Strategic cloud policies for the Icelandic government

V1.0

5.12.2023

Content

General / Inngangur

Eftirfarandi skjal er unnið af fjármála- og efnahagsráðuneytinu og gefið út og samþykkt í desember 2023 í útgáfu 1.0. Undirbúningur þess er samvinna margra ríkisaðila í formi vinnuhópa og rýni ásamt aðkomu erlendra ráðgjafa á sviði skýjalausna. Eigandi skjalsins er skrifstofa stjórnunar- og umbóta og eru breytingar og viðbætur skjalsins rýndar og samþykktar af arkitektúrráði Microsoft verkefnisins / ríkissamningsins.

Tilgangur skjalsins er að útfæra nánar markmið sem sett eru fram í öryggis- og þjónustustefnu um hýsingarumhverfi – stefna um notkun skýjalausna sem gefin var út í júní 2022.

Í þessu skjali má finna nánari útskýringar og leiðbeinandi grundvallarreglur (Strategic cloud policy) sem styðjast skal við þegar tæknilegar leiðbeiningar og kröfur eru gerðar fyrir notkun á skýjaþjónustum sem keyptar eru af þjónustuaðila. Grundvallarreglur þessa skjals geta einnig verið notaðar til útfærslu á þarfa- og kröfulýsingum fyrir innkaup s.s. í gegnum útboð eða gagnvirkt innkaupakerfi (DPS).

Kafli 6 er yfirlit yfir þær grundvallarreglur sem eru í skjalinu og hentar vel til þess að fá yfirsýn en frekari útskýringar og dæmi eru í kafla 4.

Mun þetta skjal verða hluti af heildstæðri umgjörð um högun upplýsingatækni ríkisins. Er það birt m.a. á:

- Island.is: Stefnur og skilmálar
- Stjórnarráðið: Verkefni – Upplýsingatæknimál ríkisins

Þetta skal er á ensku til að tryggja að hugtakanotkun sé samræmd við þær skilgreiningar og hugtök sem notuð eru í skýjalausnum sem eru að jafnaði alþjóðlegar staðlaðar þjónustur.

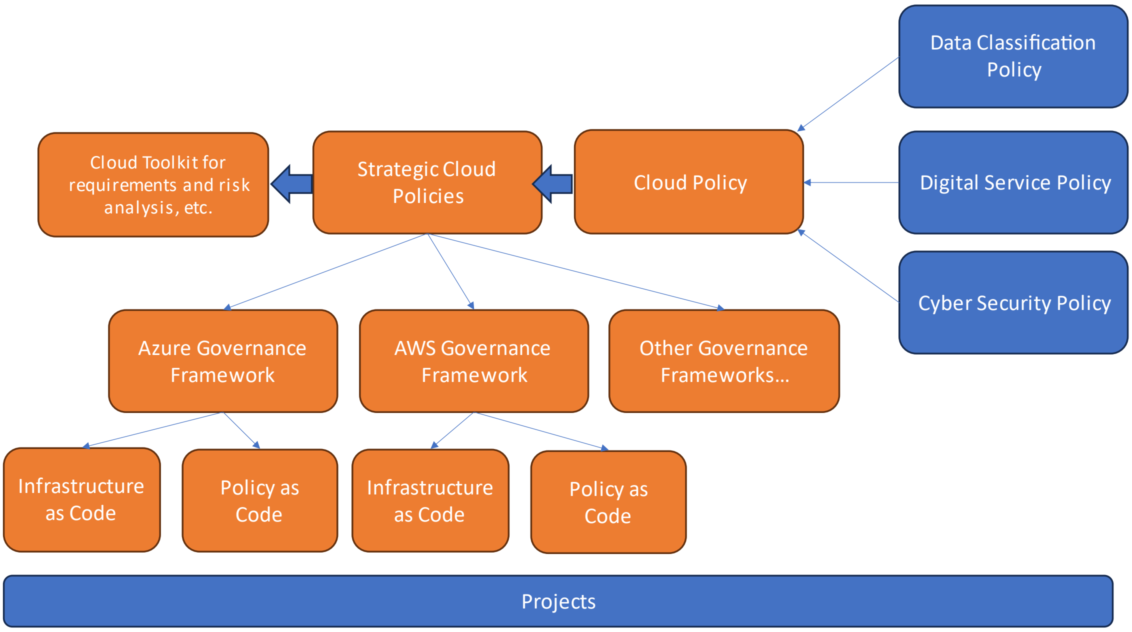
Útgáfa	**Lýsing**	**Dags.**
1.0	Fyrsta útgáfa uppfærð og aðlöguð.	2023-12-5

1. Introduction

1.1. Purpose of this document

This document includes guidelines and key principles for using and promoting public cloud services in Icelandic government. In addition, the document includes key aspects that should be evaluated when designing new solutions based on cloud services.

This document is part of the overall governance structure for cloud services for the Icelandic government:



1.2. Who is this document for

This document is intended for the following parties:

Target audience	Perspective
Ministry of Finance	*Overall ownership of these strategic cloud policies. Responsibility for the implementation support for these policies. Founding the governmental capabilities to support cloud service adoption in the Icelandic government.*
Top management of a governmental institution	*Overall understanding of cloud service trends and different cloud services. An overview of the cloud principles for public administration. An assessment of the utilisation of the principles within their own organisation.*
ICT management of a governmental institution	*Good understanding of the trend of cloud services replacing local services. Vision of applying cloud services in their own organisation. Consideration and application of cloud principles in the digital service*

	development within their own organisations. Orderly promotion of cloud service utilisation within their organisation.
Operational developers and digital specialists in a governmental institution	*Understanding of different cloud services, the trend of them replacing local services. A vision of how the fast, low-investment, and flexible utilisation of cloud services will enable new development model types.*
ICT experts and system architects	*Understanding of different cloud services, the trend of them replacing local services. Vision of applying cloud services in their own organisation.*
Security and data protection specialists	*Understanding the special conditions and terms in public cloud service. Knowledge of the main strategic cloud policies and how they integrate to security and data protection.*
Procurement specialists	*Understanding the meaning of cloud services for procurement. Reforming processes and documents to support the procurement of cloud services.*

1.3. Exclusions and limitations

The following exclusions and limitations apply:

- The work has identified different implementation and service models for cloud services, but the content mainly focuses on public cloud services and their utilisation.
- This document reviews the general trends of cloud services. More detailed application instructions and instructions will be implemented later in guidelines and operating models. Toolbox for helping individual agencies to use cloud services are compiled in Government Cloud Adoption Playbook
- This document does not take any stance on detailed content and services of different public cloud vendors.

2. What are cloud services

2.1. Cloud services in general

The concept of cloud services is still relatively new. A wide variety of services are generally labelled as cloud services – and sometimes on quite loose terms.

Typical features of cloud services

A cloud service is generally scalable, flexible, and dynamic. This guide defines cloud services in public administration as services that are characterised by the following basic features:

- The service can be managed as a self-service.
- The service has comprehensive online access.
- The service enables rapid changes according to changing usage needs.
- The individual physical resources are grouped into a larger entity that covers the physical implementation layer (pool).
- The quality of service can be defined and measured.

Typical additional features of cloud services include:

- Computing capacity is available for all needs of the user organisation without prior reservation or ordering.
- Quality of service is based on service level agreements, not on physical resources.
- The customer only pays for the service they use, not for reservations.

For the purposes of this guidance, the following are NOT considered as cloud services: physical virtual platforms or systems that:

- do not scale based on usage, and
- in which the customer must pay full or partial investments of the physical infrastructure or redeem parts of the platform at the end of the service.

Cloud service models

There are a variety of cloud services - from infrastructure services to higher value-added services. Different cloud service models have different user groups.

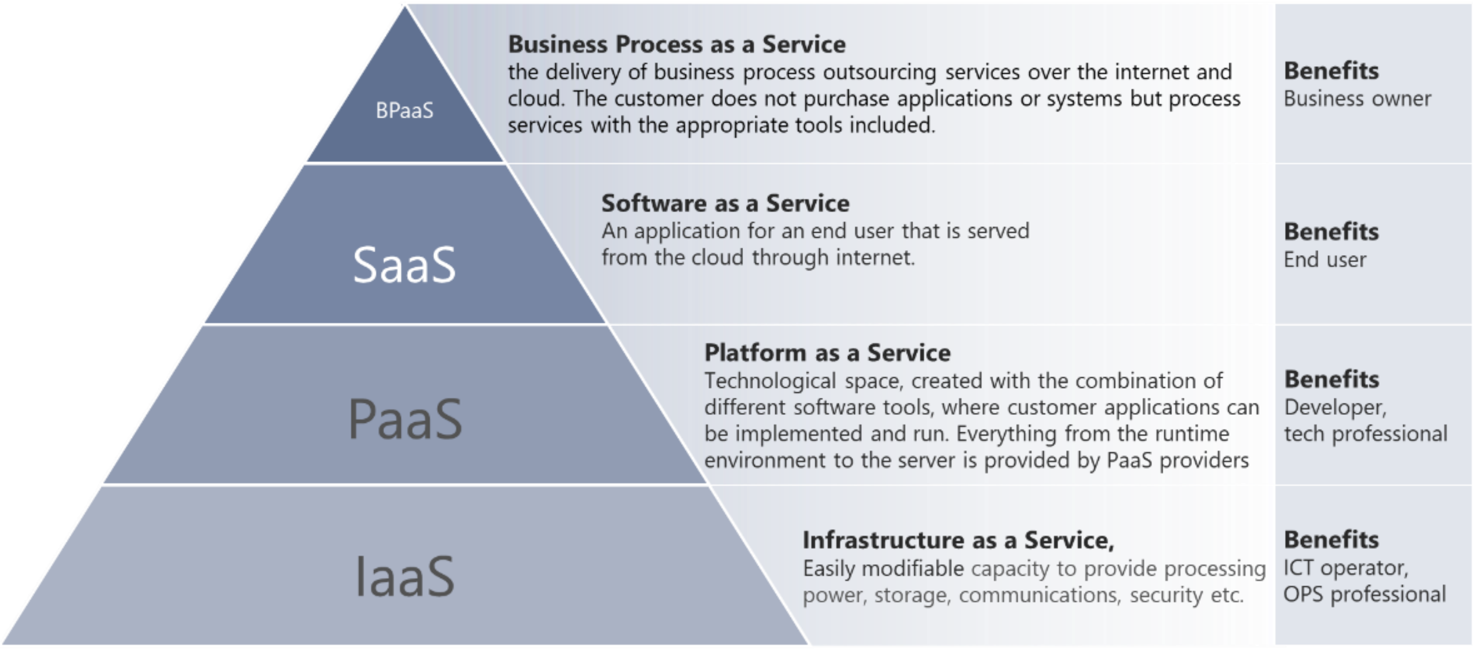

BPaaS
Business Process as a Service
the delivery of business process outsourcing services over the internet and cloud. The customer does not purchase applications or systems but process services with the appropriate tools included.
Benefits
Business owner
SaaS
Software as a Service
An application for an end user that is served from the cloud through internet.
Benefits
End user
PaaS
Platform as a Service
Technological space, created with the combination of different software tools, where customer applications can be implemented and run. Everything from the runtime environment to the server is provided by PaaS providers
Benefits
Developer, tech professional
IaaS
Infrastructure as a Service,
Easily modifiable capacity to provide processing power, storage, communications, security etc.
Benefits
ICT operator, OPS professional

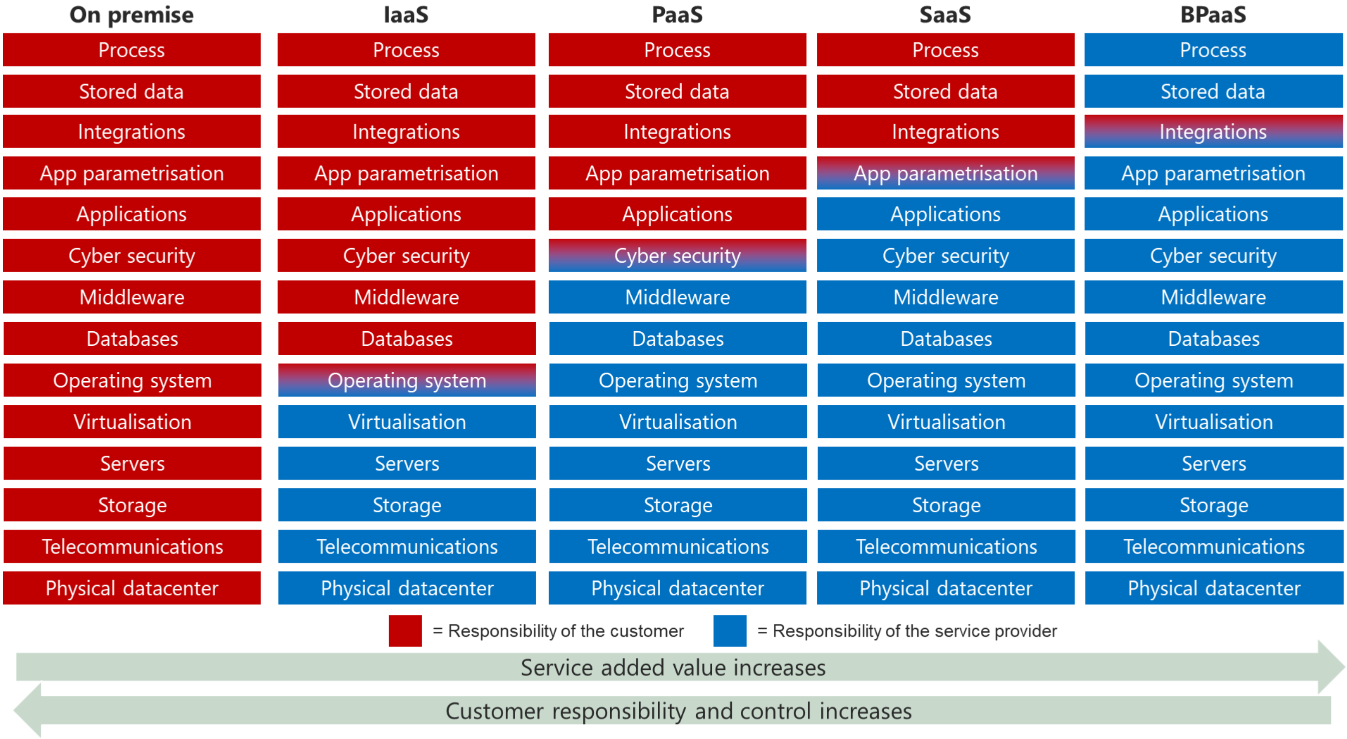
Figure 2 Could Service Models

Acquisition of the entire business process as a service (BPaaS) has been indicated in the picture as a “highest degree” service refinement. As this is not a technology, it is often not identified as a cloud service at all. However, it fulfils the key features of the cloud service, and as part of it, users often have access to an information system that enables the business process. But in such case, the customer does not subscribe to an information system but rather to a business service. The service provider selects the information system which it provides to the customer as part of the service.

In addition to the previous main service models, there are also other cloud service trade names on the market that are used in a variety of ways; for example CaaS (Capacity as a Service), FaaS (Function as a Service), STaaS (Storage as a Service or Software Testing as a Service), QAaaS (Quality assurance as a Service), SECaaS (Security as a Service), DaaS, (Data as a Service).

Responsibility split in most common cloud service models

In the most important cloud services (and in completely self-developed solutions), the responsibilities of the service are divided as follows:



On premise	IaaS	PaaS	SaaS	BPaaS
🟥 Process	🟥 Process	🟥 Process	🟥 Process	🟦 Process
🟥 Stored data	🟥 Stored data	🟥 Stored data	🟥 Stored data	🟦 Stored data
🟥 Integrations	🟥 Integrations	🟥 Integrations	🟥 Integrations	🟥🟦 Integrations
🟥 App parametrisation	🟥 App parametrisation	🟥 App parametrisation	🟥🟦 App parametrisation	🟦 App parametrisation
🟥 Applications	🟥 Applications	🟥 Applications	🟦 Applications	🟦 Applications
🟥 Cyber security	🟥 Cyber security	🟥🟦 Cyber security	🟦 Cyber security	🟦 Cyber security
🟥 Middleware	🟥 Middleware	🟦 Middleware	🟦 Middleware	🟦 Middleware
🟥 Databases	🟥 Databases	🟦 Databases	🟦 Databases	🟦 Databases
🟥 Operating system	🟥🟦 Operating system	🟦 Operating system	🟦 Operating system	🟦 Operating system
🟥 Virtualisation	🟦 Virtualisation	🟦 Virtualisation	🟦 Virtualisation	🟦 Virtualisation
🟥 Servers	🟦 Servers	🟦 Servers	🟦 Servers	🟦 Servers
🟥 Storage	🟦 Storage	🟦 Storage	🟦 Storage	🟦 Storage
🟥 Telecommunications	🟦 Telecommunications	🟦 Telecommunications	🟦 Telecommunications	🟦 Telecommunications
🟥 Physical datacenter	🟦 Physical datacenter	🟦 Physical datacenter	🟦 Physical datacenter	🟦 Physical datacenter

🟥 = Responsibility of the customer 🟦 = Responsibility of the service provider

Service added value increases
Customer responsibility and control increases

Figure 3 Responsibility split in different cloud service models

The communication layer in the figure above mainly refers to the communication between the data centre and the technical components of the system. In all cases, the customer organisation must arrange a secure high-quality connection to cloud services from its own network.

In higher value-added cloud services, the service provider assumes an increasing share of the implementation responsibility required by a particular service process. For example, when utilising SaaS services, the customer organisation is primarily responsible for using the cloud software and managing the data stored in the service. The service provider is responsible for the entire process implementation and data stored in the tools when an organisation outsources an entire function (e.g. payroll). On the other hand, in local data centre implementations all technical components are in the responsibility of the customer organization - either self-developed or procured.

It is good to note that in all models, the customer organisation is at least responsible for needed integrations from their own systems into the cloud services.

BPaaS implementations currently focus largely on industry-independent generic services such as payroll or financial management. The trend is to focus into organisations' core businesses and all other services are considered to be procured from outside as a service. This fuelled the development of BPaaS services.

It is good to recognise that in case of cloud services, responsibilities are often transferred from the vendor to the customer. In the cloud service model, an organisation may need additional personnel, new expertise, or a trusted partner to manage the cloud services.

Implementation models of cloud services

Typical implementation models of cloud services are:

- **Public cloud**
    - The entire cloud infrastructure and its services are unrestrictedly available to contract customers.
    - The service provider implements the physical platform and the services in a completely transparent way. The customer only pays for the service they use.
- **Hybrid cloud**
    - A combination of public and private cloud.
    - The public cloud has been extended into a private cloud.
- **Community cloud**
    - A cloud service shared by several players in the same reference group or community (e.g., a state provided cloud service, a security organization provided cloud service).

In this policy document, a **private cloud is NOT considered as a cloud service** because it does not meet all the cloud service features described above. In practice, a private cloud is an organisation provided virtual platform or virtual services.

The focus is on utilisation of public cloud service model. Other cloud service models may be used when public cloud service model cannot not fulfil organisations' service needs, or required services are not appropriately available via public cloud. In certain specific use cases it may also be appropriate to implement a shared or hybrid clouds between the state administrations and/or municipalities. However, these should only be developed for specific purpose and limited use cases.

2.2. Services from cloud are inevitable

The Ministry of Finance estimates Icelandic public administration is in early phase in the process of utilising cloud services. Data protection guidelines and practices have limited the use of cloud services, and Public Administration have to consider the specific needs and requirements of national security. It is not reasonable to think that cloud related ease-of-use and cost-effectiveness would be the main drivers in utilizing cloud services to store and process classified information. However, the use of cloud services should not be “all-or-nothing” and cloud services indeed enable development of new and improved security controls. As with any other procurement, the overall management of the procurement and the careful drafting of contracts are in key role.

Cloud services is the basis for modern ICT and digitalisation. Usage of cloud services cannot be avoided. Many off-the-shelf solutions and service models have already largely been transformed into cloud only.

A strong trend is that general-purpose, industry-independent off-the-shelf solutions are moving almost exclusively to a SaaS model. Such solution are likely to discontinue as on-premise installations in next 3-5 years.

The ever-increasing use of cloud services is a trend itself, and it is part of a wider digitalisation and digital transformation development. Cloud services have come to stay and enable new types of operational and business models. The services that required local servers and infrastructure in past have already been moved or are in the process of moving to the cloud. For example, the streaming services of music and movies has discontinued the business of selling audio discs and physical video recordings.

Cloud services play a key role in digital transformation. They enable faster and smoother transformations without huge one-off investments. Public administration can be promoting new, smoother services for citizens and communities. Cloud services play an important role in promoting integration and accelerating the development.

Nowadays no organisation can afford to customise all the systems and technologies they need. Public administration organizations need to evaluate and decide where to invest in custom development, and where to utilize off-the-shelf solutions to their benefit. Such off-the-self solutions will be mostly provided as SaaS solutions in the cloud.

Conclusion: Cloud is inevitable but not the only solution

Many services are moving to cloud. It is a megatrend and the prominent business model of the vendor. Cloud cannot be neglected; it is the main solution model for many services – now and in the future. Still, not all services can be moved to cloud. Some special needs will still need local solutions. Cloud use should be evaluated case by case, based on factual needs and identified risks.

3. Cloud adoption strategy for the Icelandic public sector

3.1. Safe and productive adoption of cloud services

The strategy to accelerate a safe and productive adoption of cloud-based services for the Icelandic government is defined as **Cloud Smart**.

Cloud Smart strategy is basis for the strategic cloud principles of the Icelandic government. It is about understanding the purpose and requirements of the developed service, controlling the risk, and making facts-based decisions to use cloud services according to key strategic policies. Cloud Smart promotes utilizing cloud services always when they meet the needs and risks of the customer and are a cost-effective solution.

3.2. Strategic cloud principles of the Icelandic government

1. **Cloud solutions utilized in the most effective way**
   Cloud solutions utilized in the most efficient way possible. Solutions should be designed and structured in such a way that they use the available tools and procedures offered to streamline and modernize services. Consideration should be given to the sharing and re-use of data among public bodies and companies from the outset to the benefit of society, individuals and businesses.

2. Fact based decision making
   Decision-making based on facts and proactive risk assessment. Identify needs, opportunities and risks based on relevant data at any given time. Make cloud specific considerations for individual services to set the right controls, mitigations and risk accepted.

3. **Using cloud solutions where applicable**
   Cloud solutions used where applicable. Cloud services should be selected in accordance with a comprehensive risk assessment that meets security level and risk appetite. Public cloud services should be used unless otherwise specified. Consider and compare with the risks of using your existing solutions. Do not re-invent the wheel and build solutions if you can buy an existing one safely.

4. **Trusted service providers and cost control**
   Trusted service providers and cost control. Purchase cloud services from selected and shared public channels, and from cloud vendors that have been selected through a formal process. Be cost conscious and use public funds responsibly – only buy what you need at any given time. Contracts should guarantee the full right to transfer and ownership of data at the end of a contract.

5. **Standardized products and services**
   Standardized products and services. Services should be used in a dynamic, efficient, and sustainable manner with low impact on the environment. All the opportunities of cloud solutions should be utilized for progress with as much automation of processes and flow of data as possible.

6. **Protect data and services**
   Protect information and services. Data, information and security services should be handled responsibly. Be responsible with your data and secure service and business continuity. Understand how data affects design, security and operations. Design data rchitectures early in the process. Understand how data and the purpose of data affects interoperability,

security and privacy. Respect data privacy and deploy security controls that diminishes the risks to an acceptable level.

7. **Continuous measurements and improvements**
   Continuous measurements and improvements. Ensure that the cloud provider you choose can provide metrics that support your forecasting and analytics needs of cloud usage. Proactively monitor your cloud usage, verify cloud integrity and health and confirm security in real time. Ensure cost effectiveness and optimize services & licenses – use only what you need at any point of time, be environmentally sustainable. Analyze and update your architecture and solutions in order to utilize new and emerging cloud capabilities.

8. **Collaboration and training**
   Collaboration and training. Continuously accumulate know-how. Grow multidisciplinary teams' expertise, invest in education, training and hands-on experience. Experiment and learn by doing. Be active in cloud professional networks, help and educate others, and collaborate across public and private sectors.

3.3. Cloud Center of Excellence (CCOE)

While **Cloud Smart** is about identifying true needs and making facts-based decisions, it is also about collaboration, learning and re-using what is available, including capabilities.

The role of central government is to build, provide and maintain needed key policies and capabilities to enable **Cloud Smart** adoption in ministries and institutions. This is typically implemented as a **Cloud Center of Excellence** that is a cross discipline capability to support the strategy implementation. Cloud Center of Excellence includes capabilities from technical, procurement, legal, HR, security and privacy as well as oversight and impact from general management and supervisory bodies.

“A cloud center of excellence is the best-practice approach to drive cloud-enabled transformation.

To ensure cloud adoption success, organizations must have the right skills and structure in place. The optimal way to achieve this is by setting up a centralized cloud center of excellence (CCOE). A CCOE is a centralized governance function for the organization and acts in a consultative role for central IT, business-unit IT and cloud service consumers in the business. A CCOE is key to driving cloud-enabled IT transformation.

The CCOE is an enterprise architecture function. Its responsibilities include setting cloud policy, guiding provider selection, and assisting with solution architecture and workload placement, with the goals of improving outcomes and managing risks. The CCOE doesn't have day-to-day operational responsibilities. The CCOE should oversee the organization's cloud computing practices and actively solicit contributions from across the business.” (*Gartner*)

Where the role of central government is to guide, enable and support the responsibility of institutions, to implement the policies, and re-use to their benefit. It means collaboration where each party can add up on each other's resources and capabilities, focusing on each other's strengths and avoiding unnecessary overlaps.

4. Key policies to support strategy implementation

4.1. Structure and properties of policies

Each policy falls under a specific cloud policy theme, and includes following structure and properties:

- Justification for the policy – **WHY** the policy is needed.
- Description of the policy – **WHO** should act on **WHAT,** and what is what.
- Outcomes of the policy – what are the **desired outcomes** when policy is being followed.

4.2. Capabilities and competences in central government

This chapter is for

Target audience	Perspective
Ministry of Finance	*Need for governmental Cloud Centre of Excellence. Understanding the essential cloud service capabilities and competences needed nationally and centrally in Iceland.*
Top management of a governmental institution	*View of the main guiding policies for governance, organisation and competence in central government.*
ICT management of a governmental institution	*Overview of the central government capabilities and responsibilities for cloud adoption in Iceland. Understanding how this reflects to institutional cloud adoption responsibilities and cloud initiatives.*
Operational developers and digital specialists in a governmental institution	*Overview of the central government capabilities and responsibilities for cloud adoption in Iceland. Understanding the support role of the central government and the need to share knowledge and good examples in the common knowledge share platform.*
ICT experts and system architects	*Overview of the central government capabilities and responsibilities for cloud adoption in Iceland. Understanding the support role of the central government and the need to share knowledge and good examples in the common knowledge share platform.*
Security and data protection specialists	*Overview of the central government capabilities and responsibilities for cloud adoption in Iceland.*

Procurement specialists	*Overview of the central government capabilities and responsibilities for cloud adoption in Iceland.*

Strategic cloud theme 1:

The co-ordination and guidance of governmental cloud services and platforms are collected to a Governmental Cloud Center of Excellence. Shared guides and governance models for cloud services are created.

Ownership and responsibility for cloud adoption in Iceland

Justification for the policy

The current state analysis shows that the cloud initiatives in Iceland are now dispersed, and common guides and governance is needed for effective and secure cloud adoption in the government of Iceland. A high level and clear ownership and responsibility is needed for the cloud adoption in Iceland.

Strategic cloud policy 1.1: Central government should name a responsible organisation for leading and supporting secure and value creating cloud service adoption in Iceland.

Outcomes of the policy

Guides and tools for institutions to accelerate their cloud adoption and develop cloud competences. Adoption of cloud services based on guides and tools shall have positive outcomes for institutions, including assistance from central government and increased operational efficiency.

Capabilities to collect cloud components, best practises and implemented cloud services or components from the institutions to the Cloud Knowledge Platform. This information is available for all institutions.

Governmental Cloud Knowledge Platform will integrate individual services and methods of individual institutions to functional holistic services and promote the development of silo free services based on the life events of citizens and business events of the companies.

Governmental Cloud Center of Excellence

Justification for the policy

CCoE helps the government of Iceland to realize the full potential of the cloud and accelerate the safe execution of cloud adoption strategies and policies. Centralized organisation is required to accumulate needed cloud knowledge for a successful cloud adoption.

Strategic cloud policy 1.2: A nominated governmental organization should create a Cloud Center of Excellence (CCoE) function to drive and support safe and value creating cloud adoption in the government of Iceland.

Outcomes of the policy

A Governmental CCoE will be a cross-functional group of cloud aware professionals with governmental executive support that lead other professionals (and the government as a whole) through cloud adoption, migration and operations – and establish repeatable processes and cloud standards for everyone to follow in the selected Cloud Smart approach. Capabilities and roles shall be developed to ensure that the CCoE can support cloud adaptation. Resources can be dedicated, shared or sourced from other organizations or service providers. Governmental CCoE has a coordinating and guiding role. It does not necessarily create cloud services for institutions but helps the institutions to achieve their goals by using cloud services.

Responsibility for top level key cloud policies

Justification for the policy

Key cloud principles and policies are top down, non-negotiable guardrails for cloud adoption in Icelandic government. There needs to be a single entity ownership for collecting the needs and requirements and turning those into guidelines to build on.

Strategic cloud policy 1.3: The Cloud Center of Excellence should be the owner for the cloud principles and key cloud policies.

Outcomes of the policy

CCoE will create and continuously update cloud principles, policies, governance model and toolkits to serve as a broker, partner, and representative to the institutions. All deliverables must serve the needs of the institutions.

Institutions are involved in governmental cloud governance.

Cloud capabilities in Government CCoE

Justification for the policy

Cloud adoption is not only a set of new cloud technologies. New thinking and know-how and new processes are needed for the successful cloud service utilization. A holistic approach in developing cloud capabilities ensure security and benefits of cloud.

Strategic cloud policy 1.4: The Cloud Center of Excellence should develop holistic governmental cloud capabilities covering all aspects of successful and safe cloud adoption.

Outcomes of the policy

Capabilities stand for the overall components needed to achieve a commonly set goal – i.e. the Cloud Vision of the Icelandic government. Capabilities include for example resources (technical components, premises, systems etc), roles, human competences, data, methods, processes, funds and management structures.

At least the following cloud capabilities are developed:

- Structures and governance

  - Management structures of the cloud adoption in Iceland
  - Named GovCloud responsible
  - Named core staff of governmental CCoE
- Processes, services, guides
  - Common practices, reference architectures and more detailed guides and instructions
  - Cloud native development methods
  - Cloud governance and management practices
  - Cloud architecture guidelines
  - Cloud procurement guidelines and instructions
- Security and data protection
  - Risk management and controls fitted for the cloud
  - Data protection guidelines and instructions fitted for the cloud
- Technology
  - Technical monitoring, management, and document management systems
  - Automatic and real time scalability of cloud platforms and services
- Competences, knowledge
  - Understanding the needed cloud roles
  - Understanding and knowledge of security and privacy relating to the cloud services
- Funding
  - Sufficient funding for the CCoE
  - Sufficient funding for the GovCloud initiatives and activities including funding for communication, training, support & dynamic funding for PoCs and experiments
  - Preparing to move budgeting from CapEx to OpEx in cloud services
- Continuous improvement capability
  - Clear and definitive KPI’s shall be developed for skill transformation for each target audience.

Cloud competences in Government CCoE

Justification for the policy

Building the digital skills to support cloud use is a key need for government to successfully adopt and utilize cloud services safely. The public sector professionals in institutions need support in cloud skills to build, modernize, implement, manage, monitor, procure and govern cloud services, across providers and across environments.

Strategic cloud policy 1.5: Governmental Cloud Center of Excellence should have needed cloud competencies to lead and governs holistic cloud adoption.

Outcomes of the policy

CCoE is the primary vehicle for leading and governing cloud adoption across all services models — infrastructure, platform, and software as a service (IaaS, PaaS and SaaS).

Critical roles can include: cloud Architects, cloud Engineers, developers, and project managers.

Competence development of the CCoE professionals is continuous and based on personal learning development plans.

Sharing the knowledge

Justification for the policy

Sharing knowledge is a key accelerator for cloud capabilities and competencies. Building on others results instead of re-inventing the wheel helps people focus on their core value innovation. Sharing is a two-way street, sometimes you give and sometimes you receive.

Strategic cloud policy 1.6: Governmental Cloud Centre of Excellence should provide a cloud knowledge platform through which cloud capabilities and competences are shared in networks & communities.

Outcomes of the policy

A common knowledge sharing platform collects and combines all cloud know how in Iceland. Examples, commonly reusable cloud components (APIs) and knowledge sharing, and peer-to-peer support accelerates the national cloud adoption and improves its quality.

Governmental Cloud Centre of excellence should develop a Cloud Knowledge Platform (CKP) function to support sharing of common practices, know-how and commonly reusable cloud components. It will connect institutions and private providers and provide access to resources and information to support cloud adoption. With CKP all cloud knowledge can be aggregated and utilized. Institutions with limited resources or capabilities will be able to leverage and utilize the results, knowledge, services, and experiences of other institutions and CCoE.

Sharing cloud knowledge and know-how of cloud services across government will enable institutions and the entire government of Iceland to move into cloud with improved insight. Also shared products and components that can be reused, lessons learned, and common technology creates a competence uplift for institutions that iterates and shares good practices and reduces duplication or the same product across several institutions.

4.3. Capabilities and competences in institutions

This chapter is for:

Target audience	Perspective

Ministry of Finance	*Guiding and supporting the cloud capabilities development in institutions.*
Top management of a governmental institution	*Understanding the requirements for development of institutional cloud adoption capabilities and competence in general.*
ICT management of a governmental institution	*Building capabilities and competencies according to key policies. Defining institution specific policies for cloud adoption.*
Operational developers and digital specialists in a governmental institution	*Building competence to utilize cloud computing opportunities. Contributing to institution specific cloud adoption policies.*
ICT experts and system architects	*Building competence to utilize cloud computing opportunities. Contributing to institution specific cloud adoption policies.*
Security and data protection specialists	*Building cloud adoption related security and data protection competence and enablers. Defining institution specific security and data protection cloud policies.*
Procurement specialists	*Building cloud adoption related procurement competence and enablers. Defining institution specific cloud procurement policies.*

Strategic cloud theme 2:

All institutions should prepare to cloud adoption and be responsible for their own capabilities, competences, and initiatives. Clear responsibility and structures for cloud adoption are needed.

Organizing readiness for cloud adoption in institutions

Justification for the policy

Actual Cloud adoption will happen at the institution level. The role of central governance is to support and enable the adoption. Institutions need to take initiative and organise for driving the adoption.

Strategic cloud policy 2.1: Every governmental institute should organise their own cloud adoption function. At least a cloud service responsible person should be nominated.

Outcomes of the policy

Institutions have nominated a person(s) responsible for cloud, and persons nominated have commitment and support from the leaders in institutions. Leaders are responsible regardless if the services are outsourced or done by the institution itself. The person responsible for cloud develops sufficient competences and know-how to drive the cloud adoption in the institution.

Institution level responsibility for cloud strategy and policies

Justification for the policy

Central government cloud strategy and policies are generic, providing guidance across the whole government. Institutions need more specific strategies and policies that fit to their specific needs.

Strategic cloud policy 2.2: Institutions should create their own cloud adoption strategy based on the governmental cloud vision, principles, and cloud adoption strategy.

Outcomes of the policy

All institutions are familiar with the GovCloud Cloud vision, principles and key policies described in this document.

Institution level strategies and policies cover:

- value case and connection of cloud strategy to the institute strategy
- human resources and skills plan
- ‘best fit’ cloud models
- service readiness and transition approach

Cloud capabilities and competencies needed in institutions

Justification for the policy

Each institution needs to evaluate their requirements for cloud capabilities and competencies based on their own cloud adoption strategy and policies.

Strategic cloud policy 2.3: Institutions should build and develop systematically required cloud capabilities and competencies for their needs.

Outcomes of the policy

Cloud Smart -strategy requires that institutions have sufficient capabilities to evaluate their options based on their service and mission needs, technical requirements, and existing policy limitations.

The cloud responsible in the institution will develop sufficient competences and know-how to drive the cloud adoption in the institution.

All institutions actively participate the governmental Cloud Knowledge Platform to share cloud knowledge and leverage the know-how and solutions created by others.

Utilizing existing capabilities and competencies as a priority

Justification for the policy

Cloud capabilities and competencies available via government CCoE or 3rd parties should not be replicated to institutions. Re-use of capabilities and competencies drives scale of economies.

Strategic cloud policy 2.4: Institutions should utilize existing capabilities and competencies where feasible. External support or outsourcing should augment internal capabilities when needed.

Outcomes of the policy

Through government CCoE institutions access capabilities and competencies to their benefit. Instead of building overlapping capability they should prioritize utilizing the existing ones when feasible. In addition to government CCoE institutions also utilize additional 3rd party capabilities to complement their needs.

4.4. Security, privacy, and risk management

This chapter is for:

Target audience	**Perspective**
Ministry of Finance	*Overview of the pursue for risk-controlled cloud use.*
Top management of a governmental institution	*Overview of the pursue for risk-controlled cloud use. Understanding the main policies regarding security and risk management in cloud. Making decisions of the acceptable level of risks and approving the risks and mitigation means*
ICT management of a governmental institution	*Overview of the pursue for risk-controlled cloud use. Understanding the main policies regarding security and risk management in cloud. Using the*
Operational developers and digital specialists in a governmental institution	*Know-how of creating fact-based requirements for developed services and solutions.*
ICT experts and system architects	*Know-how of creating fact-based requirements for developed services and solutions from a technical and interoperability point of view.*
Security and data protection specialists	*Understanding the need for case-by case security and data protection evaluation and searching for cloud enabling risk controls.*
Procurement specialists	*Understanding the non-negotiability of the security terms and controls in the public cloud services.*

Strategic cloud theme 3:

The security and risk management of cloud services is ensured in all situations based on fact-based requirements and risk mitigation controls. Data is stored and handled in cloud services based on legislation, institutional data strategies and common guidelines.

Requirements and needs first

Justification for the policy

There is no single solution for selecting cloud or not. Only a case by case executed fact-based requirement and risk analysis can ensure the optimal and secure cloud use. Each case shall be scoped so that risks can be identified and actionable mitigation plans developed. Cases can be systems, projects, capacity needs, services or any other information asset or combination of assets.

Strategic cloud policy 3.1: Understand your needs based on justified facts. Do not make your decisions only based on technology.

Outcomes of the policy

Understand the needs and requirements of the “business” you are developing the solution for. It is only based on identified requirements that an assessment can be made whether cloud services can meet the needs and requirements of the purposed use.

The requirements can at first still be made at **high level** and specified in more detail in the procurement or solution design phase. However, the requirements should be so detailed that you are able to evaluate how different solution alternatives fulfil the necessary requirements.

Understand your information

Justification for the policy

Information, data and the use and purpose of that data creates the basis for understanding the security and data protection requirements of the solutions.

Strategic cloud policy 3.2: Create a clear view of the information stored and processed in the cloud. Classify your data, understand its use and purpose. Create a sufficient data governance model.

Outcomes of the policy

Each institution is the owner and responsible of its information on behalf of the people and organisations in Iceland. Institutions are responsible for identifying and classifying their information and determining their own governance model for cloud stored data.

Before entering the data to cloud, institutions should ensure that they have a continuous access to log data; and they must be notified promptly by the CSP if a cybersecurity incident, breach, or other adverse event occurs or is suspected to have occurred.

Common data classifications that are cross-organizational throughout the government can accelerate cloud adoption and greatly improve the sharing of data and services.

Identify your risks

Justification for the policy

While cloud services provide many benefits, at the same time, it introduces risks on several areas that need to be governed and managed by the institutions. Well-managed institutions must recognize and understand and then mitigate these risks to better leverage their cloud initiatives.

Strategic cloud policy 3.3: Identify the risks based on the fact-based requirements and the purpose of the data. Assess the risks of cloud based on defined criteria. Verify that the potential solutions can control the risks.

Outcomes of the policy

Institutions should be able to evaluate their potential cloud solutions based on their service and development needs, technical requirements, and existing policy limitations – based on relevant and current facts. This requires identifying and evaluating the risks related to solution options.

Risks regarding the cloud should be assessed from many viewpoints and at different stages of procurement. Key viewpoints include the data processed in the service and the service environment’s criticality to the operation of your own and stakeholders’ organisation. This serves as a basis for defining the scope for the service and what kind of data can be processed in the service. The criticality of the service influences what backup procedures can be implemented. An assessment of the risks and contingency situation may lead to a different type of development or procurement.

Use a pre-defined and holistic criteria framework to assess the information security of cloud services. In addition to the security, evaluate all common risk areas of cloud:

- Security
- Privacy
- Contractual terms
- Technology
- Operational
- CSP continuity
- Financial
- Politics

Consider also the risks and impacts if you cannot find sufficient risk controls for using a cloud solution. What risks rise for not using the cloud and not finding an alternative solution that is flexible and fulfils the functional needs and requirements.

Control your risks holistically

Justification for the policy

Cloud Smart strategy in Iceland requires comprehensive view for risk controls in cloud – e.g., the assurance of confidentiality, integrity, availability and business continuity and privacy in all situations. Institutions should search for solutions that allows them to use cloud in the safe and correct way rather than finding ways to prevent the use of cloud services.

Risk identification shall include all aspects of risks and the entire service stack from cloud service to end-user.

Strategic cloud policy 3.4: Seek for holistic risk controls that enable cloud use. Amend cloud native risk controls using your own additional risk cloud controls where necessary.

Outcomes of the policy

It is still essential that institutions consider and manage security and privacy risks and continuity risks to information and services when making cloud procurement and deployment decisions and build needed controls that enable cloud services. Risk controls should be proportionate to the risks and only applied to the appropriate scope. Do not implement unnecessary risk controls. Instead, take the time to properly understand your risk profile and control the relevant risks.

Sound risk management practices to prevent and detect cyber security attacks can be as successfully implemented in cloud as they can in traditional data centres. The automation in cloud minimises human error. Cloud services are not inherently more or less secure than any other device with an internet connection. Procurement of more advanced cloud services can include more security related controls that need to be implemented in accordance with business requirements to provider acceptable risk mitigation.

The service and technology ecosystem and architecture must be based on clearly defined security controls that are proportionate to the risks.

Accept the concept of shared responsibility in risk management and compliance. Risk controls in public cloud services may have to be amended by local risk controls. Use native security controls where you can. Implement advanced security features from third-party providers only where your risk assessment indicates it is required. For example, the storage time for security logs in a cloud service may not be long enough for the purpose and use of the data stored in that service. A local or a third-party log service can then be used and the security logs can be stored locally for the needed period.

Exploit proven and best-practice cloud native approaches to creating secure cloud services to avoid re-inventing the wheel. For example, primary access control should be user based.

Monitor your risks and verify your controls

Justification for the policy

Cloud services and cloud service providers evolve fast. It is essential that institutions perform continuous monitoring to the entire service to detect malicious activity in the cloud, verify that the risk controls are mitigating the risks and dedicate effort to improving systems governance.

Strategic cloud policy 3.5: Monitor your risk and their mitigation continuously. If the risks change, verify and amend the risk controls if needed.

Outcomes of the policy

The security of cloud services must be reviewed and proven at key development milestones as well as in the run phase. Automated security testing should be built into the software release cycle using secure DevOps practices.

Security Awareness of end-users, developers, operators and management needs to be addressed in training and processes.

Privacy – minimum use policy

Justification for the policy

Protecting privacy and personal data is paramount in cloud services. Compliance of the solution with the data protection legislation and guides is essential for cloud services.

Strategic cloud policy 3.6: Use of personal data shall be minimize and reducted as much as possible.

Outcomes of the policy

Legitimate purpose for the processing of Personally Identifiable information (PII) is required at all times. By assessing each processing of information in cloud services it is possible to reduce, redact, anonymize or in other ways protect privacy.

Example of this is the use of summary entries in dashboards and analytics, where reduced datasets are pre-processed and anonymized before transferring the data to the analytics/dashboard service.

Privacy – implement risk based privacy controls

Justification for the policy

PII shall at all times be protected by organizational and technical safeguards. To ensure that appropriate controls are in place from contractual requirements to encryption and key management a Data Protection Impact Assessment (DPIA) is required.

Strategic cloud policy 3.7: DPIA shall guide the design and implementation of privacy safeguards based on the impact for the registered person.

Outcomes of the policy

DPIA outcomes shall be the justification for implementing controls to safeguard PII and the individual's rights in all cloud based services and projects. All cloud services and projects shall be in compliance with applicable privacy related requirements, including but not limited to GDPR.

4.5. Procurement and cost allocation

This chapter is for:

Target audience	**Perspective**
Ministry of Finance	*High level view of the paradigm change of the procurement process. Understanding that very detailed centrally created mandatory guides may not be the right approach in cloud services procurement.*
Top management of a governmental institution	*High level view of the paradigm change of the procurement process. Good overview of the new pre-study-based paradigm of cloud service procurements.*
ICT management of a governmental institution	*Good overview of the specialities in cloud procurement and understanding the paradigm change.*
Operational developers and digital specialists in a governmental institution	*Understanding that the procurement and thus requirement specification is different for purchasing cloud services.*
ICT experts and system architects	*Understanding that public cloud contracts are mainly fixed for all customers. Some of your special requirements may be implemented a bit differently in the cloud services.*
Security and data protection specialists	*Understanding that public cloud contracts are mainly fixed for all customers. Some of your special requirements may be implemented a bit differently in the cloud services, sometimes amended risk controls may be needed.*
Procurement specialists	*Understanding the new normal of procurement process in cloud services – traditional process of setting very rigid and detailed mandatory requirements for RFP:s needs to be updated*

Strategic cloud theme 4:

A pre-study oriented procurement process is used. The fit of cloud services is examined before the actual RFP since cloud terms are usually not negotiable. Utilization based cost allocation model is used in common cloud platforms and services.

Procurement paradigm and process is somewhat different in cloud services compared to the procurement of traditional services. There is a limited ability to affect the terms of contracts in global cloud services and the cost model is operational cost based.

Funding and budgeting moves to OpEx

Justification for the policy

Cloud services do not require large up-front investments, but they are purchased as pay-as-you-go basis. You rent the cloud services you do not buy technology in advance to your own ownership.

Strategic cloud policy 4.1: Cloud moves your technology budget from CapEx to OpEx.

Outcomes of the policy

Traditionally, organisations have relied on models where building technology have required large CapEx investment as investments in data centers, servers, other equipment, software, and reqruiting workforce have been needed to build and run new technology and services. One of the changes and benefits of cloud is to switch IT spending to a pay-as-you-go model and reduce CapEx needs and costs. The new model also keeps your financial forecasts stable and predictable. This brings new flexibility to costs but requires changes in budgeting models and budgeting rules in institutions.

Utilize the flexibility of cloud purchasing model, update your budgeting model and only buy what you need at any given moment.

Cloud purchasing is different: Streamlined and pre-study-based procurement process

Justification for the policy

The standardized commercial delivery model of cloud computing is fundamentally different from the traditional model for on-premises IT purchases (which has a high degree of customization and is usually tailored for the individual use). CSP:s rely on the business model where ALL customers get the same modular service. This means that the contract and service terms for the global public cloud service providers are very much fixed and mainly non-negotiable.

Strategic cloud policy 4.2: Follow the official procurement procedure. Streamline the purchasing process - put your effort on pre-study, cloud is purchased differently. For cloud platforms, create frame agreements for catalogue based quick purchasing.

Outcomes of the policy

Cloud Service Providers (CSPs) offer commercial cloud services at massive scale and in the same way to all customers. Customers use standardized commercial services on demand. Utilize pre-defined service packages for easy purchase and deployment.

This shifts the focus on fixed and detailed technical requirements and customer driven terms to using standardized services and studying the capabilities and terms of CSPs in the pre-study phase. Understand your needs and requirements, model your risks and find out which cloud services can fulfil your needs. Only after this study, create the requirements carefully. Successful cloud procurement strategies focus on application-level performance-based and cloud specific security and data protection requirements that prioritize workloads and outcomes, rather than detailing the underlying methods, infrastructure, or hardware used. Verify the essential contractual terms, security, data protection controls and the interoperability of the cloud architecture beforehand in the pre-study phase. Use RFI:s before entering the formal purchasing process. Verify that there is a cloud solution in the market that fits your needs. This pre-study is typically carried out as market surveys, and may consist of some of the following methods:

- Written study on what is available on the market
- Utilisation of experiences by peer groups or other public organisations, and listing potential providers and their service conditions
- Identifying and contacting CSP:s. surveys or meetings in which CSP:s present their solution models
- The organisation orders demo credentials for cloud solutions, where available, and studies independently the solutions’ properties, contract terms and technical capabilities
- The organisation experiments (PoC or other means) one or more solutions. No production use at this stage.

After the verification that there are cloud solutions in the market that are suitable for the purpose, cloud services should be procured using formal processes in accordance with the legislation and with the principle of fairness, meaning that no specific restrictions on competition should be put in place without good grounds.

High availability by architecture and SLAs

Justification for the policy

Availability of the technical services should always be based on the true requirements of the services and processes that is being developed. Cloud service SLAs are fixed in cloud service provider contracts and they are usually he same for all customers. The sanctions from SLA breaches are usually quite modest. A cloud native architecture is needed to meet the service level requirements.

Strategic cloud policy 4.3: The continuity and availability requirements of the processes are achieved by developing a cloud native high availability architecture together with SLAs in the cloud contracts.

Outcomes of the policy

Do not rely only on cloud contract SLA:s. They are usually at appropriate level but also the largest and strongest CSP:s may have errors or faults. The low sanctions of SLA breaches do not generally cover the harm from service outages. In addition to SLAs in cloud contracts architect your solutions so that they are designed for high availability and disaster recovery based on the availability requirements of services and processes. Use the flexible cloud technology in your architecture in order to multiply the key components and automate load transfer in case of breakdowns.

Continuity of services shall be ensure both in system design and vendor relationships. Critical system shall be design so that the survivability of the service is not tied to one vendor or architecture.

Verify the cloud service contract terms before signing

Justification for the policy

Due to the fixed terms of public cloud contracts, verify in advance the essential contract terms and cost effectiveness in advance. Terms are usually not negotiable.

Strategic cloud policy 4.4: “Buy cloud services as they are sold”. Accept that you cannot usually change cloud contract terms. Verify the terms and the cost structure in advance.

Outcomes of the policy

Accept that global cloud contracts are pretty much fixed and same for all customers. Verify the contracts beforehand, understand what you are getting and control your risk using additional solutions and contracts if needed.

Use only business grade cloud solutions with business grade. Do not use consumer cloud solutions and contracts in business-critical services.

Check the essential terms in the cloud contracts:

- The cloud service is working on the “pay as you go” model without prepayments or fixed costs
- Plan your cloud use. Verify that the cloud service supports easy and automatized purchasing based on your changing needs
- Verify that the cloud contract can be terminated smoothly
- Ensure your budget – remember that cloud services are mostly budgeted as operating costs – not as investments
- Use predefined check lists for cloud contract term verification
- Ensure that exit-costs and strategies can be implemented.

Easy purchasing and management of costs in cloud services

Justification for the policy

One of the main benefits of cloud comes from the flexibility of cloud service capacity and/or licenses. Use this flexibility for your advantage.

Strategic cloud policy 4.5: Make purchasing and ordering of general cloud platform services (capacity, technical services) easy and quick. Utlilize cloud elasticity to optimize the entire life cycle costs of the service.

Outcomes of the policy

The rapid iteration and release cycle of cloud services makes them well suited for a streamlined procurement of common cloud services. Create architecture, purchasing processes and other capabilities that support purchases through a catalogue-based or fully automated e-procurement approach. This approach would include the ability to click-to-buy and dynamic pricing and create opportunities for small scale experimentation and innovation.

Utilize the elasticity in costs and adaptation of the cloud services to your need. Purchase-as-you-go. The new purchasing model requires understanding and new knowledge on cost optimization in cloud services.

Buy sensibly - use cloud services in a cost-efficient and environmentally sustainable manner.

When comparing life cycle costs of cloud solutions to other platforms all capital and operational costs shall be included for both solutions as well as the manpower required to develop and operate the service.

Cost allocation of common cloud platforms

Justification for the policy

Cost allocation of common, nation wide cloud services and technology should be fair. Organisations that use the cloud should cover the costs based on their usage. No organisation should pay the costs of others.

Strategic cloud policy 4.6: Costs of common governmental cloud services are allocated according to utilization

Outcomes of the policy

Fair, capacity and licence utilization based pricing model should be developed for the possible common cloud services. Upfront costs should be avoided. The expansion of the usage should not affect negatively existing customers. The pricing principles of common cloud services are:

- The pricing and cost structure should be transparent for institutions – no hidden costs
- No up-front costs
- No fixed cost
- Entirely dynamic pay-as-you-go pricing for the cloud services

- Fair cost allocation model

4.6. Designing for the cloud

This chapter is for:

Target audience	**Perspective**
Ministry of Finance	*Overview of the pursue for risk-controlled cloud use.*
Top management of a governmental institution	*Overview of the pursue for risk-controlled cloud use. Understanding the main policies regarding security and risk management in cloud.*
ICT management of a governmental institution	*Overview of the pursue for risk-controlled cloud use. Understanding the main policies regarding security and risk management in cloud.*
Operational developers and digital specialists in a governmental institution	*Know-how of creating fact-based requirements for developed services and solutions.*
ICT experts and system architects	*Know-how of creating fact-based requirements for developed services and solutions from a technical and interoperability point of view.*
Security and data protection specialists	*Understanding the need for case-by case security and data protection evaluation and searching for cloud enabling risk controls.*
Procurement specialists	*Understanding the non-negotiability of the security terms and controls in the public cloud services.*

Strategic cloud theme 5:

User centric services are developed using agile and iterative development processes. The flexibility and technical services of the cloud are used to rapidly develop cloud native services that can be used by end-users and other systems

Needs first approach

Justification for the policy

The needs of the organization need to be understood before embarking on a technical journey to the cloud. Think of the goals that you have set for yourself and your end user's to get a holistic view about what needs to be done.

Strategic cloud policy 5.1: Always think of your and your customer's and end user's needs, goals and requirements, before thinking about technology. After that, what does your future look like? Do a current state analysis on your services before moving forward.

Outcomes of the policy

Narrow the target and find out and describe the needs for which a new solution is sought. Understand activities and user activities and goals. Identify the information and the conditions under which it is processed. Model your solution for your key requirements.

All technological solutions and services are based on the needs and objectives of the operation and the boundary conditions set by its legislation. Utilizing cloud services requires a holistic view of the need and the risks associated with it. The secure acquisition and use of cloud services is based on fact-based risk management.

At the beginning of the development, the most important requirements of the object to be developed must be identified. Only on the basis of identified and fact-based requirements can the next step be to assess whether cloud services are suitable for these requirements.

Compile requirements and make decisions on a fact-based basis based on the real need for operations and the guidelines of binding legislation and regulations. Don't claim your own opinions as facts. On the basis of fact-based needs and requirements, the associated risks can be identified and various solution options can be assessed on the basis of the risks and requirements.

Leveraging the capabilities and automation of the chosen cloud service

Justification for the policy

When you have chosen a cloud environment or service, try to use as many capabilities as possible. Using the native automation tools and services will be you much needed cost efficiency and better service going forward.

Strategic cloud policy 5.2: Leverage a wide range of the technical capabilities of the chosen cloud environment. Use native automation tools and value add services.

Outcomes of the policy

Services are designed utilizing cloud-based architecture and features of the selected cloud service. This leads to two main policies:

A. As such, the existing architecture and existing operating models will not be transferred to cloud platforms and, as a result, the cloud service will be tailored to match previous solutions. Instead, both the solution architecture and operating models are being redesigned to take advantage of the features of the chosen cloud technology and increase automation and flexibility in change. A good general principle when using cloud services is: Configure and parameterize - do not Customize.

B. Make full use of the value-added features of the selected cloud technology. Develop our own solutions and services so that they can utilize the ready-made value-added services of the cloud service effectively to support the needs of operations. The strength of the rapidly evolving public cloud services is that they offer strong strengths for easy utilization. technical services and features designed for the cloud service, which are constantly being developed. Take advantage of this development and avoid customizing standard solutions, as this may prevent the use of evolving features.

Underline B in practice means that in solutions for a specific special need, cloud diagnostics can be abandoned in a controlled and prudent manner. This can increase supplier dependence. In general, supplier dependence is understood as a negative thing, but it can also provide efficiency benefits such as:

- Less need for self-written code or in-house development
- Less time required for parameterization or configuration
- The solution to be developed is simplified, it does not have to be made so complex due to its own development

Thus, the benefits of the value-added services of the selected cloud service, e.g. in terms of development costs and speed, may exceed the ability to throw in the service over immediately to another platform. It is good to note that in SaaS and BPaaS, cloud diagnostics is impossible to achieve in any case. In all cases, however, care must be taken to ensure the portability of the data stored in the cloud service - see the next strategic cloud line.

Continuity and easy transferability

Justification for the policy

A good starting point when building new services, is to think about the continuity and transferability of your services and information. Make sure that your services are transferrable to other environments if needed.

Strategic cloud policy 5.3: The data in cloud services must be easily transferable to other platforms or systems. Continuity must be ensured in all cases based on the business continuity needs.

Outcomes of the policy

Not all cloud-developed services can always be immediately transferred to another cloud platform. However, in all situations, developers must ensure that the data and data stored in the cloud service can be transferred to government institutions or other services.

All aspects of continuity must be covered, this includes survivability of the service; resilience to disaster and major events, ability to scale for performance as well as mitigate risks due to negotiations and contractual risks, including legal requirements as well as price structure.

The tools available for porting data (and metadata and logs) should be clarified in advance about cloud services. Make sure that the data is smoothly removed from the cloud service before you sign a contract for the cloud service and store the data there. At the beginning of the development, make a plan for how the data will be transferred out of the service. In some cases, the data retention time of the selected cloud services (special message SaaS and BPaaS) is not sufficient for the needs of institution in question. In these cases, the retention period for the cloud service may need to be extended by transferring data and documents from the operational system to a long-term storage system or solution selected by the entity.

Utilize elasticity with iterative development

Justification for the policy

Cloud services are constantly evolving and you first need to get a “feel” for them. Try to experiment as much as possible to find what works and what doesn’t before locking in a design.

Strategic cloud policy 5.4: Utilize the elasticity of cloud services using iterative and experimentative development model. Publish and test often, start small and expand according to growing needs.

Outcomes of the policy

One of the key benefits and features of cloud services is the absence of the need for upfront investment and the rapid response to the growing need for use. It is a good idea to make full use of this flexibility. In cloud services, avoid reserving capacity in advance unless a capacity plan is in place. Develop iteratively and experimentally. Leverage continuous integration and publishing technologies and automation in PaaS platforms. Preferably develop in small pieces and test new features in real use often. Constantly learn about new features and experiments.

Prepare to share

Justification for the policy

The architecture of a lot of Icelandic services are heavily integrated. Make sure that you can easily share data through API’s if needed.

Strategic cloud policy 5.5: Prepare to share data from day one. Create APIs and versatile data and infrastructure architecture to support re-use of created cloud-based services.

Outcomes of the policy

Preparations are being made to share the data collected in the service right from the start of the design. Completely and carefully define and plan the interfaces to be developed for the service (and in SaaS and BPaaS services, the requirements for ready-made interfaces). Extensively assess the need to use the data to be produced:

- Identify potential stakeholders - who could all benefit from the data collected and generated by the service
- Identify the purposes for which the data could be used
- Find out the legal framework conditions for the use and sharing of this data
- Find out if there are national or international standards or standard formats for the data or interfaces in question that should be followed in the service being developed. Leverage standard protocols, formats, and approaches to ensure interoperability of solutions and services
- Design security measures for secure data sharing and utilization

Create high-performance software integration interfaces (APIs) to leverage data and system functionality that can be effectively leveraged by legitimate parties. Define APIs for service level needs and implement or require technical solutions that meet those service level needs.

Avoid implementing custom and rigid integrations. Take advantage of standardized APIs for cloud services.

4.7. Running the cloud

This chapter is for:

Target audience	**Perspective**
Ministry of Finance	*Overview of the pursue for risk-controlled cloud use.*
Top management of a governmental institution	*Overview of the pursue for risk-controlled cloud use. Understanding the main policies regarding security and risk management in cloud.*
ICT management of a governmental institution	*Overview of the pursue for risk-controlled cloud use. Understanding the main policies regarding security and risk management in cloud.*
Operational developers and digital specialists in a governmental institution	*Know-how of creating fact-based requirements for developed services and solutions.*
ICT experts and system architects	*Know-how of creating fact-based requirements for developed services and solutions from a technical and interoperability point of view.*
Security and data protection specialists	*Understanding the need for case-by case security and data protection evaluation and searching for cloud enabling risk controls.*

Procurement specialists	*Understanding the non-negotiability of the security terms and controls in the public cloud services.*

Strategic cloud theme 6:

High automation is the main target in cloud services. The integrity, confidentiality, availability, privacy and effectivity are verified regularly using technical and governance controls.

Automation first

Justification for the policy

Automation is key to cost effectiveness and automatic scalability in the cloud. This is a high value priority for running cloud services, so make sure you investigate this area heavily when designing for the cloud.

Strategic cloud policy 6.1: Fully automize your services. Leverage automation tools to scale your services based on demand and automate changes to your environment.

Outcomes of the policy

Ensure automation and easy customization of cloud services from design. We design self-developed services to adapt to usage needs and volumes automatically. The utilization rate of all cloud services should always be as high as possible, without compromising the required performance.

Once the main requirements have been implemented in the cloud solution, it is good to pay attention to the technical optimization of services and resources.

Cloud services are changing and evolving rapidly - new and better services are constantly emerging. Prepare for flexible changes in architecture and take advantage of new services. Take advantage of cloud-based operating models and solutions to make changes easier. The utilization of new, more efficient functionalities and technologies requires that both operations and information management in the institutions adapt to the fact that small changes are constantly made to services and that services and solutions are continuously developed and made more efficient.

In cloud services, the time for long-lasting solutions, updated only every few years, is over.

Continuous monitoring of services

Justification for the policy

Constant monitoring of services gives you insight into how your services are working. Setup monitoring early on so you can leverage the data and make better and more informed decisions in the future.

Strategic cloud policy 6.2: Constantly monitor your services. Create technical capabilities to provide real-time insight on your environment's health.

Outcomes of the policy

It is good to create a clear overall picture of the state of cloud services. Take advantage of the native monitoring features of the cloud service and create a comprehensive snapshot of the technical functionality of your cloud service. Technically monitor, for example:

- Technical integrity of services
- Security and privacy related events
- Availability of key components
- The performance and volumes of key components and related trends
- Functionality, volume and trends of transactions

Keep track of technology constantly, optimize often.

The institution must develop comprehensive monitoring solutions that bring together situational data from different cloud services into a comprehensive snapshot. In networking operations, the development architecture is increasingly based on component-based reusability - a technical service or data implemented in one service is reused and utilized in other services (eg identification, log service, core data interfaces, etc.). In this case, ensuring overall functionality requires a holistic control view of the functionality of the various components.

Cloud entity control is typically layered:

- Component level monitoring

  Monitoring at this level focuses on the technology components: computing power, server, database, communication device, etc. Typical items to be monitored are: availability, component performance

- Application and technology service level monitoring

  Application level as well as the overall technical service (eg network) monitoring level. Typically, the items to be monitored are total technical services - response times and availability.

- Process level monitoring

  Process-level monitoring evaluates the functionality and performance of the entire service process. Already at this level, the so-called end-to-end (E2E) control.

- User experience level monitoring

  In the user experience monitoring, the whole process is monitored, extending the supervision to the users' various terminals, simulating the genuine use of the total service.

Continuous governance of the cloud

Justification for the policy

From the start, you should implement a constant development and measuring way of working in your organization. As cloud services are always evolving and changing, make sure you have the necessary skills and solutions available to you at any given time.

Strategic cloud policy 6.3: Measure and manage your cloud suitability, continuity, security, and costs on a day-to-day basis.

Outcomes of the policy

In addition to technical supervision and management, the institution should monitor and manage cloud services from an administrative perspective. Aspects of administrative control include:

- Suitability for use
- Cost efficiency
- Conformity
- Security, privacy, and continuity

Suitability for use

Service owners should monitor whether the cloud service meets the needs of the institutions, end-user or other stakeholders. Both the cloud service and the needs of operations are changing and evolving. It is a good idea to check and ensure at regular intervals that the cloud service in its current form still meets the current needs of the operation and that the cloud service still meets the requirements set for it (both operational requirements and legislation review requirements that may have changed).

Cost efficiency

By monitoring the use of cloud resources and access rights on a regular basis, the cost-effectiveness of cloud services can be ensured. The flexibility and automatic scalability of cloud services is an advantage in change, but it can also easily lead to “loose” use of cloud resources. For example, access to SaaS services is reserved by adding users to people who rarely need that system. Likewise, different components of IaaS and PaaS services can be set up for different experimental use, without, however, driving the services down to the end of the experiments. Easy utilization of resources can also lead to the development of a ladder where application code is not optimized with sufficient precision for the use of resources.

A prerequisite for monitoring cost-effectiveness is a good overall picture of cloud resources and their costs.

Conformity

Regularly ensure that the services comply with the agreement. Check that the services are produced in the manner and with the content described in the contract and at the agreed costs.

4.8. Summary: Cloud policies vs principles and outcomes

The strategic cloud policies contribute to the cloud principles in the following way:

Policies / Principles	1: Be Facts based	2: Cloud smart when risks are acceptable	3: Design your services to be cloud native	4: Use trusted purchase channels and be cost conscious	5: Utilize common public cloud capabilities to your benefit	6: Take care of information and continuity	7: Monitor, verify and optimize	8: Learn, educate and collaborate
Theme 1: Capabilites and compentences in central government								
Policy 1.1: Ownership and responsibility for cloud adoption in Iceland								Indirect
Policy 1.2: Governmental Cloud Center of Excellence								Direct
Policy 1.3: Responsibility for top level key cloud policies								Indirect
Policy 1.4: Cloud capabilities in Government CCoE								Direct
Policy 1.5: Cloud competences in Government CCoE								Direct
Policy 1.6: Sharing the knowledge								Direct
Theme 2: Capabilites and compentences in institutions								
Policy 2.1: Organizing readiness for cloud adoption in institutions		Direct						Direct
Policy 2.2: Institution level responsibility for cloud strategy and policies								Indirect
Policy 2.3: Cloud capabilities and competencies needed in institutions								Direct
Policy 2.4: Utilizing existing capabilities and competencies as a priority					Direct			Direct
Theme 3: Security, identity, risk mgmt								
Policy 3.1: Requirements and needs first	Direct	Direct	Indirect	Indirect	Indirect	Direct	Indirect	Indirect
Policy 3.2: Understand your information	Direct	Direct	Indirect	Indirect	Indirect	Direct	Indirect	
Policy 3.3: Identify your risks	Direct	Direct				Direct	Indirect	
Policy 3.4: Control your risks holistically	Direct	Direct				Direct	Indirect	
Policy 3.5: Monitor your risks and verify your controls	Direct	Direct				Direct	Direct	
Policy 3.6: Data privacy – minimum use policy	Direct	Direct				Direct	Indirect	
Theme 4: Procurement and cost allocation								
Policy 4.1: Funding and budgeting moves to OpEx		Indirect	Indirect	Direct				
Policy 4.2: Cloud purchasing is different: Pre-study-based procurement	Direct	Direct		Direct				Indirect
Policy 4.3: High availability by architecture and SLAs		Indirect	Direct	Direct	Indirect			
Policy 4.4: Verify the cloud service contract terms before signing				Direct	Indirect			Indirect
Policy 4.5: Easy purchasing and management of costs in cloud services				Direct	Indirect			
Theme 5: Designing for the cloud								
Policy 5.1: Needs first approach	Direct		Direct	Indirect	Direct			
Policy 5.2: Leveraging the capabilities and automation			Direct	Indirect	Direct			
Policy 5.3: Continuity and easy transferability			Direct		Direct			Indirect
Policy 5.4: Utilize elasticity with iterative development			Direct		Direct		Indirect	
Policy 5.5: Prepare to share			Direct		Direct	Direct	Indirect	
Theme 6: Running the cloud								
Policy 6.1: Automation first					Indirect		Direct	Indirect
Policy 6.2: Continuous monitoring of services					Indirect		Direct	Indirect

‘Direct’ means that the policy (in rows) directly implements the cloud principle (in columns). ‘Indirect’ means that the policy has an indirect effect on implementing the cloud principle.

The strategic cloud policies contribute to the desirable cloud benefits in the following way:

Policies Outcomes	Efficiency	Innovation	Increased speed	Better service	Increased security
Theme 1: Capabilites and compentences in central government					
Policy 1.1: Ownership and responsibility for cloud adoption in Iceland	Indirect	Indirect	Indirect	Indirect	Indirect
Policy 1.2: Governmental Cloud Center of Excellence	Indirect	Indirect	Indirect	Indirect	Indirect
Policy 1.3: Responsibility for top level key cloud policies	Indirect		Indirect	Indirect	
Policy 1.4: Cloud capabilities in Government CCoE			Indirect	Indirect	Indirect
Policy 1.5: Cloud competences in Government CCoE			Indirect		Indirect
Policy 1.6: Sharing the knowledge	Direct	Indirect	Direct	Indirect	Indirect
Theme 2: Capabilites and compentences in institutions					
Policy 2.1: Organizing readiness for cloud adoption in institutions	Indirect	Indirect	Indirect	Indirect	Indirect
Policy 2.2: Institution level responsibility for cloud strategy and policies	Indirect			Indirect	Indirect
Policy 2.3: Cloud capabilities and competencies needed in institutions			Indirect	Indirect	Indirect
Policy 2.4: Utilizing existing capabilities and competencies as a priority	Direct	Indirect	Direct	Indirect	
Theme 3: Security, identity, risk mgmt					
Policy 3.1: Requirements and needs first				Direct	Direct
Policy 3.2: Understand your information	Indirect	Indirect		Indirect	Direct
Policy 3.3: Identify your risks	Indirect			Indirect	Direct
Policy 3.4: Control your risks holistically	Indirect			Indirect	Direct
Policy 3.5: Monitor your risks and verify your controls	Indirect			Indirect	Direct
Policy 3.6: Data privacy – minimum use policy	Indirect			Indirect	Direct
Theme 4: Procurement and cost allocation					
Policy 4.1: Funding and budgeting moves to OpEx	Indirect				
Policy 4.2: Cloud purchasing is different: Pre-study-based procurement	Indirect			Indirect	
Policy 4.3: High availability by architecture and SLAs			Indirect	Direct	
Policy 4.4: Verify the cloud service contract terms before signing	Indirect			Indirect	Direct
Policy 4.5: Easy purchasing and management of costs in cloud services	Indirect		Indirect	Indirect	
Theme 5: Designing for the cloud					
Policy 5.1: Needs first approach				Direct	Indirect
Policy 5.2: Leveraging the capabilities and automation	Direct	Indirect	Direct	Indirect	Indirect
Policy 5.3: Continuity and easy transferability			Indirect	Direct	Indirect
Policy 5.4: Utilize elasticity with iterative development	Indirect	Direct	Direct	Indirect	
Policy 5.5: Prepare to share	Direct	Direct	Direct	Direct	
Theme 6: Running the cloud					
Policy 6.1: Automation first	Direct				
Policy 6.2: Continuous monitoring of services	Indirect			Indirect	Direct
Policy 6.3: Continuous governance of the cloud	Indirect			Indirect	Direct

‘Direct’ in this table means that the policy directly advances the desired benefit (outcome) of cloud. ‘Indirect’ means that the policy has an indirect effect on achieving the benefit.

5. Implementation guidelines

A detailed plan for implementing these cloud policies in the government of Iceland should be created. Here we describe the main principles for implementing strategic cloud policies and achieve the cloud benefits in a controlled manner.

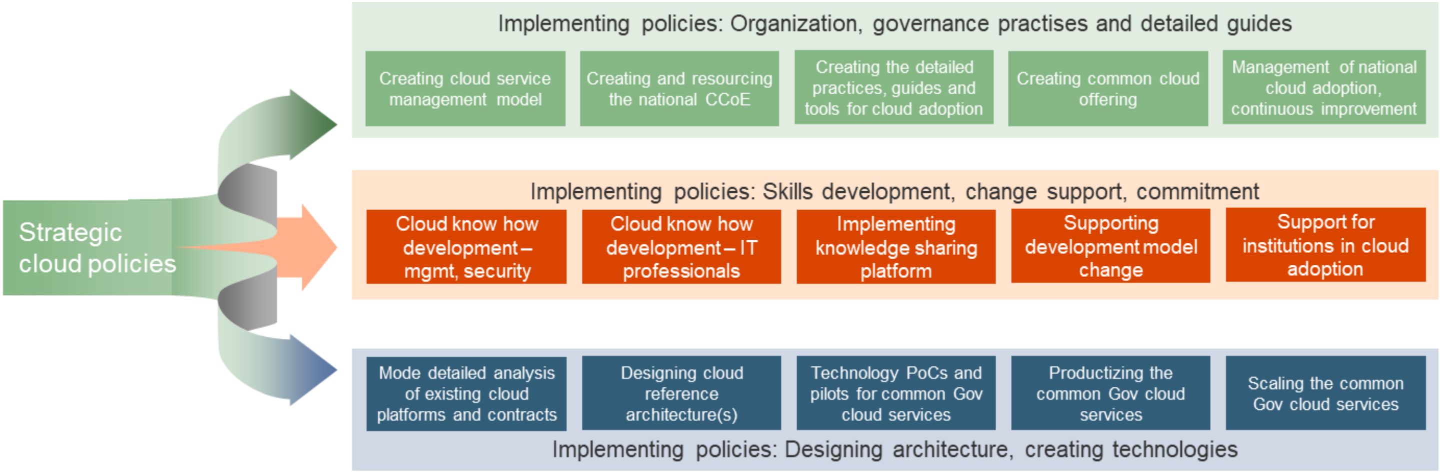
Main principles of implementing the strategic cloud principles in Iceland

The cloud adoption in Iceland and implementing the strategic cloud policies is based on developing holistically and persistently the needed cloud capabilities. The next phase of the implementation is structured into three main implementation streams:

A. **Developing the governance and practices**
Developing organisation, processes, practices and detailed guides & tools to accelerate safe and value creating cloud adoption both in central government and in institutions. Founding the governmental Cloud Centre of Excellence.

B. **Developing skills and supporting the change**
Training the management and technical professionals, enhancing the cloud skills, ensuring the sufficient resourcing – both in central government and in institutions. Supporting for the institutions, ensuring the commitment for the policies.

C. **Developing technology and common cloud offering**
Executing technological PoCs. Purchasing and deploying the cloud technologies. Designing cloud architectures.



Strategic cloud policies

Implementing policies: Organization, governance practises and detailed guides

Creating cloud service management model

Creating and resourcing the national CCoE

Creating the detailed practices, guides and tools for cloud adoption

Creating common cloud offering

Management of national cloud adoption, continuous improvement

Implementing policies: Skills development, change support, commitment

Cloud know how development – mgmt, security

Cloud know how development – IT professionals

Implementing knowledge sharing platform

Supporting development model change

Support for institutions in cloud adoption

Mode detailed analysis of existing cloud platforms and contracts

Designing cloud reference architecture(s)

Technology PoCs and pilots for common Gov cloud services

Productizing the common Gov cloud services

Scaling the common Gov cloud services

Implementing policies: Designing architecture, creating technologies

Managing the cloud policies implementation and cloud adoption in Iceland

Ministry of Finance is accountable and leads the cloud adoption and implementing these strategic cloud principles in Iceland. The governmental Cloud Centre of Excellence will be operatively responsible for the national cloud adoption when it is founded and resourced.

A detailed implementation plan should be created. The plan should cover at least the following topics:

- The measurable goals of implementation
- Analysis of the dependent projects and initiatives
- Phases and structuring of the main projects or work packages of the implementation
- Schedule of the projects or work packages
- Organisation, roles and resources involved in the implementation
- Budget
- Metering of the implementation (e.g., Objectives and Key Results (OKR) indicators)
- Implementation governance methods (e.g., decision making, change management, communication, risk analysis etc.)

6. Strategic cloud policies

Capabilities and competences in central government

Strategic cloud theme 1:
The co-ordination and guidance of governmental cloud services and platforms are collected to a Governmental Cloud Center of Excellence. Shared guides and governance models for cloud services are created.

Strategic cloud policy 1.1: Central government should name a responsible organisation for leading and supporting secure and value creating cloud service adoption in Iceland.

Strategic cloud policy 1.2: A nominated governmental organization should create a Cloud Center of Excellence (CCoE) function to drive and support safe and value creating cloud adoption in the government of Iceland.

Strategic cloud policy 1.3: The Cloud Center of Excellence should be the owner for the cloud principles and key cloud policies.

Strategic cloud policy 1.4: The Cloud Center of Excellence should develop holistic governmental cloud capabilities covering all aspects of successful and safe cloud adoption.

Strategic cloud policy 1.5: Governmental Cloud Center of Excellence should have needed cloud competencies to lead and governs holistic cloud adoption.

Strategic cloud policy 1.6: Governmental Cloud Centre of Excellence should provide a cloud knowledge platform through which cloud capabilities and competences are shared in networks & communities.

Capabilities and competences in institutions

Strategic cloud theme 2:
All institutions should prepare to cloud adoption and be responsible for their own capabilities, competences, and initiatives. Clear responsibility and structures for cloud adoption are needed.

Strategic cloud policy 2.1: Every governmental institute should organise their own cloud adoption function. At least a cloud service responsible person should be nominated.

Strategic cloud policy 2.2: Institutions should create their own cloud adoption strategy based on the governmental cloud vision, principles, and cloud adoption strategy.

Strategic cloud policy 2.3: Institutions should build and develop systematically required cloud capabilities and competencies for their needs.

Strategic cloud policy 2.4: Institutions should utilize existing capabilities and competencies where feasible. External support or outsourcing should augment internal capabilities when needed.

Security, privacy, and risk management

Strategic cloud theme 3:
The security and risk management of cloud services is ensured in all situations based on fact-based requirements and risk mitigation controls. Data is stored and handled in cloud services based on legislation, institutional data strategies and common guidelines.

Strategic cloud policy 3.1: Understand your needs based on justified facts. Do not make your decisions only based on technology.

Strategic cloud policy 3.2: Create a clear view of the information stored and processed in the cloud. Classify your data, understand its use and purpose. Create a sufficient data governance model.

Strategic cloud policy 3.3: Identify the risks based on the fact-based requirements and the purpose of the data. Assess the risks of cloud based on defined criteria. Verify that the potential solutions can control the risks.

Strategic cloud policy 3.4: Seek for holistic risk controls that enable cloud use. Amend cloud native risk controls using your own additional risk cloud controls where necessary.

Strategic cloud policy 3.5: Monitor your risk and their mitigation continuously. If the risks change, verify and amend the risk controls if needed.

Strategic cloud policy 3.6: Use of personal data shall be minimize and reducted as much as possible.

Strategic cloud policy 3.7: DPIA shall guide the design and implementation of privacy safeguards based on the impact for the registered person.

Procurement and cost allocation

Strategic cloud theme 4:
A pre-study oriented procurement process is used. The fit of cloud services is examined before the actual RFP since cloud terms are usually not negotiable. Utilization based cost allocation model is used in common cloud platforms and services.

Strategic cloud policy 4.1: Cloud moves your technology budget from CapEx to OpEx.

Strategic cloud policy 4.2: Follow the official procurement procedure. Streamline the purchasing process - put your effort on pre-study, cloud is purchased differently. For cloud platforms, create frame agreements for catalogue based quick purchasing.

Strategic cloud policy 4.3: The continuity and availability requirements of the processes are achieved by developing a cloud native high availability architecture together with SLAs in the cloud contracts.

Strategic cloud policy 4.4: “Buy cloud services as they are sold”. Accept that you cannot usually change cloud contract terms. Verify the terms and the cost structure in advance.

Strategic cloud policy 4.5: Make purchasing and ordering of general cloud platform services (capacity, technical services) easy and quick. Utlilize cloud elasticity to optimize the entire life cycle costs of the service.

Strategic cloud policy 4.6: Costs of common governmental cloud services are allocated according to utilization

Designing for the cloud

Strategic cloud theme 5:
User centric services are developed using agile and iterative development processes. The flexibility and technical services of the cloud are used to rapidly develop cloud native services that can be used by end-users and other systems

Strategic cloud policy 5.1: Always think of your and your customer's and end user's needs, goals and requirements, before thinking about technology. After that, what does your future look like? Do a current state analysis on your services before moving forward.

Strategic cloud policy 5.2: Leverage a wide range of the technical capabilities of the chosen cloud environment. Use native automation tools and value add services.

Strategic cloud policy 5.3: The data in cloud services and platforms must always be easily transferable to other platforms or systems. Continuity must be ensured in all cases based on the business continuity needs.

Strategic cloud policy 5.4: Utilize the elasticity of cloud services using iterative and experimentative development model. Publish and test often, start small and expand according to growing needs.

Strategic cloud policy 5.5: Prepare to share from the day one. Create APIs and versatile data architecture to support re-use of created cloud-based services.

Running the cloud

Strategic cloud theme 6:
High automation is the main target in cloud services. The integrity, confidentiality, availability, privacy and effectivity are verified regularly using technical and governance controls.

Strategic cloud policy 6.1: Fully automize your services. Leverage automation tools to scale your services based on demand and automate changes to your environment.

Strategic cloud policy 6.2: Constantly monitor your services. Create technical capabilities to provide real-time insight on your environment's health.

Strategic cloud policy 6.3: Measure and manage your cloud suitability, continuity, security, and costs on a day-to-day basis.