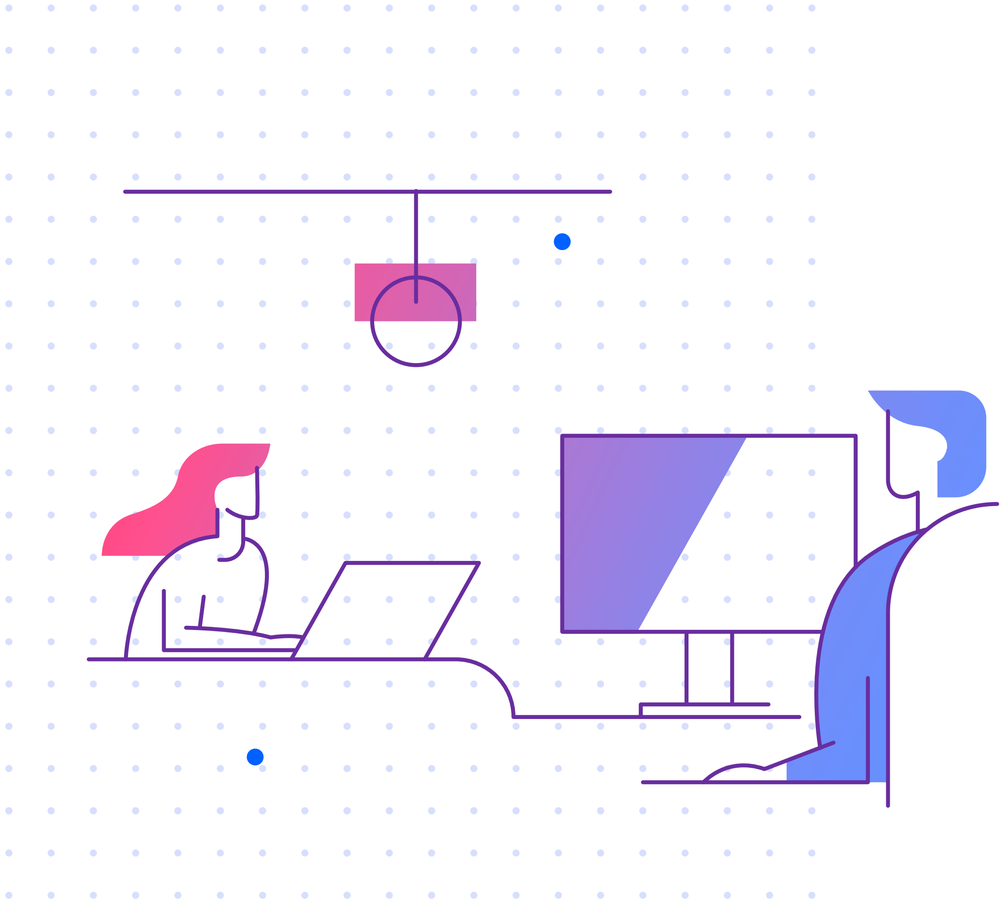
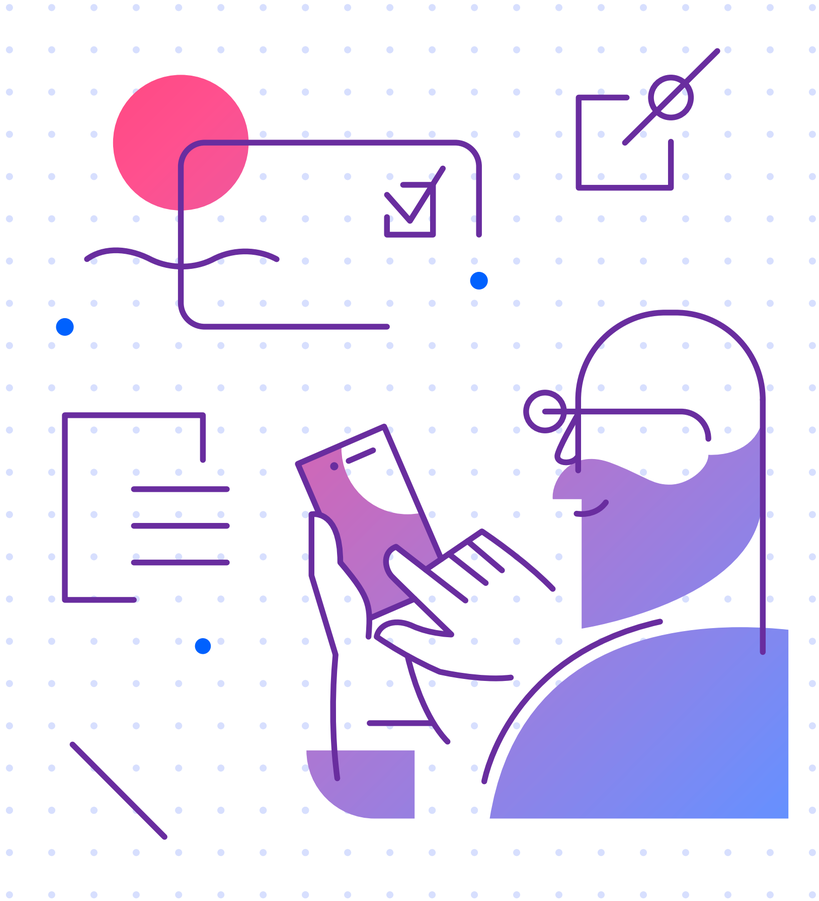
March 2022

# Cloud Policy of the Icelandic Public Sector



Stjórnarráð Íslands
Fjármála- og efnahagsráðuneytið

SAMBAND ÍSLENSKRA SVEITARFÉLAGA



# Strategic planning

The purpose of the Icelandic public sector cloud policy is to define objectives across the Icelandic public sector in the use of cloud solutions and their implementations and set out the desired outcomes of cloud usage. Since cloud solutions are already in use by many public entities it is important that efforts are coordinated for optimization and increased security.

The focus on digital services and user-oriented service design has put pressure and demands on government bodies for supplying faster and more efficient services. Cloud solutions shorten the delivery time of IT services and promote faster, more cost-effective and safer digital services.

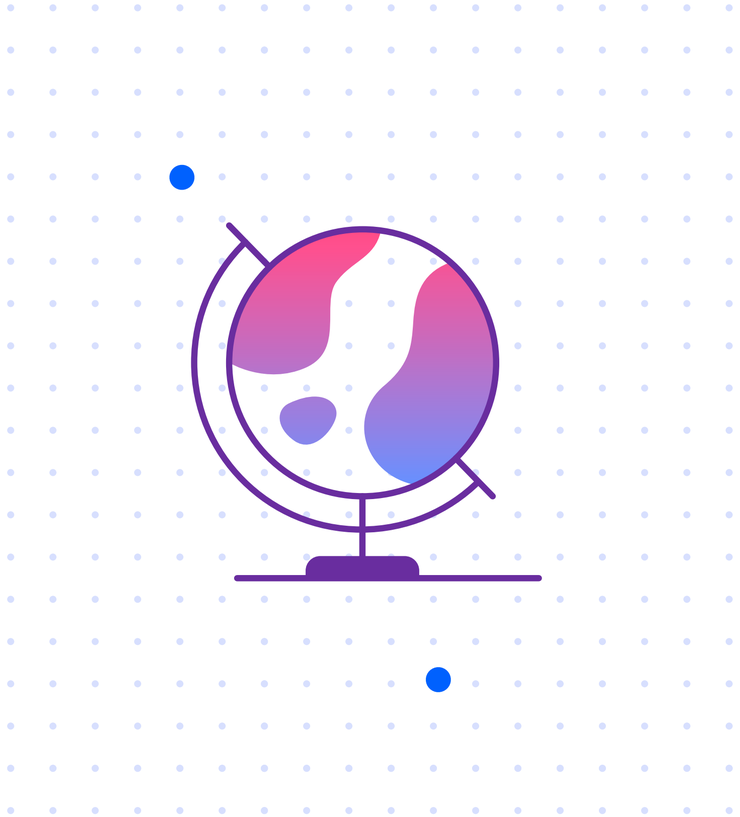
Cloud services also create opportunities for new and innovative applications, such as artificial intelligence and data analysis, which would otherwise be difficult or impossible to achieve.

Governance and structure of cloud solutions usage must be implemented in a way that the capabilities and qualities of the services are not diminished, e.g. flexibility, contractual status and innovation. If these attributes are not considered during implementation and procurement, there is a risk of increased costs, greater security risks and the loss of opportunities for innovation.

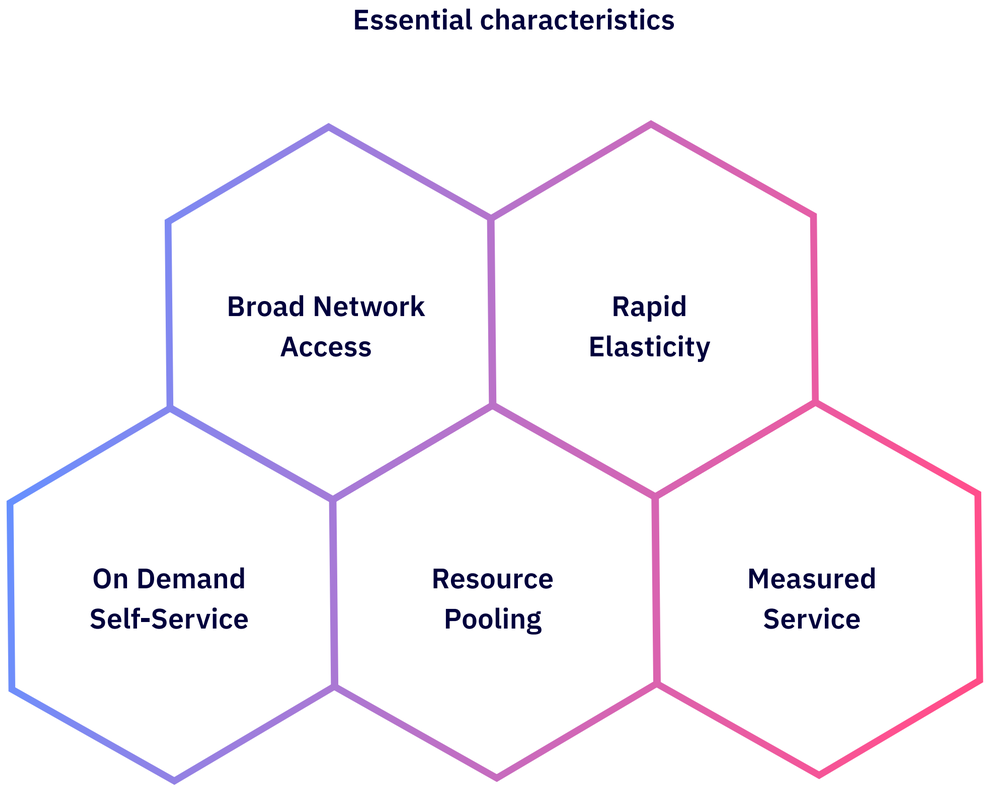
# Cloud services

Cloud computing / cloud services refers to services where a user can use online self-service provision as needed at any given time. Thus, cloud services are flexible, accessible, measurable, shared and self-directed IT services. Entities using the service are independent of each other but share a technical infrastructure provided by a service provider.

**Cloud services neither means that data of customers is shared nor that the data is open without restrictions.**



# International definition of cloud services




Source: National Institute of Standards and Technology (NIST)

# International definition of cloud services

Service models

**IaaS** **PaaS** **SaaS**

Deployment models

**Public Cloud** **Hybrid Cloud** **Community Cloud** **Private Cloud**

Source: National Institute of Standards and Technology (NIST)

## Necessary characteristics

| | |
|---|---|
| **On demand, self service** | The service can be managed as a self-service. |
| **Broad network access** | The service has comprehensive online access. |
| **Resource pooling** | The service enables rapid changes according to changing usage needs. |
| **Rapid elasticity** | The individual physical resources are grouped into a larger entity that covers the physical implementation layer (pool). |
| **Measure service** | The quality of service can be defined and measured. |

## Service model

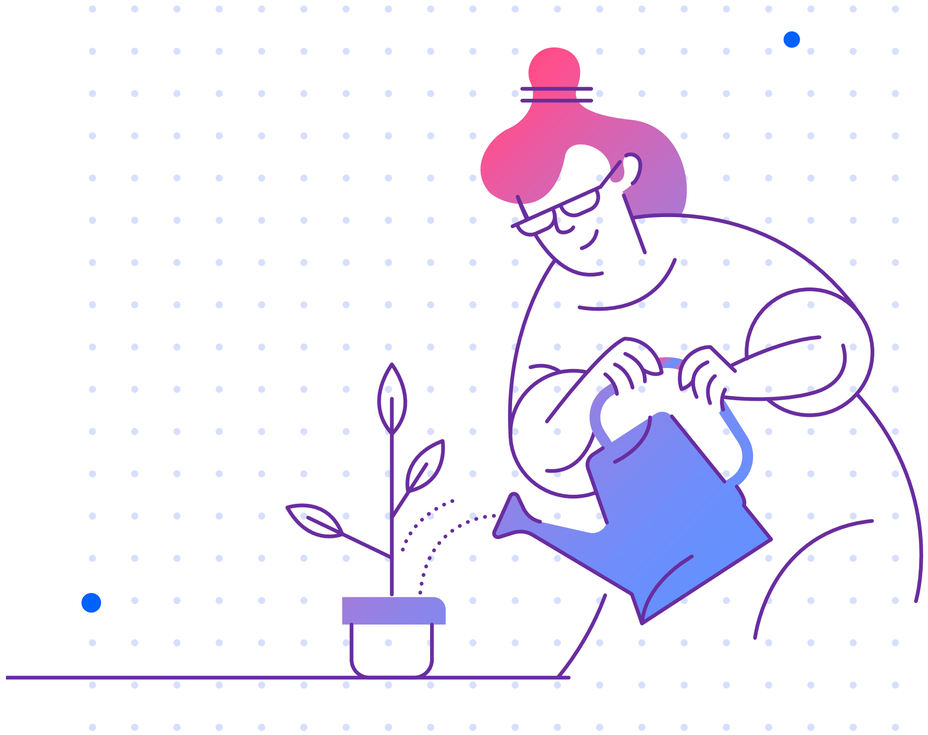
| | |
|---|---|
| **Infrastructure-as-a-Service:** IaaS | Easily modifiable capacity to provide processing power, storage, communication/networking, security, etc. |
| **Platform-as-a-Service:** PaaS | A technological space, created with the combination of different software tools, where customer applications can be implemented and executed. Everything from the runtime environment to the server is provided by the PaaS provider. |
| **Software-as-a-Service:** SaaS | An application for an end user that is served from the cloud through network access. |

## Deployment model

| | |
|---|---|
| **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 a 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). |
| **Private cloud** | The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. |

## Vision

Iceland is among the world’s leading nations in the field of digital services. By utilizing flexible and diverse cloud services, where appropriate, public entities provide safe, reliable, and efficient services where the public and businesses instantly get service and data, anywhere and anytime. Innovation is enhanced by enabling the use of IT in a flexible way, minimizing costs and efficiently using public funds by adapting services to real-time use demands.



## Outcomes

The use of standardized operating environments and advanced cloud solutions in the public sector supports more secure, more cost-effective and efficient operation of IT systems.

1. Increased security of information systems and data
2. Improved services that are efficient and agile
3. More innovation within the public sector

**With access to standardized operational IT environments based on current and state-of-the-art technology, professional procurement methods and access to specialist knowledge and support, it is possible to provide outstanding public services to the public and businesses.**

# Outcome 1 – Increased security

Raise and maintain security levels for services and data of citizens, businesses, and the public sector.

- A comprehensive risk assessment and data security classification supports appropriate protection of data and systems
- Protect data of individuals, companies, and agencies against internal and external threats
- Reduce risks through standardization of information systems, automation, and continuous monitoring
- Ensure that systems can withstand increased usage and loads, attacks, and other cyber threats by having access to dynamics resources and security capabilities

# Outcome 2 – Improved, efficient and agile services

Provide better services to the public and businesses while public funds are used more efficiently.

- Share, use and re-use of data and simplify use of digital solutions
- Improve digital services provided to the public and businesses

Provide the public sector with robust and improved solutions to carry out tasks more efficiently and by gaining access to the required IT resources.

- Access to the best solutions at any given time
- Increase emphasis on the development and promotion of public sector bodies within their field of expertise
- Increase emphasis on public sector coordination, e.g. through processes and shared data

Minimize implementation time through use of standard digital solutions.

- Sharing of designs and know-how
- Shorten delivery times of services
- Minimize development time

**Standardized solutions should be used to increase automation and efficiency of public entities and services to individuals and the private sector.**

## Outcome 3 – More innovation within the public sector

Enable the public sector to increase innovation in its operations by using services and products, for example in the fields of artificial intelligence, automation and data analysis.

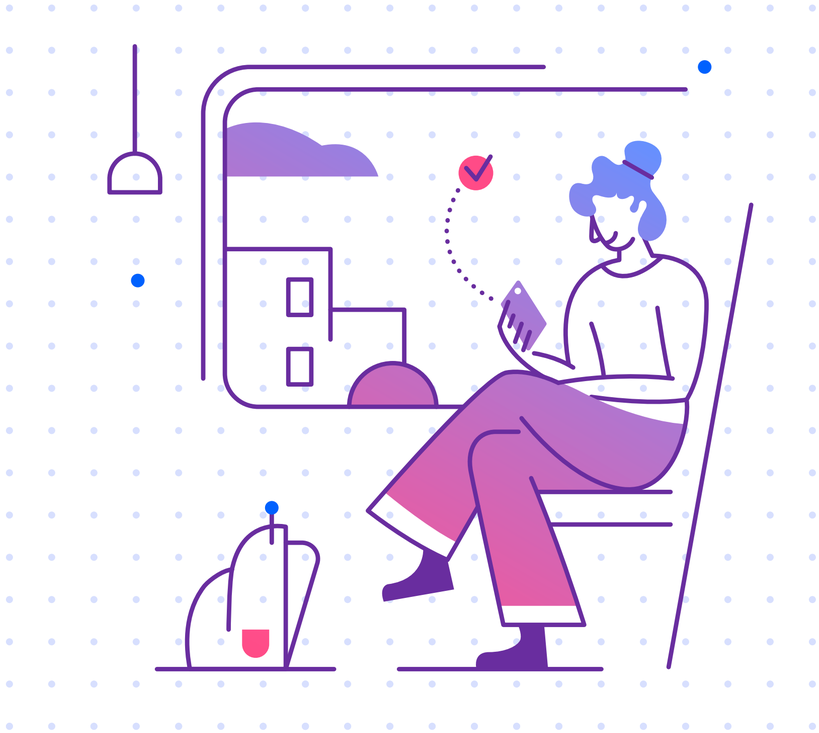
- Use new methods and processes
- Provide the public sector with new tools for digital transformation

**By using the full benefits of the functionality of cloud solutions, the public sector can use and access advanced and powerful tools.**

# Strategic cloud principles

To coordinate the procedures and use of cloud services in the public sector, the following strategic principles should be followed to achieve the objectives of this policy, such as decision-making on procurement and feasibility of solutions, standardization, cost management and selection of suppliers, as well as up-skilling and knowledge buildup. The principles are intended for guidance to achieve maximum performance in operations and public services by utilizing cloud services.

1. Cloud solutions utilized in the most efficient way
2. Fact based decision making
3. Using cloud solutions where applicable
4. Trusted service providers and cost control
5. Protect data and services
6. Continuous measurements and improvements
7. Collaboration and training

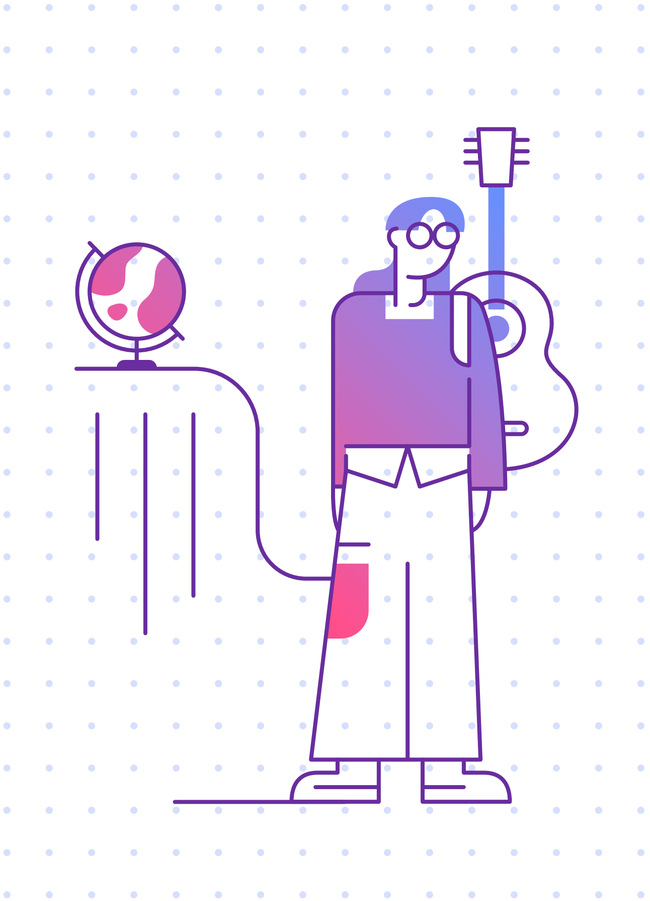


# Strategic cloud principles – detailed

1. **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. **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. **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.

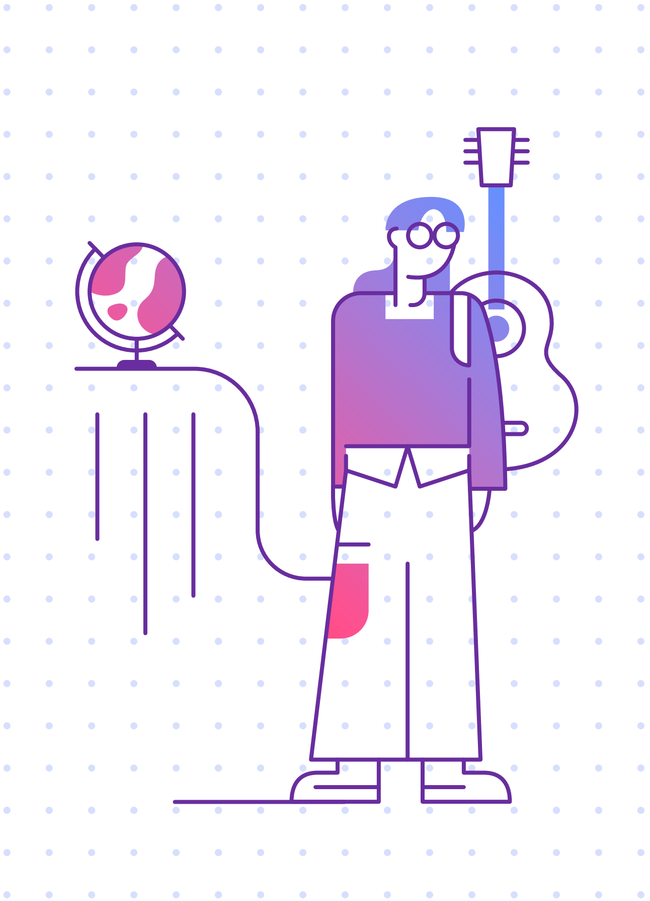


# Strategic cloud principles – detailed

4 **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.** 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 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 architectures 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.



# Strategic cloud principles – detailed

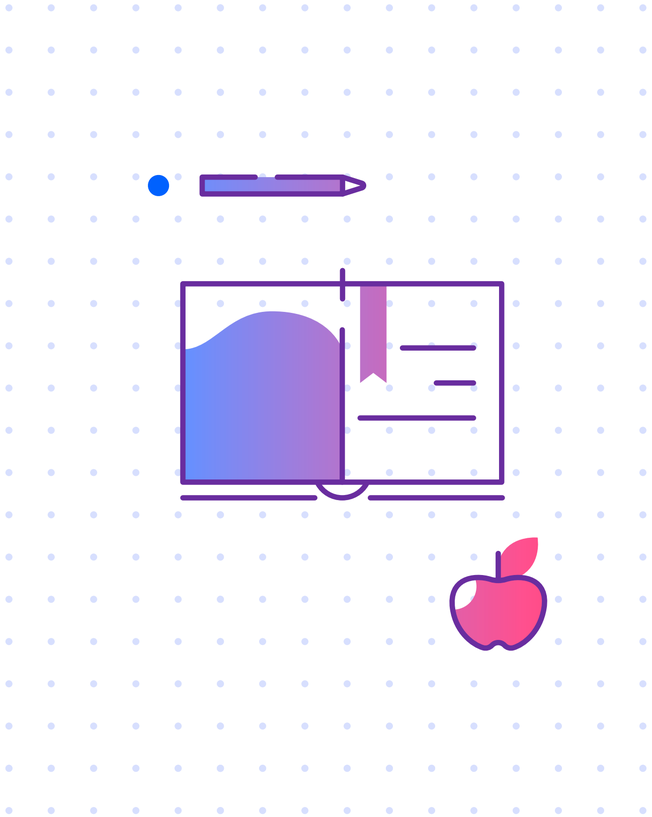
7 **Continuous measurements and improvements.** Ensure that the cloud provider you choose can provide metrics that support your forecasting and analytics needs of cloud usage. Proactively monitor your cloud usage, verify cloud integrity and health and confirm security in real time. Ensure cost effectiveness 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.** 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.

## Strategic cloud policy themes

To achieve the objectives of this policy, the following strategic policies are set out in the following categories that need to be followed at all stages of use:

- Governance and architecture
- Organizational structure and competence
- Security, privacy, and risk management
- Procurement and cost control
- Selection and design of cloud environments
- Operation of cloud environments



# Theme 1 – Governance and architecture

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 practices 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.

# Theme 2 – Organizational structure and competence of institutions

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

The number of data entry and exit points should be reduced from a security point of view, and governance structure shall be in accordance with the best known international standard and practices at all time.

# Theme 3 – Security, privacy and risk management

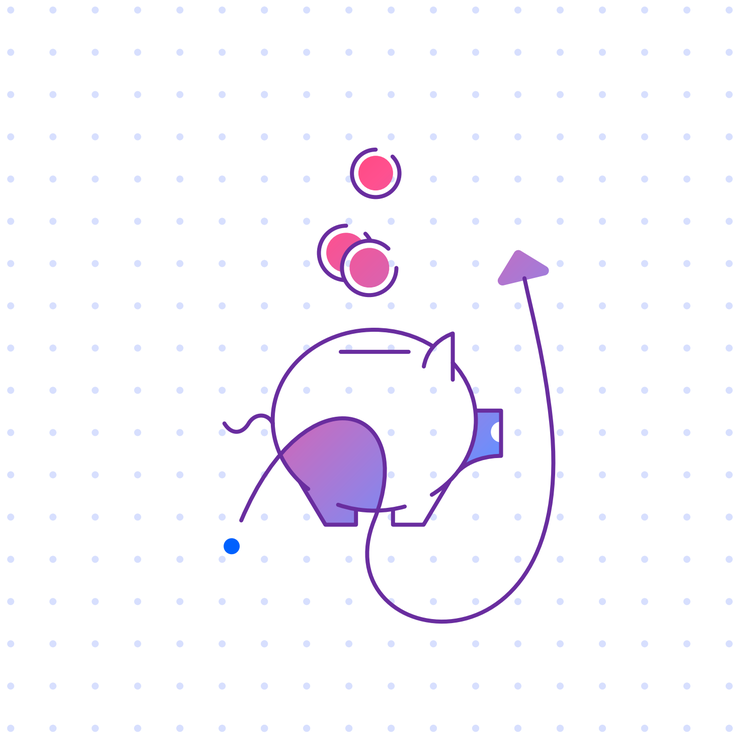
The level of security of cloud solutions compared to traditional IT operations needs to be assessed comprehensively through systematic risk assessment to assess the current operational risks and risks involved in the use of cloud solutions.

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 on whether cloud services can meet the needs and requirements of the purposed use.

The requirements can at first still be made at a 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 fulfill the necessary requirements.

Access and permissions should be minimized at all levels. Fundamental requirements in the design of all information systems are privacy and security. Amend those with additional capabilities from other platforms where needed, based on risk assessment results.

System and operational environments shall be resistant to attacks and other threats.



# Theme 4 – Procurement and cost control

Agencies and other public bodies shall identify their IT needs and requirements prior to selecting a platform or service methodology. The procurement of services shall be centralized, where applicable, for optimization purposes. Costs should be predictable, and transparency guaranteed for buyers. Cost incentives shall be regularly reviewed, and contracts shall allow for iteration of the architecture and design during the contract period.

The service provider must meet the relevant conditions in accordance with the importance and classification of the platform in question, including security certifications, service levels, disaster recovery, jurisdiction and ownership of information and processing systems.

Contracts shall ensure the buyers’ full ownership of the data they place in the service and that at the end of the contract period. It shall be possible to transfer data to another service provider or directly to the buyer. Central procurement shall ensure that public entities have access to qualified and competent bidders and make it possible for institutions to use the latest possible services and expertise at any given time.

# Theme 5 – Selection and design of cloud environments

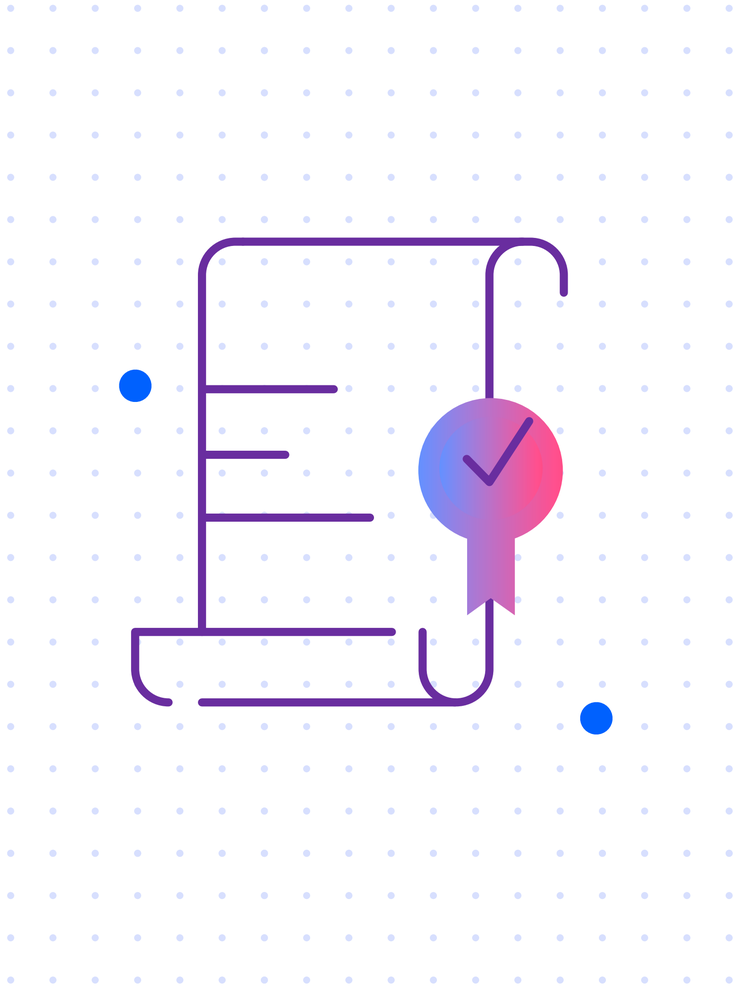
Standardized solutions, that require minimal adjustment to meet user requirements and minimize development and delivery times, shall be used. The operating environment shall be implemented with as standardized services and included within the platform as much as possible in order to maximize the functionality within the environment.

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 based on identified and fact-based requirements can the next step be to assess whether cloud services are suitable for these requirements.

# Theme 5 – Selection and design of cloud environments

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. Events, data, and functionality shall be shareable in a standardized way to other systems and services. The retention of data shall be ensured in accordance with applicable requirements at any given time and ensure that data is easily archived to the relevant parties as appropriate.



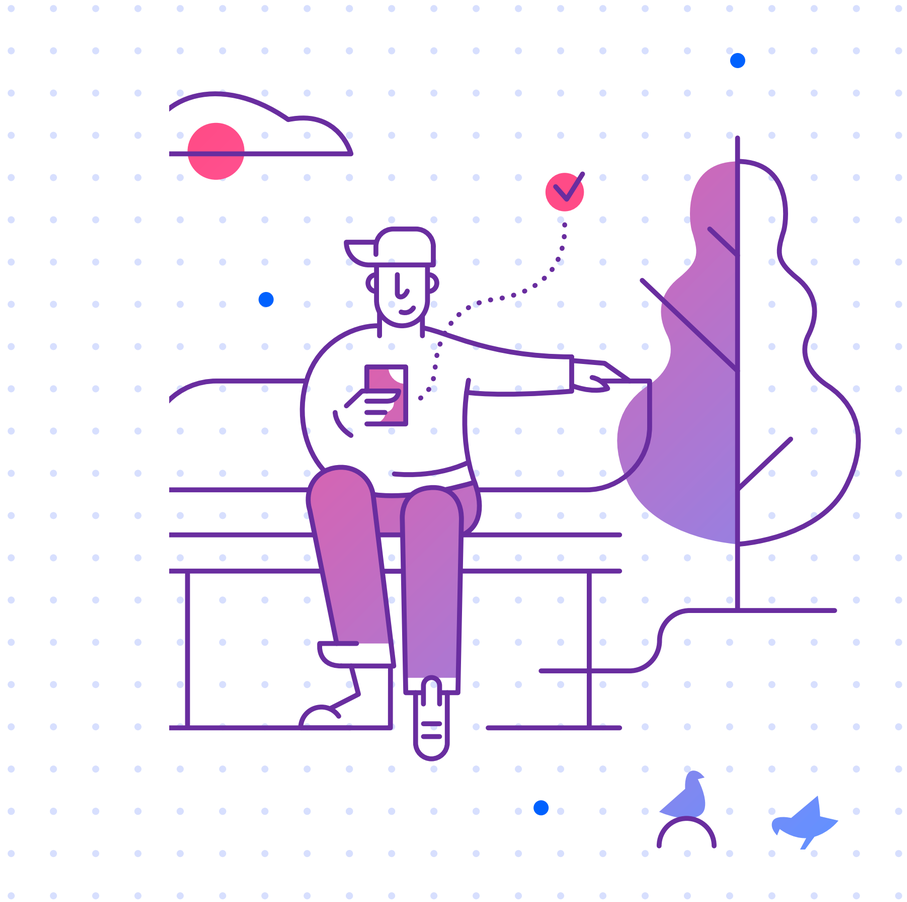
# Theme 6 – Operations of cloud environments

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.



# Next steps

The public sector’s cloud policy is intended to give guidance in the ongoing coordinated development and structure us of cloud solutions within the public sector in Iceland.

Following the publication of the policy, an action plan that supports its objectives and provides guidance and assistance to the public sector in building their own cloud adaptation plans will be presented. Such guidance is part of the framework of government digital services that public sector entities will use to create their own IT policies and digital transformation roadmaps.

The Ministry of Finance and Economic Affairs is responsible for the policy and is subject to sectors 5.3 and 6.1 of the Federal Budget. The implementation of the policy and actions is with the Ministry of Finance and Economic Affairs in close cooperation with public sector entities and other ministries, municipalities and private companies. The Icelandic Association of Local Authorities has adhered to the policy and is working on its progress among Icelandic municipalities.

Stjórnarráð Íslands
Fjármála- og efnahagsráðuneytið

SAMBAND ÍSLENSKRA SVEITARFÉLAGA

island.is