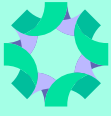# Analysis of the Use of Cloud Services

Huoltovarmuusorganisaatio
Digipooli

Huoltovarmuusorganisaatio

www.huoltovarmuuskeskus.fi

Security of supply refers to the capability to maintain essential economic functions of society that are necessary to ensure the living conditions of the population, the functionality and security of society, and the material conditions for national defence during severe disruptions and exceptional circumstances.

The National Emergency Supply Agency (NESA) is an institution under the Ministry of Economic Affairs and Employment, responsible for the planning and operational activities related to maintaining the country's emergency preparedness.
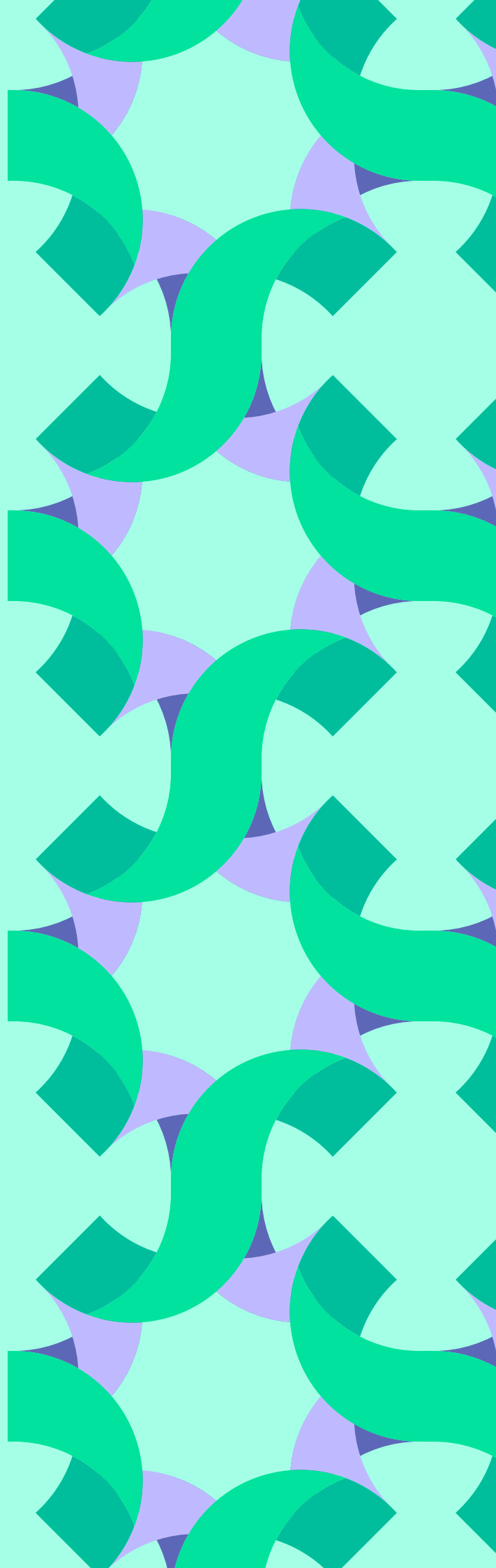
Table of contents

Summary of results

The use of cloud services is common and growing

The use of cloud services is widespread among the organisations that responded to the survey: 60% of respondents currently have over half of their ICT application portfolio in cloud services, and the majority plan to increase their use of cloud services in the near future. 80% of respondents estimate that in five years, over half of their organisation's application portfolio will be in cloud services, and half of the respondents estimate that the majority (>75%) of the application portfolio will be in the cloud environment in five years.

The general attitude towards the use of cloud services is positive (3.2/4), and the majority (81%) have predominantly good experiences with cloud services. Positive experiences emphasise ease of use, flexibility, cost efficiency, and data security. However, some respondents find it challenging to predict costs and are concerned about the security level of service providers. Risks are, however, relatively well managed: for example, 63% of respondents follow some form of security standard.

The majority (76%) of large organisations (> 250 employees) have addressed the use of cloud services either in a separate cloud strategy or as part of the organisation's digital strategy or general strategy. This is less common in smaller organisations.

The skills for developing cloud services are at a fairly good level, but about half of the respondents feel that there is insufficient expertise to meet future needs, and there is a need to invest in capabilities.

The survey was answered by organisations across various sectors that influence Finland's emergency preparedness.

Survey timing: **April 2024**
Respondents: **136 organisations**
Industry Distribution**: 14 sectors**

Cloud services are used in critical operations, but more cautiously

Cloud services are also used in the critical operations of organisations, but the threshold is higher and the attitude is more cautious. Only about one-third of respondents report being more cautious about using cloud services in critical operations, but when looking at the adoption rate, the actual attitude is likely even more cautious: only 40% of respondents have more than half of their critical operations in cloud services. 12% of respondents have completely excluded their critical operations from cloud services, and about one-third of respondents (35%) have excluded the majority (>75%) of their critical operations from cloud services.

The most common reasons for using or avoiding cloud services in critical operations are the same as the general attitudes towards the use of cloud services. The responses emphasise continuity management, ease of use, cost, and concerns related to data security. However, outages in critical operations are rare (on average 1-2 times per year) and are usually short (0-2 hours).

Ease of use, continuity management, and costs are the most important factors in decision-making

For about half of the respondents, emergency preparedness is an important factor in decision-making regarding the use of cloud services (weight over 50%). Other significant factors for decision-makers include ease of use, costs, overall architecture, and the organisation's expertise.

What proportion of operations or application portfolio relies on cloud services? Differentiation between critical operations and all operations

Number of organisations

Application portfolio in cloud services
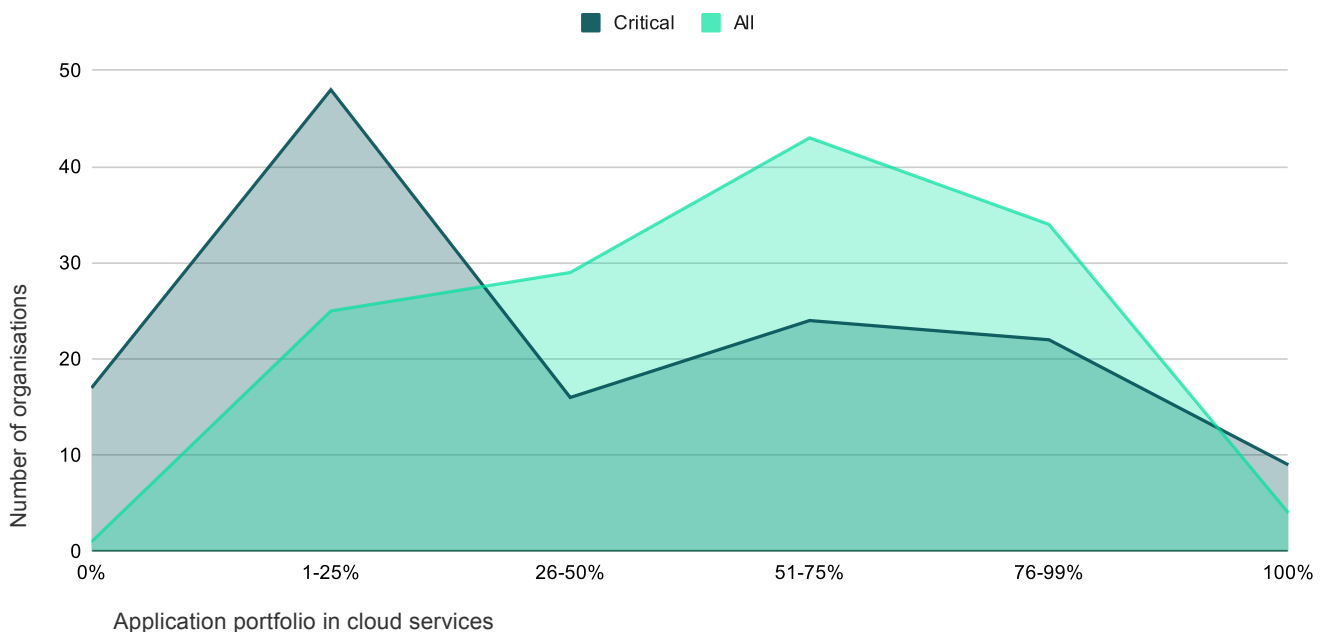
Introduction

In April 2024, the **Cloud Services Division of the Digipool** within the National Emergency Supply Organisation conducted a survey on the use of cloud services in collaboration with **Futurice**. The aim of the survey was to investigate the use of cloud services among organisations in various sectors of the National Emergency Supply Organisation – how much they are used, in what contexts, and how decisions regarding their use have been made or what factors have weighed most heavily in these decisions.

A total of 136 organisations from 14 different sectors responded to the survey. The majority of responses came from industrial sector organisations, but there were also significant responses from other sectors (see sector distribution below).

The survey was answered by organisations of various sizes.

Organisation size	Number of responses (n)
Under 50 employees	30
51-250 employees	43
251-2000 employees	44
Over 2000 employees	18

Industry distribution

Number of organisations
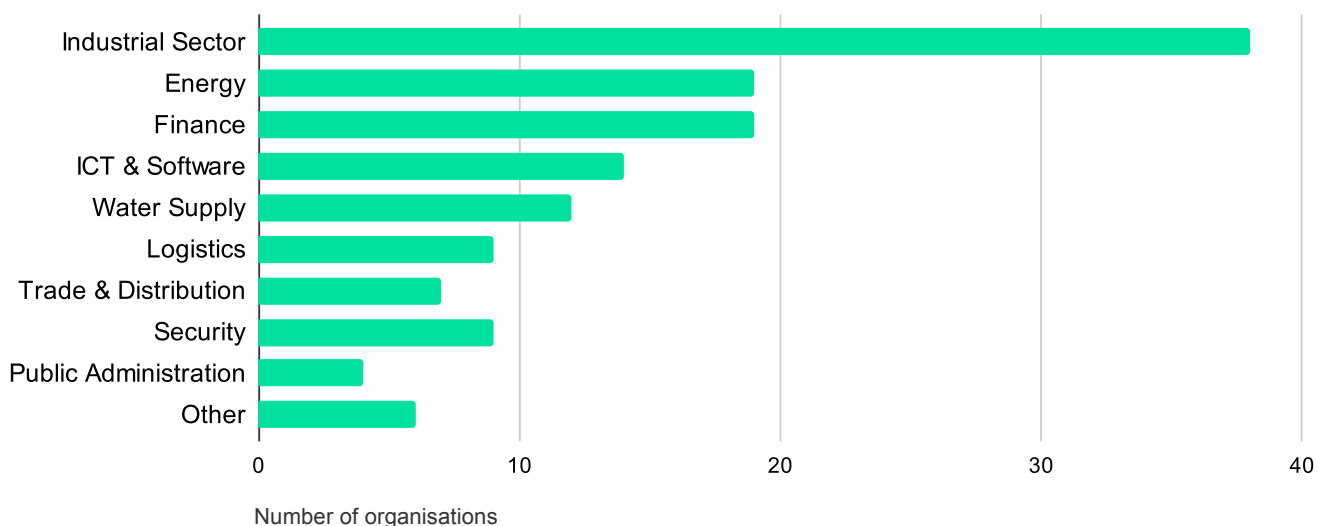
General use of cloud services

This section describes the survey results on the general use of cloud services: the extent to which cloud services are used, what the near future development looks like, why organisations have chosen to use or not use cloud services, and the organisations' own capabilities related to cloud service development.

The following sections will examine the use of cloud services in business and emergency preparedness critical operations, as well as decision-making related to cloud services.

The use of cloud services is common, and the attitude towards using cloud services is quite positive

The attitude towards the use of cloud services is generally positive (average: 3.2/4), and the use of cloud services is widespread: approximately 60% of the respondent organisations have over half of their application portfolio in cloud services. The size of the organisation does not seem to affect the extent of cloud service adoption, as the ratio remains fairly consistent regardless of the organisation's size.

Attitude towards the use of cloud services
(1 = cloud services are avoided / 4 = cloud services are preferred)

Proportion of organisations' ICT (application portfolio) currently operating on cloud services
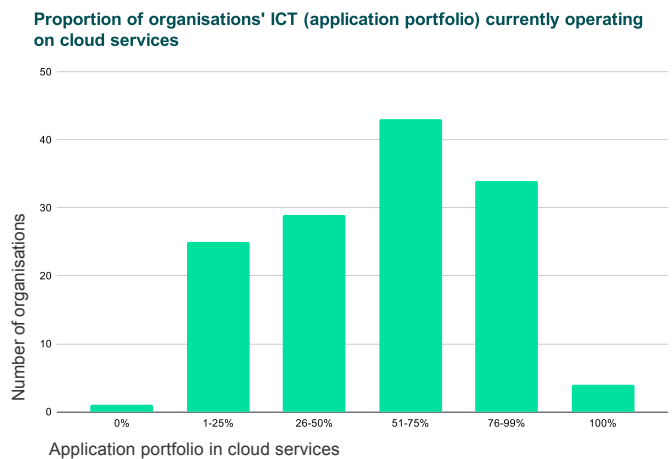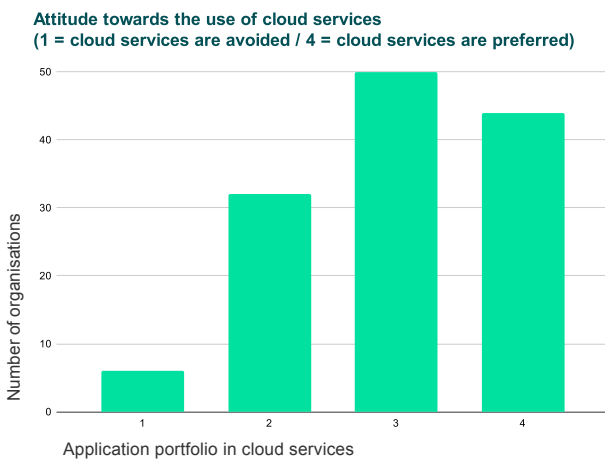
The use of cloud services is increasing

The organisations that responded to the survey plan to significantly increase their use of cloud services in the future: approximately 80% of respondents expect that over half of their organisation's entire application portfolio will be in cloud services within five years. Additionally, about half of the respondents believe that the majority of their application portfolio (> 76%) will rely on cloud services in the near future.

The chart below illustrates the shift towards more extensive use of cloud services. Currently, the distribution is relatively even, but in the future, the focus will shift significantly. In five years, an increasing number of the organisations that responded to the survey will have the majority of their applications in cloud services. This trend is evident in the quantitative responses of the survey and is also reflected in the open-ended responses.

To what extent does your organisation's ICT (application portfolio) currently rely on cloud services and in five years
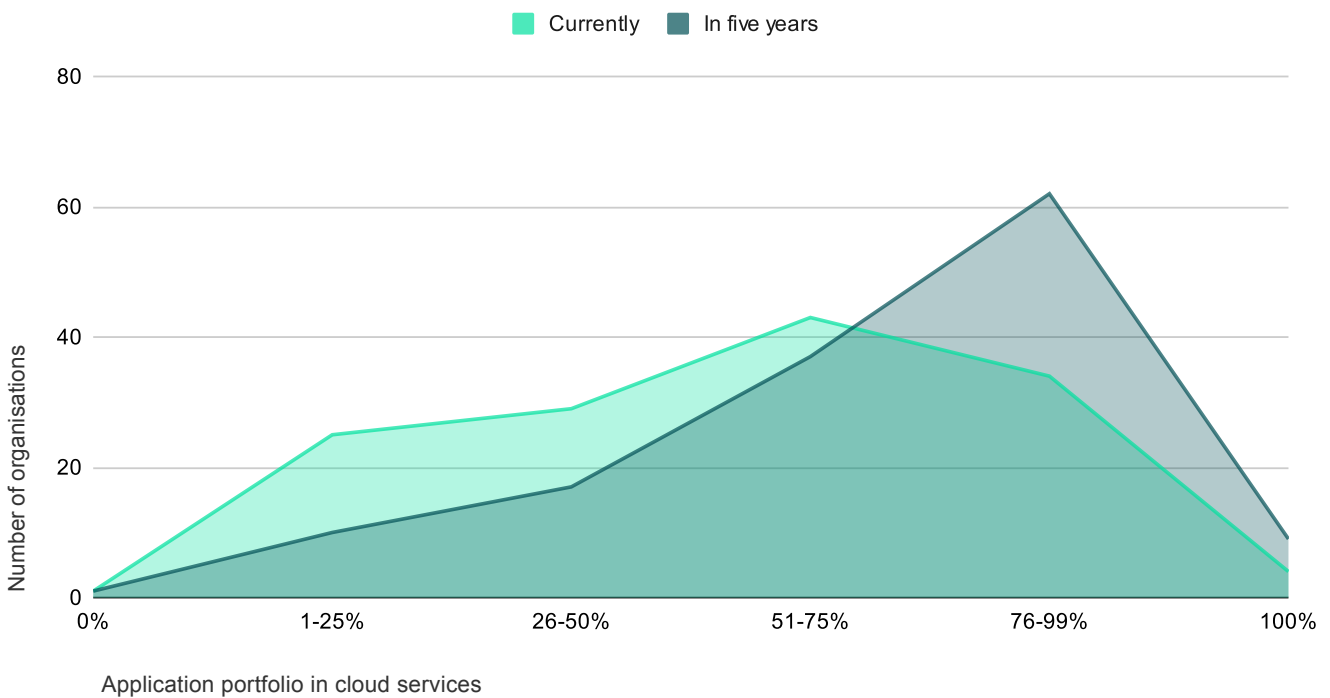
In what areas are cloud services used in organisations?

As stated in the previous section, the use of cloud services is common and on the rise. The use of office tools in cloud services is typical, with well-functioning solutions provided by Microsoft and Google, among others. However, cloud services are also favoured in other operations. The most common application areas are:

- Financial management and HR-related systems (47.46%)
- ERP and production control systems (42.24%)
- Core business (custom) applications (40.68%)

When examined by industry, the distribution of application areas is relatively even, with a couple of exceptions:

- **In the security sector** (consolidated), 60% of organisations use cloud services for information security, compared to the average of 16.95% across all sectors.

- **In the ICT & Software sector**, 72% of organisations use financial and HR systems as cloud services, compared to the average of 47.46% across all sectors.

The open responses do not provide an explanation for these deviations.

In the chart, "Other business" refers to software designed and built according to the company's unique business needs. These support the company's core functions, which distinguish it from its competitors and create added value for customers. These applications are not off-the-shelf but are customised around the company's unique business model.

Examples include: customer-specific e-commerce platforms, proprietary logistics and supply chain management applications, risk management applications, and algorithmic trading systems.

In which areas/application domains are cloud services used (excluding office services such as calendar, email, etc.)?
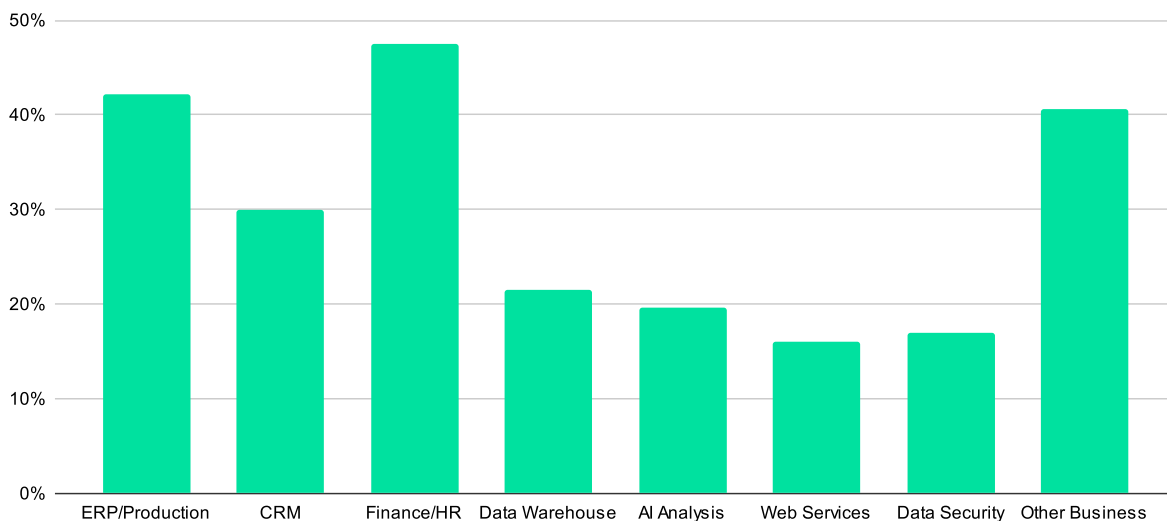
Experiences with the use of cloud services are generally good

Organisations that extensively use cloud services are generally satisfied with them, although there are also variable and unsatisfactory experiences among them. Many respondents emphasise that it is important to identify how qualitative factors (such as continuity, preparedness, and data security) are managed in cloud services with different arrangements, and how the benefits of cloud services are planned to be measured.

Interestingly, the biggest benefits and challenges are perceived to be the same and vary by organisation. The adoption of cloud services has brought comprehensive cost savings to many organisations. On the other hand, many have found it difficult to predict cost increases and have had limited influence over them. Some also mentioned that the actual costs have been higher than advertised.

Data protection is another factor that divides respondents: some feel that the security level of service providers can be trusted and is better than what they could implement with on-premise solutions. Others are concerned: Can the service provider really be trusted? How can they know where the servers and thus their data are located? A recurring reason for avoiding cloud services in certain operations was the belief that what is managed in-house can also be controlled in-house.

Many respondents highlighted that before adoption, they reviewed where the service providers' servers are located and how the service providers prepare for risks that are critical to their own organisation.

Sentiment analysis of experiences with cloud services

Unsatisfactory
0.9%
Variable
17.2%

Good
81.9%
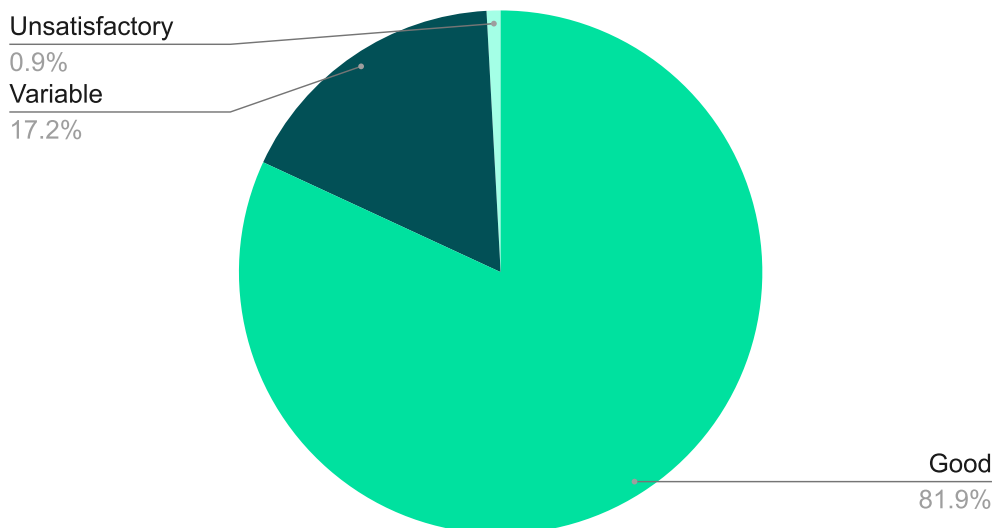
Benefits and challenges of using cloud services – observations from the survey

The results highlighted both the benefits and challenges experienced by respondents. Some aspects that are seen as challenges by some respondents are perceived as benefits by others. For example, concerns related to data security divide opinions: some believe that the security of cloud service providers cannot be trusted, while others believe that service providers have significantly better resources to ensure data security than their own organisations.

The table below presents observations from the survey on the use of cloud services, reflecting the experiences of the organisations that responded. It is worth noting that positive experiences were mentioned significantly more often than challenges, with approximately 80% of the responses being positive and 20% varying or negative.

Benefits	Challenges
For some, overall costs are lower compared to on-premise solutions	Service prices can vary greatly, and predicting cost increases is difficult
Usage is flexible and easily scalable, accommodating spikes in user demand	Actual costs have been higher than advertised
Easy to use and user-friendly for both internal users and customers	Customisation can be challenging
Service providers have significant resources to ensure data security	Concerns about data security, privacy, service outages, and data handling: it can be difficult to know where servers are located
Service providers offer better reliability than on-premise solutions	The transition can be laborious: it involves more than just a technological change. Changes are also needed in the organisation's operational models, working methods, and processes.
Cloud services enable the utilisation of modern technologies (e.g. AI), allowing similar services to be offered to customers	Impersonal and difficult-to-reach customer service
	Some feel that cloud services cannot be controlled in the same way as on-premise solutions
	Uncertainty about the use of cloud services: What functions can be moved to the cloud? How do you change cloud service providers?
	Uncertainty about continuity management: How will services function if the internet connection is lost, for example?

Cloud services are an important part of ICT for many organisations, and their use has been specifically addressed

It is quite common for the use of cloud services to be addressed either directly in a separate cloud strategy, or as part of the organisation's general or digital strategy. Separate consideration of cloud services is less common in smaller organisations (< 250 employees). This is understandable, as smaller organisations tend to have less documentation and fewer written guidelines. In larger organisations, it is fairly common for the use of cloud services to be addressed in the digital strategy, organi-

sational strategy, or a separate cloud strategy (approximately 76%). There are no significant differences when examined by industry.

Organisations without a specifically defined cloud strategy mention that guidelines have been discussed informally, the digital strategy is a work in progress, or there is no need for a strategy because current operations already define everything needed regarding the use of cloud services: all functions are primarily in the cloud, or all services are on-premise.

In cloud strategies, the most common objectives are clearly cost and data security

About half of the respondent organisations have a defined cloud strategy, or the use of cloud services is addressed in their strategy

No
45.6%

Yes
54.4%
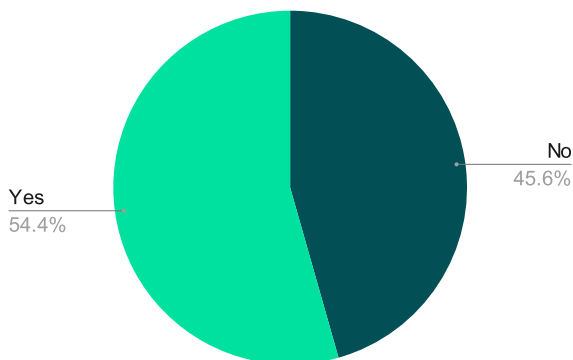
3/4 of the largest companies (>250 employees) have defined a cloud strategy

No
24.2%

Yes
75.8%
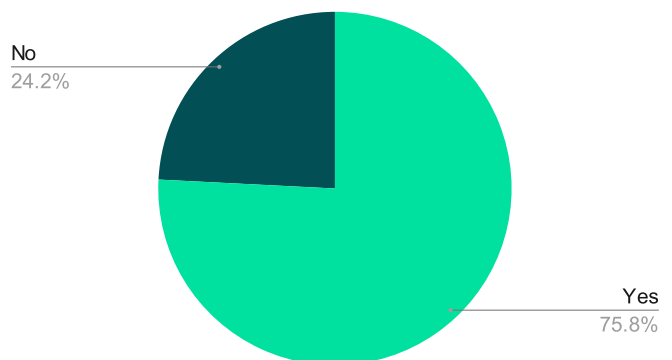
What objectives do organisations set in their cloud strategies?

Cost efficiency and scalability: Many organisations emphasise the cost efficiency and scalability provided by cloud services. Cloud services enable the flexible use of resources as needed, which can lead to significant savings in infrastructure costs.

Data security and compliance: Data security is a central concern and the focus of many strategies. Organisations highlight the need to comply with data protection requirements and regulations, such as the EU's GDPR. Cloud services are also aimed at improving system security and ensuring business continuity.

Modernisation of technology and services: Many pointed out that cloud strategies often support technological development and system modernisation. Operating in the cloud allows for the efficient utilisation of the latest technologies, such as artificial intelligence and big data.

Business flexibility and efficiency: Cloud services enhance business agility and efficiency. Through automation and flexible resource management, organisations can quickly respond to market changes and business demands.

Strategic compatibility, integration, and "Cloud First": Strategies emphasise the need to integrate cloud services into the broader IT infrastructure and business strategy, ensuring service compatibility and smooth operation. Some organisations follow a "Cloud First" strategy, where cloud services are the primary option for application and infrastructure development.

Investment in cloud service expertise is necessary

The majority of respondents feel that they currently have sufficient expertise in cloud services for their current needs. However, a significant portion (33%) believe that they do not have enough expertise for current requirements. This concern is also reflected in the survey's "Open Comments" section, which includes several questions about the use and development of cloud services. Organisations are concerned about which functions can be safely moved to the cloud environment and how to switch cloud service providers.

It is also noteworthy that a significant portion of cloud service development is outsourced. Over 60% of respondents outsource more than half of their cloud service development, and 16% have fully outsourced their cloud service development.

The need for expertise related to cloud services is growing as the use of cloud services is expected to increase in the near future. About half of the respondents feel that their organisation has sufficient necessary expertise either internally or through external sources. The other half report that they do not have sufficient expertise to meet future needs, and therefore, investment in capability is necessary, either by training their own staff or by acquiring expertise from partners.

Do organisations have sufficient cloud service expertise for current and future needs? (%)
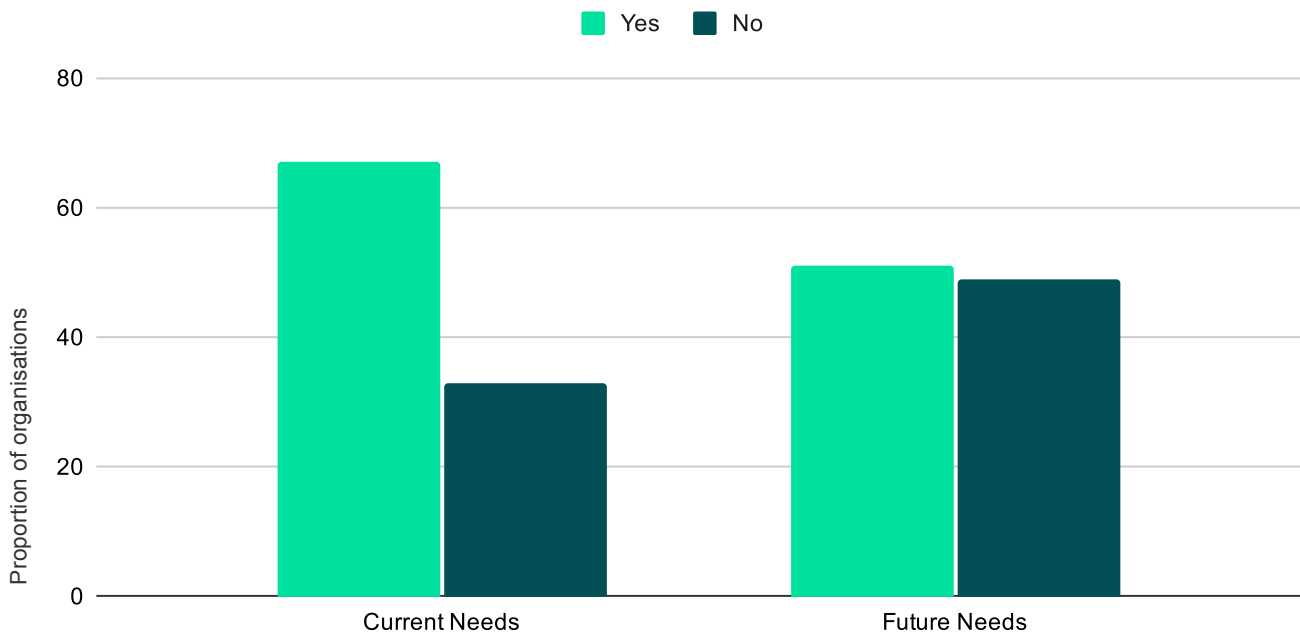
Risks are managed and broadly mitigated

From the perspective of emergency preparedness and organisational security, it is encouraging that the survey respondents generally have good risk management and preparedness measures in place.

Nearly two-thirds of the respondents have implemented security standards and practices for cloud service environments. Among organisations employing over 250 people, 81% have security standards and practices in place. For organisations with over 2,000 employees, 95% have implemented some form of security standard.

The survey did not look into which specific security standards the organisations use. Examples of security standards include ISO/IEC 27001, an international standard for information security management. There are also cloud-specific standards such as CSA STAR (Cloud Security Alliance's Security, Trust and Assurance Registry) or PiTuKri (Cloud Service Security Evaluation Criteria: "Pilvipalveluiden turvallisuuden arviointikriteeristö"). These standards help organisations ensure that the cloud services they use are secure and that data is properly protected.

All organisations that responded to the survey have functions that are important for Finland's emergency preparedness in some way. It is desirable to be as well-prepared as possible for exceptional situations, and to have robust information security practices in place. While the average score of the organisations that responded to the survey is good, there is still room for improvement.

Preparedness can also be achieved through means other than following security standards, and the majority have measures in place for preparedness: 87% of respondents have a plan for data recovery and system backup in the event of disruptions.

Does your organisation have security standards and practices in place for cloud service environments?

No
36.8%

Yes
63.2%

Does your organisation have a plan for data recovery and ensuring system continuity in case of disruptions?

No
13.2%

Yes
86.8%
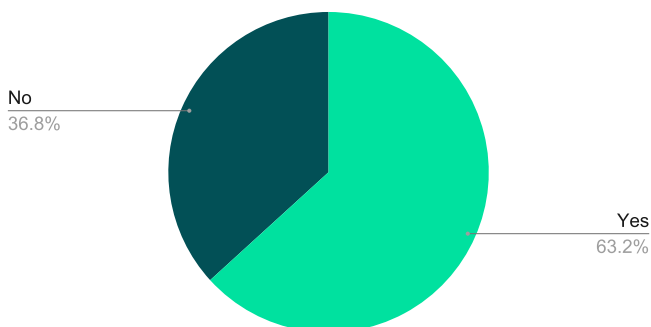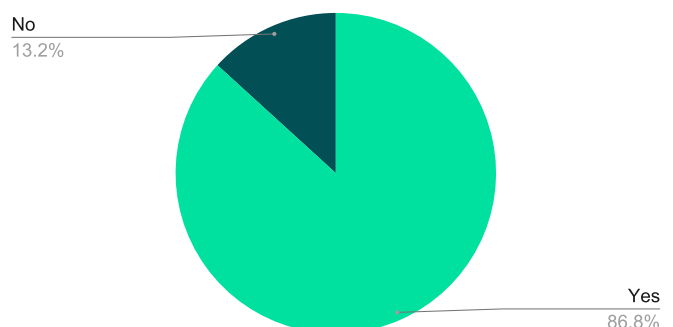
Use of cloud services in critical operations

This section examines the use of cloud services in critical operations. The definition of "critical operations" was intentionally left open to interpretation in the survey due to differences across industries and organisations.

The application areas mentioned on page 9 were defined as critical operations by at least one respondent. According to the survey, the most common critical operations are

ERP systems, core business systems, and financial management systems. However, there were also respondents who did not consider these to be critical operations. Therefore, there is considerable variance in how "critical operations" are defined.

What proportion of operations or application portfolio relies on cloud services? Differentiation between critical operations and all operations

Number of organisations

Application portfolio in cloud services
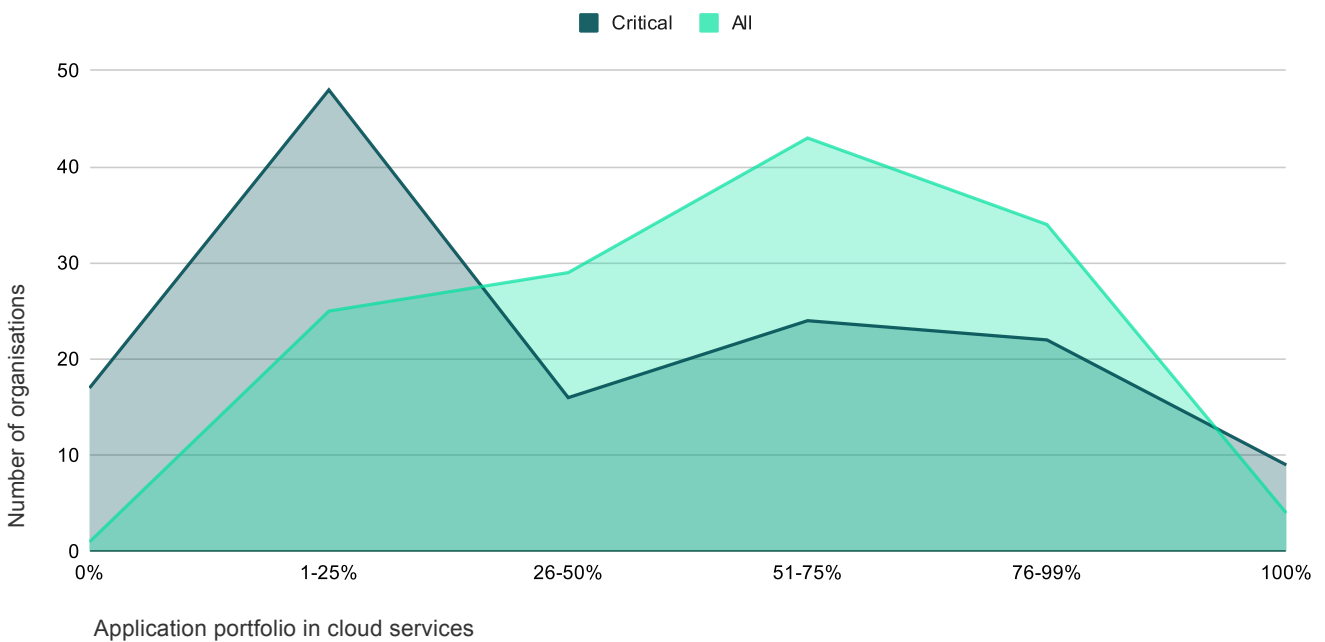
The use of cloud services in critical operations is more cautious compared to other application areas

The use of cloud services in critical operations is more cautious compared to other application areas: approximately 60% of organisations have more than half of their application portfolio in cloud services, but only 40% have more than half of their critical operations in cloud services. 12% of respondents have completely excluded their critical operations from cloud services. Additionally, about one-third of respondents (35%) exclude the majority of their critical operations (>75%) from cloud services. There are no significant differences between organisations of different sizes or industries.

This caution is also reflected in the attitudes towards the use of cloud services in critical operations: one-third of respondents have a different approach to using cloud services in critical operations.

Is the attitude towards the use of cloud services for critical operations different from the organisation's general attitude towards the use of cloud

Yes
34.3%

No
65.7%
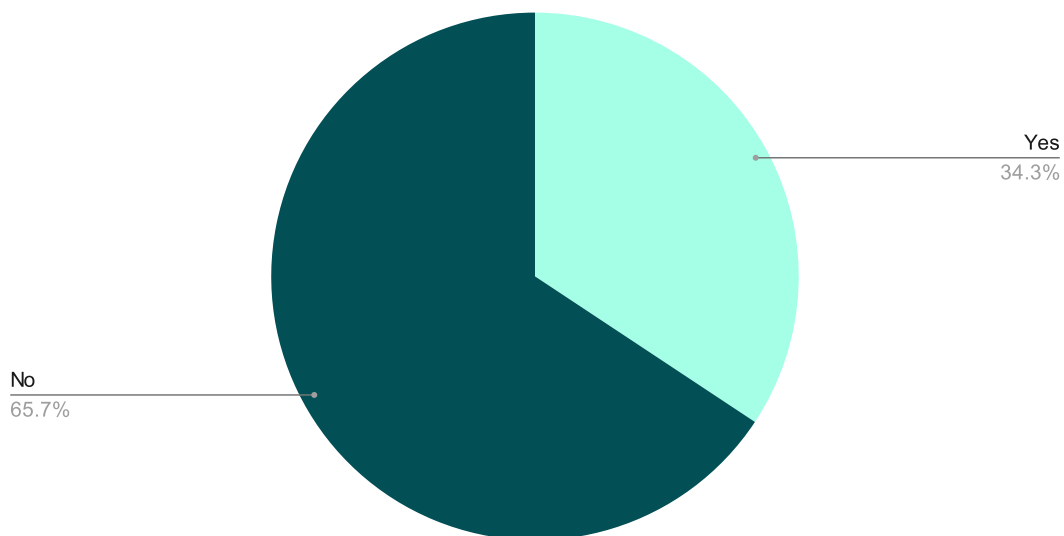
How does the attitude towards the use of cloud services differ for critical operations?

Organisations that have a different attitude towards the use of cloud services for critical and non-critical operations (i.e. organisations that answered "yes" to the question) all approach the use of cloud services in critical operations more cautiously. Below are the most common arguments respondents provided to justify their caution:

Continuity and reliability: For critical operations, there is a greater emphasis on the need for continuity and fault tolerance. The supplier's data centre infrastructure and backup solutions are crucial, whereas, for regular services, longer recovery times may be acceptable.

Risk management: There is significantly more detailed risk-based evaluation for critical operations. Usability and data security are crucial factors that may prevent certain functions from migrating to the cloud. Additionally, many organisations reported conducting carefully considered risk analyses before adopting cloud services.

Regulation and compliance: Ensuring compliance is stricter for critical operations. Critical operations for national security require particularly careful consideration regarding operational reliability, data security, and personal data protection.

Localisation and control: Many organisations aim to keep their critical operations within Finland's borders to ensure they function even in exceptional circumstances. They prefer to maintain control with on-premise solutions and avoid dependence on third parties.

Contingency plans: The need for contingency plans is emphasised in critical operations. Cloud services must be bypassable or replaceable to ensure continued operations in the event of disruptions.

Individual consideration: A few organisations highlighted that each critical operation is evaluated individually, and decisions on using cloud services are made on a case-by-case basis.

The same factors are emphasised by organisations with very few critical operations in the cloud environment:

The most common reasons why cloud services are not used in critical operations

Number of responses
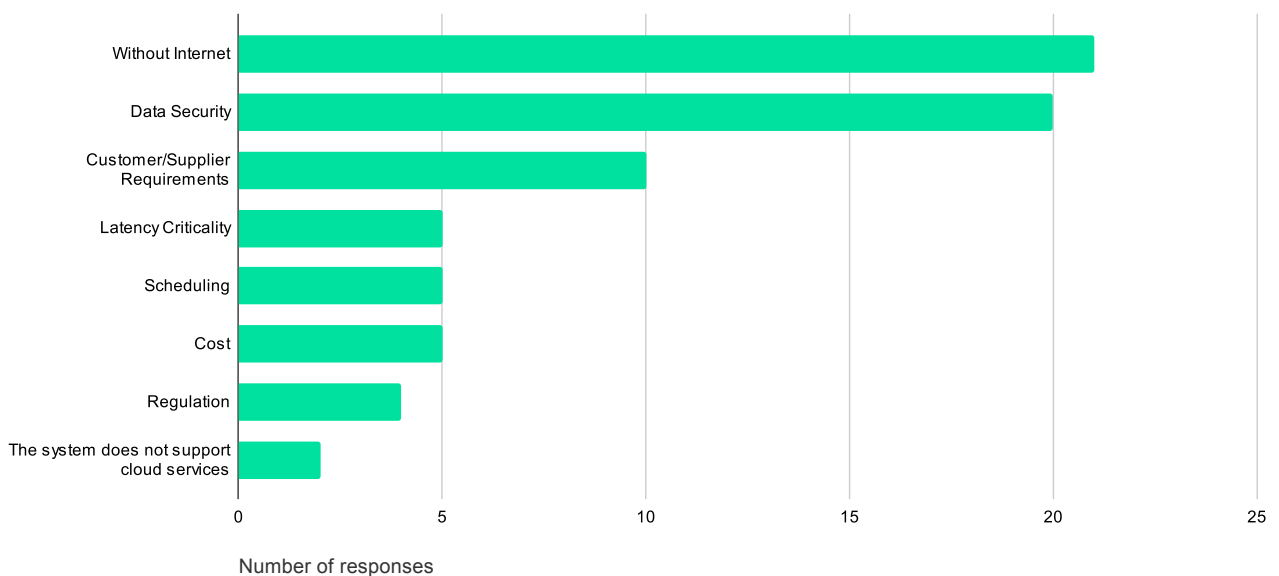
What types of cloud services are used in critical operations?

Most respondents use cloud services for some critical operations, especially in core business functions, although there is a small group of organisations where no critical operations are in the cloud.

The most popular public cloud platforms are Microsoft Azure and Amazon Web Services (AWS). SaaS and PaaS solutions are widely used, and in some cases, customised cloud services are employed.

Nearly all respondents who use cloud services for ERP do so as a SaaS solution. The most mentioned ERP solutions in the cloud are SAP Hana Cloud, Microsoft Dynamics 365, and NetSuite.

As noted in previous sections, data security, service availability, and continuity are the main concerns regarding the use of cloud services in critical operations. To address data security, respondents employ various measures such as encryption, identity management, and access control. Additionally, some respondents have contingency plans for their own systems in case the cloud service fails.

In the chart, "Other business" refers to software designed and built according to the company's unique business needs. These support the company's core functions, which distinguish it from its competitors and create added value for customers. These applications are not off-the-shelf but are customised around the company's unique business model.

Examples include: customer-specific e-commerce platforms, proprietary logistics and supply chain management applications, risk management applications, and algorithmic trading systems.

Which critical operations (including emergency preparedness-critical operations) rely on cloud services?
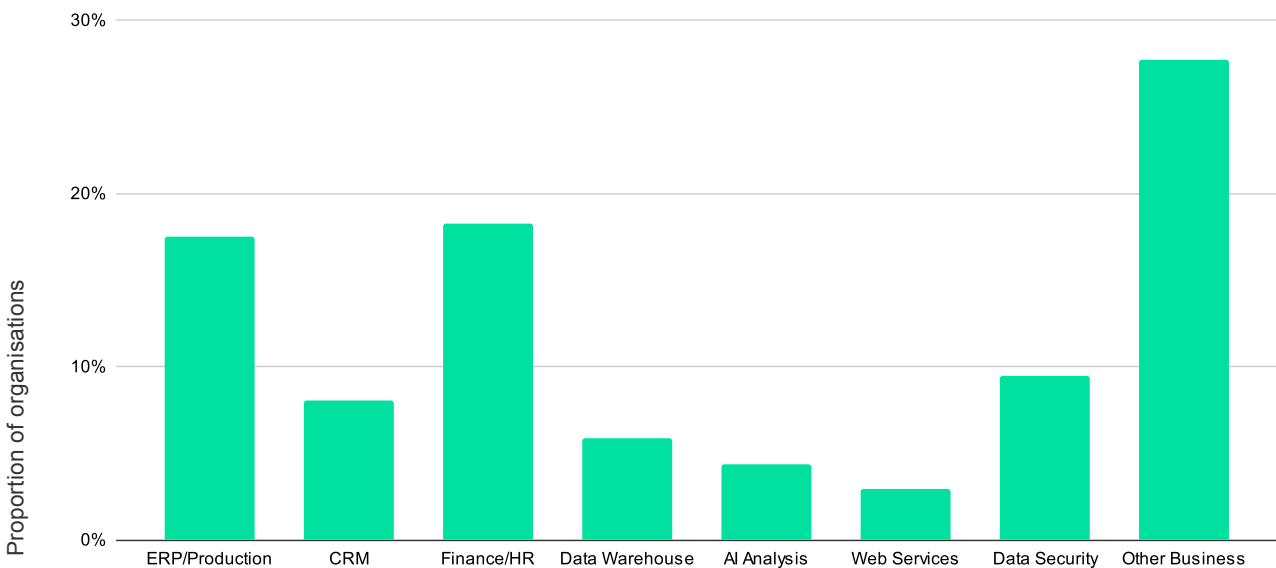
Service interruptions in critical operations are rare and temporary

Nearly half of the respondents have experienced service interruptions in their critical operations. These interruptions are typically brief (less than 2 hours) and occur "rarely" or "very rarely," according to respondents, usually about 1-2 times per year. In large organisations (> 2,000 employees), interruptions occur slightly more often (1-10 times per year).

The most common causes of service interruptions are network connectivity issues, outages from service providers, or power outages. Other recurring causes include equipment failures, various system faults, and human errors during updates, which lead to interruptions.

Three respondents reported that a cyberattack had led to a service interruption.

Have you experienced service interruptions in critical operations?

Yes
43.8%

No
56.2%
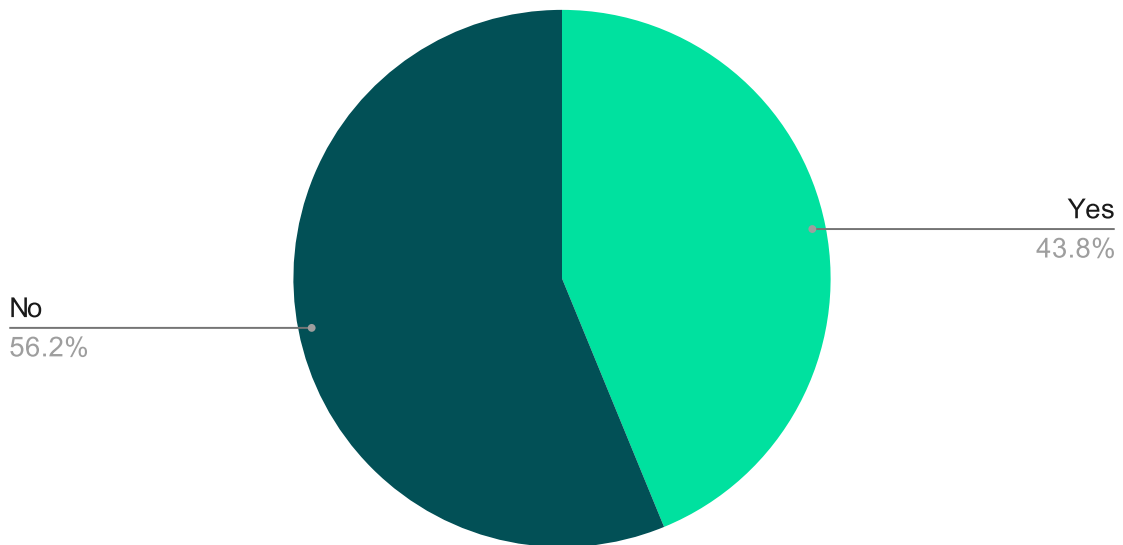
Respondents have remarkably good resilience to service interruptions

Over half of the respondents believe their organisation could endure a service interruption in critical operations lasting more than 24 hours, while a quarter could manage if the interruption stays under 24 hours. Only about 20% feel that interruptions in critical operations must be resolved within two hours.

Organisational resilience to service interruptions is impressively good. Fortunately, according to the survey results, interruptions occur rarely and typically last less than two hours – well within the tolerance levels estimated by most respondents.

There are minor differences in resilience among various industries, but they are not significant. The only notable exception is in the industrial sector, where one-third of respondents feel they can withstand a maximum service interruption of two hours.

How long do you estimate you could withstand a service interruption in critical cloud services?
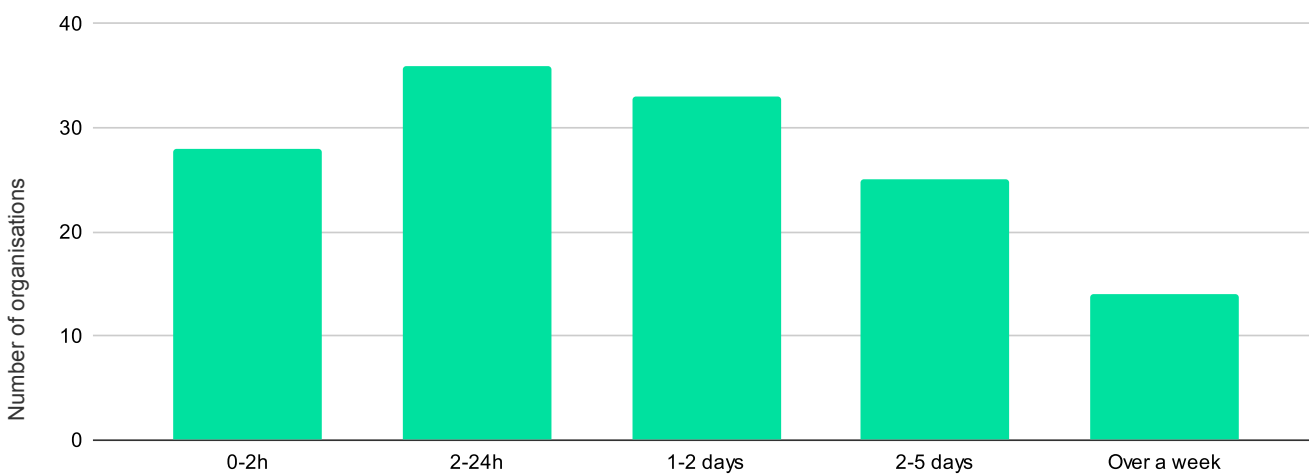
Cloud services & decision-making

Emergency preparedness is a significant factor when making decisions about the use of cloud services. 52% of the organisations that responded to the survey reported that the importance of emergency preparedness weighs more than 51% in their decision-making. For some, it is a decisive factor, while for others, different factors influence their decisions more. Some reported that emergency preparedness has not been considered at all in their decision-making regarding cloud services.

The significance of emergency preparedness in decision-making is lower among organisations that have moved very few or no critical operations to the cloud. On average, organisations that extensively use cloud services, including for critical operations, reported that emergency preparedness was carefully considered in their decision-making. However, there are exceptions in both comparison groups.

The responses are somewhat contradictory to the results presented in the previous section. The most significant reasons for not using cloud services in critical operations are ensuring operations during exceptional situations, such as internet connection interruptions, or concerns related to data security.

This discrepancy may be explained by the fact that operations are primarily implemented with on-premise solutions, and thus decision-making regarding the use of cloud services has not been relevant. In organisations that extensively use cloud services, decision-making about their use has naturally been on the management's agenda, leading to more thorough consideration of the matter.

How much does emergency preparedness weigh in the decision-making process for the use of cloud services
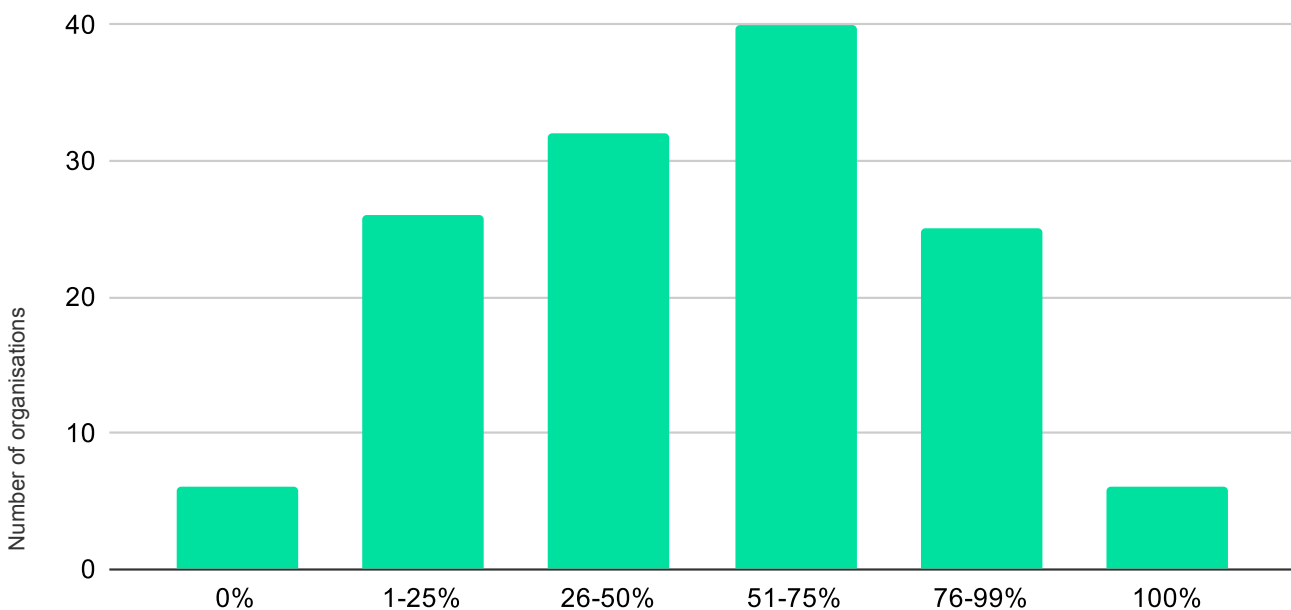
Other factors influencing decision-making

In addition to emergency preparedness and continuity management, other factors also influence decision-making. These include the benefits of cloud services pre-sented in the first section, such as ease of use, flexibility, user-friendliness, outsourced maintenance, cost benefits, overall architecture, and expertise.

On what basis are decisions made regarding the use of cloud services
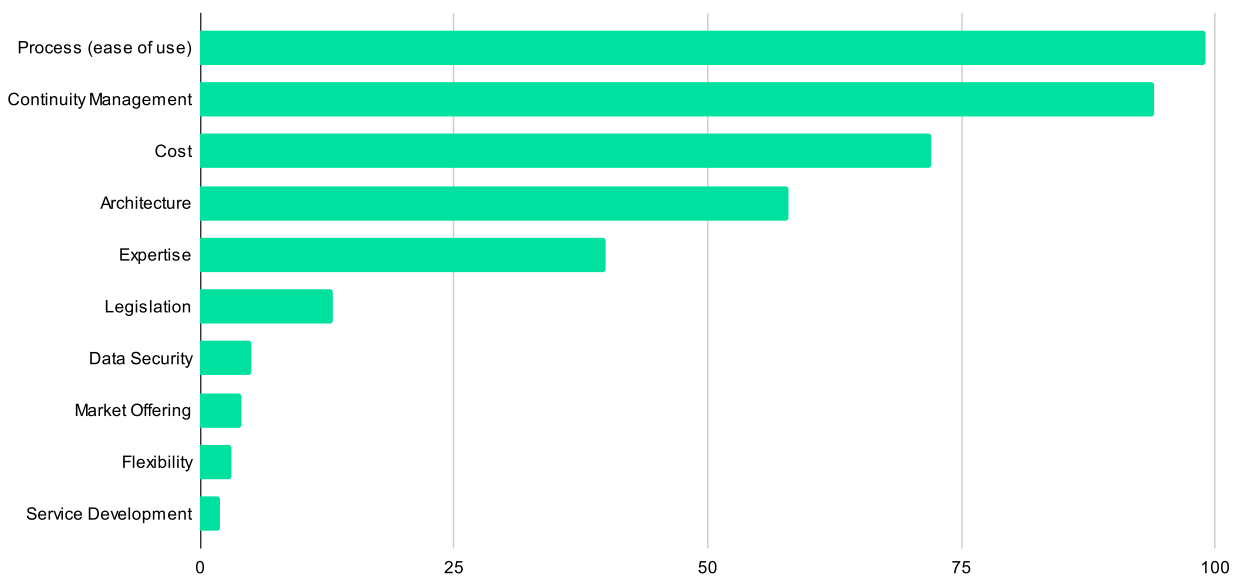
Multiple-choice question and open responses aggregated

Conclusions

The survey results reveal that the use of cloud services is widespread and will continue to grow. Along with the increasing use, the benefits and drawbacks of cloud services become more pronounced.

The respondents' organisations have a solid foundation for broader use of cloud services, but more attention must be paid to adhering to security standards in the future, and there needs to be an investment in expertise. Additionally, it is particularly important to consider aspects related to emergency preparedness and continuity management when adopting cloud services for critical operations.

As expected, larger organisations have more detailed processes for adopting, maintaining, and preparing for the use of cloud services compared to smaller organisations. Smaller organisations, in particular, could benefit from best practices in cloud services and technical comparisons of the most common service providers from an emergency preparedness perspective.

However, similar questions arose in the open responses regardless of the size of the organisation. This suggests that there is still room for improvement in the use of cloud services from an emergency preparedness perspective in organisations of all sizes.

The most common questions

- Which critical functions for emergency preparedness can be safely moved to the cloud?
- What are the limitations of using cloud services in emergency preparedness-critical operations?
- Which service providers or geographical areas should be avoided?
- Is there a national guideline or contingency plan related to emergency preparedness?
- How is the cloud service framework managed for emergency preparedness-critical systems? Is there a standard for this?
- How can users ensure that their data is securely "stored"?
- How easy is it to switch service providers, and what should be considered?

The Cloud Services Division within the Digipool of the National Emergency Supply Organisation will address these and other questions raised in the survey, and continue its work in promoting emergency preparedness awareness and sharing best practices.

Thank you to all the organisations that participated in the survey!

For more information:

Antti Nyqvist
Preparedness Manager
antti.nyqvist@teknologiateollisuus.fi

Appendices

Appendix 1: Terminology

Cloud services:
Cloud services refer to the provision of IT infrastructure, software, and data over the internet. They enable the flexible use of resources without the need for the user to own physical hardware. Examples of cloud services include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Compliance:
Compliance: Compliance refers to the adherence of an organisation's operations, processes, and practices to laws, regulations, and standards. It ensures that the company operates properly and meets all regulatory requirements, which may include data security, data privacy, and financial regulations.

Cloud First:
Cloud First is a strategy where organisations primarily use cloud services for the development of new systems and applications. The goal is often to enhance agility, scalability, and cost-efficiency compared to other IT solutions.

GDPR:
The General Data Protection Regulation (GDPR) is an EU data protection regulation that came into effect in May 2016 and has been applied since May 2018. It sets rules for the processing of personal data and enhances the protection of individuals' privacy.

Data security:
Data security refers to the methods and practices used to protect information systems and data from unauthorised access, damage, or alteration. It includes physical security, access control, encryption techniques, and security training.

Data privacy:
Data privacy refers to the protection of individuals' personal data and the proper management of its processing. The aim of data privacy is to ensure that personal data is handled lawfully, transparently, and with respect for the rights of the individuals concerned.

Appendix 2: Survey questions

Below are all the survey questions in order, including the response options.

How many people does your organisation employ?
Under 50, 51-250, 251-2000, Over 2000

What is your organisation's turnover?
Under 10 MEUR, 11-50 MEUR, 51-400 MEUR, Over 400 MEUR

Does your organisation have international business?
Yes / No

What is your organisation's primary industry?
Telecommunications, ICT & Software, Finance, Energy, Healthcare, Logistics, Media, Food Industry, Manufacturing, Water Supply, Trade & Distribution, Ports & Maritime, Security, Other (please specify)

Does your organisation have a cloud strategy, or is the use of cloud services addressed in other strategic documents?
Yes / No

If you answered yes to the previous question, what are the objectives of the cloud strategy? If you answered no, why not?
(Open response)

What experiences does your organisation have with the use of cloud services?
(Open response)

On a scale of 1-4, what is your organisation's attitude towards the use of cloud services?
Scale 1-4. 1 = Cloud services are avoided / 4 = Cloud services are recommended (Cloud First)

To what extent does your organisation's ICT (application portfolio) currently rely on cloud services?
0%, 1-25%, 26-50%, 51-75%, 76-99%, 100%

To what extent will your organisation's ICT (application portfolio) rely on cloud services in five years?
0%, 1-25%, 26-50%, 51-75%, 76-99%, 100%

How much of your ICT is restricted in a way that cloud services cannot be utilised?
0%, 1-25%, 26-50%, 51-75%, 76-99%, 100%

In what areas/application domains are cloud services used (excluding office services such as calendar, email, etc.)?
(Open response)

On a scale of 1-4, what is your organisation's attitude towards the use of cloud services in critical operations?
Scale 1-4. 1 = Cloud services are avoided / 4 = Cloud services are prioritised (Cloud First)

How much of your critical operations (including emergency preparedness-critical operations) rely on cloud services?
0%, 1-25%, 26-50%, 51-75%, 76-99%, 100%

Which critical operations (including emergency preparedness-critical operations) rely on cloud services?
(Open response)

What types of cloud services do you use in critical operations? What technology do you use and what processes are in the cloud? For example, ERP as a service (e.g., SAP Hana Cloud, Microsoft Dynamics), or in-house developed services installed in a public cloud, such as Google Cloud, AWS, or Azure.
(Open response)

If you do not use cloud services in critical operations, what is the reason?
(Open response)

Is the attitude towards the use of cloud services in critical operations different from the organisation's general attitude towards cloud services?
Yes / No

If you answered yes to the previous question, can you explain how the attitude differs?
(Open response)

What are the most important factors in the decision-making process for the use of cloud services? (You can choose multiple options)
Process (ease of use), Cost, Continuity management, Expertise, Architecture, Legislation, Other (please specify)

What factors have influenced your decisions?
(Open response)

In your estimation, what weight has continuity/emergency preparedness been given in decision-making regarding the use of cloud services?
0%, 1-25%, 26-50%, 51-75%, 76-99%, 100%

Do you feel that your organisation has enough expertise to meet current needs related to cloud service development?
Yes / No

Do you feel that your organisation has enough expertise to meet future needs related to cloud service development?
Yes / No

How much of cloud service development is outsourced?
0%, 1-25%, 26-50%, 51-75%, 76-99%, 100%

Does your organisation have security standards and practices in place for cloud service environments?
Yes / No

Are cloud services used in areas where data must be restricted to the EU region, e.g., GDPR content?
Yes / No

Does your organisation have a plan for data recovery and ensuring system continuity in case of disruptions?
Yes / No

Have you experienced service interruptions in critical operations (including emergency preparedness-critical operations)?
Yes / No

If you answered yes to the previous question, how many service interruptions have there been, and what were the causes?
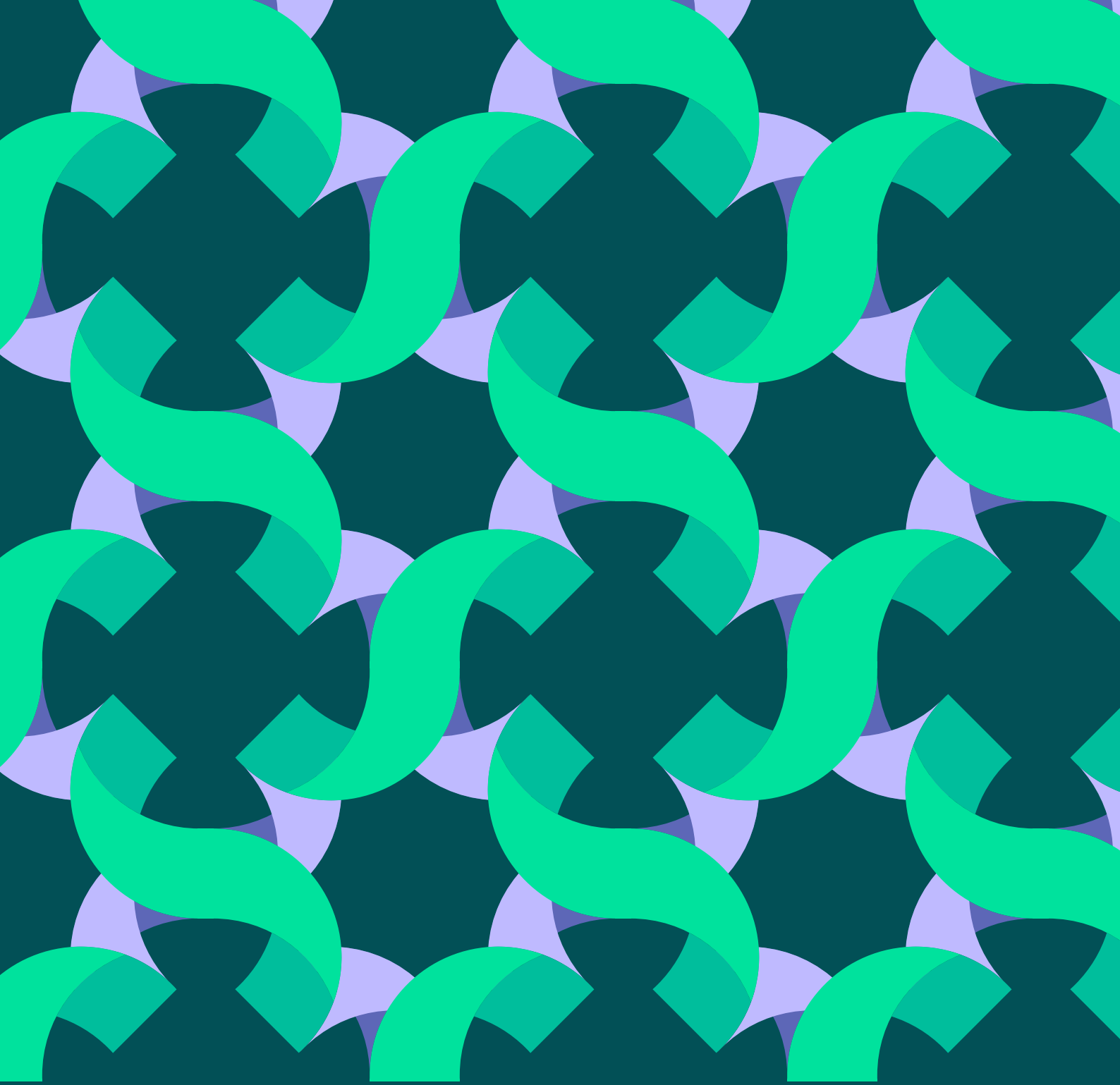(Open response)

How long do you estimate you could withstand a service interruption in critical cloud services (access or other disruption)?
0-2 hours, 2-24 hours, 1-2 days, 2-5 days, Over a week

Open feedback: What questions related to cloud services and emergency preparedness would you like answers to?
(Open response)

Huoltovarmuusorganisaatio
Digipooli