Cloud Security Report

2019
www.pwc.com

pwc

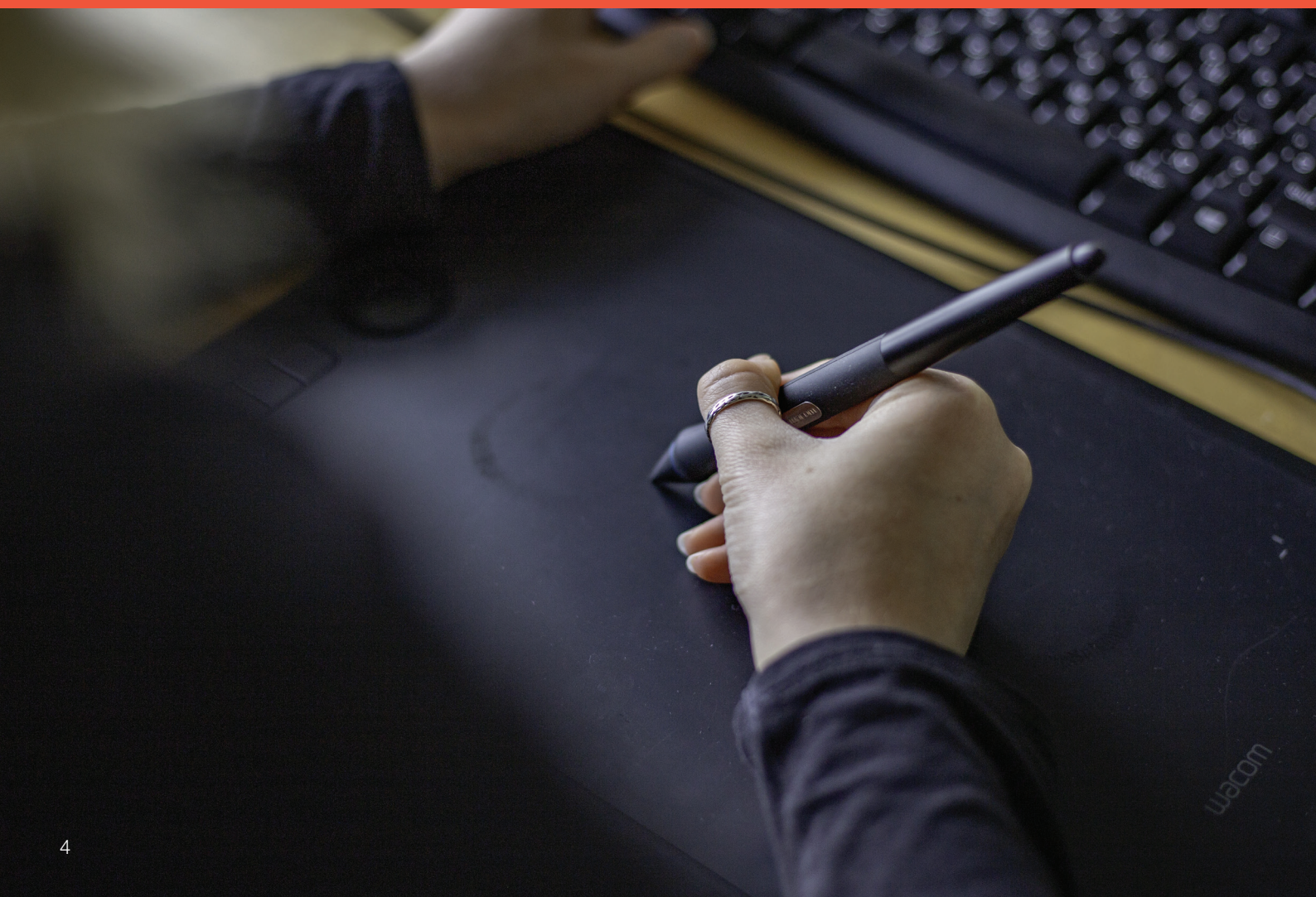
Content

Introduction

Fast adoption of cloud services, migration of traditional data centres to cloud systems, and development of new solutions with a ‘cloud-first’ approach is already resulting in discussions on such topics that were, only few years ago, exclusive to the academic level, or they were based on assumptions and estimations only.

While the technological advantages and disadvantages of transformation to cloud services can already be seen, and decisions between “Infrastructure as a Service”, “Platform as a Service” and “Software as a Service” are being taken based on rational and empirical evidence, cybersecurity questions are still considered something of a ‘Pandora’s box’. Opening this closed mystical box, even by just asking a direct question, can be scary.

We decided to replace myths and prejudices with facts, and we have conducted a survey.

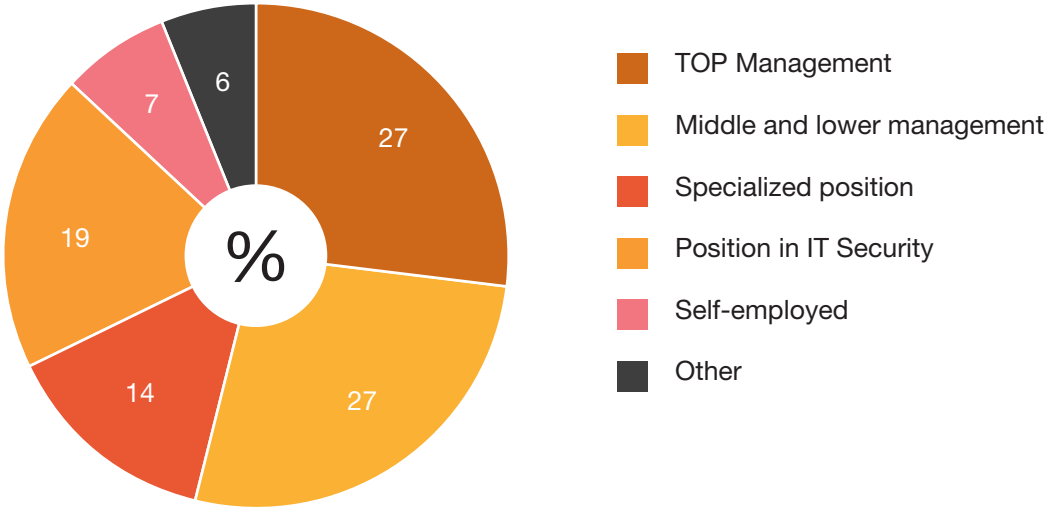


About the Survey

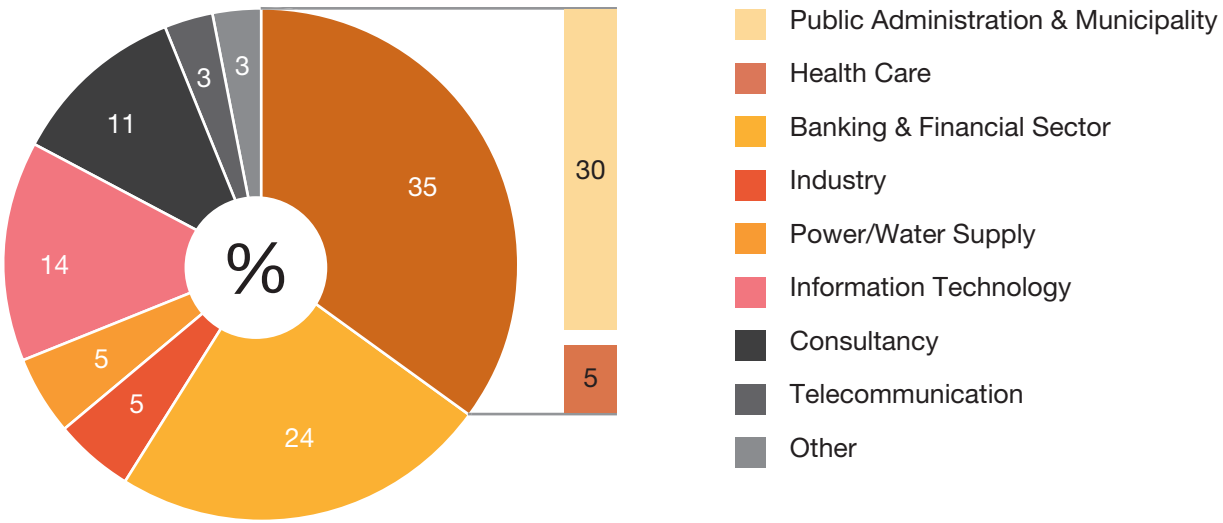
PwC, in cooperation with TATE International, has prepared the “Cloud Security in the Public and Private Sectors” survey. The main objective of the survey was to uncover what, according to our respondents, are the main security risks and benefits of cloud services compared to traditional (on-premise) infrastructure. Another objective of the survey was to discover how corporations are currently using, or planning to use, cloud services; which controls they have in place; and whether they are using standards aimed at cloud computing at all.

Data was collected at 3 occasions – ICT Management Academy, held by TATE International; Summer Soirée, held by the same organisation; and Business Continuity Forum, held by PwC. The main target group was managers. 102 respondents took part in the survey. Our respondents represent various branches of the public, as well as, private sector, with 55 % of them working at the managerial level.

Position



Sector

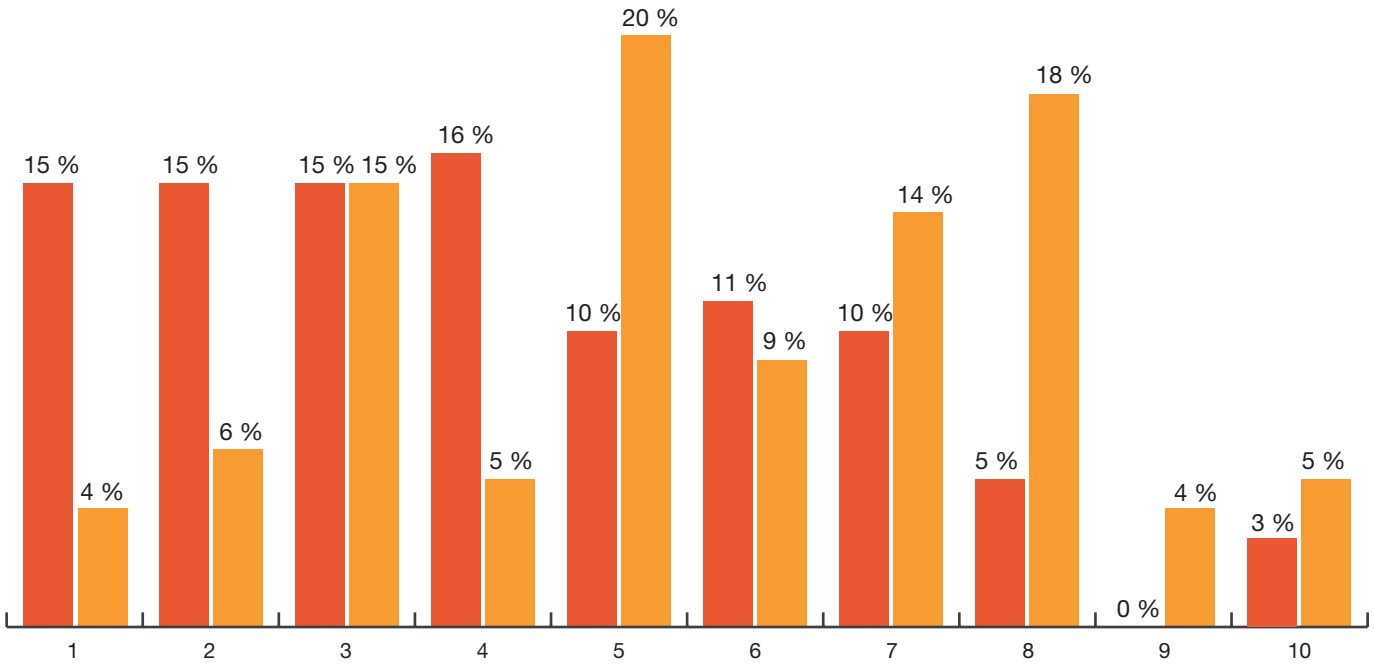


Governance

Current state vs planned usage of cloud services

To what extent do organizations currently use cloud services?

What is the long-term objective of using cloud services in the organizations?



1 – only on-premise infrastructure

10 – only cloud services

Cloud service usage can no longer be considered insignificant

Currently, traditional (on-premise) infrastructure is more widespread

A mere 25% of organisations are planning to continue using primarily traditional infrastructure

27% of organisations are planning to use mostly cloud services in the future

4,1

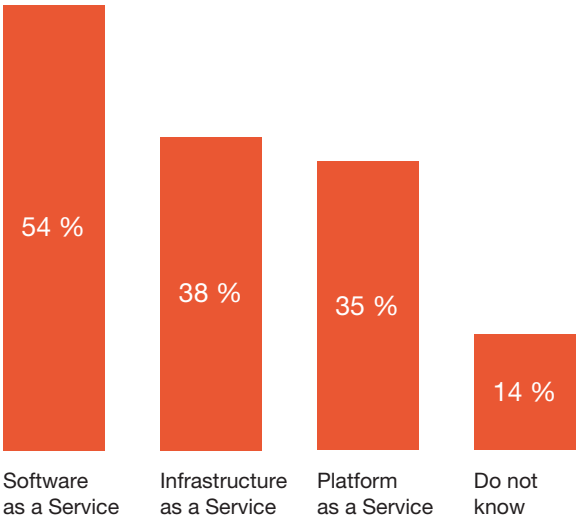
Average values
Current vs planned usage

5,6

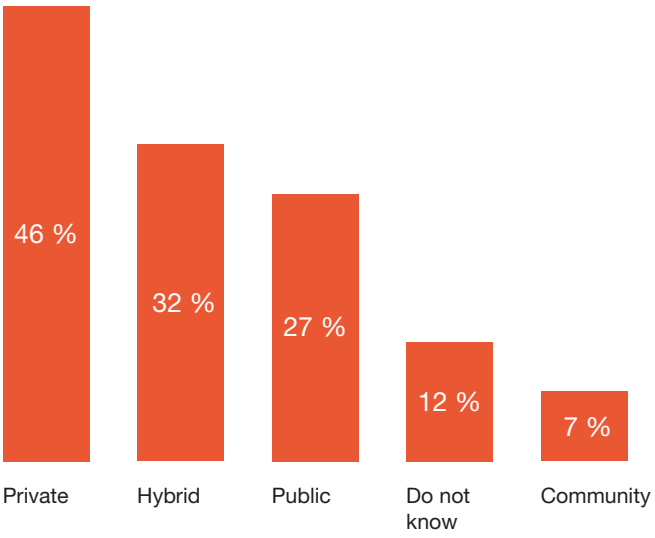
Cloud services will become even more popular in the future

Types of currently used cloud services

Distribution model perspective



Deployment model perspective



14%

or 12% of respondents do not know what type of cloud they use

Distribution model
Determines what components (HW, SW) are delivered as part of a service

Infrastructure as a Service (IaaS)
- Provider delivers IT infrastructure
- E.g. storage, servers, virtualisation, network components
- Client deploys its own operational system and applications

Platform as a Service (PaaS)
- Provider delivers IaaS + operational system, middleware, libraries for developers, etc.
- Client deploys its own applications

Software as a Service (SaaS)
- Provider delivers PaaS + applications, tools and data management

Deployment model
Determines how and to whom the services are delivered

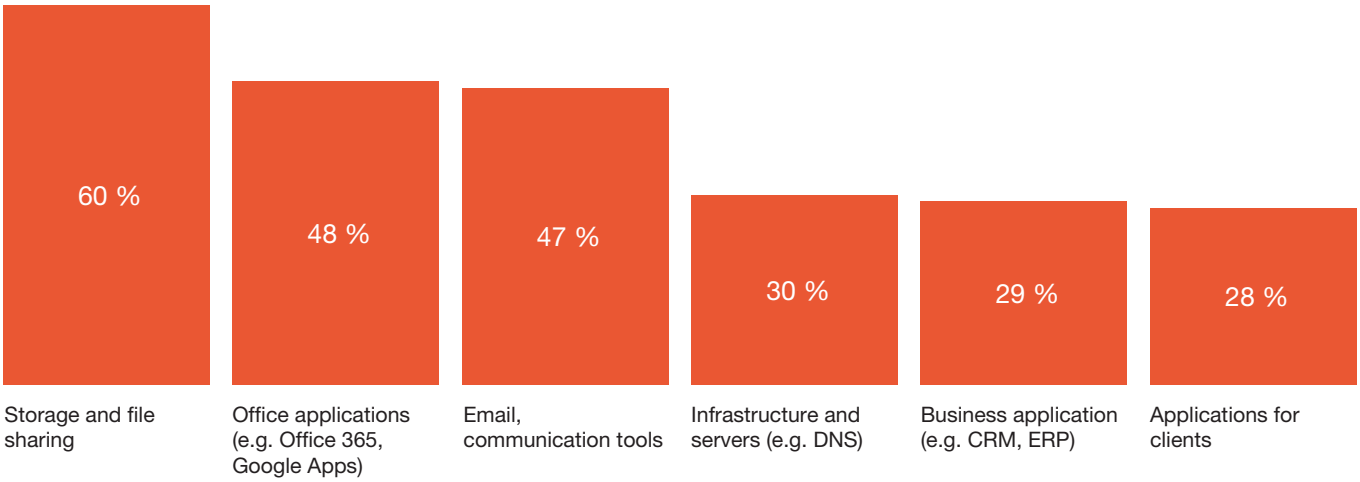
Public cloud
- The most widespread type of cloud
- Provided to the general public

Private cloud
- Cloud dedicated only to one particular client
- It is used for security reasons

Community cloud
- It is used by a particular group of people sharing common interests / objectives

Hybrid cloud
- Combination of 2 or more types of clouds
- Increasing trend in the usage of this type of cloud

Specific type of service / application perspective



Further answers:
Tools for IT services (e.g. administration, help desk) (22%), Cloud not used / Not possible to answer / Unwilling to answer (10%), Security tools (6%), Other (4%)

Users are using cloud services way more than they are aware of.
While using personal emails, internet storage, calendars, other online tools – in all these cases, they use cloud services.

What about PwC and Cloud platforms?

The main cloud platform deployed in PwC is Google Apps. Employees can use services such as Gmail, Google Drive, Hangouts, Meet, Calendar, Vault, Google Docs, Google Sheets, Google Slides, etc. PwC also uses Microsoft's cloud services (e.g. Azure, Power BI).

Besides these, PwC has deployed some additional cloud services, such as Salesforce (CRM system).

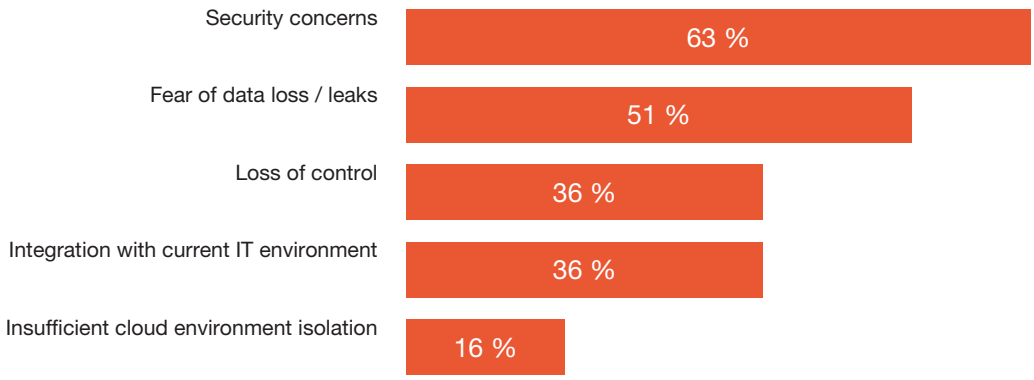
What about other, widely used, cloud platforms?

Among them, we can count mainly Office 365, providing a package of services comparable with Google Apps. Individual services are deployed to Microsoft Office applications, such as Word online, Excel online & PowerPoint online.

Clients are used to renting computing capacity from cloud providers. Platforms offering the most computing resources are Google Cloud Platform, Microsoft Azure, Amazon Web Services and IBM Bluemix.

Barriers to the adoption of cloud services

What limits and barriers does the adoption of cloud services bring to organisations / users?



Further answers:
Limited monitoring and logging (12%), Cloud not used / Not possible to answer / Unwilling to answer (11%), Performance concerns (6%), Other (1%)

Adoption of cloud services
Organisationally significant transformation
Transformation has its own phases and rules

Transformational framework used by PwC – PwC Transformation Strategy Framework
- Applicable to any IT change
- From strategy to operations
- Developed on the good practice basis

All phases are covered by activities:
- Program management office
- Change management

Individual phases – PwC Transformation Strategy Framework:
- Strategise & Assess
- Design
- Construct
- Implement
- Operate & Review

All phases are interconnected by quality control and evaluated to determine if the transformation is going in the right direction.
For more information, see the end of this Report.

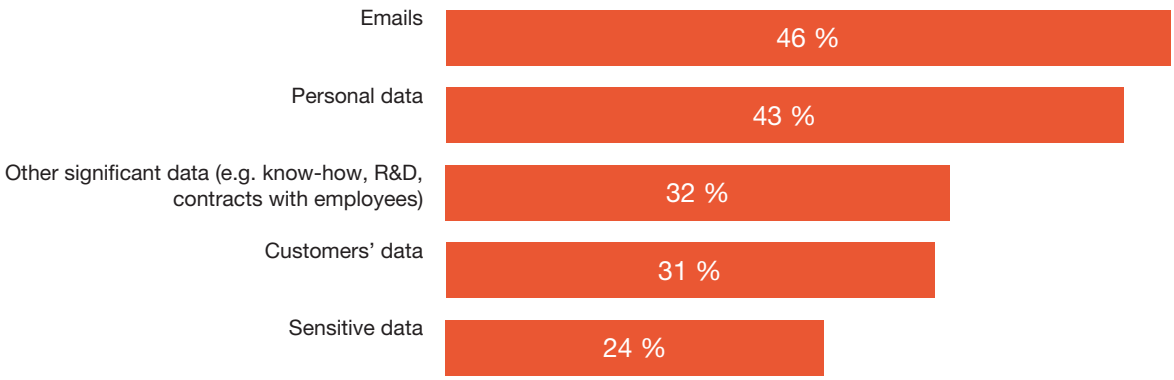
Transformation to cloud services is an extremely complex process, since everything about how IT resources are used in the organisation is being changed.

Local computing components are replaced with integrated components that are located outside the organisation and which are not exclusively controlled by the organisation.

Alongside this, new requirements on contracts, policies, procedures, data protection, controls, security settings and many more are set.

Data sent to the cloud environment

What data do companies send to the cloud environment?



Further answers:
Cloud not used / Not possible to answer / Unwilling to answer (16%), Other (9%), Health data (3%)

Perspective of a cloud services user:

- Sends emails containing personal and sensitive data
- Shares photos on Facebook and Instagram
- Uses Dropbox, Google Drive or OneDrive to store documents
- Uses application to remember passwords (sometimes also debit card numbers)
- Sends photos via mobile applications to a spouse (including intimate photos)
- Forwards work-related data to a personal email / stores work-related data on a personal internet storage

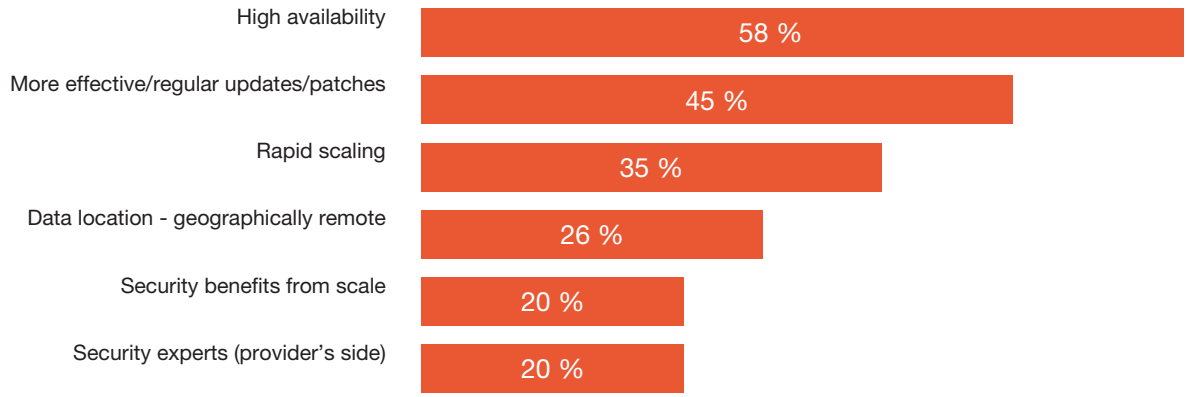
It is important to know that the user is hardly ever aware of the following facts:

- Where his data is being stored
- Existing number of copies
- How the data is being secured
- How easy / difficult it is for an attacker to hack a service provider and steal data
- What are the legal regulations of the state where the data is stored

Security, Risks

Security benefits of cloud services

What security benefits do cloud services bring?



Further answers:
Strong security features – providers' reputation is determined by the security of the services they are providing (15%), Cloud not used / Not possible to answer / Unwilling to answer (12%), Application and network (6%), Other (3%)

47%

Actualisations, patching

These processes are usually secondary to operational and business priorities and they need to fit into a specific maintenance window. In the case of cloud services, customers do not need to maintain these processes, since providers take care of it.

Rapid scaling

Cloud services enable customers to gain more computing capacity quickly. From the security perspective, this can become automated, e.g. for Denial-of-Service types of cases.

35%

26%

Data location – geographically remote

Data is usually stored in more copies in geographically remote data centres. In case of a breakdown of one of them (e.g. natural disaster) and consequent destruction of all the data stored there, only the data in the one centre will be lost; meaning permanent data loss will not occur, since there are other copies in different data centres.

Security benefits from scale, Security experts

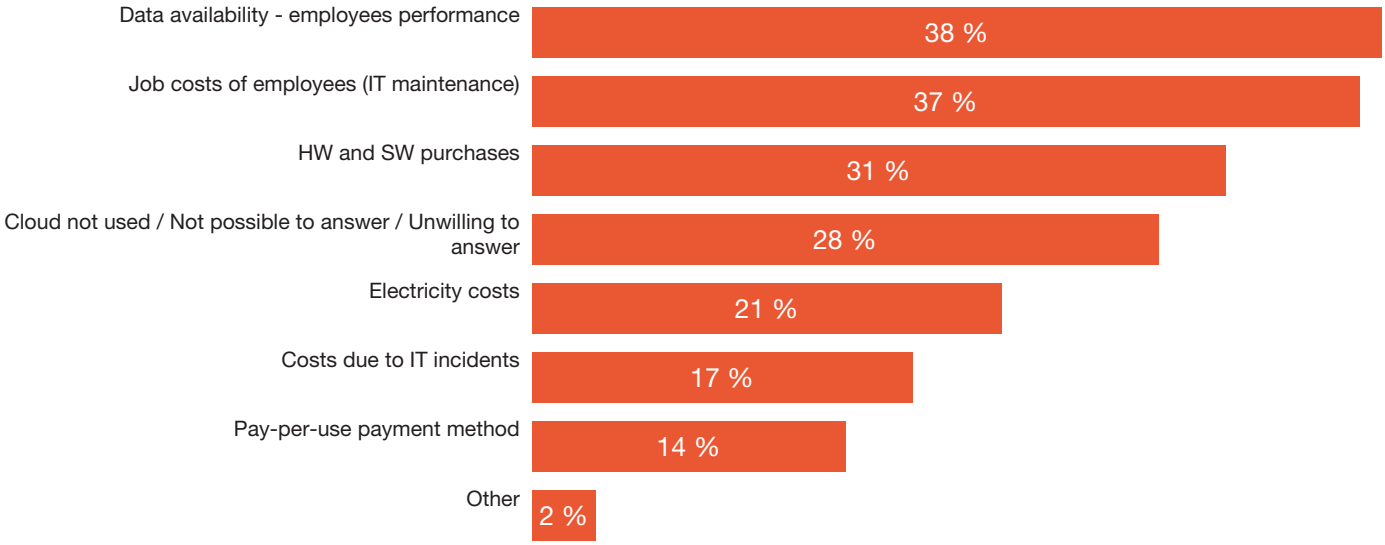
Cloud products offered by Cloud service providers are secured way better than IT resources in traditional organisations. Moreover, cloud service providers usually employ more security experts, who are directly responsible for the services' security.

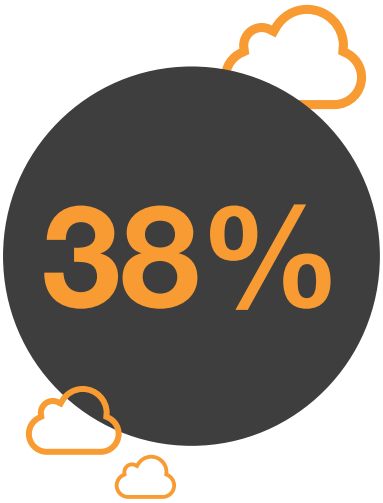
20%

Cloud service providers are aware of the interdependence between their reputation and the security of their services, which is typical for intangible service providers.

Financial benefits of cloud services

In what areas do companies see the highest financial savings that the use of cloud services bring?





High data availability influences cloud service performance. Incident-free operation of cloud services is dependent on the data centres' quality, where the data is being stored. Evaluation of the data centres' quality is based on Tier qualification.

Data Centre Tiers

Classification of data centre infrastructure
Quality of systems, countermeasures against external factors, security and others are evaluated

Tier 1 – Basic infrastructure, absence of redundant deployment, cooling the majority of IT equipment.
- Available for 99,67 % of the time – acceptable breakdown of 28,8, hours per year.

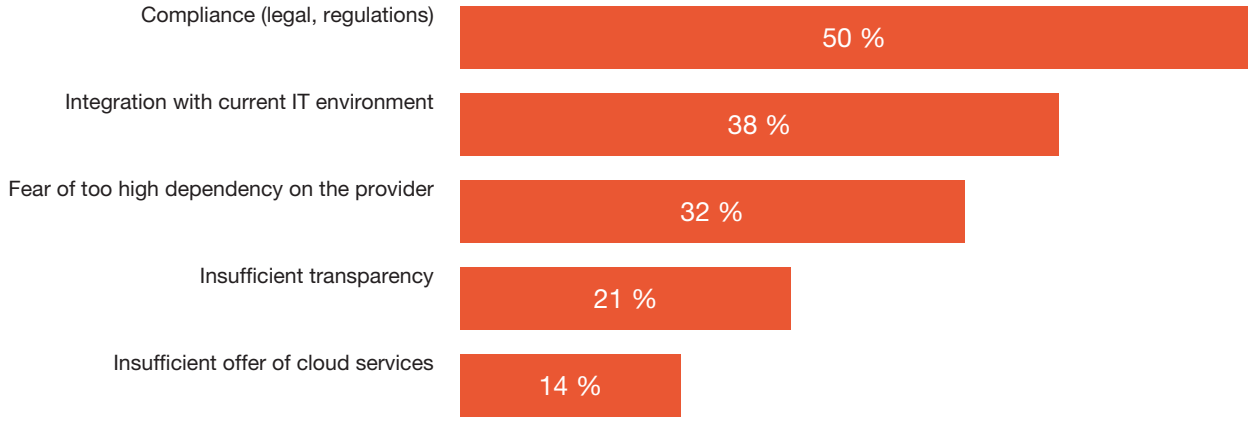
Tier 2 – Redundancy of selected components is added (but not deployment and cooling).
- Available for 99,74 % of the time – acceptable breakdown of 22 hours per year.

Tier 3 – Redundancy of deployment, cooling and other selected components is added.
- Available for 99,98 % of the time – acceptable breakdown of 1,6 hour per year.

Tier 4 - Redundancy of all components. Failure of any component of the data centre does not influence the operation of the system / services at all (fault tolerance).
- Available for 99,99 % of time – acceptable breakdown of 0,8 hour per year.

Security constraints of cloud services

What do organisations consider as security threats that are relevant to cloud services?



Further answers:
Cloud not used / Not possible to answer / Unwilling to answer (14%), Insufficient knowledge (12%), Finance (12%), Insufficient adjustment of cloud services (12%), Availability (7%), Other (2%)

What is our experience? What are the key issues of our clients?

Currently, many organisations are scared of **outsourcing regulations**, which influence cloud services as well.

Among the most regulated is the **financial sector,** and critical state infrastructure.

Common problem of cloud service integration is **identity management,** in particular the federation of the identities of the cloud services and systems of our clients.

Cloud service clients need to have enough trust in the service **provider,** since data protection will no longer be in their exclusive competency.

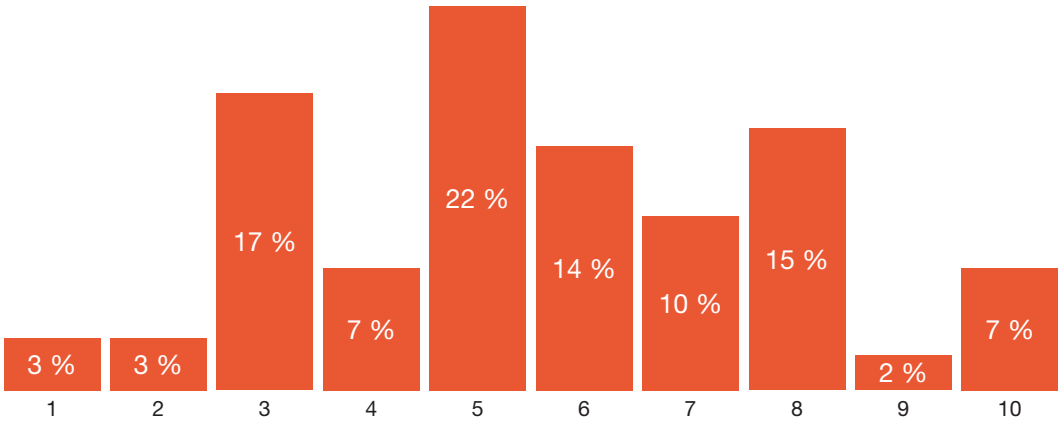
Federation of identities, Identity as a Service

Federation of identities is a principle that enables the clients' employees to access cloud services with the same login information that they use in the internal systems.

Federation of identities is a common part of services, known as Identity as s Service, which offers capabilities and options on how to manage identities in organisations. A common part of Identity as a Service is the Single Sign-On principle, which allows for a unified login to all systems in the organisation, including cloud services.

Security constraints – traditional infrastructure vs cloud services

Do you consider security risks to be linked more with cloud services or traditional on-premise infrastructure?



1 – traditional infrastructure
10 – cloud services

5,57
Average value from the figure

Organisations consider security risks to be linked more with cloud services. The difference, however, is not significant.

Doing a risk analysis is always essential when assessing the current state and correct settings of security controls

Comparison of cloud services risk analysis with traditional on-premise systems risk analysis

Other controls
- E.g. only selected data is shared to cloud services

Other measures
- E.g. implement rules on acceptable use of cloud services in the organisation

Other catalogues of threats, vulnerabilities and assets
- E.g. Cloud Computing: Benefits, Risks And Recommendations For Information Security published by ENISA

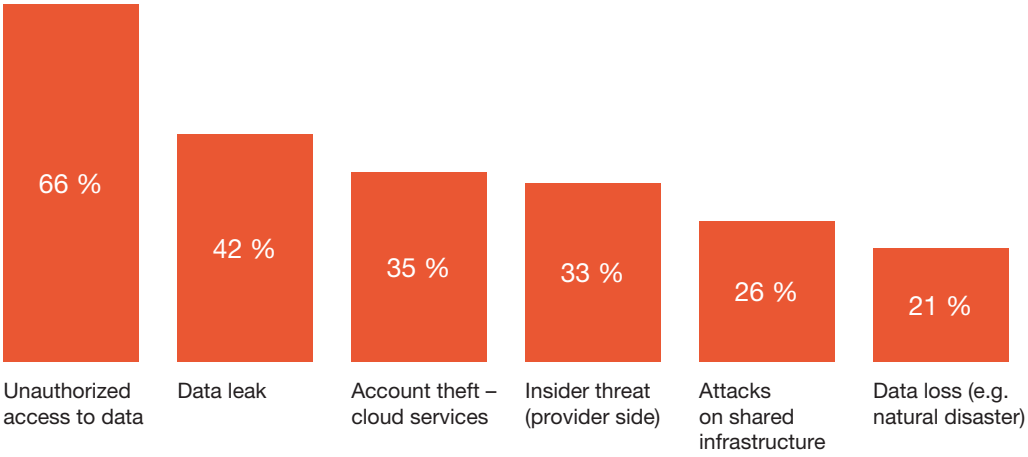
Other risk scenarios
- Published in the above-mentioned publication

Other approaches
- E.g. the need to include security concerns on the side of the service provider

Other components
- E.g. include special standards, legislation, migration process

Security constraints of cloud services

What do organisations consider security threats relevant to cloud services?



Further answers:
DoS attack (11%), Malware detection (10%), Cloud not used / Not possible to answer / Unwilling to answer (9%)

TOP 12 cloud computing threats according to Cloud Security Alliance (CSA)

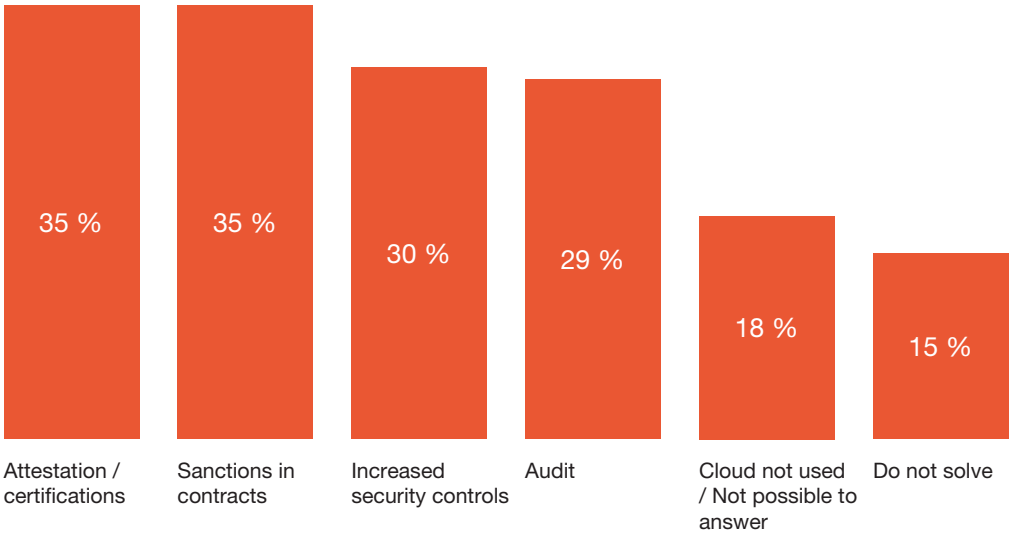
1. Data leakage
2. Insufficient identity management, login information and access management
3. Unsecured interface and API
4. System vulnerability
5. Account theft
6. Insider threat
7. Advanced Persistent Threat
8. Data loss
9. Insufficient Due Diligence
10. Misuse, criminal use of cloud services
11. Denial of Service
12. Shared technology vulnerability

Source: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

Security Controls & Countermeasures

Data security in cloud

How do organisations react to the fact that the providers partly control the security settings?



What do different security confirmations mean?

Assurance
- General confirmation about the particular state of the environment, usually issued in the form of ‘reasonable’ or ‘negative assurance’
- The certifying party issues confirmation that there is no indication that the reported status of the environment is not true

Audit
- Specific form of confirmation, generally connected with a statutory (financial) audit confirming the validity of the final accounts
- Audit can also be conducted in accordance with a specific standard

Attestation
- Written confirmation about the test conducted
- Term without an exact definition in international audit standards

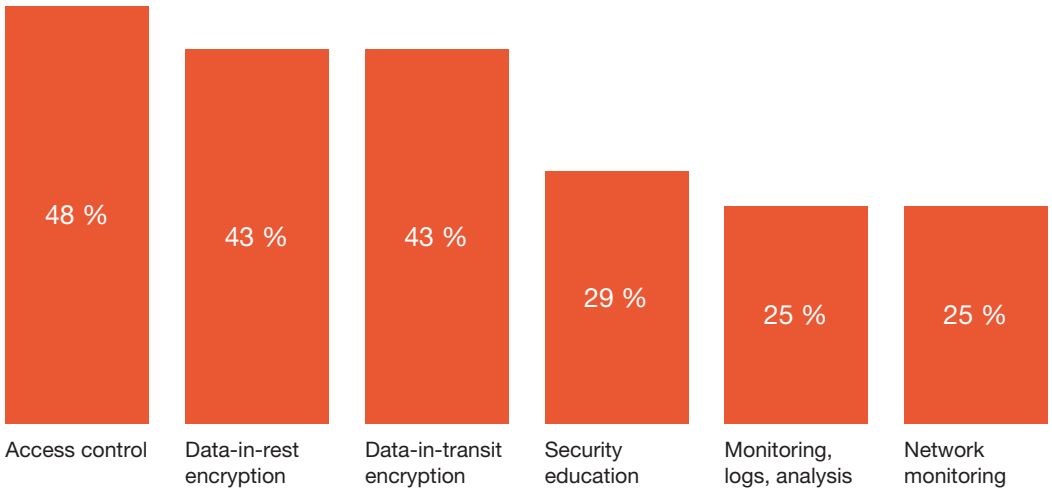
Certification
- Confirmation that the current state of the environment is in compliance with an established standard
- E.g. the family of ISO/IEC 27000 standards

Service Organization Controls
- Introduce a specific form of confirmation about the compliance of controls in place in organisations in our supply chain (IT outsourcing)
- The number of SOC report (SOC 1; 2; 3) indicates the area which is covered by the report and to whom is intended

Accreditation
- Superordinate party’s consent to use a specific operational system (or its object) in the environment

Security controls and countermeasures of cloud services

What cloud service security controls and counter measurements are currently being used (planned to be used) in the organisations?



Security configuration of cloud services is crucial

The right configuration of cloud services prior to their operation, especially in terms of security, is very crucial. In this way, usage of the service is optimised and clients are protected against threats to services with predefined settings.

Examples of security configurations that should not be omitted:

- Set-up strong authentication for users
- Set-up multi-factor authentication for administrators
- Set-up access privileges for specific roles/users/groups
- Set-up appropriate data classification and relevant security measures

Security incident

Case study: Hotel chain – data leak

Data leak of more than 600 clients of this Hotel chain – names, credit cards numbers, email addresses, passport numbers, etc.

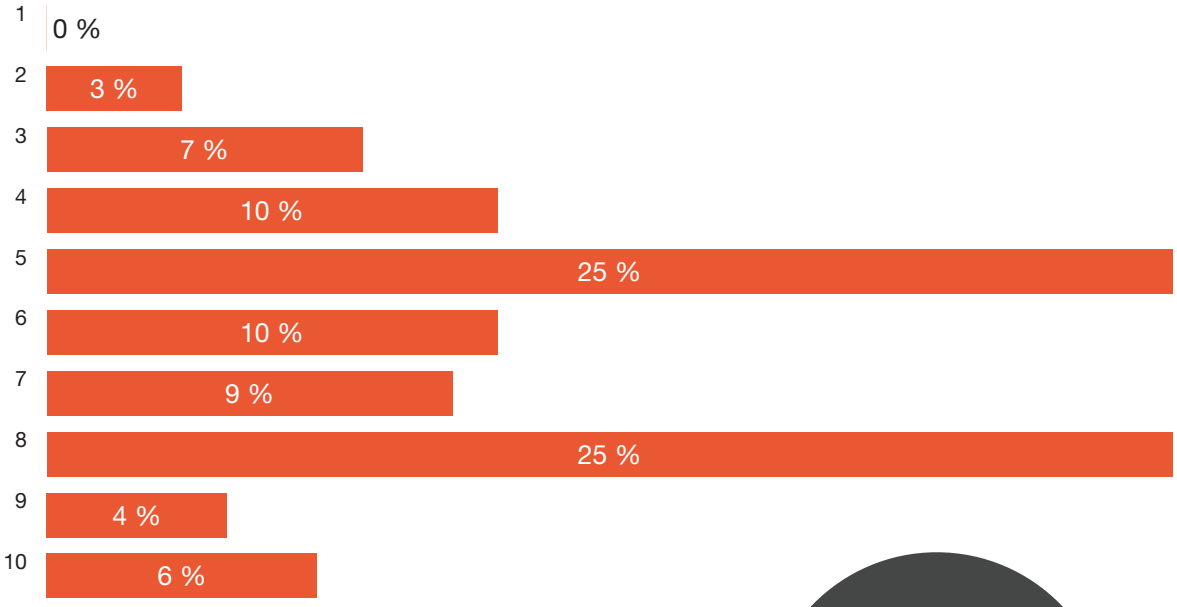
Security tools detected unauthorised access to the database in 2019; however, the attacker had been present in the system since 2013.

Attacker managed to hack the booking database via the hotel reservation system which is freely available on the internet. Access to the database was not secured enough and, moreover, activity inside the database was not monitored properly.

Among measures to limit possible data leaks we can find, for example, DLP and PAM solutions, threat hunting, access data controls, regular revision of security measures.

Sufficiency of security controls and measurements of cloud services

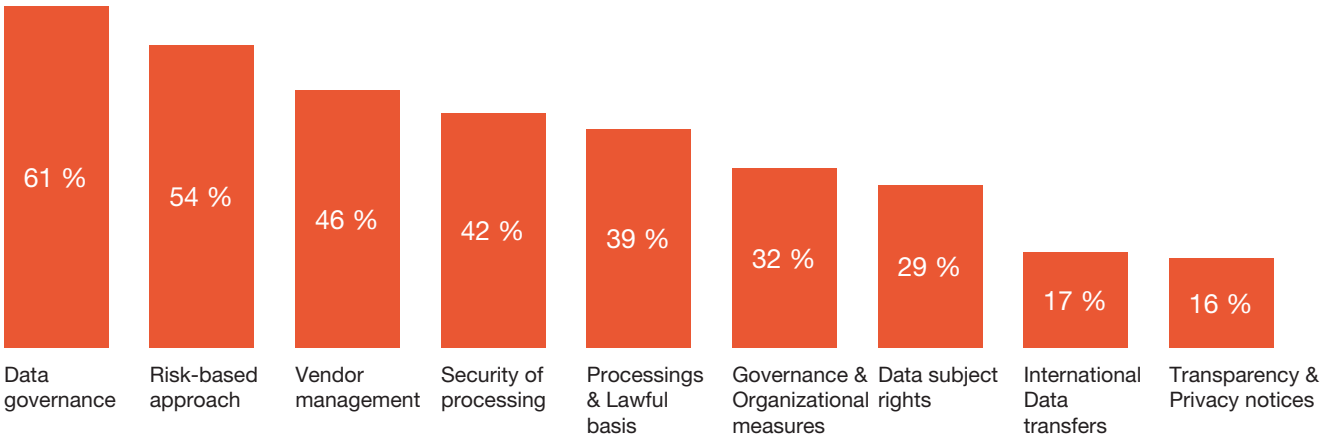
Do organisations consider the implemented cloud service security controls and measures to be sufficient?



1 – Insufficient
10 – Sufficient

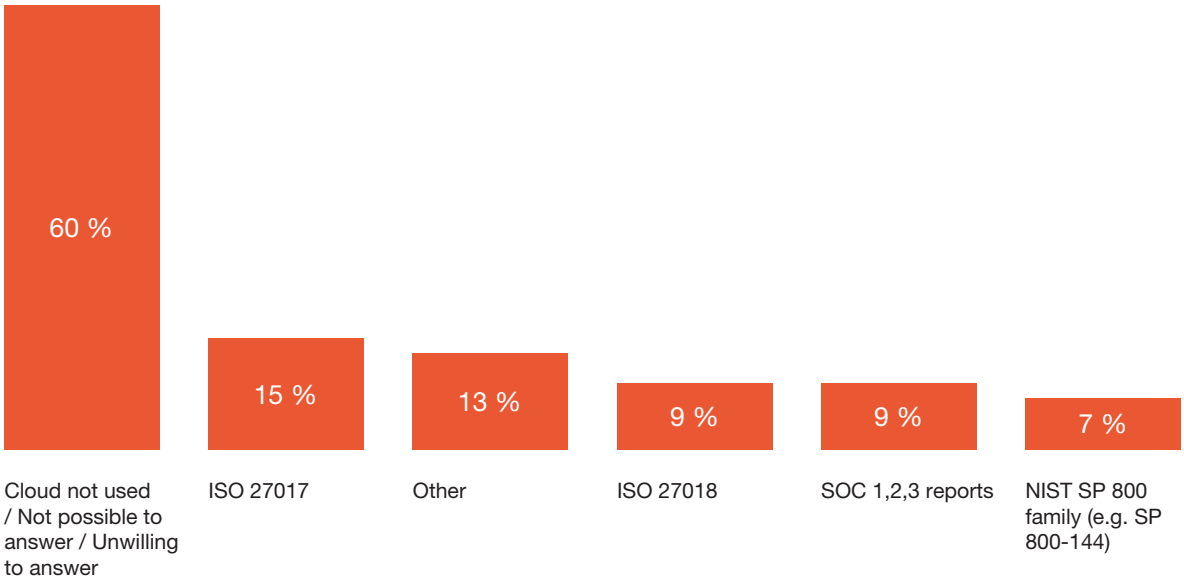
Personal data protection

Personal data protection and compliance with regulations, such as GDPR, is becoming a standard and inseparable part of the cloud security strategy. Locating data centres outside the EU makes it necessary to implement additional measurements. The number of companies that were not able to fully implement all the measures can be found below.



Security standards of cloud services

What specialised cloud computing standards do organisations use?



Example of security standards and controls

- **ISO/IEC 27000 family** – Security standards issued by the Organisation for Standardisation, effective primarily in Europe.
- **NIST SP 800 family** – Security standards primarily used in the USA. Standards are linked to American legislation.

- **ISO/IEC 27017** – ISO/IEC 27002 security standard extended about cloud service specifications. It covers reviews of providers and users of cloud services.
- **ISO/IEC 27018** – Extension of the ISO/IEC 27002 security standard. It is specialised in protecting individually identified information on public clouds.

- **SOC 1 report** – Review of financial reporting, targeted on audits of financial records, 3rd party report (limited distribution).
- **SOC 2 report** – Review of IT environment, data security, data processing, 3rd party report (limited distribution).
- **SOC 3 report** – Review of IT environment, data security, data processing activities, public reports (unlimited distribution).

Publicly available data on compliance with security standards

Some organisations publish information on compliance with various standards, legislation, etc.

E.g. Amazon Web Services (AWS) – https://aws.amazon.com/compliance/programs/

PwC Services

PwC services offer

PwC Cloud Transformation Services

Strategy & Assess

- Analysis of cloud security risks, assessment of current cloud security measures and processes
- Benchmarking of cloud security maturity
- Identification of all gaps to remove/all areas to improve related to cloud services
- Assessment of compliance with ISO/IEC 27017, 27018
- Definition of target operating models
- Definition of transition roadmaps, timelines and supporting prioritised business cases

Design

- Design of possible solutions, cloud security measures and processes
- Identification of key cloud services to onboard
- Development of a detailed transition plan
- Selection of a cloud service provider (support in RFI/RFP process)

Develop

- Development of cloud security processes, tools, frameworks, policies and other deliverables
- Analysis of security development lifecycle in cloud (both Agile and Waterfall)
- Security architecture review in relation to cloud services
- Security assessments of cloud service providers and contracts (i.e. due diligence)

Implement

- Implementation of cloud security processes, tools, frameworks, policies and other deliverables into the company environment
- Implementation of cloud service governance
- Delivering management training and workshops to understand the specifics of cloud security
- Quality assurance over onboarding and ensuring a smooth transition
- Day 1 readiness for cloud implementation (dry runs, tabletops, full-scale exercises)

Operate & Review

- Continuous monitoring of cloud security, integration to SOC monitoring
- Regular security audits, vulnerability assessments and architecture reviews
- Advisory on cloud identity management solutions (digital identity trust, federation)
- Providing management reporting that supports top management decisions within the cloud security area
- Setting steps and actions related to cloud services to ensure business continuity
- Involvement of the forensic department in the event of an investigation
- Assessment of IT environment/cloud services to provide SOC2 Report

Applicable for all phases of Transformation Framework:

1 Programme Management Office — Providing expertise in IT Project management

2 Change Management — Managing all changes within the company related to cloud security transition

3 Quality Control/ Assurance — Including independent attests to provide assurance in service organizations

Acknowledgements

To begin, I would like to thank all of you who have helped us by answering our questions. Our survey would only have very limited or even no data at all without your insights and answers. Furthermore, without your help, we would not be able to come up with any conclusions at all and outputs would possibly stay just as speculations and estimations.

Cooperation with TATE International was a pleasure for us and we are grateful for your support, which was essential for the realisation of this survey.

We would also like to thank everyone for taking the time to read this report. We hope that you found the time dedicated to reading it both interesting and well spent. Your interest in cybersecurity is a source of hope for the future security of our society and for the development of the cybersecurity industry as a whole.

Contact us

Petr Špiřík

Petr works as a Director in Cyber & Privacy. He has more than 15 years of experience in the information and cyber security area. Petr has led a number of teams in the PwC global structure and he also worked as a regional CISO.

petr.spirik@pwc.com
+420 774 191 101

Michal Wojnar

Michal is a cofounder of the Business Continuity Forum in the Czech Republic. He specialises in information security and crisis management. He has more than 9 years of experience in this field.

michal.wojnar@pwc.com
+420 724 726 166

Michal Čábela

Michal is the leader of Cyber Resilience Team. He has more than 10 years of experience in information security, SW development and IT consultancy, with the main focus on the area of cyber security.

michal.cabela@pwc.com
+420 775 214 115

Martin Zbořil

Martin works as a senior consultant in the Cyber & Privacy. His main specialisation is cyber security from the technical and process perspective. His post-gradual studies have been dedicated to cloud security problematics.

martin.zboril@pwc.com
+420 734 783 921