastructure is provided by third-party service providers and accessible to the general public over the Internet. Organisations share the same pool of resources, making it a cost-effective option for businesses of all sizes.

Private cloud Infrastructure

Private cloud infrastructure is solely dedicated to a single organisation. It can be hosted on-premises or by a third-party provider. Private clouds offer enhanced security and control, making them suitable for businesses with stringent compliance requirements.

Hybrid cloud Infrastructure

Hybrid cloud infrastructure combines the features of public and private clouds, offering a flexible and versatile solution. It allows organisations to leverage the benefits of both models while addressing specific workload requirements.

Community cloud Infrastructure

Community cloud infrastructure is a shared computing environment tailored to meet the needs of a specific community or industry. It enables organisations within the community to collaborate, share resources, and achieve cost savings and operational efficiencies. Community clouds offer industry-specific compliance, specialised services, enhanced data governance, and shared costs. It needs to be investigated if this model is of use for statistical organisations.

On-premise IT infrastructure

On-premises refers to on-site IT infrastructure, hardware, and software applications. This contrasts with IT assets hosted by a public cloud platform or a distant data centre. Businesses have more control over on-premises IT assets by monitoring performance, security, upkeep, and their physical location. Many traditional and legacy data centre resources are on-premises. However, there has been a movement in recent years toward migrating IT assets to the cloud or developing hybrid environments that employ a mix of cloud and on-premises solutions.
https://www.virtualtechgurus.com/on-premise-it-infrastructure/

Software as a Service (SaaS)

SaaS is a cloud computing model that delivers software applications over the internet. With SaaS, businesses can access and use applications hosted by third-party providers without the need for installation or maintenance on the client's side. Users can conveniently access SaaS applications through a web browser, enabling seamless collaboration and accessibility from any device. Popular SaaS examples include customer relationship management (CRM) systems, project management tools, and email services. SaaS eliminates the hassle of technical and operational support of the application and the organisation can focus more on its core task. It can also provide a cost-effective and scalable solution for businesses.

Platform as a Service (PaaS)

PaaS is a cloud computing model that provides a platform and environment for developers to build, deploy, and manage applications. With PaaS, developers can leverage pre-configured frameworks, tools, and resources to streamline the application development process. PaaS eliminates the need for managing underlying infrastructure and allows developers to focus on coding and application logic. It offers flexibility and scalability, enabling rapid application deployment. PaaS is ideal for businesses seeking efficient development environments and supports various programming languages and databases. Examples of PaaS include hosting platforms, database management systems, and application development frameworks.

Infrastructure as a Service (IaaS)
IaaS is a cloud computing model that provides virtualized computing resources over the internet. It offers businesses on-demand access to virtual machines, storage, networking, and other essential infrastructure components. With IaaS, organisations can scale their resources up or down based on demand, paying only for what they use. IaaS provides a cost-effective alternative to maintaining and managing physical hardware. It offers flexibility, allowing businesses to deploy and manage their chosen applications, databases, and operating systems. IaaS is suitable for businesses with complex infrastructure requirements, offering them scalability, security, and control over their IT environment.

Scalability
Scalability is simply the ability of a system to add or remove resources to meet workloads within the system's existing resources. Scalability is planned, persistent, and best meets predictable, longer-term growth and the ability to increase workloads.
https://www.outsystems.com/glossary/cloud-scalability-vs-elasticity/

Elasticity
An elastic cloud system automatically expands or shrinks in order to most closely match resources to your needs. Elasticity denotes adaptability and the ability to scale rapidly. With scale, you add resources and keep them whether you use them or not; with elasticity, you have a base state and then use more of what you need, when you need it, and return to a 'normal' state otherwise.
https://www.outsystems.com/glossary/cloud-scalability-vs-elasticity/

Corporate Support
Corporate support activities support standardisation. They cover the cross-cutting activities required by the organisation to deliver its work programme efficiently and effectively. When a capability improvement is fully integrated in Production, its support is transferred to one or more activities of Corporate Support.
https://statswiki.unece.org/display/GAMSO/Generic+Activity+Model+for+Statistical+Organizations

Production
The Production activity area covers all steps necessary to design, implement and manage statistical production processes or cycles, including surveys, collections based on data from administrative or other sources and account compilations. They deliver the outputs approved under Strategy and Leadership, utilising the capabilities developed under Capability Development and the resources managed under Corporate Support.
https://statswiki.unece.org/display/GAMSO/Generic+Activity+Model+for+Statistical+Organizations

Hosted Services/Solutions
Hosted services are software applications, compute resources and other information technology (IT) services that reside and are managed remotely, usually in the cloud. A third-party provider typically hosts these services and maintains and manages the necessary infrastructure. Hosted services can be used for a variety of purposes — from running an online store to running a contact centre.

https://www.genesys.com/definitions/hosted-services

Open source
Open source software is software with source code that anyone can inspect, modify, and enhance. "Source code" is the part of software that most computer users don't ever see; it's the code computer programmers can manipulate to change how a piece of software—a "program" or "application"—works. Programmers who have access to a computer program's source code can improve that program by adding features to it or fixing parts that don't always work correctly.
https://opensource.com/resources/what-open-source

Cloud Procurement

Hyperscaler
Hyperscalers get their name from hyperscale computing, a method of processing data that allows for software architecture to scale and grow as increased demand is added to the system.
https://www.redhat.com/en/topics/cloud/what-is-a-hyperscaler

Cloud marketplace
A cloud marketplace is an online storefront where customers can purchase software and services that easily integrate with or are built on the cloud provider's offerings. It also offers cloud-native applications that customers can purchase and manage on the platform.
https://www.redhat.com/en/topics/cloud/what-is-a-cloud-marketplace

Vendor agnostic
Being vendor agnostic refers to the practice of designing systems, especially in payments and IT, that are not dependent on a single product, vendor, or platform. Instead of being tied to one specific software or solution, businesses that adopt a vendor-agnostic approach get the redundancy and flexibility of selecting from a wider range of products and services. This approach is rooted in the idea of not being bound by limitations or limiting risk of a particular vendor, ensuring that the business's needs and best interests always come first.
https://www.spreedly.com/blog/vendor-agnostic

Vendor lock-in
Vendor lock-in refers to a situation where the cost of switching to a different vendor is so high that the customer is essentially stuck with the original vendor. Because of financial pressures, an insufficient workforce, or the need to avoid interruptions to business operations, the customer is "locked in" to what may be an inferior product or service.
https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/

Open Standard
An open standard is a standard that is freely available for adoption, implementation and updates. A few famous examples of open standards are XML, SQL and HTML. Businesses within an industry share open standards because this allows them to bring huge value to both themselves and to customers. Standards are often jointly managed by a foundation of stakeholders. There are typically rules about what kind of adjustments or updates users can make, to ensure that the standard maintains interoperability and quality.

https://www.ibm.com/blog/open-standards-vs-open-source-explanation/

Cloud Adoption

7Rs of cloud Migration:Refactor, Rehost, Revise, Rebuild, Replace, Retire, Retain
https://dzone.com/articles/what-are-the-7-rs-of-cloud-migration-strategy

- **Repurchase** - The Updated Newbies: In this strategy, we withdraw an existing application and replace it with a cloud-based version**.**
- **Relocate** - Switch Up Locations: Relocate is the option where we move our infrastructure to the cloud without purchasing new hardware, rewriting applications, or modifying existing operations.
- **Rehost** - Modify None, Lift, and Shift More: In this strategy, we move on-premise applications to the cloud environment, without modification. This option is chosen when there is a need to migrate large-scale legacy apps to meet targeted business objectives.
- **Replatform** - Modify Less, Lift, and Shift Extra: In this strategy, we replace a few components of the application and host them in the cloud environments. The components are replaced or rebuilt in such a way that they take advantage of the cloud environment.
- **Refactor/Re-Architect** - Almost Building Them From Scratch: This is the most expensive approach to cloud migration. Here, the application undergoes a complete makeover to adapt itself to the cloud environment.
- **Retain** - Services Which Can Camp-In: Retain is when we opt to keep the items as it is in our existing IT portfolio. We retain applications under circumstances where there are strict regulations to store data on-premises only. We also retain our applications and workloads when cloud migration is not feasible.
- **Retire** - Done and Dusted: Retire is a cloud migration strategy option where we turn off services that are no longer needed. These services are identified in the early areas of mapping the cloud migration. This may include redundant workloads also.

Cloud-native
Cloud native is the software approach of building, deploying, and managing modern applications in cloud computing environments.
https://aws.amazon.com/what-is/cloud-native/

Zero Trust security
The zero trust security model, also known as zero trust architecture (ZTA), and sometimes known as perimeterless security, describes an approach to the strategy, design and implementation of IT systems. The main concept behind the zero trust security model is "never trust, always verify," which means that users and devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified.
https://en.wikipedia.org/wiki/Zero_trust_security_model#:~:text=The%20main%20concept%20behind%20the%20zero%20trust%20security,LAN%20and%20even%20if%20they%20were%20previously%20verified.

DevOps

DevOps is a methodology in the software development and IT industry. Used as a set of practices and tools, DevOps integrates and automates the work of software development (Dev) and IT operations (Ops) as a means for improving and shortening the systems development life cycle.
https://en.wikipedia.org/wiki/DevOps

DevSecOps

In the collaborative framework of DevOps, security is a shared responsibility integrated from end to end. It’s a mindset that is so important, it led some to coin the term "DevSecOps" to emphasise the need to build a security foundation into DevOps initiatives. DevSecOps means thinking about application and infrastructure security from the start. Effective DevOps security requires more than new tools—it builds on the cultural changes of DevOps to integrate the work of security teams sooner rather than later.
https://www.redhat.com/en/topics/devops/what-is-devsecops

Cloud Security and Privacy

Data privacy

Data privacy is about safeguarding personal information shared over the internet and is the digital equivalent of someone respecting your personal boundaries and secrets. It focuses on ensuring that this data isn’t misused or accessed without permission. While security is a part of it, online data privacy goes beyond just technical measures. It dives into the ethics of how data should be treated. There’s a significant human element here. When users hand over their data, they’re placing a lot of trust in you. They believe that you’ll handle their information with care, respect their choices, and be transparent about any data practices.
https://www.websitepolicies.com/blog/data-privacy-vs-data-security

Data security

Data security is the practice of protecting digital information from unauthorised access, corruption, or theft to ensure the confidentiality, integrity, and availability of sensitive data. It’s a critical aspect of maintaining user trust and complying with security and privacy regulations. It’s a term that likely resonates with many online business owners. Think of all the sensitive data you handle: customer information, financial records, proprietary content, and more. Without adequate security measures in place, this data is vulnerable. Not only could a breach harm your customers, but it could also severely damage your brand’s reputation and lead to financial losses.
https://www.websitepolicies.com/blog/data-privacy-vs-data-security

Data Sovereignty

Data sovereignty refers to the concept that the data an organisation collects, stores, and processes is subject to the nation's laws and general best practices where it is physically located. In layman's terms, this means that a business has to store the personal information of its customers in a way that complies with all the data privacy regulations, best practices, and guidelines of the host country.
https://permission.io/blog/data-sovereignty/

Sovereign cloud

Sovereign cloud describes a cloud architecture to provide security and data access while adhering to local laws and regulations around data privacy and security. Depending on where the cloud servers and data are situated, there is a wide range of criteria for a sovereign cloud. Data that is sensitive or private is protected by sovereign cloud laws and regulations. They make sure that it is always in their owners' hands alone. A sovereign cloud guarantees that all data, including metadata, remains on sovereign territory and, in all cases, forbids foreign access to data. It offers a secure environment for processing and storing data bound to one jurisdiction and can never be transmitted across borders.
https://www.cncf.io/blog/2023/01/16/what-is-a-sovereign-cloud-and-what-is-its-importance/

Shared Responsibility Model

The Shared Responsibility Model is a security and compliance framework that outlines the responsibilities of cloud service providers (CSPs) and customers for securing every aspect of the cloud environment, including hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network controls and access rights. In its simplest terms, the Shared Responsibility Model dictates that the cloud provider must monitor and respond to security threats related to the cloud itself and its underlying infrastructure. Meanwhile, end users, including individuals and companies, are responsible for protecting data and other assets they store in any cloud environment. Unfortunately, this notion of shared responsibility can be misunderstood, leading to the assumption that cloud workloads – as well as any applications, data or activity associated with them – are fully protected by the cloud provider. This can result in users unknowingly running workloads in a public cloud that are not fully protected, making them vulnerable to attacks that target the operating system, data or applications. Even securely configured workloads can become a target at runtime, as they are vulnerable to zero-day exploits.
https://www.crowdstrike.com/cybersecurity-101/cloud-security/shared-responsibility-model/

Security Information and Event Management (SIEM) solutions

Cloud-based security information and event management (SIEM) solutions — also known as cloud SIEM or SIEM as a Service — unify security management into one, cloud-based location. Cloud-native SIEM also takes advantage of the speed and economies of scale to grow and take advantage of innovations without disruption. Organisations can leverage cloud SIEM technology to gain better visibility into distributed workloads. Cloud SIEM can help monitor all assets, including servers, devices, infrastructure components, and users connected to the network — through a single cloud-based dashboard.

https://www.exabeam.com/explainers/next-gen-siem/cloud-siem-features-capabilities-and-advantages/

Cloud Capacity and Competencies

Cloud Architect

A cloud architect is responsible for designing and implementing cloud solutions that meet business and technical requirements. They have in-depth knowledge of cloud architecture and are skilled in designing scalable and secure cloud solutions. Having a cloud architect early on in cloud adoption will be critical to ensure your platform is built on a solid foundation.

Cloud Engineer

A cloud engineer is primarily responsible for cloud implementation, monitoring and maintenance. They set up and operate the cloud infrastructure designed by the architects. This requires engineers to possess detailed knowledge of a cloud's operation and be able to set up and configure resources, including servers, storage, networks and an array of cloud services. This may involve a significant amount of automation.

Platform Engineer

A cloud platform engineer builds and maintains one or more developer platforms that helps software solutions run seamlessly. In collaboration with software development teams, the platform engineer ensures that the platform is reliable, scalable and capable of handling the needs of the solutions that are underpinned by the platform.

Cloud Developer

A cloud developer is responsible for building cloud-native applications that are optimised for cloud platforms. They have expertise in programming languages, cloud frameworks, and tools for building scalable and secure cloud applications. Often, working in CI/CD environments. Most cloud projects are typically focused on three goals:○ migrate an existing application to the cloud;○ modify an existing application for the cloud; or○ create an entirely new cloud-native application.All of these use cases involve a team of professional cloud software developers responsible for designing, coding, testing, tuning and scaling applications intended for cloud deployment.

Cloud Security Engineer

A cloud security engineer is responsible for ensuring that cloud-based applications and infrastructure are secure and compliant with regulatory requirements. They have expertise in cloud security best practices, identity and access management, and data protection. A cloud security specialist sometimes oversees the architected infrastructure and software under development and ensures cloud accounts, resources, services and applications meet security standards. Security specialists also review activity logs, look for vulnerabilities, drive incident post-mortems and deliver recommendations for security improvements.

Cloud Operations Engineer

A cloud operations engineer is responsible for ensuring that cloud infrastructure is highly available, scalable, and performs optimally. They have expertise in monitoring, troubleshooting, and automating cloud infrastructure.

Cloud Data Engineer

A cloud data engineer is responsible for designing and implementing cloud-based data solutions that support analytics and machine learning. They have expertise in data storage, processing, and analysis technologies in the cloud. The cloud data engineer will work closely with an organisation's Information Management (IM) group.

Cloud Business Analyst

A cloud business analyst is responsible for identifying and evaluating cloud solutions that meet business needs. They have expertise in cloud technologies and can analyse business requirements to recommend cloud solutions that align with business objectives.

FinOps3

This is a new discipline that takes a strategic approach to managing and optimising cloud costs. It involves collaboration between finance, operations, and engineering teams to make the most of cloud investments. By adopting FinOps, organisations can improve cost transparency, enhance resource utilisation, and make more accurate budget forecasts, ultimately striking a balance between cost, performance, and business value. Implementing FinOps can help companies gain better control over their cloud expenditures and maximise the return on their cloud investments. To ensure cloud implementation is efficient and manageable within an organisation, it is recommended to have FinOps roles created early in the cloud adoption process.

Day 0, Day 1, Day 2(or N)

In IT, the terms Day 0/Day 1/Day 2 refer to different phases of the software life cycle. In military parlance, Day 0 is the very first day of training, when recruits enter their formative stage. In software development, it represents the design phase, during which project requirements are specified, requirements engineering is conducted, and the architecture of the solution is decided.

Day 1 involves developing and deploying software that was designed in the Day 0 phase. In this phase we create not only the application itself, but also its infrastructure, network, external services and implement the initial configuration of it all.

Day 2 is the time when the product is shipped or made available to the customer. Here, most of the effort is focused on maintaining, monitoring and optimising the system. Analysing the behaviour of the system and reacting correctly are of crucial importance, as the resulting feedback loop is applied until the end of the application's life.
Day 0/Day 1/Day 2 operations & meaning - software lifecycle in the cloud age - CodiLime

Day 2 (or Day N) operations: the daily operations of the component, so it can provide service until it reaches end-of-life (the end of its life-cycle). In some cases, any "pre-prod"

preparation (like compliance and optimization) is called Day 2 operations, and the daily operation is called Day N.
https://kingnaldo.medium.com/day-1-0-1-2-n-operations-7b35534cf216

Annex 2 - Uses of Cloud Technology

Use 1 - Two modern solutions in the Serbia Census of Population[17]

(Note to readers: most of the text below was extracted directly from section 7 of the referenced paper)

The post-enumeration phase of the Serbia Census of Population includes the classification of occupations and economic activities, based on the International Standard Classification of Occupations (ISCO) and the Statistical Classification of Economic Activities in the European Community (NACE). Such an operation usually involves a large workload, especially when conducted manually, even when assisted by computers.

In their 2022 Census, the Statistical Office of the Republic of Serbia (SORS) introduced automation to run their classification operation. At that time, machine learning (ML) had emerged as a natural solution, in particularly with the research, development and experimentations conducted by UNECE HLG-MOS Machine Learning Project (ML Project) and the United Kingdom's Office for National Statistics (ONS) – UNECE Machine Learning Group 2021 (ML Group 2021)[18]. The task involves creating an algorithm that can classify activities and occupations on the basis of a written description the interviewer inputs listening to answers to open-ended questions.

To build an ML model, data sets were created on the basis of information derived from the census and other statistical surveys, including various descriptions of occupations, activities, education levels, and age and gender of respondents. To create the ML model, a combination of two datasets from different sources was used. The first source was the Labour Force Survey, which collected data from approximately 30,000 respondents every three months. This survey provided a constant influx of new data and included traditional and emerging occupations and activities. The second source was the Central Register of Mandatory Social Insurance, which contained about 2.5 million records of officially registered occupations and activities for all the citizens of the Republic of Serbia who had social insurance.

The size of the dataset generated by the algorithms is extensive, requiring more powerful hardware than a standard PC to process the data efficiently and reduce model training time. The SORS used a cloud for ML due to its scalability, security, and user-friendly interface. Anonymisation was done before moving the data to the cloud to protect sensitive information and secure privacy. Only necessary variables were extracted from the database and a unique row identification was created to later connect the original database with the rows extracted for data processing on the cloud. After the classification using ML, data were pulled out from the cloud and transferred to the SORS data centre to be connected with the

[17] Miladin Kovačević, Mira Nikić, Branko Josipović, Snežana Lakčević, Vesna Pantelić, Nevena Mitrović, Adil Kolaković, Petar Korovićh, Digital population and housing census – the experience of Serbia, Wiadomości Statystyczne. The Polish Statistician, 2023, 68(10), 49–70 https://doi.org/10.59139/ws.2023.10.3

[18] Machine Learning for official Statistics, https://unece.org/sites/default/files/2022-09/ECECESSTAT20216.pdf

corresponding records via unique row identification. Appropriate security and access controls were implemented (including encryption, firewalls, and IAM (Identity Access Management) tools) to prevent unauthorised access or disclosure of sensitive data. The system used on the cloud for the ML purposes was equipped with 64 CPUs, 256 GB of RAM, an Intel(R) Xeon(R) Platinum 8370 C CPU @ 2.80 GHz 2.79 GHz processor, and a 64-bit operating system, x64-based processor.

In its previous censuses, the process of manually coding responses to open-ended questions from seven million paper responses was completed nine months after the forms were filled. In the 2022 Census, coding was completed from digital responses in two hours, thanks to machine learning technology and cloud solutions[19]. The classification accuracy achieved 98% after training and validating on the training set. Classification accuracy testing was conducted on a sample checked by coders, and the reports were satisfactory.

This innovative approach was informed by the lessons learned in the HLG-MOS Machine Learning Project and provided a valuable example on the use of cloud to achieve speed and effectiveness in a typically manual intensive operation. These, and other innovations, enabled the SORS to release its census data in six months compared to 18 months in its previous census.

Use 2 - UK Digital Services strategy applied to the 2021 Census

The following text combines highlights from two use case reports published by the Office for Official Statistics (ONS) on changing workplace culture in adopting cloud[20] and using cloud to deliver its Census 2021 digital service[21]. The highlights selected are good examples of practices shared in this publication. We invite readers to consult these reports for more relevant information.

At the start of 2019, the ONS launched a Digital Services Technology strategy[22] to move their technology base to the cloud (80% by 2023). The objective of the strategy is to help its core functions operate more efficiently and effectively by gaining access to technology services and greater flexibility. They also set a concrete objective of achieving a 75% online completion rate in its 2021 Census. This would need scalable cloud services.

During the census data collection period, the Census 2021 website served as the gateway for the cloud hosted secure electronic questionnaire (eQ), through which households and individuals across England, Wales, and Northern Ireland were able to complete their census. It was designed, built and delivered in-house by ONS teams using Google Cloud.

[19] https://customers.microsoft.com/en-us/story/1650106395318946801-stat-national-government-azure-en-serbia

[20] https://www.gov.uk/government/case-studies/how-ons-changed-workplace-culture-to-get-the-best-out-of-cloud

[21] Delivering the Census 2021 digital service - Office for National Statistics (ons.gov.uk)

[22] ONS DIGITAL AND TECHNOLOGY STRATEGY (2019 -2023)

ONS started by doing a lot of small proof-of-concepts to explore different providers, improve capability, show the value of cloud and fail fast. The Chief Technology Officer maintained an honest and open conversation with staff to make it clear that experimenting and sometimes failing was ok. ONS made use of flexible architecture, serverless cloud-based infrastructure and excellent relationships with their cloud providers to build in massive scalability. The Cloud model used was IAAS on public cloud, where Google provided the infrastructure but the application development, runtime and operating system configuration was undertaken by ONS digital staff.

The Digital Services and Technology (DST) directorate at ONS developed a comprehensive strategy to ensure the adoption of cloud throughout the organisation and championed a cloud-first approach. This included round table discussions with subject matter experts from different professions across the organisation. To ensure employee buy-in, it was clearly communicated that migration was not just a cost-saving exercise; honest responses were provided to staff's concerns at talks delivered by the organisation and cloud providers. They also adapted the message to specific teams to make it clear what it meant to them. For the IT staff, this included the introduction of DevOps and DevSecOps to remove the traditional split between developers and operations and resulted in more collaborative working across the organisation. ONS encouraged employees to 'Think Big, Do Small, Act Fast' while maintaining an honest and open conversation with staff to make it clear that experimenting and sometimes failing was ok. Finally, misconceptions about the cloud were removed by ensuring transparent and focused communication on contentious topics like security.

DST recognised that upskilling of technical staff was going to be an important part of safe and effective cloud adoption. DST convinced the leadership that increasing the training budget was critical to achieving business goals. This additional investment was spent towards addressing the gaps in capability created by the move to cloud technologies across the organisation.

ONS took responsibility for the security of its cloud usage within the provider's service. This meant taking on the security management of people, data, applications, operating system and networks. Concretely, in the 2021 Census strict measures were taken to protect the online collection and support sites against data infiltration attacks and service disruption attacks and events. Measures taken included: working closely with the National Cyber Security Centre; building a robust architecture with encrypted data both at rest and in transit; round the clock surveillance; use of the cloud provider's tools to quickly block suspicious traffic; and, many others.

The objective of achieving 75% of census responses on-line was greatly surpassed. Indeed, 88.9% of household responses were completed online. The scalability and flexibility of cloud architecture was essential to scale up to meet the very high demand expected and experienced on Census Day, where under half a million census submissions per hour were received at the peak. The success of the Census 2021 digital service showed that large government digital services can be securely delivered in-house using cloud architecture and Agile development.

Annex 3 - Myths, fears, perceptions

Like many other new technologies, cloud migration harbours numerous myths, fears, and perceptions. This publication aims to demystify the main ones.

Security - It's less secure than traditional IT infrastructure. This myth is especially prevalent in the public sector, where data security is of utmost importance..

Price - It's too expensive. You have to pay for cloud servers every month. It may seem like your own server is cheaper because, over the years, the rental costs will exceed the cost of purchasing your own server.

Skills - Specialised specialists are required to maintain cloud infrastructure, leading to an expansion of your staff.

It is forever - It's believed that if you fully transition a complex infrastructure to the cloud, it will be challenging to revert. This would entail repurchasing equipment, redesigning the IT infrastructure, and reinstalling and configuring everything, incurring significant costs.

Reliability - It is not secure. There is concern that the provider's cloud could experience downtime due to server failures or power outages in the data centre. There is also the fear of DDoS attacks compromising access to the infrastructure.

Complexity - The cloud environment is too complex for regular staff and they will either not be able to work in a cloud environment or the cost of training will be very high.

Data storage - As most of the companies providing cloud storage and functionality are international entities, the fear is that data will be stored in a geographical location where the rules are different (or more relaxed) than in the country of the origin of the data.