EuroCloud
TRUSTED DIGITAL COMPETENCE PLATFORM

KPMG

THE POWER OF THE CLOUD

Mitigate the risks and embrace the opportunities

EuroCloud
SWISS | SWICO

PROVIDED BY EUROCLOUD
CLOUD KNOW HOW
knowhow.eurocloud.org
TRUSTED DIGITAL COMPETENCE PLATFORM

18

EuroCloud Swiss
c/o Swico
Josefstrasse 218
8005 Zurich
Switzerland

info@swico.ch
http://www.eurocloudswiss.ch

EuroCloud Europe a.s.b.l.
66-68, rue de Gasperich
L-1617 Luxembourg
Luxembourg

contact@eurocloud.org

PRINT SPONSOR
KPMG AG
Badenerstrasse 172
8036 Zurich
Switzerland

Tel. +41 58 249 30 30
kpmg.ch/advisory

TABLE OF CONTENTS

1. PREFACE

Cloud computing is not only driving digital transformation across the public and private sectors today, it's also the engine behind the Internet of Things (IoT). Keeping up with the pace of change, many businesses have integrated cloud-based solutions to remain competitive, while others are just getting started.

Nevertheless, there's still a reluctance among senior decision makers to fully embrace cloud technology. Executives worry about cyber security, data privacy, third-party risk posed by cloud providers and cross-border data transfer risks.

This paper shines some light on these key risks and concerns so that you can make appropriate and risk-aware choices when considering cloud computing services. You'll find the white paper offers insight into: cloud security risk; data privacy and cross-border compliance issues; and certification to mitigate third-party risk.

By outlining the risks and concerns of the various forms of cloud computing, the white paper provides you with a better understanding of the key issues to address when considering the adoption of cloud services. This white paper was created in a cooperative process between EuroCloud Switzerland, Glenfis and the various experts from KPMG Switzerland: Reto Grubenmann, Dr. Matthias Bossardt, Prafull Sharma, Michael Nordhoff, Reto Mathys, Saner Çelebi and Nienke Meester. Special thanks go out to Reto Grubenmann from KPMG Switzerland, who with great personal commitment, assumed the leading role in terms of content – elaborating every detail over several sessions with me.

We hope you'll find the content useful on your journey to successfully integrating cloud solutions and transforming your enterprise.

Zurich, April 2018

Martin Andenmatten
President EuroCloud Switzerland
Vice-president EuroCloud Europe

Tobias Höllwarth
President EuroCloud Europe

2. THE CLOUD'S ROLE AS ENABLER FOR DIGITAL TRANSFORMATION

The term 'digital transformation' stands for the continuous, profound changes in business models, processes and competencies as well as client interactions – driven by a mix of new, disruptive digital technologies – impacting all aspects of society. The cloud serves as the underpinning foundation for much of this digital transformation because of its adaptability, accessibility, scalability, resilience and favourable economics. Of all the disruptive technologies, cloud in all its forms has had the biggest impact and provides the basis for most of the other technologies and their ability to disrupt.

The cloud serves as the underpinning foundation for much of this digital transformation because of its adaptability, accessibility, scalability, resilience and favourable economics.

2.1. DRIVERS FOR CLOUD ADOPTION

As you might expect, the business world's digital leaders are investing significantly in all three cloud delivery models (IaaS, PaaS and SaaS) at rates that are two to three times higher than their competitors[1]; and they can be expected to maintain their investment lead over the next one to three years as others try to catch up. This trend has continued over the past year, with businesses investing in cloud less to save money, and more because IT leaders value the reliability, agility and responsiveness that these services bring.

Today, it's essential that companies possess the ability to rapidly respond to changing market conditions and needs through either business responsiveness or the availability of IT resources. Many smaller organizations are turning to the cloud in order to access enhanced availability, stability and resilience compared with in-house operations. Larger organizations, however, more often see the cloud as a means of performance enhancement to improve their agility and responsiveness and invest in cloud to accelerate product innovation.

Today, it's essential that companies possess the ability to rapidly respond to changing market conditions and needs through either business responsiveness or the availability of IT resources.

2.2. MORE THAN A SILVER LINING

Businesses initially approached the cloud with a primarily IT-centric lens. However, over the past few years this attitude shifted as executives realized that cloud requires a much broader view. In many situations,

[1] Navigating Uncertainty, Harvey Nash/KPMG CIO Survey 2017

cloud is driven by an ecosystem of participants. So, it's vital to think of the evolution of cloud in terms of three broad sets of participants: people and principals; service providers and business users; and IT users. Another challenge is that size matters. Smaller organizations, with less legacy IT infrastructure and fewer constituents, are able to more rapidly and aggressively invest in deploying cloud capabilities. Any cloud implementation requires cooperation, agreement and compromise along with intensive focus and hard work. The challenge going forward will be to balance objectives, needs and wants against real capabilities and risks. As such, coordinating and harmonizing the advancement of the cloud represents a massive undertaking. But the rewards can be significant and transformative.

Smaller organizations, with less legacy IT infrastructure and fewer constituents, are able to more rapidly and aggressively invest in deploying cloud capabilities.

2.3. THE ROLE OF THE CLOUD AS AN ENABLER OF DIGITAL TRANSFORMATION

Of all the disruptive technologies, cloud in all its forms has had the biggest impact and provides the foundation for most of the other technologies and their ability to disrupt. The availability of very low-cost, on-demand, and easily provisioned infrastructure as a service (IaaS) has all but made obsolete the need for many organizations to build and operate their own data centers. Meanwhile, the growing portfolio of application software as a service (SaaS) has enabled business organizations to directly procure solutions with little or no assistance from IT, eliminating the need for upfront capital and reducing the lag time from decision to value from months or years to weeks or days.

The availability of very low-cost, on-demand, and easily provisioned infrastructure as a service (IaaS) has all but made obsolete the need for many organizations to build and operate their own data centers.

The 2017 Harvey Nash/KPMG CIO Survey "**Navigating Uncertainty**" confirmed this journey to the cloud with the vast majority of respondents planning to make significant investments in cloud services. Of the large organizations (IT budgets greater than US$ 250 million) surveyed, 58 percent reported that they will make significant investments in IaaS; 56 percent will make significant investments in platform as a service (PaaS); and 64 percent will make significant investments in SaaS over the next 1 – 3 years. Of the three, PaaS investments will grow the fastest, with a 78 percent jump expected.

As the market for cloud services has matured, it is being deployed well beyond serving as a utility for storage and servers. Applying a cloud-first strategy has many compelling advantages not the least of which is freeing IT from the heavy burden of building and operating data centers. This significantly reduces IT's constant need for capital that can now be deployed elsewhere and eliminates the need for a large operations staff. Furthermore, with the appropriate governance processes in place, favouring SaaS solutions over internally

developed ones helps the business become more self-sufficient, reducing demand and freeing up additional resources to work on more complex and high-value initiatives.

Applying a cloud-first strategy has many compelling advantages not the least of which is freeing IT from the heavy burden of building and operating data centers.

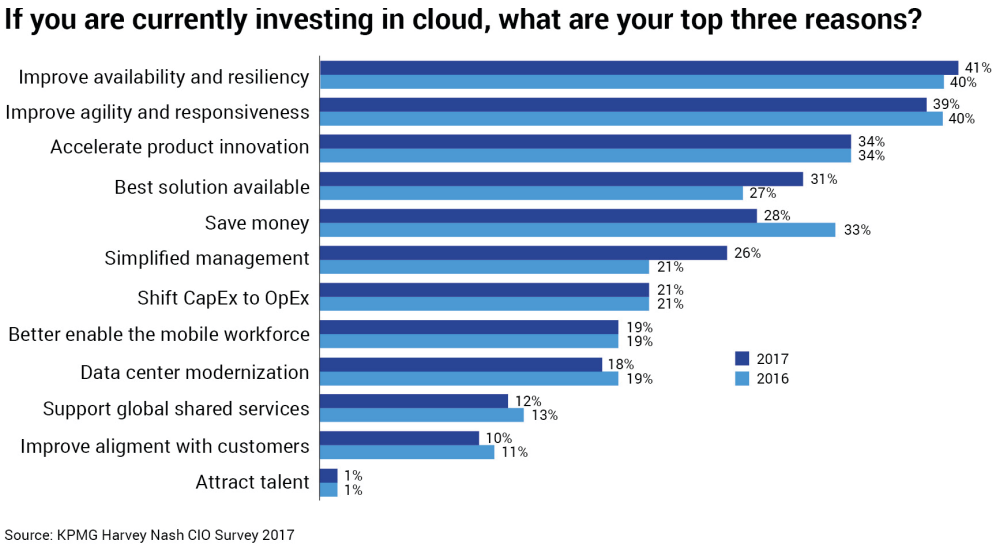
There may still be certain situations where putting applications or data in the cloud is not an option, including concerns around cross-border data flows, privacy and security, but reasons for such exceptions are being addressed and eliminated at a rapid rate. The big cloud service providers are rapidly expanding their geographic footprints so that they can respond to requirements to keep data within country borders and are making significant investments in securing their networks and data centers. Most of the major data breaches to date have occurred in the data centers of private sector and government organizations – not public cloud providers.

2.4. THE STATE OF CLOUD ADOPTION IN EUROPE

For every argument against cloud adoption, there is a counter argument for cloud adoption, supported by cloud services and cloud service providers that demonstrate that the cloud model has the maturity, breadth and experience to meet the often very diverse needs of the market. Cloud services are particularly well suited to meet the needs of the more agile project and operations delivery methodologies being adopted throughout industry.

Security, privacy, data governance concerns are three of the top four inhibitors for cloud adoption.

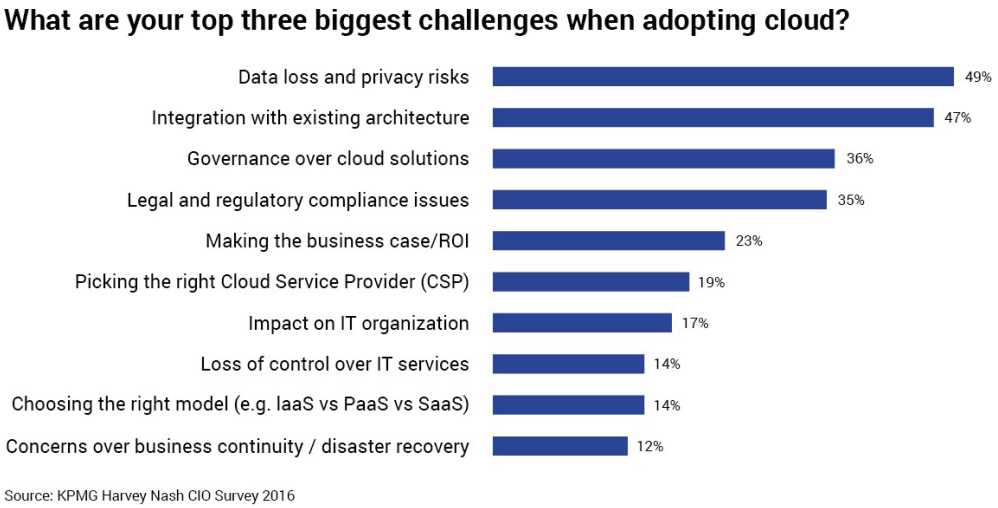
In Europe, the IT leaders continue to prioritize cloud resiliency and responsiveness:



Source: Harvey Nash CIO Survey 2017

2.5. TOP INHIBITORS FOR CLOUD ADOPTION

According to the 2016 Harvey Nash/KPMG CIO Survey "**The Creative CIO**", almost half of IT leaders (49 percent) report data loss and privacy risks as the biggest challenge with adopting cloud technology. A similar proportion (47 percent) have concerns about the integration with existing architecture. Governance and compliance concerns are a challenge for more than three in ten, while more than one in ten (12 percent) cite concerns with disaster recovery[2].



Governance and compliance concerns are a challenge for more than three in ten, while more than one in ten (12 percent) cite concerns with disaster recovery.

As a consequence, industries that are heavily regulated and/or process sensitive data, either business/ national secrets or sensitive personal data, such as financial services, healthcare, and government seem more reluctant to adopt cloud technology and hence may not benefit from the cloud in terms of improved resiliency, agility and accelerated product innovation.

2.6. DATA GOVERNANCE AND SECURITY AS FOUNDATION FOR SUSTAINABLE CLOUD ONBOARDING

When thinking about cloud computing there are many non-functional dimensions which should be taken into account, including data protection, data security and data sovereignty. These considerations apply to any form of technology service but can become more complex in cloud, where the cloud platform may be shared with many other unknown tenants and where customer data may be stored and processed in

[2] The Creative CIO, KPMG/Harvey Nash Survey 2016

many different jurisdictions. Despite these complexities, the benefits of cloud can be immense as cloud can enable organizations to deliver business outcomes and innovation quickly, securely and sustainably with little, if any, capital expenditure.

When thinking about cloud computing there are many non-functional dimensions which should be taken into account, including data protection, data security and data sovereignty.

Independent assurance is critical in the cloud model due to many cloud providers' lack of support for a customer right to audit. Assurance reports may be the only vehicle for cloud consumers to use to make informed decisions on whether the cloud provider's controls sufficiently meet their minimum security requirements.

Transitioning to the cloud is a non-trivial decision for most organizations and those responsible and accountable for making such a decision must evaluate data and service(s). In order to manage the major security and compliance related inhibitors listed above, it's crucial to address the following questions:

- How sensitive is the data, and does the cloud provider offer the necessary minimum-security controls in terms of maintaining confidentiality, integrity and availability of data?
- Is the data regulated by data privacy or other laws and regulations, and are the corresponding requirements adequately addressed by the governance over such data, including corresponding organizational and technical controls?
- Do organizational controls include roles and responsibilities as well as processes in and between cloud provider and the cloud adopting organization?
- Is the cloud provider able to demonstrate that their security control framework is effective (e.g. SOC 1,2,3 assurance reports and/or certifications such as ISO/IEC 27017, ISO/IEC 27018, EuroCloud StarAudit)

Transitioning to the cloud is a non-trivial decision for most organizations and those responsible and accountable for making such a decision must evaluate data and service(s).

2.7. CLOUD IS NO LONGER A CHOICE

Cloud adoption is fast becoming the default option for new services across many different sectors and will be fundamental to the evolution of the Internet of Things. After many years of being an up-and-coming

trend, cloud computing is now established as a tried-and-tested delivery option: any organization refusing to acknowledge the benefits on offer may soon find themselves being left behind by their users – and their competitors.

After many years of being an up-and-coming trend cloud computing is now established as a tried-and-tested delivery option.

3. HOW TO MITIGATE CLOUD SECURITY RISKS

The lure of scale, cost efficiency and agility is attracting a growing number of enterprises to adopt cloud solutions. With the rise of the sharing economy, migration to the cloud is no longer a question of "if" but rather "when". Still, the burning question on the minds of many top executives remains: How to mitigate cloud security risks? The problem of sharing IT services with other enterprises poses several security concerns for CIOs such as data loss and privacy risks, loss of control, legal and regulatory compliance, risk of intellectual property theft, system availability and business continuity risks.

The lure of scale, cost efficiency and agility is attracting a growing number of enterprises to adopt cloud solutions.

3.1. DETERMINE YOUR CLOUD RISK EXPOSURE

The first step in mitigating risk is assessing your enterprise's risk category. This means taking a close look at the interplay of three factors that determine your level of cloud risk exposure: how international your business is, the size of your organization and the data sensitivity of your organization's information assets (generally consistent across an industry sector). It's the combination of these three factors that defines an organization's individual risk exposure and risk tolerance.

The problem of sharing IT services with other enterprises poses several security concerns for CIOs such as data loss and privacy risks, loss of control, legal and regulatory compliance, risk of intellectual property theft, system availability and business continuity risks.

3.2. UNDERSTAND THE FOUR KEY POTENTIAL RISK CATEGORIES

These risks appear on a very volatile and situational basis. That's why it's essential to identify these risks in a structured manner, analyzing them both systematically and regularly to assess their effectiveness to adequately define mitigating measures. Keep in mind that individual risk exposure to current threats and corresponding requirements are influenced by many risk factors such as:

1) **Confidentiality** or integrity breaches due to a Cloud Service Provider's implementation of lower security measures. Many factors or weaknesses may lead to a confidentiality or integrity breach of data. Be it the lack of cyber protection capabilities, improper logical separation of tenants, uncontrollable state access to data (e.g. US Patriot Act), or unclear definition of roles and responsibilities between client and Cloud Service Provider (CSP).

2) **Unavailability** of service or data if your CSP neglected to implement a continuity plan. Along with service disruption, it's important to classify service impairment, such as slow performance rendering a system unusable. It's also important to be able to enforce service level agreements, which can be especially difficult when a small regional client consumes a cloud service from a multinational technology giant. A lack of continuity plans, ineffective testing of continuity plans, and insolvency of the provider or subcontractors are just some of the causes for unavailability (especially if servers are legally confiscated for liquidation and not accessible until sold).

CSPs operating abroad cause higher legal process costs due to jurisdiction or to different specific legal processes abroad. Factors to be carefully considered include:

Along with service disruption, it's important to classify service impairment, such as slow performance rendering a system unusable.

a) The geographic location of the physically stored data or data center. You must know where sensitive data is stored, which applications/systems/people have access to it and from which geographic locations the data is accessed.

b) "Take-it-or-leave-it" contract changes offered by a large provider with low-price mass service and compared to smaller providers with more expensive but negotiable services.

c) Lock-in situations need to be considered before consuming a service and exit clauses must be clearly defined for sensitive data to be permanently erased.

d) The risk of non-enforceability of legal requirements in foreign jurisdictions and of the importance of the security/audit reporting (usually kept/provided by the CSP), which build an essential basis for evidence when it comes to legal processes due to violations.

3) **Compliance with internal regulatory or state requirements** such as notification requirements, due diligence protection and security measures required by regulators (i.e. monetary authorities) or law (i.e. data protection laws). Compliance and legal requirements changes must be continuously monitored and retraced accordingly. Non-observance of local data protection laws is a growing risk for international companies. The risk includes fines such as that imposed by the European Union's General Data Protection Regulation (GDPR) of up to EUR 20 million or four percent of global annual turnover – whichever is higher – and reputational risk. Failure to comply with industry specific requirements may lead to sanctions or even revocation of licences. For example, FINMA requires that non-encrypted customer data stored abroad be made anonymous and public health authorities such as the FDA require an entire end-to-end test in case of software changes, including the CSP.

Compliance with internal regulatory or state requirements such as notification requirements, due diligence protection and security measures required by regulators or law.

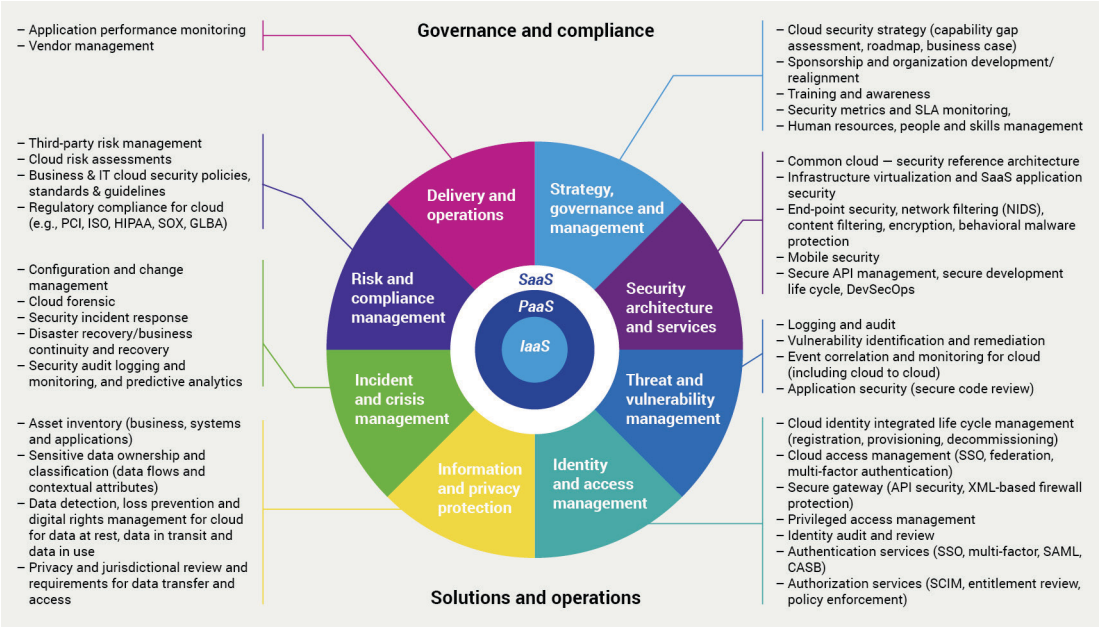
4) **Subcontractor implications** including the loss of data due to the bankruptcy of a subcontractor. Insufficient delegation of compliance requirements to subcontractors, insolvency of subcontractors and poor control of subcontractors are amongst the risks you're exposed to via subcontractor relationships.

3.3. DESIGN A CLOUD SECURITY STRATEGY AND GOVERNANCE FRAMEWORK

Your cloud security strategy is vital to ensure you achieve your business goals and mitigate cloud risks. When considering your strategy, be sure to assess the following criteria:

- State-of-the-art technical security controls, which are updated to prevailing technology conditions and regulatory requirements
- Rigorous control of data, storage locations and lifecycle
- Regular security testing
- Organizational processes: Clear governance, roles and responsibilities with a transparent interplay between on premise and cloud
- Transparent reporting
- Both technical and organizational compliance
- Subcontractors
- Sufficient legal assurance
- Legal enforceability.

A cloud governance and security framework should take a comprehensive view of people, process and technology – enabling your organization to identify critical assets, understand areas of vulnerability and prioritize areas for remediation – thereby turning cloud risk into business advantage. The diagram below depicts the governance and compliance and operational considerations that may be defined by a solid cloud-security governance framework:



Source: KPMG

A cloud governance and security framework should take a comprehensive view of people, process and technology –enabling your organization to identify critical assets, understand areas of vulnerability and prioritize areas for remediation.

3.4. TAKE STEPS TO MITIGATE CLOUD SECURITY RISKS

You'll have to first systematically analyse the different risks, before evaluating a cloud solution or provider; then define explicit requirements to your CSP and ensure that systematic controlling and proper controls can be established. Once your organization has identified the specific risks it could face in a cloud environment, you must then take steps to mitigate them. Some high-level steps include:

1) Establish a cloud strategy

Cloud security strategy should align your activities regarding cloud technologies, therefore business and IT leaders must work closely together to choose the appropriate options (private cloud vs. public cloud, IT strategy, core vs. non-core functions, etc.).

2) Design reference/ target architecture

The issues identified during the assessment stage must be addressed. This includes actions to improve protection measures, such as access control, but also actions to ensure effective detection and response integration with the CSP.

Once your organization has identified the specific risks it could face in a cloud environment, you must then take steps to mitigate them.

Continue by deploying your remediation actions to implement a secure cloud architecture. Taking a long-term view of technology architecture principles and standards will help ensure interoperability, data integration, security as well as controls across internal and external providers.

3) Establish a governance model that focuses on key risks
Cloud doesn't require complex governance, but it does require clear rules. Do your employees know when they can use cloud services for personal purposes, or what they should be aware of when storing business data in cloud solutions? Does your IT staff understand how to connect the cloud to their on-premise systems and how to enable secure access management?

Continue by adapting your existing IT policies and end-user code of conduct to make them cloud ready. Establish new governance models and compliance strategies involving vendor executives to ensure transparency around the organization's risk exposure and drive effective decision making.

Do your employees know when they can use cloud services for personal purposes, or what they should be aware of when storing business data in cloud solutions?

4) Define vendor due diligence model/ guidelines/ approach
As the number of cloud service providers continues to grow, it's becoming more of a challenge to identify and assess the security posture. You'll have to assess whether your existing or planned use of the cloud fits in with your organization's risk appetite.

Continue by assessing the identified or planned cloud services against your policies and define the required actions. Address issues including contract terms, service level agreements and controls that will help prevent business units from circumventing IT and setting up their own cloud services.

As the number of cloud service providers continues to grow, it's becoming more of a challenge to identify and assess the security posture.

5) Establish ongoing risk management, IT controls, continuity planning
You can't manage what you can't see. With that in mind, you first need to know whether your employees or contractors are already using cloud services with or without your consent.

Continuously identify all cloud services used by your employees and contractors. Consider how cloud affects the organization's risk profile, changes its IT processes and IT controls and impacts the components of disaster recovery planning.

3.5. STARAUDIT

It's a challenge for cloud customers to select the best cloud provider from among the many competitors and offerings on the market today. At the same time, it is difficult for cloud providers to stand out and prove they are capable of delivering trustworthy and high-quality services. By generating this trust and transparency, StarAudit enables better defined business cases and reduces the time and cost of sales and procurement processes.

StarAudit is provided by EuroCloud Europe. It assesses cloud services according to a well-defined catalogue of criteria (published online), and evaluates all participants in the specific supply chain of a cloud service. The result of this process is easy to understand and allows for services to be compared by making their maturity and compliance levels fully transparent.

In this sense, StarAudit is a meaningful selection tool for customers: It provides real competitive advantage by reducing the need for costly individual audits and supporting effective multi-provider governance.

Advantages for cloud customers include:

- delivers a framework, assessments and a certificate as relevant selection tools for customers who want to use trustworthy cloud services
- reduces the need for costly individual assessments
- provides a valuable instrument with a high level of transparency and guidance for customers and providers alike
- enables an efficient process of knowledge transfer and accreditation.

3.6. MIND THE GAP

The perceived risk differs depending on the business size and subjective perception of the threat landscape, geographic activities and related critical data types. The actual risk goes beyond the perceived risk. It's therefore vital to systematically and carefully assess the risks pertaining to the cloud adoption in advance – before considering a cloud evaluation.

Client expectations regarding cloud security permanently increase due to the rise of cybercrime, incremental compliance requirements (e.g. GDPR, etc.) and changing political circumstances. There are currently only a few CSPs who can cover their client's security and compliance requirements. In most cases, the gap

between demand expectation and market supply is remarkably large, which makes proper risk assessment and customization of cloud adaptations inevitable.

The actual risk goes beyond the perceived risk. It's therefore vital to systematically and carefully assess the risks pertaining to the cloud adoption in advance – before considering a cloud evaluation.

4. THE CLOUD'S ROLE IN MANAGING THE RISKS OF THE INTERNET OF THINGS

Today, the Internet of Things (IoT) has rapidly evolved to encompass applications across business sectors and for practically every area of society and personal life. However, as the IoT creates tremendous business opportunities and competitive advantage, it also generates risks that need to be anticipated and managed. Such risks include typical cloud computing risk, those associated with the individual networked IoT components or risks arising from the complex integration of the components and actual use cases. In any case, cloud computing is both a driving force behind the IoT's rapid growth potential and an avenue for managing the risks.

As the IoT creates tremendous business opportunities and competitive advantage, it also generates risks that need to be anticipated and managed.

4.1. IOT BRINGS OPPORTUNITY

The cloud is facilitating the integration of the IoT's many components and technologies at such a rate that today we see applications and use cases considered to be science fiction just a few years ago. In 2020, there will be roughly two times more internet-connected devices than people on earth. It's providing enormous future opportunity – changing our lives, our society and our businesses.

Let's take a closer look at what is already possible today by using examples from just two areas the IoT currently impacts:

- In **transport**, we are seeing: Smart solutions using GPS to track vehicles and parcels that communicate via internet; the emergence of autonomous driving with car-to-car communication and data recorders communicating directly with our car insurance companies; as well as integrated ticketing and billing systems using our mobile device positioning, RFID tags, smart cards and other communicating sensors.

In 2020, there will be roughly two times more internet-connected devices than people on earth. It's providing enormous future opportunity – changing our lives, our society and our businesses.

- In **healthcare and pharma**, we are seeing: Remote patient observation collects detailed data and sends it to hospitals and/or physicians to improve treatment effectiveness and efficiency; so-called fitbits measure health and behaviour and may communicate with health insurers; pacemaker and insulin pumps communicate with control and monitor systems via wireless networks and the internet; smart pills can even send data from inside your body to, for example, track your drug intake remotely.

4.2. WHY IS CLOUD COMPUTING SO IMPORTANT FOR IOT?

Cloud computing has characteristics that are essential enablers for IoT. Cloud computing services generally have a broad network access and are accessible from any location via internet. This allows IoT devices necessary access – essential because such devices are typically not installed in data centers and not always situated at locations with a specific network infrastructure access.

Cloud computing has characteristics that are essential enablers for IoT.

Another key characteristic of cloud computing is its flexibility, elasticity and rapid scalability. IoT applications with big data analytics depend greatly on this characteristic as there are no feasible and cost-efficient alternatives. Additionally, the integration of several IoT applications and data collections is supported by cloud computing approaches where the application platforms are situated on the same cloud platform. IoT applications are often based on more than one backend application and data processing. Cloud computing enables this without copying big data from one data center to another.

4.3. WHAT ARE THE KEY RISK TYPES REGARDING IOT SECURITY?

Much of the risk is related to each unique IoT application. Generally, IoT may have an impact on the physical and real world, not just on the cyber world. That is why risks can, for example, be related to security of supply, to critical infrastructures, or to people's health.

Generally, IoT may have an impact on the physical and real world, not just on the cyber world.

There are also significant risks when it comes to processing data related to individuals. Especially when collecting and processing big data obtained from personal IoT devices, when recording data related to a person's behaviour or location and performing profiling – the privacy of the data subjects is at risk. Processing sensitive data such as health-related information also presents a higher risk.

From a business point of view, you may have additional risks related to the protection of customer data. Data may be your business's crown jewel – from the relevant information about client and market behaviour to insights gleaned from machine learning and other intellectual property. Generally, IoT business risks are often related to compliance, trust and/or reputation and loss/leakage of sensitive data.

From a business point of view, you may have additional risks related to the protection of customer data.

4.4. SPECIFIC IOT SECURITY AND PRIVACY CHALLENGES

Challenges and inherent risks apply to the IoT in the area of governance and control, cyber security and privacy.

- KPMG's Cyber Security Survey 2017 unveiled the challenges companies face in governing IoT usage in their organization. Companies are finding that their security strategy and policies do not cover IoT devices. For example, many businesses do not know which IoT devices were introduced and used across their organization and networks. IoT devices are typically not handled by the IT department which struggles to govern usage. Companies are finding that an IT security strategy and framework focused on enterprise IT systems does not apply to IoT. Moreover, a rigorous ban on all computing devices procured outside the IT department fails to achieve its goal. Clearly, the security threats related to IoT devices must be addressed.

Many businesses do not know which IoT devices were introduced and used across their organization and networks.

- IoT integrates various components, mainly cloud computing, mobile devices, embedded systems, and sometimes complex network and communication solutions. Each of these components has its own attack surface and potential vulnerabilities. Combining these components with an IoT solution generally results in a higher attack surface and combined vulnerabilities may allow for new attack vectors.
- A very IoT-specific problem is that smart devices are often not properly managed, especially when under the control of end users. Often device-specific vulnerabilities are not managed and software and firmware patches and updates are not conducted. Additionally, physical security is often not feasible for smart devices and hackers may use a smart device as a gateway to further attack the backend infrastructure and cloud environment of your IoT application. There is a real risk of IoT device specific threats related to access control, secure authentication and trust among IoT devices and between devices and the infrastructure.

A very IoT-specific problem is that smart devices are often not properly managed, especially when under the control of end users.

- Regarding privacy and data protection, there are specific challenges related to data sovereignty and customer consent. For example, when smart devices are used and personal data is collected, the data subject (i.e. the person the data is related to) should have and retain data sovereignty. Using and/or interacting with smart devices may not necessarily require the user's active participation. Simply being in an environment where IoT devices are used may – without the subject's knowledge – result in the collection of personal data. The principles of obtaining explicit consent as a legal

basis for personal data processing may be challenging. In a traditional non-IoT scenario, personal computers with screens enable adequate information about the processing of data and the user can be asked to accept the conditions and express consent via click. In IoT use cases, this becomes more difficult when smart devices are collecting personal data.

Simply being in an environment where IoT devices are used may – without the subject's knowledge – result in the collection of personal data.

4.5. SIX ASPECTS TO CONSIDER FOR IOT SECURITY AND PRIVACY

Some points to keep in mind when thinking about how to secure IoT applications:

1) **Ensure cyber security governance**: IoT applications and solutions must be covered by the organization's cyber security governance and policy framework. Guidelines should address all users and consider IoT devices, subscribe for service, and provide their personal data. Depending on the type of business, the solution- and product- development teams should have guidelines and principles on how to securely integrate IoT in service and product offerings.

2) **Follow security and privacy by design**: When designing an IoT solution, security and privacy need to be considered from the beginning. Doing so can ensure secure and compliant IoT services and applications – keeping risk at an acceptable level for individuals and the community. Security and privacy by design should be applied to developing and/or procuring devices, the cloud infrastructure, software applications, and all other integrated components and services.

IoT applications and solutions must be covered by the organization's cyber security governance and policy framework.

3) **Minimize data**: Although the advantages of data analytics derive from big data, you should consider minimizing and reducing data, especially personal data. For many data processing activities, it's not relevant to relate the data with personal identity. Thus, you can apply techniques creating a pseudonym or anonymization.

4) **Determine justification for processing personal data**: Define the processing of personal data by determining the processing method as well as the purpose and the type of personal data. As a general rule, data subjects need to be informed about the processing. Obtaining an explicit consent from data subjects can be a legitimate justification for processing.

As a general rule, data subjects need to be informed about the processing.

5) **Ensure proper authentication**: A correct and strong authentication is key, especially among smart devices and between IoT devices and the infrastructure. Proper key management and device initialization is essential. A suitable and securely operated public key infrastructure (PKI) may support this and practical blockchain solutions for IoT may emerge in the future.

Proper key management and device initialization is essential.

6) **Manage and protect IoT devices throughout the full lifecycle**: Cloud computing technology should be used to manage the IoT devices and to face cyber threats. You should use cloud computing to detect, monitor, update and manage the devices. Vulnerability management, software updates and controlled configuration changes of IoT devices are key for IoT security. IoT device and lifecycle management should be integrated into the IoT and cloud solution. Cloud-based and IoT-relevant cyber security capabilities should also be considered and include cloud-based threat detection, intrusion detection, and 'denial of service' prevention.

IoT device and lifecycle management should be integrated into the IoT and cloud solution.

4.6. THERE'S ALWAYS A SILVER LINING

When using IoT, risks may arise for individuals, businesses and communities. To be able to exploit the potential of IoT, these risks need to be managed and reduced to an acceptable level. Companies should provide IoT services to their customers and integrate IoT applications into their business model in a responsible way to build trust among customers and stakeholders. Security and privacy by design are key principles when designing IoT services and applications. The security of the connected smart devices is usually crucial for providing, operating or using an IoT application. Cloud computing can help manage and control these devices as well as prevent cyber-attacks and reduce the cyber security risks related to the IoT.

5. DATA PRIVACY AND CROSS-BORDER COMPLIANCE IN THE CLOUD

For many enterprises, storing data in the cloud is a fact of life and the benefits are numerous. Yet, to avoid non-compliance risks associated with the borderless nature of cloud operations and the complexity of cross-border data exchanges, companies must consider data protection and privacy regulations. With regulators cracking down on non-compliance and the General Data Protection Regulation (GDPR) just around the corner, it's essential to fully understand your company's data flows and the applicable regulations before defining your cloud adoption strategy and implementation/usage approach.

How do you maximize the benefits of cloud computing while minimizing the risk of non-compliance? This section highlights the three cross-border data transfer governance components key to maximizing your "in control" cloud benefits while reducing your risk of regulatory non-compliance.

To avoid non-compliance risks associated with the borderless nature of cloud operations and the complexity of cross-border data exchanges, companies must consider data protection and privacy regulations.

5.1. WHEN CONTEMPLATING THE CLOUD, DON'T FORGET COMPLIANCE

Companies are adopting various private and public cloud solutions available on the market – from 'Infrastructure as a Service' to 'Software as a Service' – as attractive alternatives to maintaining a data center. Cost efficiency (pay as you use), data security, readily available functionality, interconnectivity as well as immediately accessible and flexible storage are just a few reasons why companies outsource their data storage to external cloud providers.

Still, regulation such as the General Data Protection Regulation (GDPR), which provides a comprehensive compliance framework for data protection in Europe and takes effect on 25 May 2018, must be considered. The GDPR applies not only to companies based in the EU (or their subsidiaries in the EU), but also to Swiss-based companies offering goods or services to EU data subjects.

Cost efficiency (pay as you use), data security, readily available functionality, interconnectivity as well as immediately accessible and flexible storage are just a few reasons why companies outsource their data storage to external cloud providers.

Which cross-border data transfer governance components maximize "in control" cloud benefits and reduce the risk of regulatory non-compliance?

The following section highlights the key cross-border data transfer governance components for maximizing "in control" cloud benefits and reducing the risk of regulatory non-compliance.

5.2. CROSS-BORDER DATA FLOWS AND REGULATIONS

Although there are many advantages to cloud computing, decisions on a cloud adoption strategy and implementation/usage approach cannot be taken lightly. The adoption of cloud solutions should be subject to careful study, and consider the following elements:

1) **Multiple laws and regulations that apply to different types of data transfers**. Personal data, financial data, export control data and tax data all have their own regulatory requirements. Hence, as a starting point, identify and map the types of data and the level of sensitivity of data that is processed in your company's IT systems.

Personal data, financial data, export control data and tax data all have their own regulatory requirements.

2) **Cross-border data flows and limitations to where data can be stored**. Under GDPR, the personal data of EU-citizens can move freely within the EU. It becomes more complex, however, if personal data is processed outside of the EU (for instance while storing data in a data center in the US). This data transfer is only permitted if the third country provides a level of protection deemed adequate according to the European Commission. The EU and the US have negotiated an arrangement facilitating personal data transfers to the US (the so-called EU-US Privacy Shield). A similar framework is in place for personal data transfers from Switzerland to the US. If personal data is to be processed in a country that doesn't provide an adequate level of protection, the data could still be transferred lawfully when the following legal grounds are met:

- The European Union's standard contractual clauses
- the Council of Europe's model contract for safeguarding an appropriate level of data protection in trans-border data transfers
- The FDPIC's (Federal Data Protection and Information Commissioner) model contract for the trans-border outsourcing of data processing.

Be aware that the company determining the means and purpose of processing (i.e. generally the company owning the data) remains responsible for ensuring and demonstrating the lawful transfer of data, even if the actual processing of the data is done by an external cloud provider. Hence, any contract governing cloud computing must also cover the transfer of data to third countries as well as basics such as the nature and purpose of processing.

5.3. IT PROCESSES, SECURITY AND ARCHITECTURE

Personal data should only be transferred if and when your company can ensure that the data is adequately secured and will not fall into the 'wrong' hands. The legal and regulatory security obligations for the information to be stored, managed and transmitted in the cloud should be carefully assessed and measures defined, implemented and monitored. Even if the cloud provider offers a full-service cloud solution, it is still necessary for the contracting company to ensure the correct use of Privacy Enhancing Technologies. And to ensure that sufficient privacy controls are put in place by the cloud provider. We recommend – as is required by some regulations – that companies contractually govern such obligations regarding security measures and the monitoring thereof, taking into account the applicable regulatory requirements regarding data protection and privacy.

Personal data should only be transferred if and when your company can ensure that the data is adequately secured and will not fall into the 'wrong' hands.

5.4. BUSINESS PROCESSES

For each cross-border data exchange, we advise applying a business-driven decision process that integrates the aforementioned regulatory and contractual considerations as a fundamental component of your company's cloud adoption strategy and implementation/usage approach. Make sure you align and integrate your strategy and approach with your company's internal processes and procedures and regularly review these to ensure permanent compliance.

5.5. THE COST OF NON-COMPLIANCE

Regulators are cracking down on non-compliance. Authorities are issuing massive fines and enforcing system shutdowns and the cessation of outsourcing projects such as data handling if data protection in the outsourced country is ruled as inadequate. Moreover, companies risk losing assets and market position as well as trust and reputation.

Make sure you align and integrate your strategy and approach with your company's internal processes and procedures and regularly review these to ensure permanent compliance.

5.6. COMPLIANCE IS ONGOING

To avoid these negative effects, your company's cross-border data transfers must be actively managed and permanently controlled to make sure they remain compliant. Be sure to focus on:

Data flows and regulations: Concentrate on the types of data and countries where the data is stored and processed, and what the relevant rules and regulations are for those data types and countries regarding the processing of data.

IT processes, security and architecture: Focus on the underlying IT processes for the processing of data. Knowing what the applicable rules are regarding data transfers is not enough. The required IT processes need to be implemented correctly by setting up the correct IT security baselines.

To avoid these negative effects, your company's cross-border data transfers must be actively managed and permanently controlled to make sure they remain compliant.

Business processes: Your business processes should be aligned with the rules and regulations regarding cloud computing. Take this into account from an early stage. In some cases, companies may be required to redesign their business processes.

6. ISO/IEC 27018 CERTIFICATION: SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION IN THE CLOUD

When customers entrust sensitive data to a Cloud Service Provider (CSP), they expect that their data and information are in safe hands.

Today, ISO 27018 is the "Code of practice for protection of personally identifiable information (PII)" in public clouds acting as PII processors and focuses on protecting personal data in the cloud.

For certification assessment, the ISO/IEC 27001 is used for the baseline information security management system (ISMS). These principles and requirements of ISO/IEC 27001 guide the main control objectives to create the supplementary control set given in the standard ISO/IEC 27018.

When customers entrust sensitive data to a Cloud Service Provider (CSP), they expect that their data and information are in safe hands.

The regulator has adopted control objectives to the new standard ISO/IEC 27018 for the Cloud Service Provider (CSP) to help reassure their customers about the security of their data. An extension of ISO/IEC 27001 and ISO/IEC 27002, towards to the cloud security standard ISO/IEC 27018 provides guidance to organizations concerned about how their cloud service providers are handing personally identifiable information (PII).

As the number of PII breaches rise, organizations controlling or processing PII, including smaller newcomers (e.g. small and medium enterprises) will increasingly need guidance on how they should protect PII in order to reduce the risk of privacy breaches occurring, and to reduce the impact of breaches on the organization and on the individuals concerned.

The regulator has adopted control objectives to the new standard ISO/IEC 27018 for the Cloud Service Provider (CSP) to help reassure their customers about the security of their data.

This means that ISO/IEC 27018 certification aims to gain a holistic view of any cloud environment (from a commodity IaaS offering to a sophisticated SaaS offering) by going beyond the technical aspects of the CSP's data center and services.

6.1. WHAT ARE THE REAL BENEFITS OF AN ISO/IEC 27018 CERTIFICATION AS-SESSMENT?

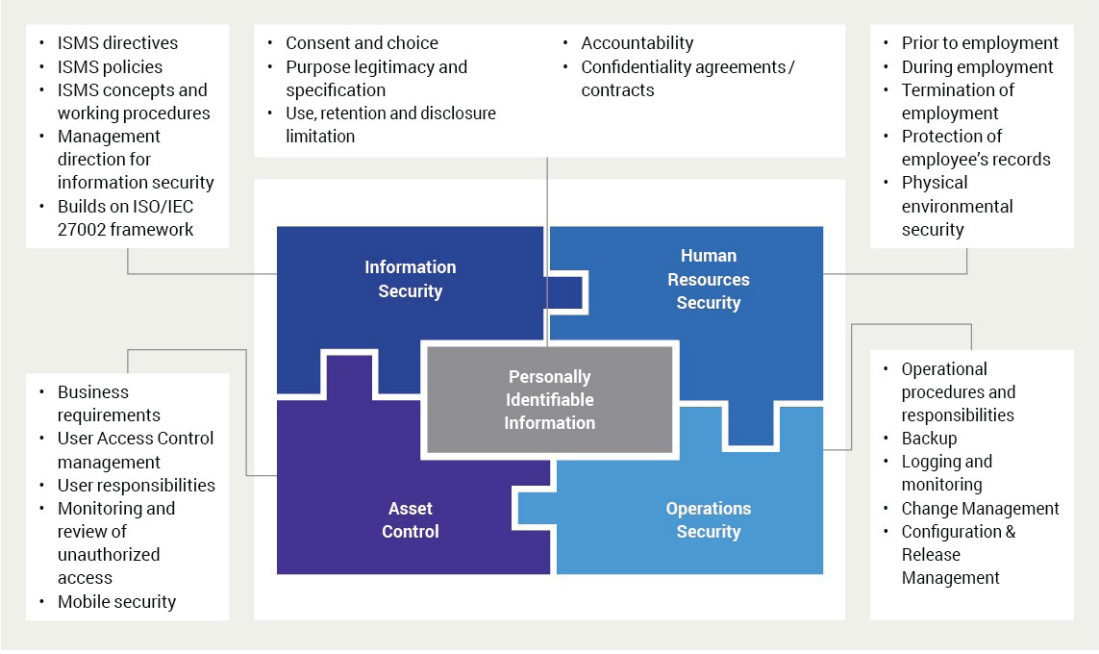
When senior management considers the entire control framework outlined by the certified norm ISO/IEC 27018, the real benefits of a certification assessment include:

- Ensure certified companies of the confidentiality, integrity and availability of data and information in a cloud environment.
- Inspire trust in your business – provides greater reassurance to your customers and stakeholders that personal data and information is protected.
- Create competitive advantage – stand out from your competitors by protecting personal information to the highest level.
- Protect your brand – reduces the risk of adverse publicity due to data breaches.
- Reduce risks – ensures that risks are identified and controls are in place to manage or reduce them.
- Protect against fines – ensures that local regulations are complied with, reducing the risk of fines for data breaches.
- Help grow your business – provides common guidelines across different countries, making it easier to do business globally and gain access as a preferred supplier.

ISO/IEC 27018 certification aims to gain a holistic view of any cloud by going beyond the technical aspects of the CSP's data center and services.

6.2. ISO/IEC 27018 TAKES A COMPREHENSIVE LOOK AT A CSP'S CLOUD ENVI-RONMENT

ISO/IEC 27018 allows a CSP with infrastructure certified to the standard to tell their customers that their data is safeguarded and will not be used for any purposes for which the customer doesn't specifically give consent. To do so, the ISO/IEC 27018 certification is comprehensive and continuous over a three-year cycle period as shown below:



Source: KPMG

The ISO/IEC 27018 certification is comprehensive and continuous over a three-year cycle period.

The ISO/IEC 27018 certification assessment will focus on the following areas in an organization:

There are several main fields focus if a CSP performs an assessment against ISO/IEC 27018. The most important focus areas which can be a security advantage, include:

- **Protecting stakeholder confidence**: Compliance with ISO 27018 inspires greater trust as CSPs can demonstrate that they have implemented security controls to protect confidential information in the cloud.
- **Increasing agility across jurisdictions**: Widely accepted and common guidelines across different countries helps you to conduct and grow your business as ISO 27018 enables CSPs to operate globally.
- **Delivering the supply chain requirements**: ISO 27018 certification provides CSPs with evidence demonstrating they have implemented procedures to protect PII, thus reducing the time required to acquire new business and negotiate new business contracts which creates competitive advantage.
- **Reducing risks**: Certification according to ISO 27018 guarantees a standardized approach to data protection that helps CSPs address their data security risks and operate within the law.

Compliance with ISO 27018 inspires greater trust as CSPs can demonstrate that they have implemented security controls to protect confidential information in the cloud.

6.3. TYPICAL APPROACH TO AN ISO/IEC 27018 CERTIFICATION AUDIT

The following chart describes the Certification Audit Approach for a certification audit over three years.

Approach: ISO/IEC 27018 certification

Identify Risks / Gaps (Pre-Audit)	Certification Audit Stage I: Documentation Audit Stage II: Implementation Audit	Audit Report and certificate issuance ISO/IEC 27018
• Health Check Gap Analysis • Risk Assessment • Review of Policies and Guidelines • Review of pre-selected control objectives based on ISO/IEC 27018	• Conduct on-site audits and planning • Involve subject matter specialists • Documentation audit • Take and assess samples in the cloud environment • Walkthrough audits and site inspections • Technical console testing • Create a draft audit report	• Discuss the draft report with the client • Finalize the reporting using client input • Release the final report • Countermeasure planning of non-conformities, observations, and recommendations • Issuance the ISO/IEC 27018 certificate if the cloud is deemed mature enough • Planning for the surveillance audit

Source: KPMG

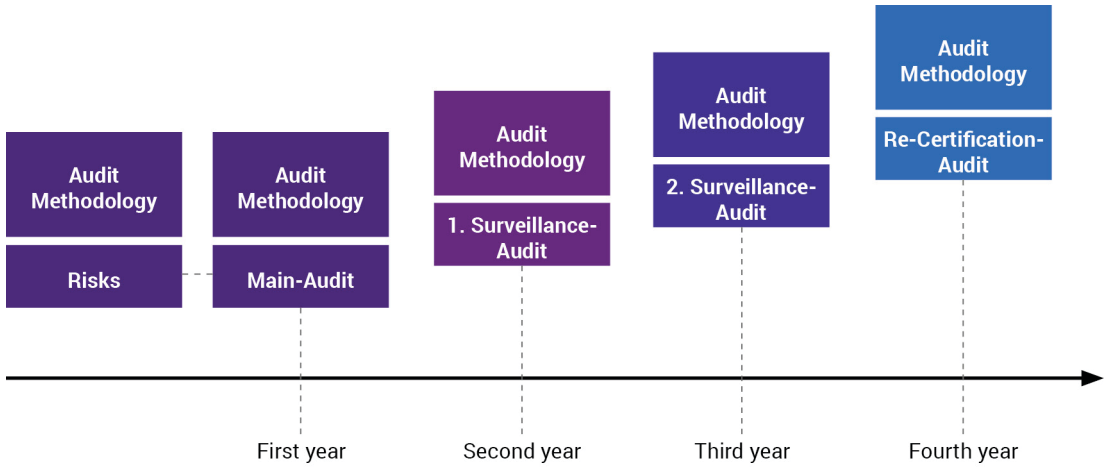
In the **Pre-Audit** phase, the main control objectives of the Certification Audit are reviewed. Afterwards, the CSPs can implement any essential improvement measures.

During the initial stage of the Certification Audit phase, the auditor reviews all relevant documents and then discusses the result of the document review with the CSP. The implementation of the cloud security controls are verified in the second stage. A subject matter expert also carries out technical console checks to validate the logical configuration settings on operating and database management systems which are then integrated into the draft audit report created by the audit team.

In the Pre-Audit phase, the main control objectives of the Certification Audit are reviewed.

In the final phase Audit Report and Certificate Issuance, the audit team discusses the draft report with the client and provides observations and recommendations. If there are no critical deviations (non-conformities), the certification body provides the client with the official ISO/IEC 27018 certificate and plans the surveillance audits for the next three years.

The following diagram depicts the full ISO/IEC 27018 certification audit process over three years:



Source: KPMG

6.4. SAFEGUARD CUSTOMER DATA WITH ISO/IEC 27018 CERTIFICATION

Independent assurance is critical in the cloud model due to many cloud providers' lack of support of a customer right to audit. Assurance reports may be the only vehicle for cloud consumers to use to make informed decisions whether the cloud provider controls sufficiently meet their minimum security requirements.

Independent assurance is critical in the cloud model due to many cloud providers' lack of support of a customer right to audit.

A CSP can be certified according to ISO/IEC 27018 and prove to stakeholders that they have implemented adequate security controls to protect confidential information in the cloud, particularly personally identifiable information.

Certification is not a one-off assessment as the CSP's compliance with controls is audited by an accredited independent certification body at regular intervals. As a result, certification offers considerable advantages such as inspiring trust, protecting your brand and reducing risk, especially for CSPs.

To achieve ISO/IEC 27018:2014 certification, a company must show a continuous, structured commitment to the protection of personally identifiable information and customer data. Throughout the audit process of becoming compliant with ISO/IEC 27018 standard, companies demonstrate that the cloud provider environment protects personal information in accordance with data privacy laws. In addition, customers of the cloud service provider retain full control of their data such that customers' data will not be used for any unauthorized purpose. Moreover, the company is transparent about where customers' data is stored and how it is processed.

Certification is not a one-off assessment as the CSP's compliance with controls is audited by an accredited independent certification body at regular intervals.

It does not matter in which cloud-based solution (e.g. IasS, SaaS, PaaS) or data center or industry you have stored or maintained data, the ISO/IEC 27018:2014 certification applies a 'highest bar' approach to implement the most stringent internationally-certified security standards. We believe that privacy is a right, not a luxury – protecting the customers' data and privacy is paramount.

7. SUMMARY

Cloud is the enabler for digital transformation. Cloud computing is a primary requirement for deploying new technology trends such as Artificial Intelligence (AI) and Deep Learning, Big Data, Blockchain, or the Internet of Things (IoT), which in turn are the foundation of the digital future. The term 'digital transformation' stands for the continuous, profound changes in business models, processes and competencies as well as client interactions – driven by a mix of new, disruptive digital technologies – impacting all aspects of society.

Cloud technology has found wide acceptance. Today, our main concern is the consequences of the cloud's ubiquity for our companies and society. When thinking about cloud computing, there are many non-functional dimensions which should be taken into account, including data protection, data security and data sovereignty. Considering a transition to the cloud is not a trivial decision for most organizations and their decision makers. It's essential that both aspects – data and services – are evaluated.

How do you mitigate cloud security risks? The first step is to determine your cloud risk exposure and understand the fourkey potential risk categories: confidentiality or integrity breaches; unavailability of service or data; compliance with regulatory or state requirements; and subcontractor implications. You have to design a cloud security strategy and governance framework based on the risk exposure.

A specific role has to be seen in the cloud management of the risks of the Internet of Things. The range of sensors, devices and systems with innovative machine-to-machine and IoT applications is growing steadily and is now also affordable for many companies. With such networked components, an incredible amount of data can be captured, condensed and analyzed.

However, as the IoT creates tremendous business opportunities and competitive advantage, it also generates risks that must be anticipated and managed. Such risks include typical cloud computing risk, those associated with the individual networked IoT components or risks arising from the complex integration of the components and actual use cases.

Additional challenges are data privacy and cross-border compliance in the cloud. With regulators cracking down on non-compliance and General Data Protection Regulation (GDPR) just around the corner, it's essential to fully understand your company's data flows and the applicable regulations before defining your cloud adoption strategy and implementation/usage approach.

ISO/IEC 27018 certification is one international well-accepted measure for providing assurance within the cloud solutions. This allows Cloud Service Providers with infrastructure certified to the standard to tell their customers that their data is safeguarded and will not be used for any purposes for which customers don't specifically give consent.

8. AUTHORS

Reto Grubenmann
KPMG AG
Director
Badenerstrasse 172, 8036 Zurich
Tel. +41 58 249 42 46
Email: retogrubenmann@kpmg.com

Dr. Matthias Bossardt
KPMG AG
Partner, Head of Cyber Security
Badenerstrasse 172, 8036 Zurich
Tel. +41 58 249 36 98
Email: mbossardt@kpmg.com

Prafull Sharma
KPMG AG
Partner, Head of Digital Transformation
Badenerstrasse 172, 8036 Zurich
Tel. +41 58 249 77 91
Email: prafullsharma@kpmg.com

Saner Çelebi
KPMG AG
Manager
Badenerstrasse 172, 8036 Zurich
Tel. +41 58 249 58 76
Email: sanercelebi@kpmg.com

Michael Nordhoff
KPMG AG
Manager
Badenerstrasse 172, 8036 Zurich
Tel. +41 58 249 40 89
Email: mnordhoff@kpmg.com

Nienke Meester
KPMG AG
Senior Consultant
Badenerstrasse 172, 8036 Zurich
Tel. +41 58 249 60 22
Email: nienkemeester@kpmg.com

Reto Mathys
KPMG AG
Manager
Badenerstrasse 172, 8036 Zurich
Tel. +41 58 249 26 27
Email: rmathys@kpmg.com

Martin Andenmatten
Glenfis AG
Managing Director
Badenerstrasse 623, 8048 Zurich
Tel. +41 44 220 8110
Email: Martin.Andenmatten@glenfis.ch

EuroCloud
TRUSTED DIGITAL COMPETENCE PLATFORM

TRUSTED DIGITAL COMPETENCE PLATFORM

European non-profit and vendor-neutral organization delivering know-how, legal orientation, quality guidance and best practice policies for global usage.

EuroCloud Europe is a pan-European cloud innovation hub, a completely vendor neutral knowledge sharing network between Cloud Computing Customers and Providers, Start-ups and Research centres. EuroCloud maintains a constant open dialogue with all partners to bring IT and business together.

Trusted cloud services & european quality scheme for global usage

Data privacy compliance in the cloud made easy

Best practice examples of cloud customers and providers

EuroCloud country awards, finding Europe's best cloud services

We enable networking & knowledge sharing for cloud customers and providers across Europe.

Well-researched and comprehensive information on cloud computing topics in the form of guidelines.

Discover more information about our activities, latest news, events or publications on https://eurocloud.org

EuroCloud Swiss
c/o Swico
Josefstrasse 218
8005 Zurich
Switzerland

info@swico.ch
http://www.eurocloudswiss.ch

EuroCloud Europe a.s.b.l.
66-68, rue de Gasperich
L-1617 Luxembourg
Luxembourg

contact@eurocloud.org