CORE®

INFORMATION SECURITY AND DATA PROTECTION IN THE CLOUD

Compliance through automation in secure infrastructures

Authors
Nicolas Freitag
Markus Frik
Dr Waldemar Grudzien
Nadine Hofmann

Author team
Christian Böhning
Philipp Gampe
Calvin Klee
Ronny Raschkowan

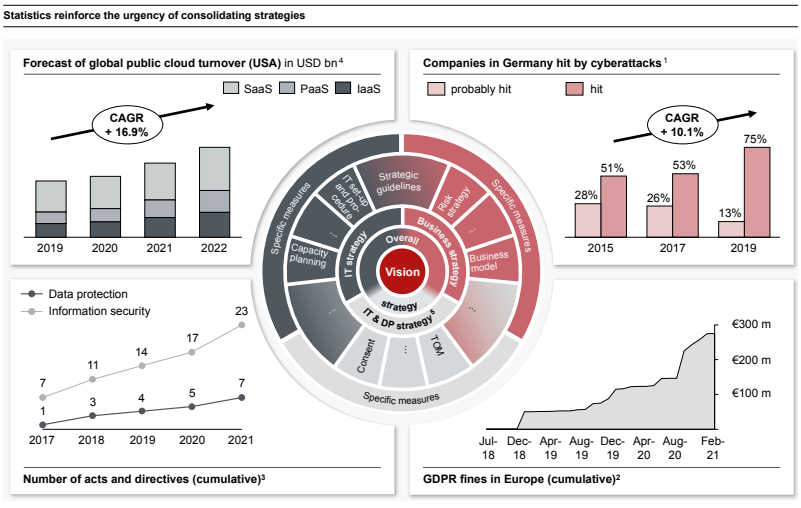
April 2021
White Paper

1 Introduction

In-house hardware is no longer an excuse for forgoing the advantages of the cloud

It is not a matter of whether a cloud is used but rather when. After all, if a company decides to do without cloud technology, it basically renounces the huge advantages of the cloud and, hence, its own competitive position. These advantages are reflected in the following five aspects: scalability, innovative potential, service quality, industrial software development and cost savings. It is true to say that cost savings alone do not justify migration to cloud. If a company has its IT and application landscape fully under control, it cannot be said that migration to cloud simply for reasons of saving costs will result in any further benefits. Otherwise, reducing costs could be motivation for migrating to the cloud. The success of the cloud can easily be seen by the 17% annual rise in global turnover (top left-hand side of Figure 1).

At the same time as the growth in hyperscalers (term used for large providers of practically infinitely scalable cloud infrastructure), which go beyond the three standard supply models – Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) and provide entire ecosystems of tools, the regulatory requirements with regards to data security and data protection for information processing are also increasing. Regulation is manifested in legislation and supervisory activities by means of a vertical compression in data protection and a horizontal expansion in information security. Data protection is not feasible without having properly organised data security. This is evident in the event of a cyberattack, which concerns information security and often also turns out to be a privacy incident – with corresponding fines.



Sources: 1 Bitkom Research | 2 CMS | 3 COREresearch | 4 Gartner | 5 Information security & data protection strategy

Figure 1: Information security and data protection are becoming increasingly relevant and should be put on a par with business and IT strategy

Accordingly, both spheres should be seen as two sides of the same coin and handled under a single strategy for information security and data protection. Indeed, the strategic approach needs to be broadened: the diversity of compliance requirements concerning data protection and information security that need to be taken into account present all market participants with the challenge of taking account of the requirements as part of the digitisation, IT and business strategy. These strategies are often considered and implemented as separate entities, meaning that the overall picture is implemented narrowly as separate and isolated solutions. In this respect, a comprehensive implementation as part of a cloud strategy is ignored.

However, the cloud not only replaces a company's own data centre and many on-premise applications for managing own data, it also contributes towards meeting compliance requirements: the automatable infrastructure as code can increasingly be supplemented with a compliance as code (CaC) that is still configured manually. Hyperscalers are providing ever-more compliance tools that enable users to implement these obligations more efficiently and effectively than is the case when they operate hardware and applications themselves. If renouncing cloud services means forgoing excellence in a company's core competence, then conversely using cloud services reinforces a company's excellence in a core competence, which will stand out against the competition. The sheer number of possibilities offered by the cloud in terms of quality and quantity are basically only a click away.

Excellence in a company's own core competence thanks to using the excellence provided by the cloud

This White Paper shows how to get to this click as well as the competitive advantages that can be gained by reducing the complexity from a commercial, technical, organisational and legal perspective.

2 Compliance-conform cloud utilisation

Cloud is not a question of time, but rather one of competitiveness

Cloud is no longer a hype, it has become reality. Hyperscalers offer quality (stability and availability of a service in the context of resilience) and quantity (in the sense of tools within a cloud eco-system) that increasingly challenge on-premise operations to the test and make them obsolete. Whereas the essence of initial cloud computer services in the mid-2000s was a supply model – i.e. own operation as opposed to IaaS, PaaS and SaaS – services provided by public cloud providers include tools and thus the possibilities of processing data that an individual company is unable to provide, both in terms of quality and quantity. The triumph of the cloud can be seen with the five striking advantages as shown in Figure 2:

1. Scalability: unlimited resources – both vertical and horizontal
2. Innovation: excellence of cloud services both in terms of quality and quantity
3. Service quality: IT has been established accordingly as the essence of added value
4. Software development: development environment and technical services with a click
5. Costs: replacing costs of acquisition with a subscription

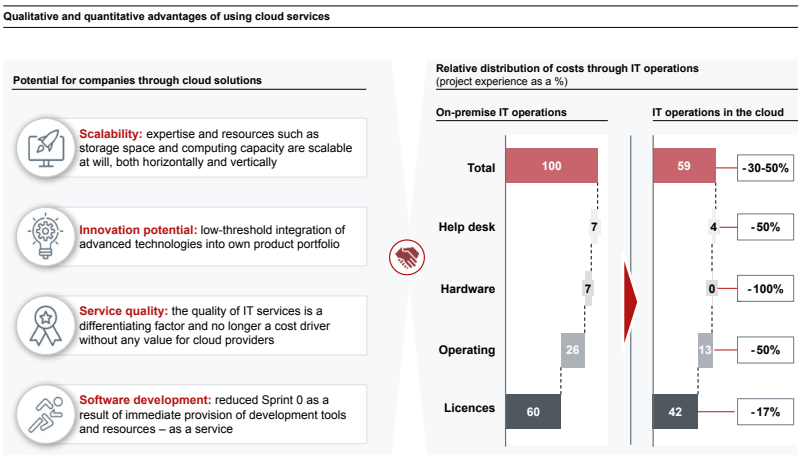


Figure 2: Utilising the cloud offers advantages in five dimensions – scalability, innovation, service quality, software development and costs

Nevertheless, the use of cloud services also means that the provider has access to the data used by companies and thus induces a new evaluation of data privacy and data security than is the case with in-house and on-premise operations.

Cloud use helps to automate organisational processes

Technological progress puts companies in a difficult position of striking a balance between modern infrastructure and security of data and information appropriate to their own business model and compliant with regulation (legislation as well as interpretation and enforcement of laws by the supervisory authority). Cloud ecosystems provide analysing and measuring tools in the fields of information security and data protection, in order to adhere to requirements from the perspective of compliance. Some of these tools can also be used for other areas of compliance, including prevention of money laundering and avoidance of financing terrorism. The increasing requirements concerning information and data security favour the technology and, hence, automation of analogue, i.e. organisational measures – hyperscalers can deliver these better with an ecosystem around the native hardware than any on-premise operator. Nevertheless, cloud services do not only offer opportunities, there are restrictions as a result of regulation:

1. Data protection: data security as opposed to sharing data that is necessary for operations
2. Information security: data security in the cloud cannot achieve that of on-site data security
3. Parallel initiative: data protection is not possible without data security – implement them together

Although cloud-based services can be more cost-effective than an on-premise solution, this cost-saving argument has taken a back seat. It is now properties such as scalability and service quality that play a dominant role in favour of the cloud. The promise made in the early years of the new century ‘IT straight from the socket’ is now a reality.

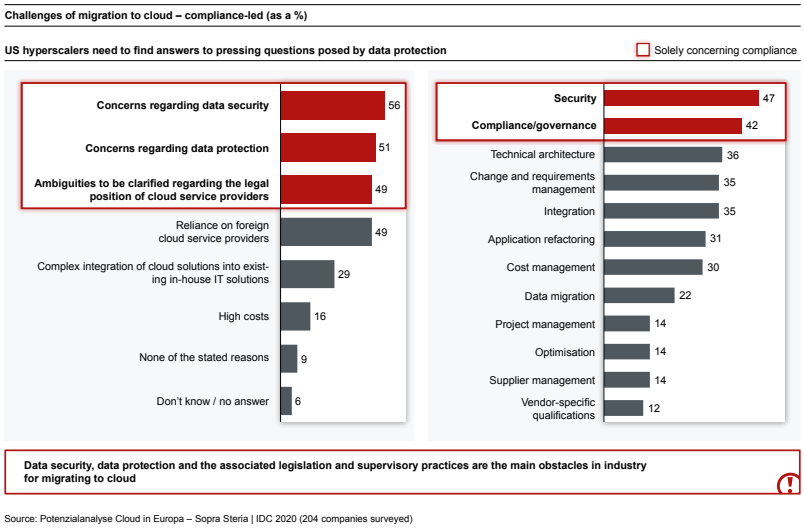


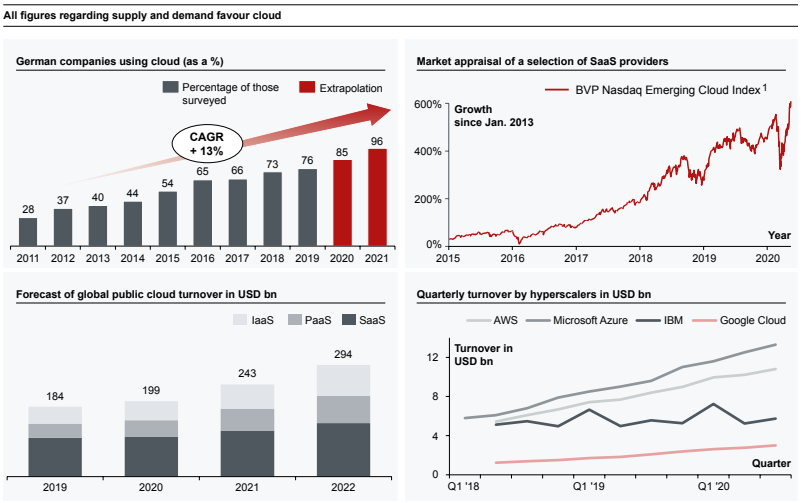
Figure 3: Compliance is the major challenge to cloud migration.

Figure 3 lists the main obstacles to migrating to the cloud: two representative surveys revealed that data security and data protection as well as the associated ambiguities concerning the legal situation of data processing at the provider’s registered offices are a major obstacle. A cloud strategy that is well thought-out and implemented can provide extensive support precisely for these two areas of compliance.

2.1 The triumphant advance of the cloud

The potential provided by cloud solutions is so diverse that not using the cloud is simply not an option

In a survey carried out in 2019 among German companies, three out of four already use cloud applications[1]. Of the remaining 24%, only 6% of the companies stated that they would not pursue the integration and use of cloud services in the future. The triumph of the cloud, beginning with 28% of companies that used cloud applications in 2011, has risen impressively for the tenth consecutive year. Consequently, it is hardly surprising that cloud service providers have been among the winners of the past decade. Hyperscalers built new business areas from nothing, and each now account for turnover in the region of a double-digit billion sum. Similarly impressive are the turnover Figures and associated market valuations of SaaS solutions. Investment in these companies were rewarded with a return on investment many times higher than the initial amount (see table in top right-hand corner of Figure 4).



1. BVP Nasdaq Emerging Cloud Index comprises 52 Nasdaq-listed companies with SaaS and cloud-based business models. Sources: Bitcom Cloud Monitor, Yahoo Finance, Amazon quarterly reports, Google and IBM, Statista and Gartner

Figure 4: The sharp rise in cloud usage is reflected in the key Figures and forecasts

Hyperscalers provide better information security and, hence, enhanced data protection

These drivers of the cloud's triumphant progress are accompanied by a steadily growing number of success stories concerning consistent integration of or migration to cloud applications. Indeed, 78% of the companies that use cloud applications stated that the switchover to cloud computing and integration of the various application options are having a positive impact on the company's development. Half of the companies, which have already successfully completed the migration to cloud services, have noted an increase in data security, thereby taking the wind out of the sails of one of the prevailing prejudices against cloud computing. A quarter of the companies have noticed a significant reduction in their IT costs[2].

[1] (Bitkom Research, KPMG, 2020)

[2] (Bitkom Research, KPMG, 2020)

Not surprisingly, the cloud continues to hold very promising prospects. Gartner, the research and forecasting firm, is predicting a further increase in market size to almost USD 300 bn in 2022[3].

These Figures demonstrate that cloud computing offers advantages for users irrespective of the size of the company or across industry sectors. The scope of the services offered and the variety of use cases for cloud computing go hand in hand with a host of motivators for cloud. If the answers in the studies[4,5] to the question of the advantages of using cloud computing are anything to go by, five core motivating factors can be seen in Figure 2. These different intended effects stemming from a migration to or integration of cloud services are the result, sometimes directly but more often than not indirectly, from technical features and the change from a supplier-customer relationship to a partnership between the two. Another striking indication of a 'cloud first' world can be seen in the fact that certain applications are only available as a SaaS, e.g. Adobe Creative Cloud.

2.1.1 Scalability as an inherent design principle of the cloud

The scalability of technical infrastructures is the basis for all types of digital business models

There is a literal link between scalability and the cloud. Behind the desire to achieve scalability lies the hope that a company's digital products or services will enjoy greater popularity than originally hoped. The cloud as a resource in terms of infrastructure basically provides computing capacity and enables the IT operating resources to be obtained flexibly, i.e. as required. This characteristic is so central that it is listed under the term 'rapid elasticity', as an essential part in the NIST definition of cloud computing, which is recognised as a reference[6]. Starting with Amazon's Elastic Compute Cloud (EC2)[7] in 2006, it became easy to scale IT resources vertically without further interaction, and with container virtualisation, rapid horizontal scalability was also easy to achieve. In this context, elasticity is more than just scalability. During times of normal operation, CapEx[8] and OpEx[9] no longer need to be reserved for the few times in a day when usage is at a peak. At first glance, the huge fluctuation of the consumption of resources appears to affect online stores, streaming portals or news sites. It is easy to see the relevance of peak load capability in the business model. However, when looked at more closely, there is also a sharp increase in enquiries with other highly sensitive services such as online or mobile banking. Apart from the legal consequences that an outage may cause, these result in severe damage to a company's reputation such as was the case in March 2020 when a greater than expected consumption of resources was triggered by increased enquiries to online brokerage firms resulting from the sudden falls in share prices on the stock exchanges[10,11].

[3] (Gartner, 2020)

[4] (Bitkom Research, KPMG, 2020)

[5] (IDG Research services:, 2020)

[6] (National Institute of Standards and Technology, 2011)

[7] (Amazon Web Services, 2006)

[8] Capital Expenditure

[9] Operational Expenditure;

The high popularity of cloud infrastructures among start-ups offering internet-based products[12] like Netflix[13], Spotify[14], Stripe[15] or Home24[16] is mainly due to this scalabilty. For young ventures, the lower CapEx and thus the lower financial risk, in addition to the ability to grow with the business success, spoke in favour of the early adaptation of the cloud.

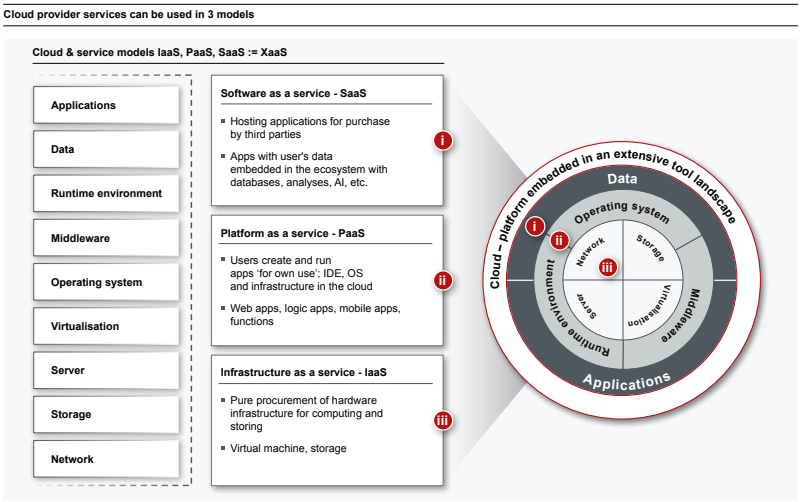


Figure 5: Cloud providers deliver unlimited resources in the three models IaaS, PaaS, SaaS := XaaS

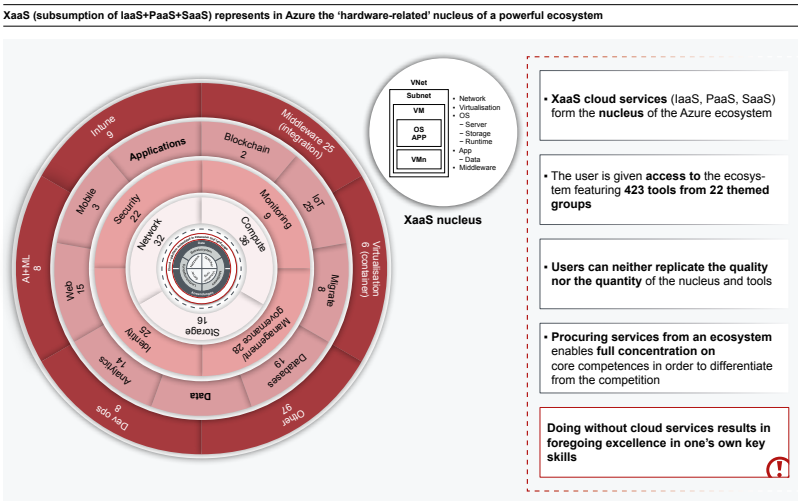
The in-house operation of IT is already a major challenge for lots of companies. Hyperscalers provide IaaS, PaaS and SaaS – collectively called XaaS in Figure 5 – at a level of quality that the vast majority of companies cannot replicate within their own operations. This delivery model – XaaS – 'only' represents the nucleus of a cloud provider's ecosystem, which the user cannot replicate in terms of diversity and service quality on their own.

[10] (Kirchner, 2020)
[11] (@DKB.de, 2020)
[12] (Lemos, 2010)
[13] (Netflix, 2016)
[14] (Beiersmann, 2016)
[15] (Amazon Web Services, 2015)
[16] (Amazon Web Services, 2018)

2.1.2 Innovation using the cloud's ecosystems

Services such as analytics, blockchain, IoT, AI and machine learning that are advertised on the websites of cloud providers challenge the very naive notion that cloud is a network folder located thousands of miles away from the user. These are not examples of use cases that can be realised using available sources, they are indeed actual services that are on offer. These complex services are the logical result of ongoing development of the original scope of services, namely computing power and storage space. Continual development pursues the idea of procuring results as opposed to goods, i.e. 'on-demand self-service[17]', listed as one of the essential characteristics of cloud computing according to the NIST definition. Figure 6 shows an example of the services contained in the Microsoft Azure universe, which are also comparable with the portfolios of all other hyperscalers.

Modern clouds bring the data centre as a commodity – the real value driver is the ecosystem



Source: COREresearch 2021

Figure 6: Solutions and products from Azure

There is no need to build up expertise and to implement proprietary applications in order to expand or complete the portfolio with modern, value-added but highly complex technologies.

The paradigm of outsourcing all functions that do not form the core of the business is also very much the case here. Examples include integrating money laundering checks and chat bots in banking; the successful online banking app with the additional functionality can set itself apart from competitors. Nevertheless, the technology of speech recognition and the artificial intelligence on which it is based cannot.

In addition to technical tools, there are also professional services available such as check-out, integration of payment service providers, shopping basket management etc. The functions that used to be available as libraries are now complete applications. And the notion of possible IT services in the cloud does not stop there. There are huge ready-made tools available that

[17] (National Institute of Standards and Technology, 2011)

go beyond the subject matter, such as Artificial Intelligence and even genome analysis. The crux of this story is that cloud users focus on their core business with their apps, whereas the cloud provides the commodity for the delivery model and tools in the ecosystem.

2.1.3 Improving the service quality of IT services

The main business of hyperscalers is to provide IT services in the three delivery models: IaaS, PaaS and SaaS. Accordingly, they have to position themselves such that they can distinguish themselves in the market. This requires a high degree of technological skills which, in turn, results in an advantage for hyperscalers because talented professionals gear themselves towards top-notch technologies. Whereas IT is 'only' a support function for the customers of hyperscalers, it actually represents a part of the creation of value for themselves.

The maximum quality of IT services is based on the highest degree of competence in technology

The fact that IT is deemed a cost centre in many companies has led to serious discrepancies. The updates and maintenance of the systems required is generally seen as a necessary evil and carried out as cheaply as possible. Consequently, it is not surprising that the result is a poor quality of service. Resources selected with costs in mind are burdened with lots of small-scale tasks, and the operating systems used are often extremely outdated. This correct view of IT as a cost centre from a commercial perspective – it is not a business-differentiating function – stands opposed to the business model of cloud service providers. The ecosystem that surrounds 'IT' distinguishes between the different areas of business. The list of possibilities is long, ranging from basic components like 'computing power' or IaaS based in the cloud. This is shown in Figure 6 by means of the 'XaaS' in the cloud universe and consists of, by way of example, replacement of faulty hardware, configuration of networks, active hazard prevention etc. These services and the level of quality at which they are offered are a cloud provider's USP in face of the competition. For the cloud user, this represents both their IT operation for production as well as administration (office, financial accounting, HR).

The use of common resources, in particular, will be used in this context[18]. The quality of a service depends first and foremost on the competence as a function of the service provider's know-how and experience and the quantity of resources used. A hyperscaler can use this overload of more competent resources effectively thanks to their huge number of customers.

Furthermore, automating organisational measures and manual processes that were not economically viable in an on-premise delivery model as a result of too few activities, is a worthwhile business case for cloud providers; the application of technical processes is associated with the elimination of human error.

This implicit shift in the necessary resources and expertise to a cloud service provider reduces, or even eliminates, the dependencies on internal staff monopolies in favour of the cloud users.

[18] Essential Characteristic 'Ressource Pooling'; (National Institute of Standards and Technology, 2011)

2.1.4 Using the cloud for industrial software development

In the first instance, it seems counter-intuitive to develop proprietary software with third-party resources. However, when examined more closely, there are potentially gains in efficiency. The initial differences are already evident at the planning stage of the software. The sheer infinite scalability of computing power and, most of all, storage capacity make the exact resource approximation less relevant. Expanding server capacity is no longer a lengthy process, sometimes lasting weeks and involving authorisation, order, delivery, installation, commissioning and testing, and is reduced to one of simply inputting a few commands. At the beginning of every software development project the required resources (development and test environments) and tools (project management and issue-tracking tools, code repositories, programs for test automation, etc.) have to be set up; this is often referred to as Sprint 0 with the scrum technique. The core resources of storage space and computing power are available in a matter of minutes as virtual machines (VM), and a whole host of tools are to hand 'as a service'.

The increase in speed is accompanied by a significant gain in flexibility in possible solution architectures. If the initial decision in favour of a certain database (e.g. MySQL) proves to be the wrong one during the course of a project, it only takes a few steps to procure and validate a different database (e.g. PostgreSQL or NoSQL) in the cloud.

Software development in the cloud is the consequence of new IT service delivery models

2.1.5 Cost savings are just one of many benefits

Costs of acquisition are replaced by subscription costs when in-house IT operations are migrated to the cloud. The former costs are depreciated where the latter costs are simply deducted.

There is no longer any need for the on-site administrator to update, service or monitor IT systems; these can be carried out in remote data centres in a highly scalable manner by the cloud provider's experts. This scalability of staffing costs is supplemented by further cost-reducing effects such as central purchasing of hardware or the option of operating with more hardware in less space at more cost-effective sites with renewable energy often generated there. These economies of scale on the part of the cloud provider are passed onto customers as lower unit costs in line with the laws of a functioning competitive market.

The maturity of cloud services also goes hand in hand with easier application possibilities. These services are therefore also easily accessible to smaller companies that do not necessarily have in-depth expert knowledge. The marginal costs for basic IT infrastructure such as email, office applications, etc. in the cloud world are theoretically[19] the same for an SME as for a multinational corporation. The potential for savings does not therefore depend on the size of the company and is independent of the particular sector in terms of the commodity.

Migration to cloud is seldom done for reasons of cost alone

[19] Cloud service providers often give huge discounts on larger volumes.

2.2 Regulatory requirements

When observed over longer periods, the accumulation of a stronger regulatory trend[20] (see Figure 8) and the almost erratic technological development of the Internet can be seen that have led to a considerable increase in regulation – laws and regulatory requirements – for processing data. Consequently, it is not surprising that fulfilling regulatory requirements has become one of the biggest challenges[22] for large[21] companies in specific sectors such as banking and insurance (see Figure 7).

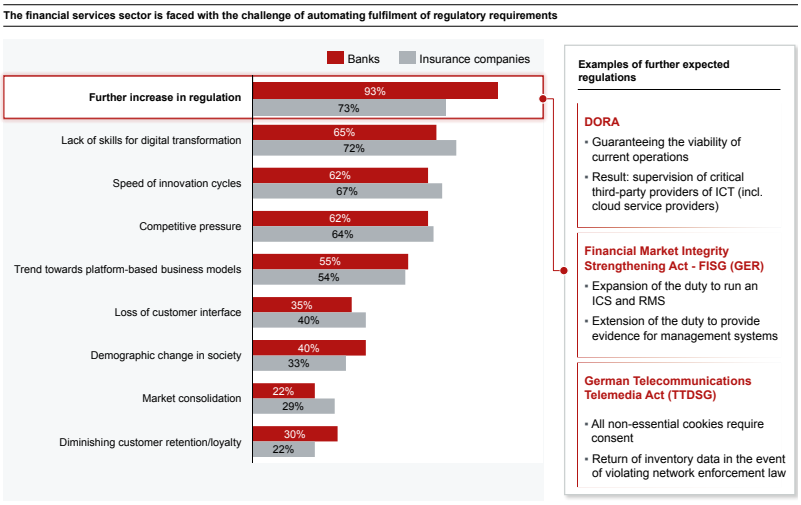


Figure 7: Regulation is the biggest challenge in the financial services industry

2.2.1 Data protection is also relevant in the cloud

Among the new laws, regulatory provisions and interpretation decisions that have appeared over the past few years, it is the General Data Protection Regulation (GDPR) which has assumed the most prominent role; data protection is a fundamental right enshrined in the European Charter of Fundamental Rights (Art. 8) and the national constitution (Art. 2 (1) in conjunction with Art. 1 (1) of the Basic Law for the Federal Republic of Germany). Consequently, it cannot be contractually overridden[23]. The main objective of the GDPR is to protect the fundamental rights and freedoms of individuals, in particular their right to the protection of personal data (Art. 1 (2) GDPR).

[20] In accordance with a trend in deregulation between 1980 and 2010 (cf. Reckwitz, 2019)

[21] (Bitkom, 2020)

[22] (Lünendonk & Hossenfelder, 2020)

[23] Data subjects may waive the protection of their personal data only in a rare exceptional case (Art. 49 (1) GDPR).

White Paper: 'Time to End the Debate – Leverage Data Protection'

https://core.se/publications/white-papers/time-to-end-the-debate-leverage-data-protection

The implications and handling of the requirements of GDPR[24], both from the perspective of users and in supervisory terms, are described in depth in our White Paper 'Time to End the Debate – Leverage Data Protection'. In summary, the situation is such that, on the one hand, GDPR can be considered a conceptual success; the USA California Consumer Privacy Act (CCPA) and more than 100 data protection laws worldwide are strongly based on this. On the other hand, inconsistencies with existing national laws have come to light in other places, or existing practices and transnational agreements have been ruled to be incompatible before courts. Examples include the judgements at European (ECJ on 01.10.2019) and German (Federal High Court of Justice on 28.05.2020) courts of law, which touched on the divergent requirements of the GDPR and the German Telemedia Act (TMG) concerning consent to cookies. Even the judgement of the European Court of Justice on 16 July 2020 found that the transmission of data to non-European countries within the framework of the Privacy Shield was incompatible with the GDPR, meaning that further new or amended data protection requirements must be met.

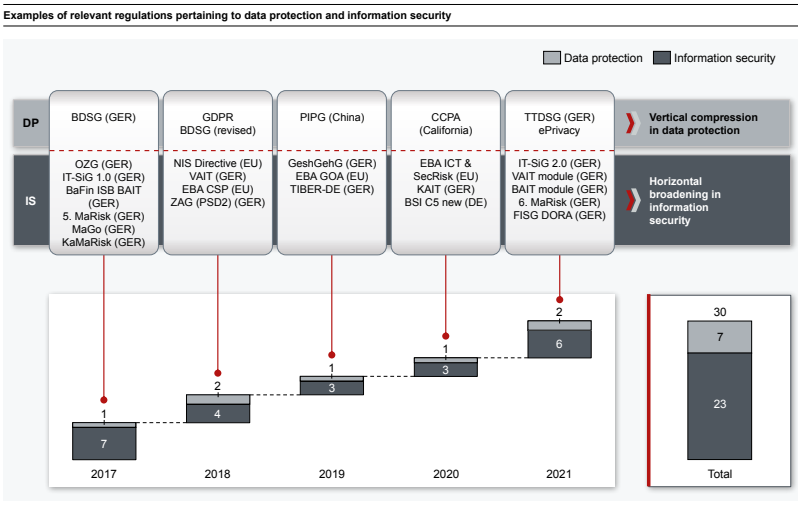


Figure 8: There has been no let-up in legislation and regulatory practice when it comes to data protection and information security

The codification of the ePrivacy Regulation is very advanced and focuses on the protection of all data that can be collected and thus protected on the Internet. The national implementation of this regulation in Germany is to take place within the Telecommunications Telemedia Act (TTDSG), an article law that brings together the two German Acts – TKG and TMG – and eliminates the previously identified dissent to the GDPR in such a way that information necessary for the user's intended access to communications and telemedia from a provider can be stored and retrieved on the user's terminal equipment. The penalties imposed by the TTDSG are in line with those already established by the GDPR.

[24] including national codifications and specifications, the new Federal Data Protection Act (BDSG (new)) as well as the data protection laws pertaining to the individual German federal states (Landesdatenschutzgesetzte)

2.2.2 Duty to adhere to information security

Basically, all regulations on information security require the same thing

Mandatory information security measures are explicitly derived from the European NIS Directive[25] (Network Information Security) and its implementation into respective national legislation. In Germany, this was done in 2016 through the IT Security Act (IT-SiG). Critical infrastructures[26] are defined here and their operators are required to implement state-of-the-art IT security as well as to report any significant IT security incidents to the Federal Office for Information Security (BSI). Apart from the operators in the energy, water, food, information technology and telecommunications, healthcare, finance and insurance sectors as well as traffic and transport sectors, this Act also concerns the three categories of digital service providers: online market places, online search engines and cloud computing services. Among other things, these organisations must prove to the relevant regulatory body at least every two years that a minimum level of IT security has been met by means of security audits, checks or certifications.

Effective information protection is necessary for legal protection

The 'Law on the Protection of Trade Secrets' (GeschGehG), which came into force in April 2019, governs the protection of confidential know-how and business information (trade secrets) against unlawful acquisition, use and disclosure. Anyone wishing to invoke a trade secret must be able to demonstrate that trade secrets are protected by appropriate security measures. Effective protection of information, therefore, contributes not only to the technical and organisational aspects, but also to the legal protection of confidentiality.

The Cloud Computing Compliance Criteria Catalogue (C5)[27], which was developed by the Federal Office for Information Security in Germany (BSI) in 2016, defines a baseline security level for cloud computing. C5 is based on internationally recognised IT security standards such as ISO 27001[28], the Cloud Security Alliance Cloud Controls Matrix 3.0.1 and BSI's own IT baseline protection catalogues. It forms a binding minimum basis for cloud security and the use of public cloud solutions. This audited standard applies first and foremost to German government agencies and organisations working with the government. However, C5 is also increasingly used as a prerequisite by the private sector.

Companies in the banking sector (KWG) and insurance companies (VAG) are obliged to provide adequate technical and organisational equipment to ensure compliance with their respective special regulations. For BaFin, the Federal Financial Supervisory Authority, information security management is required explicitly in Germany for each of the following: the specifications concerning Banking Supervisory Requirements for IT (BAIT)[29] , Supervisory Requirements in IT for Insurance Undertakings (VAIT)[30] and Supervisory

[25] (Official Journal of the European Union, 2016)

[26] Protecting Critical Infrastructure (KRITIS) are organisations/institutions or facilities of major importance to the state community where failure or disruption would result in sustained supply bottlenecks, significant disruption to public security or other dramatic consequences. (Federal Ministry of the Interior, 2009)

[27] (Federal Office for Information Security (BSI), 2020)

[28] (ISO (International Organisation for Standardisation), 2013)

[29] (Federal Financial Supervisory Authority, 2018)

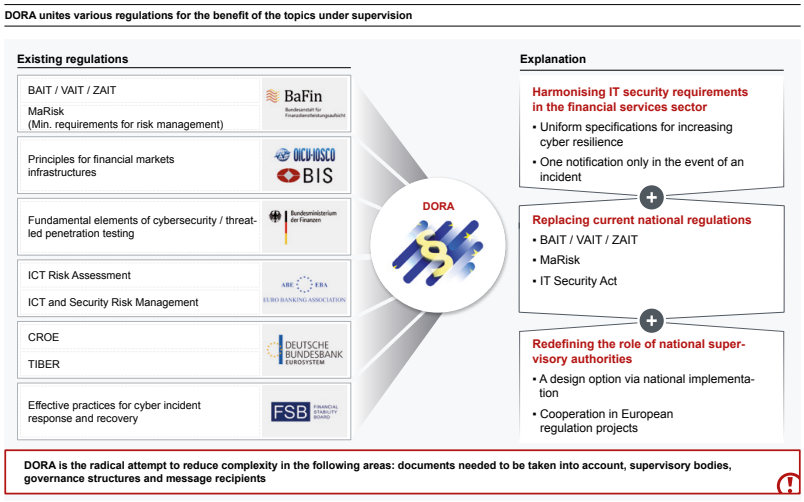
[30] (Federal Financial Supervisory Authority, 2019)

Requirements in IT for German Asset Managers (KAIT)[31]. The 2021 edition[32] of BAIT will be extended to include two modules 'Customer Relations with Payment Service Users' and 'Critical Infrastructures'. The first module was previously brought out as a circular 'Payment Services Regulatory Requirements for IT' (ZAIT).

DORA is the radical attempt to reduce complexity

This was complimented by a draft from the European Commission which was published on 24 September 2020: Digital Operational Resilience Act (DORA)[33]. This brings together several EU initiatives from different institutions (see Figure 9) and is intended to provide a basis for financial regulatory and supervisory authorities. Beforehand, companies in the financial sector were primarily audited for their financial stability. DORA also aims to ensure the sustainability of day-to-day operations. In practice, this means additional and uniform IT security and risk management requirements in all financial services sectors. Indirectly, this will result in the supervision of critical third-party information and communication technology providers, including providers of cloud services. This aligns the approach with that of data protection supervisory authorities. Specifically, financial services providers must first provide evidence of the adequacy of their security measures; this reporting can be organised efficiently as a cloud service. Secondly, the supervisory authorities can compare the performance of various financial service providers directly, meaning more transparency, higher requirements and fewer excuses. Thirdly, cloud providers can offer uniform services based on these standards which, in turn, increases the potential for outsourcing because standardised business practices are not the financial service providers' core business and can be scaled in the cloud.

Data protection cannot be achieved without information security



Source: COREresearch 2021

Figure 9: Information security to be harmonised in Europe thanks to DORA

[31] (Federal Financial Supervisory Authority, 2019)

[32] (Federal Financial Supervisory Authority (BAIT), 2020)

[33] (European Commission, 2020)

The implementation of the laws, in terms of organisational and technical aspects, suggests that an Information Security Management System (ISMS) needs to be set up and, in a best case scenario, certified in accordance with the aforementioned standard – ISO 27001 – enabling appropriate security measures to be documented to the general public. Generally speaking, this type of certification is not mandatory for companies, but is explicitly recommended by BaFin in Germany for insurance companies and financial service providers.

Other planned projects will increase digitisation needs even further, such as the obligation under the Online Access Act (OZG) by the end of 2022, which has the aim of making administrative services from the Federal Government and German states also available online via administrative portals.

2.2.3 Linking data protection and information security

Data protection and information security are often considered to be synonymous. However, in practice, these are separate spheres, albeit with overlaps. This separation may be justified, on the one hand, by the unconditional nature of data protection, as opposed to the voluntary or conditional implementation of information security for many economic organisations. This has led to the development of best practices in data protection for companies that do not have information security measures in place. The various defensive tendencies are yet a further cause. Whereas data protection protects an individual's personal data against unlawful processing by commercial enterprises and administrative units, information security prevents unauthorised access to any kind of information in the organisation by internal as well as external attackers. The definition of personal data is 'information relating to an identified or identifiable natural person […]'[34]. However, when it comes to the technical implementation, it soon becomes evident that information security and data protection are indeed two sides of the same coin in terms of protecting personal data. As regards information security, it is the responsibility of the owner of the information to determine whether access is justified or not. By contrast, with data protection it is required by law. The technical and organisational measures to prevent unauthorised access to information and the protection of personal data for the purposes of information security are congruent[35].

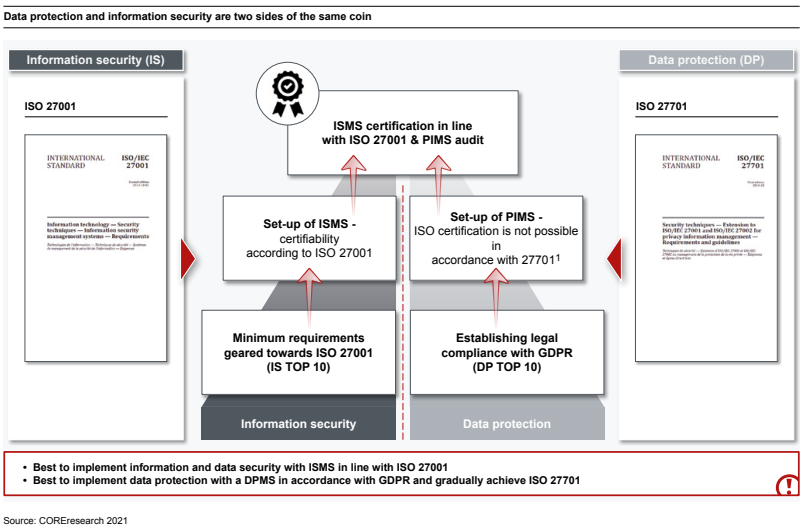
TOM is the hinge between information security and data protection

This is demonstrated clearly in Figure 10 with the overlaps between ISO 27001 for Information Security Management Systems (ISMS) and ISO 27701 for Data Protection. The set-up, operation, auditing and improvement of an ISMS in line with ISO 27001 is an approach recognised by both industry and regulators, and certification can take the pressure off a company from having to provide further evidence that adequate measures are in place for information security. On the other hand, no certification system is available for ISO 27701, meaning that a 'GDPR certification' in accordance with Art. 42 GDPR[36] is not possible.

[34] (Federal Financial Supervisory Authority, 2019)

[35] (Federal Financial Supervisory Authority (BAIT), 2020)

[36] (European Commission, 2020)



Source: COREresearch 2021

Figure 10: ISO 27701 is not recommended

Data protection can be best achieved by ISMS in accordance with ISO 27001 – ISO 27701 is not recommended

With an identical structure, both management systems address the same installation in infrastructure, organisation, personnel and compliance. Consequently, they should be considered together as a conceptual unit. A total of 39 amendments were made to ISO 27001, in order to extend it into the international standard ISO 27701. These changes can be implemented with 20 IS artefacts and nine DP artefacts. This extension of the standard poses a major problem: a standard applied to information security (one developed by information/IT security experts) cannot be transferred on a one-to-one basis to data protection because the latter is governed by the General Data Protection Regulation. It seems that the standards committee ultimately understood this, which explains why two appendices were attached to the normative part of the standard in order to comply with the GDPR, i.e. its specific vocabulary and, above all, its basic principles and mandatory documents. In short, in order to comply with the international standard ISO 27701, the 39 data protection extensions must be met in addition to the set-up of an adequate ISMS, and then all the requirements of the GDPR must be implemented in accordance with the role of the company – controller within the company as per GDPR (Appendix 1) and/or processor (Appendix 2). Indeed, the direct set-up of such a PIMS is a very ambitious undertaking with limited benefits due to the lack of ability to certify, plus the associated simplified communication on compliance. In view of the unconditional requirements of the GDPR, it is therefore best to establish an ISMS in line with the international standard ISO 27001 at the same time as achieving compliance with GDPR. Figure 10 depicts a three-step process for both management systems – ISMS and PIMS – spanning basic protection, certification capability, and certification and auditing in the case of data protection.

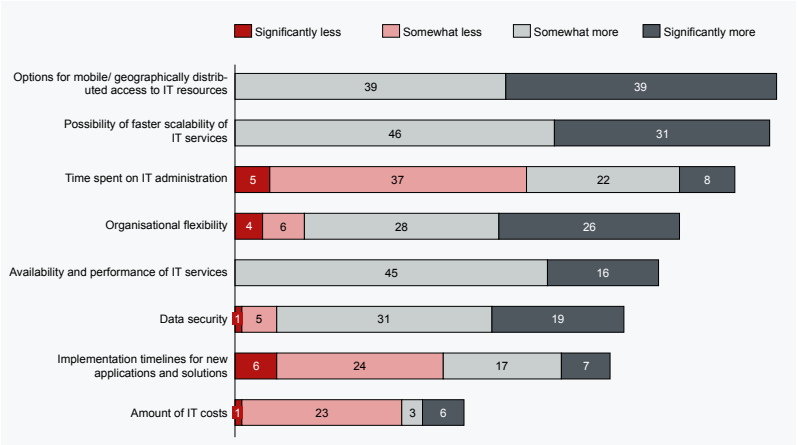
3 Cloud overwhelms all stakeholders – dangerous half-knowledge results in suboptimal solutions

There are many paths that lead to the cloud, of which some are too seldom used. The reasons for this are numerous. Scepticism towards cloud computing due to ignorance of the quality and quantity of modern cloud services, perceived insecurity of a 'loss of power' over one's own data, discrepancy between regulation and technologies in terms of time and content, lack of digitisation skills within organisations, or, quite simply, any change is seen as disruptive to the status quo.

3.1 Cloud between perception and reality

Perceived truths are more powerful than rational knowledge – 'feelings trump facts'. In times of post-factual insecurity, fake news is enough to emotionally drive people from a sense of insecurity to conclusions that guide their actions. The cool, calculating homo oeconomicus is a fairy tale most of the time; decisions concerning consumption, for example, are made primarily on an emotional level despite all rational efforts.
What is surprising, however, is that this well-known principle also applies to well-trained and experienced managers in their decision for or against the cloud. The cloud offers benefits in all decisive aspects (see Figure 11). Nevertheless, prejudices still persist. Only around 40% of decision-makers in German banks currently consider the cloud to be secure[37]. Their view is reinforced by events such as the case of the EU/US Privacy Shield or the legislative initiative to structurally weaken strong cryptography as a counter-terrorism measure via access to cryptographic keys.

Perceived effects of migration to cloud in German companies (as a %)



Source: (Bitkom Research, KPMG, 2020)

Figure 11: Benefits of a migration to cloud are evident in respect of all costs and added value.

[37] (Francke, 2020)

As a result of this scepticism, companies will not be able to take advantage of opportunities offered by a migration to cloud. Here it is often enough to have the vague feeling that storing the data in your own data centre located in the basement is more secure because it is better protected against unauthorised access. By the same token, there is the fear that data stored in the cloud will inevitably migrate to the USA and be disclosed to intelligence services and competitors there. As a result, there is a feeling that by handing over your own data to a cloud provider, you are also relinquishing control over the data. Similarly, there is a fear of losing independence and access to competitive IT know-how in the long term by abandoning in-house infrastructure.

Supplier dependence is manageable with containerisation, an exit scenario and maintaining data portability

Indeed, these prejudices hardly stand up to calm, rational scrutiny. There are now tools and methods available that ensure data is stored securely in the cloud (see Chapter 4). Cloud-agnostic platforms such as Kubernetes reduce the risk of vendor lock-in, as systems running on them can be ported between vendors without much effort. At the same time, the availability of the required know-how is growing exponentially, comparable to the spread of the technology, whilst the knowledge required to operate an in-house miniature infrastructure has to be readily available at a proportionally higher cost.

Furthermore, it is noteworthy that, in addition to the perceived risks of losing power over own data and infrastructure, there is a very real threat from inadequate information security. When busy security departments of large cloud providers employing several hundred members of staff around the clock to carry out penetration tests, security processes, monitoring and defence are compared to their counterparts, fewer in number, employed by cloud sceptics, it soon becomes clear where the actual dangers lurk. Furthermore, from an economic point of view, it should be noted that even running an in-house server operation will not survive without development platforms, test and runtime environments, where the products in question very often originate from the USA. Even open source software is, bar a very few examples, developed on the infrastructure of American companies such as Apache, Red Hat or Free Software Foundation. These, too, are required to comply with the orders from the United States Secret Service.

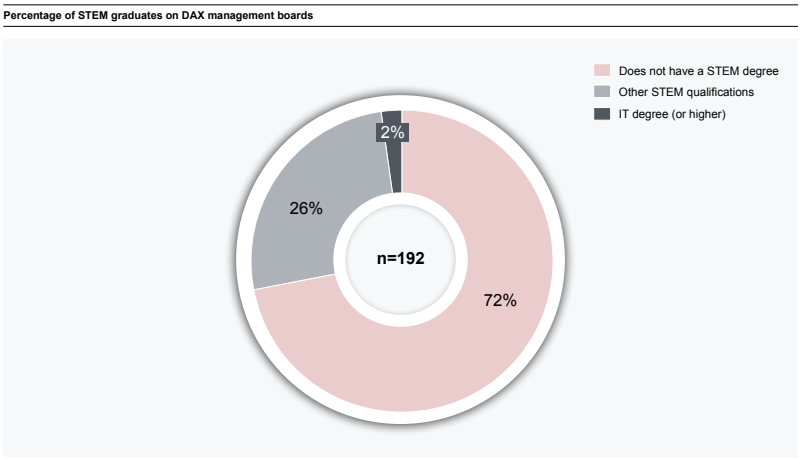


Figure 12: STEM skills are under-represented among the board of directors of German stock market companies.

Even 15 years after Amazon made cloud computing for companies suitable for the masses by means of Amazon Web Services (AWS), many companies, or more to the point, their management boards, still do not comprehend or inadequately understand cloud computing. A lack of cloud knowledge in terms of the technology, regulatory aspects and supervision, or the prevailing unease of those in charge result in delayed or a complete failure to tap into the potential uses of cloud.

It is precisely here where the blind spots begin, namely with the fundamental questions concerning the potential opportunities for synergy or the specific opportunities for use cases which go beyond pure online storage of historical cloud services, and continue with the question of the appropriate cloud strategy and the advantages and disadvantages of public and private cloud solutions. This is primarily due to the prevailing dichotomy between the demands for expertise and governance to maintain a complex status quo and the knowledge and mindsets required to transform and continuously evolve the business in an environment where IT is increasingly becoming one, if not the decisive, factor in successfully aligning the business.

There is too little know-how in STEM subjects on the management boards of German DAX companies

Indeed, traditional skill profiles for an appointment to a group board usually see management experience, familiarity with the relevant industrial sector and the associated value chains, knowledge of financial topics such as accounting, bookkeeping, law, compliance and auditing, in-depth experience in the areas of Human Resources, society, communication and media as well as general knowledge of business areas spanning different sectors. It is only recently that extensive experience in the fields of digitisation and information technology or agile methods for product and corporate development have been added to the skills profile listed above for the appointment to a management board in many companies, and in some companies this is still not the case. The percentage of board members of German DAX companies with a degree in a STEM subject as at February 2021 stood at 28% (Figure 12).

This suggests that the significance of specific skills in the composition of a group's management board also affects the weighting of these disciplines in the levels below in terms of organisation and Human Resources.

The decision to expand personnel and strategy to include the core competencies of technology and digitisation is made even more difficult by the fact that the status quo of the company's IT infrastructure is often complex. The generally prevailing desire to have an agile and technology-oriented company is overridden by the need to safeguard what has already been achieved.

The result of a lack of expertise is often the adoption of widespread prejudices against cloud computing in the fields of data and information security, costs of integration and maintenance, administration effort, availability, performance and the ability to integrate into existing IT infrastructures; usually combined with concerns about being dependent on a particular cloud provider, the so-called 'vendor lock-in'.

Ultimately, it is a question of whether feelings and ignorance are better advisors than facts and know-how, in order to ignore the huge advantages of cloud.

3.2 Development between regulation and technology

Regulatory requirements such as European directives, national laws and interpretations by the supervisory authorities are lagging behind technical developments. This is certainly not new and is acceptable. Otherwise the technical cash value of our prosperity would be in a bad shape. Nevertheless, the time lag between the state of technology in practice and its regulation must not get too large because the regulator loses 'visual contact' with the technology, the dangers of which it wishes to contain and, by contrast, unleashes the opportunities as a legislator with clever laws and as a supervisory authority with business-oriented supervisory practices.

A lack of adequacy between regulatory and technological development wastes a huge amount of potential

As a result, the state of regulatory development is not adequate for the state of the art of deployable technology. A prime example of the different pace of development concerns the length of time taken to create EU laws and standards on the Internet. Whilst it takes, on average, 19 months to develop EU regulations, internet standards take an average of 1.5 months to develop. Then there is the increasing number of regulations as described in Chapter 2.2. This loss of time is then Inherent in the misguided supervision of the 'delayed' law. This takes up the already delayed legislative thread and passes on the loss of time as 'regulatory debt' (in the same way as technological debt). Technological debt is endogenous; it results from the evaluation of technologies in use between 'legacy' and 'state of the art' and describes the loss of results due to the use of technology that is not state of the art.

Regulatory debt is exogenous; it occurs when technology that is ready for use is not adequately[38] regulated at the time it is ready for use. They have different effects depending on the time of regulation as illustrated in Figure 13. If legislators/supervisory authorities intervene too early (segment a in Figure 13) in a technology that is still developing and/or not enough in a given technology (b), the full potential of this technology for added value to the company and society will be squandered. Only at this point in time does lobbying to enable and support the technology make sense. This lobbying also contributes to paving the way for subsequent and adequate regulation (c) with an optimal balance of interests in the sense of technology assessment. An unregulated new technology is a special case (d) because its use

[38] Regulation is adequate if it regulates a relevant state-of-the-art technology in a complete, consistent and non-overlapping manner and is easy to understand.

can make the greatest contribution to an outcome. The principle here is that no regulation at all means no restrictions – thus the greatest possible contribution to income compared to adequate regulation that is valid at the same time as availability.

Adequate regulation enables technology to evolve and induces competition under fair conditions

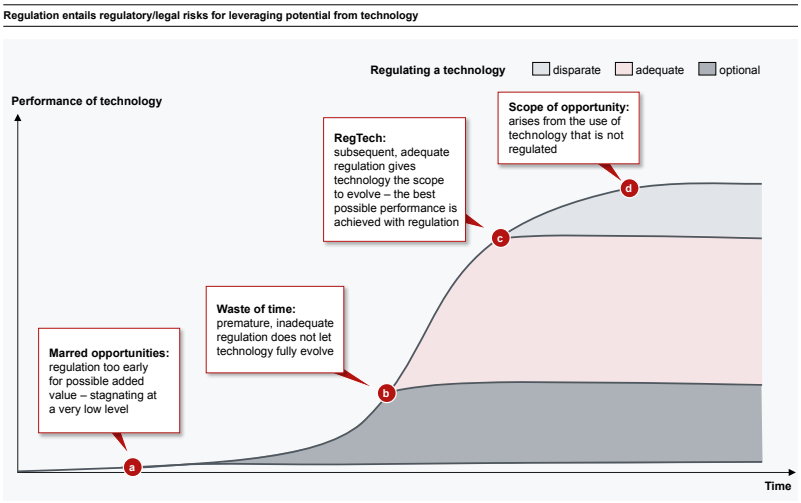


Figure 13: Graph to show how regulatory debt is the cause of underperformance

If the technology and regulatory system remain in segments a and b, this creates, for example, uncertainty among potential users ('supervisory authorities will not approve it or will immediately prohibit it's use'), suboptimal use of technology by forcing people to use suboptimal IT under their own responsibility, restrictions on digital activities and further developments, and thus delayed or even absent product innovation in the further development of business models and value chains. In the meantime, competitors operating outside of the EU are not paralysed to the same extent, which adds to the pressure.

Results stemming from a lack of congruency between regulatory and technological development leave too much room for interpretation, uncertainty and knockout arguments against new technologies that ultimately disrupt the decision-making process. This leads to a delayed use of new technologies, or not even using them at all, which decouples companies from the technical progress that competitors enjoying better regulation take advantage of.

The EU-US Privacy Shield serves as a good example. The state of the art in terms of shared data processing based on the division of labour is used in the USA; the regulatory risks of current inadequate regulation and future non-conformity are accepted. The 'Schrems II' Decision by the European Court of Justice from July 2020 now reveals the risk of a de facto ban on using a tried-and-tested technology.

EU-US Privacy Shield

Apart from the general safeguards of cloud providers, it is important to note that, as already mentioned in Chapter 2, the Schrems II Decision by the European Court of Justice overturned the Privacy Shield Agreement between the EU and USA, creating a difficult political question of principle in the use of clouds, namely when it comes to access rights of security authorities. According to the decision, the agreement no longer provides a valid basis for the transfer and processing of personal data of EU citizens to or by US American companies (especially on US-American servers).

As regards the question of the transfer of personal data, priority must be given to the location of the data. That is the reason why server locations within the EU are recommended for US-American companies and should be included, wherever possible, in the contract. Nevertheless, it should not be forgotten that US-American companies are bound by their national laws and are also required to hand over personal data to the National Security Agency if requested to do so. Therefore, against the background of Schrems II, it does not offer an absolute solution, but rather one only in conjunction with other precautions.

Consequently, in the absence of a new agreement, data-exporting companies will have to check for themselves and ensure that an equivalent level of data protection is guaranteed. This is primarily possible by means of standard contractual clauses combined with additional safeguards and measures (e.g. encryption, anonymisation, contractually agreed guarantees for data subjects, etc. The EU Commission recently published a new draft of standard contractual clauses for debate. However, it is not currently clear whether and when this new draft will be adopted and can be used, and whether it is appropriate to address the issue of access by security authorities in a manner compatible with data protection. It is therefore important to keep an eye on developments at the regulatory and political level.

3.3 The trend towards multicloud

The advantages and challenges of using cloud services can be scaled equally by using cloud services provided by more than just one provider. Very few companies have managed to organise their cloud architecture in such a way, either intentionally or by chance, as to simply rely on the services of one cloud provider. Applications, which used to be deeply integrated into the company's own IT systems, are gradually being relocated to the cloud by service providers. The choice of cloud infrastructure in this scenario is made by the provider and, depending on the complexity of the original application landscape, results in an architecture with multiple cloud providers.

Indeed, multicloud approaches also enable a choice of numerous cloud services across multiple providers according to the company's own specific requirements and have become a cross-industry standard, thanks in particular to the widespread use of workplace services that take place in the cloud, e.g. those offered by Microsoft. In companies' IT and cloud architecture, it is often Azure, i.e. the cloud solution for Microsoft workplace applications, that regularly appears alongside the following clouds: Amazon Web Services, Google Cloud Platform, SAP, Salesforce or IBM. This means that eight out of ten companies already use more than one cloud provider[39] for their chosen architecture. This intention is often pursued in order to avoid vendor lock-in, i.e. they oppose the providers' efforts to bind customers exclusively to their own services.

Reality forces companies to use several cloud services providers at the same time

The requirements for the successful use of cloud services increase with access to each additional cloud provider. Companies need experts with knowledge of all cloud technologies in use in order to efficiently manage access, users and projects, but first and foremost to ensure that the requirements imposed by regulatory and supervisory bodies are adhered to as already described in Chapter 2.2. If access, responsibilities and functionality used are monitored inefficiently, this inevitably leads to (in)direct costs in using multicloud services and the creation of shadow IT due to incorrect use of cloud functions by untrained staff.

Compliance is also challenging in multicloud environments

The expected continued diversification of cloud solutions for different IT application areas requires at least the set-up of multi-provider control systems for monitoring reliability, performance, security and costs, a focus on managing the functional and technical structure of interfaces between the various providers as well as the integration of existing and new SaaS solutions. In the past, the tools developed by the cloud providers proved inadequate in this respect and sufficed mainly only for monitoring their own cloud products.

[39] (interxion, 2019)

4 Compliance as a service – CaaS

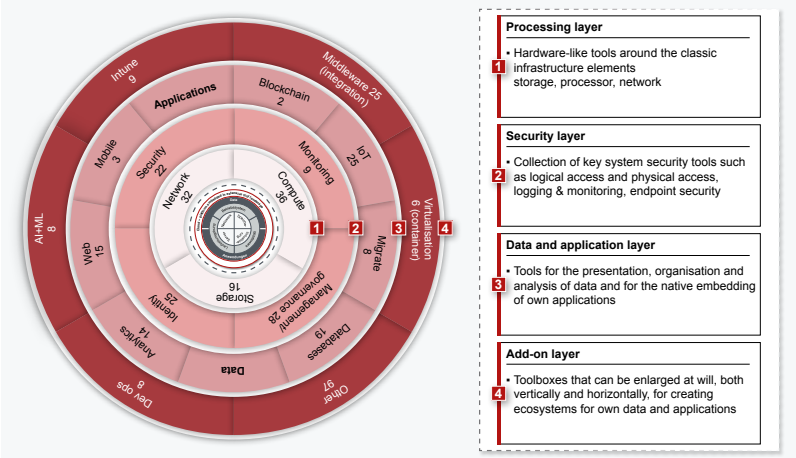
CaaS as a cloud module increases the degree of maturity in the ecosystem

Compliance stands for the entirety of all measures to comply with external as well as self-imposed rules. The dualism of this term – on the one hand a reference for the function and department, while on the other, the concept behind all operational measures to ensure the legitimate conduct of all addressees in an organisation – thus consists of the method and goal at the same time. Basically, compliance describes the adherence of self-imposed (internal policies) as well as externally imposed rules (laws and supervisory practices). Many policies serve to implement external rules. Usual fields of compliance focus on cybersecurity, information security and data protection. Other important goals include e.g. preventing money laundering and avoiding the financing of terrorism.

Cloud providers aspire to provide the cloud user the most compliant cloud infrastructure possible. The more compliance a user can draw from the cloud, the easier it is for them to use the actual services provided in the infrastructure, and the less they have to worry about compliance requirements themselves. Consequently, they are able to externalise any lack of expertise in the cloud. In this context, the users gain compliance support based on best practices for their own infrastructure and applications operated in the cloud.

Finally, the various cloud service providers are increasingly offering tools for compliance, other services such as IoT, DevOps, analytics or for the effective administration of other cloud services within their own cloud – keyword: multicloud. Figure 14 below shows, for instance, the tools included with Azure for assisting with compliance.

Azure provides a powerful ecosystem with over 420 tools in 22 themed groups around the XaaS nucleus



Source: COREresearch 2021

Figure 14: Azure's ecosystem places 423 tools in 22 themed groups which are organised in four layers.

Users are unable to recreate either the quality of the XaaS nucleus (see Figures 5 & 16) and the tools, or their diversity. Using the services provided in the ecosystem enables the user to fully concentrate on their own core competences to set them apart from the competition.

The following subsections describe a few areas of compliance to show how cloud service providers make it easier for their users to ensure compliance with both external and internal rules. Furthermore, the effective management of a multicloud environment provides possible key solutions in assisting with compliance.

4.1 Cybersecurity in the cloud

Definition
Cybersecurity and IT security are terms for the protection of networks, devices and data against unauthorised access and the practice of ensuring that specific goals such as confidentiality, integrity and the availability of these data are safeguarded. All the measures impact the 'tenant' of the user.

Azure uses multiple technical measures to protect a user's data. The basic structure of all cloud supply models – IaaS, PaaS and SaaS – consists of the nine components listed in Figure 5 (network to applications).

There are diverse security measures available in the network security level such as network segmentation with filtering (allow/deny), rules (inbound/outbound), forced tunnelling (transport encryption), route specifications and the option of integrating virtualised 'appliances' (hardware firewalls). It goes without saying that there are other powerful tools such as network traffic monitoring (logging & monitoring), DNS, global traffic routing (front door) and load balancing (at the app, network and global levels).

In view of the constantly high costs of hyperscalers for security in terms of technology and staffing, from which every single user benefits disproportionately, the high level of protection of one's own data in the cloud becomes evident when compared to maintaining their own company servers. Let us look at Azure as a prime example: 3,500 security experts are employed to look after the topic of security alone, and EUR 1 billion is spent annually on security measures.

Hyperscalers are inherently responsible for highly secure IT operations – this cannot be achieved with in-house operations

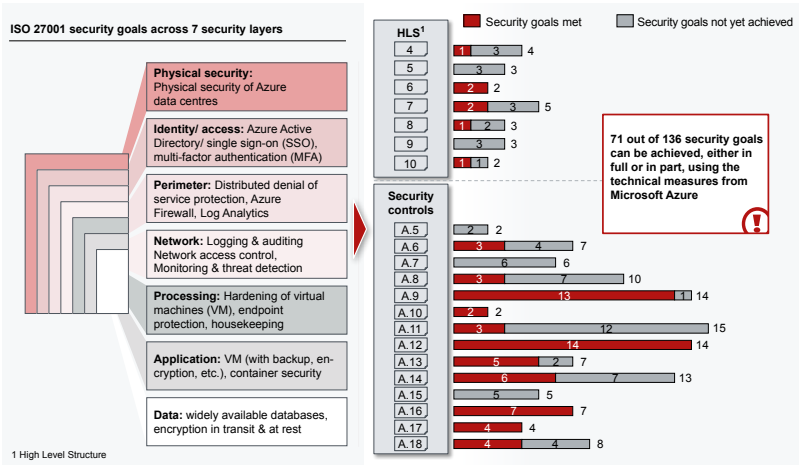
4.2 Information security in the cloud

Definition
Information security includes cybersecurity as well as the protection of information which goes beyond data – data comprises information that can be read by machines. The goals for protecting data and information are the same: confidentiality, integrity and availability. Information can come as paper documents, the spoken word in a conversation or physical data carriers.

Information security measures not only safeguard information but the end-user devices too; examples include Tools Endpoint Manager such as MDM: mobile device management (e.g. remote wipe, the roll-out of company guidelines and apps and the monitoring of compliance conformity of end-user devices) and Defender for Identity Portal (including monitoring of user activities, protection of user identities and credentials). These initiatives have an impact beyond cybersecurity measures and affect the user's own infrastructure beyond their tenant.

Azure built an ecosystem using tools that surrounds the XaaS nucleus. This is depicted in Figure 15 and is subdivided into seven security levels, from physical security to data, including the cybersecurity of the tenant. 71 of the 136 topics that are contained within the ISO standard 27001 (High Level Structure 4 to 10 and Security Controls A.5 to A.18) can be fully, or at least partially, met by the Azure ecosystem.

Overview of ISO 27001 requirements and number of associated security goals



Source: COREresearch 2021

Figure 15: Compliance in the cloud by means of automated technical processes

For instance, physical security is assured by the Azure data centres, which are secured with all structural, electronic and personal measures. Suitable certificates confirming these appropriate security measures are evidence of the quality of this physical security. These are ISO 27001 (TISAX and 27018 refer to 27001 Security Objective A.11 Physical Security), BSI C5 has its own physical security requirements that are described in Chapter '5.5 Physical Security' and subdivided into the following themes: 'PS-01 Security requirements for premises and buildings', 'PS-02 Redundancy model', 'PS-03 Perimeter protection', 'PS-04 Physical access control', 'PS-05 Protection against fire and smoke', 'PS-06 Protection against utility failure' and 'PS-07 Monitoring of operational and environmental parameters'. The security requirements of the US-American Department of Defense such as DFARS[40] and SRG[41] are also met.

Clouds meet approx. 50% of the requirements pertaining to ISO 27001 'out of the box'

[40] Defense Federal Acquisition Regulation Supplement

[41] Cloud Computing Security Requirements Guide

Business Continuity Management (BCM) is an integral part of a cloud. Backups and functionally reliable restoration are central to a BCM. Azure can help here in numerous ways. On the one hand, it has automated backups of all storage entities of a tenant, including hard drives, databases and storage allocated to VMs. On the other, it performs automated backups of a Microsoft 365 instance referred to as SaaS. Consequently, the user not only receives measures from Azure for their own tenant, but also for their company infrastructure beyond the tenant. The user must nevertheless still take care of matters such as staff, governance and all the 'non-fulfilled security goals' depicted in Figure 15.

Figure 16 describes some of the tools that are featured in the Azure ecosystem. Roughly a quarter of the 116 tools contribute directly towards security. An example of this is the Microsoft 365 information classification. Using the Microsoft information classification known as 'information protection', the user can label their office documents automatically with sensitivity labelling and company policies according to the sensitivity category. These guidelines will also take effect when the user wishes to send the classified documents by email using Outlook. For example, an e-mail to a specific customer, or which includes certain words, can be automatically encrypted.

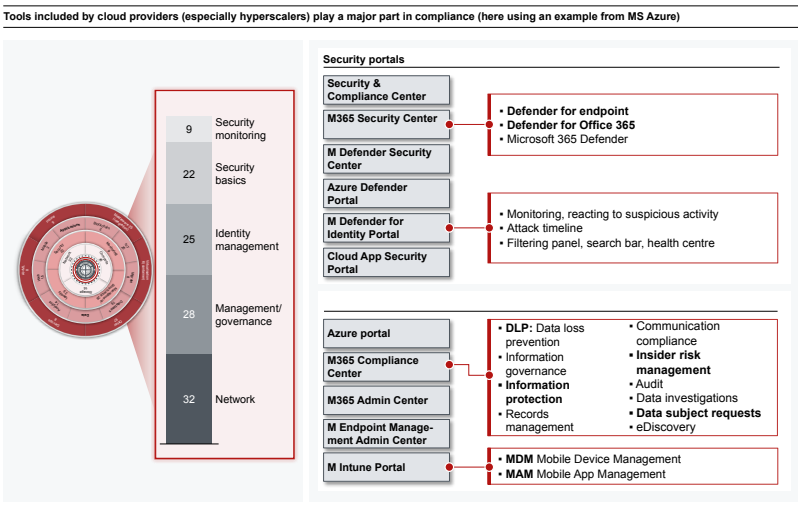


Figure 16: Compliance tools and other services using Azure

25 tools are used for identity management. Identity and access management (IAM) is carried out in the Azure Active Directory (AAD) of the Microsoft cloud, which can be synchronised with on-premise AD from Microsoft. User accounts are managed using the AD. The entire user administration, i.e. onboarding and offboarding, as well as authentication and authorisation, and also of third-party applications, is organised via Azure AD. The IAM is based on the definition of roles and responsibilities in the company, from whose tasks the necessary tools can be derived. With this granularity, this is often referred to as Role Based Access Management (RBAC).

Identity management and classification of information become less daunting as compliance monitors

The complexity of possible access and user access authorisation depends on the number of roles, tools and activities within the tools, with which principles such as segregation of duties, double-checking, least privilege, just-in-time (JIT) access during maintenance access on production data, multi-factor authentication (MFA) and self-service password reset are put into practice. Furthermore, Azure AD provides managed identity protection functions, consisting of vulnerability and high-risk account discovery as well as risk-based conditional access. In addition, PIM (Privileged Identity Management) provides the management of privileged accounts (e.g. admins), which triggers an alert to selected recipients each time they are activated. By automating the admin activities, not only is the error rate reduced, but so is the time spent and operational expenditure. Furthermore, these activities are automatically logged, meaning that they are open to scrutiny in the event of an internal random check or an audit.

'Conditional access' is yet another interesting tool in the IAM box that brings together various signals to make decisions on the basis of them and to enforce guidelines that either block, grant or use a second factor as in multi-factor authentication (MFA). Examples include the MFA which is dependent on the location (office/home, abroad) or a risk score of the login automatically calculated by AI.

4.3 Data protection in the cloud

Definition
Data protection means the protection of fundamental rights and freedoms of natural persons ('data subject') and, in particular, their right to the protection of personal data. Data protection requires adequate data security.

As a key principle of data protection, the guarantee of data security has also been enshrined in law (Art. 5 (1f) and Art. 32 GDPR). Data security is the protection of personal data by means of suitable technical and organisational measures. The goals of protection are confidentiality, integrity, availability and resilience of the systems. As previously mentioned, Azure contributes towards data security as a technical, organisational measure (TOM) in the form of IT and information security measures.

Cloud tools help to comply with data subjects' rights and the duties to delete

Based on this, Azure data protection assists with two tools 'Data Subject Requests' and 'Records Management'. Articles 12 to 20 of the GDPR govern the so-called rights of data subjects, i.e. the rights of persons whose personal data are processed by organisations. This includes the right to transparent information, the right to information, the right to correction and deletion, the right to data portability. The 'Data Subject Requests' tool allows users' accounts to be processed in the Azure AD in response to requests from a data subject.

The ‘Records Management’ tool manages, among other things, the storage and deletion settings of objects (office files, emails) with retention periods and, therefore, deletion periods. Furthermore, the tool allows settings to be approved (e.g. reading allowed, writing not possible) and blocked (e.g. deletion not possible) actions as well as logging of all activities regarding an object, including proof of the completed deletion.

4.4 Additive compliance tools in the cloud

Alongside tools for IT security, information security and data protection, the Azure ecosystem also provides other interesting tools to meet compliance requirements. The following five compliance tools are a powerful set of measures and can generally enhance the compliance of an organisation and specifically address the issues of preventing money laundering and financing of terrorism.

‘Data Loss Prevention’ (DLP) checks emails for sensitive content and, depending on the result, triggers actions such as asking the user to confirm they really want to take the intended action, notifying a control function or even prohibiting the intended action.

Data loss prevention is a typical ‘dual use’ product – a useful tool or a harmful weapon

The ‘Insider Risk Management’ minimises internal risks by detecting, investigating and responding to malicious and unintentional activities in the organisation. The user can opt to use pre-prepared guideline templates or create their own. For instance, there are templates for data theft by departing staff, general data leaks, data leaks through privileged roles (e.g. IT admin) or dissatisfied staff.

The ‘Unified Audit Log’ tool records user and admin activities in the organisation. Consequently, a check can be made as to whether a user has viewed a specific document or has deleted an item from their mailbox. The ‘Data Investigations’ tool can search for sensitive, malicious or misplaced data in all Microsoft 365 storage locations. Moreover, a check can be made as to what happened and action can be taken. Requests for judicial disclosure can be answered and the notification process for legal holds can be managed in ‘eDiscovery’.

4.5 Multicloud strategies with special provider management skills

While respecting that single provider strategies concerning cloud usage can only realistically be implemented in very few companies, the challenges stated in Chapter 3.3 must be addressed. The result of strategic considerations regarding solution elements for this are fundamental decisions for the definition of the target image for the cloud target architecture and the determination of responsibilities.

For many companies, multicloud is a necessity. Nevertheless, an explicit and concrete decision needs to be made on the target image

Irrespective of what decision is made on whether multicloud management is run in-house or via a service provider, it is important to ensure that cloud architects assemble a portfolio of cloud services that meet the current needs of business, taking into account performance and security requirements, licensing conditions and compliance requirements. In this respect it is essential to minimise the complexity of what is available on the market.

There are three possible target visions:

(1) A target vision with a single cloud service provider uses a cross-service infrastructure, where all application categories such as SAP applications, in-house developments, workplace applications and 'Software-as-a-Service' solutions are built on an IaaS platform. The prerequisite for this is that a cloud infrastructure is available that can be used by all applications. This option is often hindered by the incompatibility of the cloud for e.g. SAP services with the workplace providers' cloud.
(2) Starting with this ideal image, the second best option is to subdivide the cloud into two cloud providers. Here the choice falls on those providers that offer the possibility of mapping all cloud-based in-house developments and cloud applications obtained from third-party providers. The choice of the primary cloud providers then determines the basic structure of the IaaS, into which SAP/non-SAP services, in-house developments and SaaS solutions have to be integrated. The repercussion for subsequent extensions to the IT infrastructure is a definite restriction for all future purchasing decisions and a given cloud technology for all further in-house developments.
(3) The most complex target vision arises where it is not possible to migrate the applications necessary for the company either to the primary cloud infrastructure or onto the infrastructure of the workplace services. As a result of the challenges of integrating each additional cloud provider, the goal is to avoid, wherever possible, an infrastructure with three or more cloud providers.

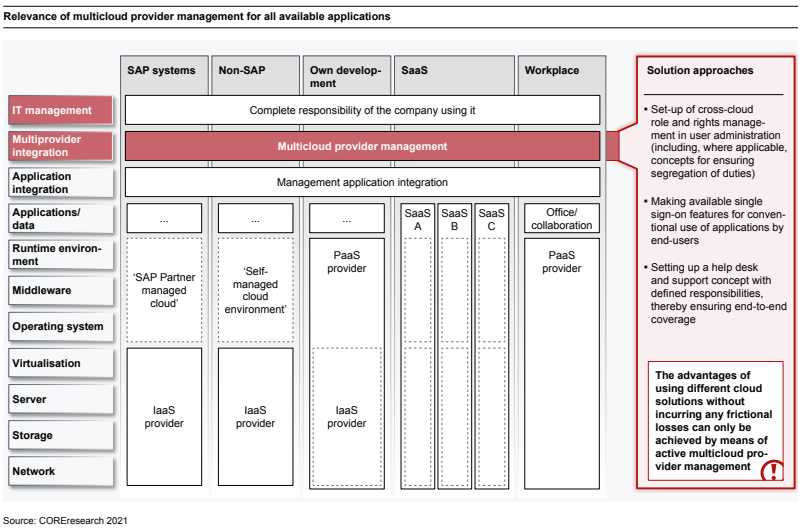


Figure 17: Utilisation of all provider strengths by means of multicloud provider management

Competence in IT management, in IT service management for operational control and monitoring of cloud services, capacities in IT architecture and IT security for 'in-house' consulting are absolutely essential for implementing a multicloud strategy and for ensuring a technical security architecture, as well as in IT security management for taking on operations, especially user administration, (see Figure 17).

Multicloud management requires special skills within the organisation

Companies need to take the decision as to whether to set up their own resources and skills or to commission specialised service providers for multicloud management. Initial specialist services are already available on the market, even though the amount of practical experience is currently low.

The offerings from multicloud management service providers can be broken down into two philosophies. The tool-based approach attempts to abstract the services of different cloud providers based on their similarities and to simplify management by providing an integrated user interface. The second approach acknowledges that a simplification of the management is achieved by means of abstracting the services of different cloud providers yet, at the same time, the conscious combination of strengths of different providers is no longer fully exploited.

Market services are currently being developed for multicloud management, actual practical experience is still low

Anticipating the customers' needs and challenges concerning multicloud management, it can be expected that providers, especially the hyperscalers, will increasingly create integrative cloud services. For instance, Google and Microsoft are already working on running SAP applications on their own cloud infrastructures, in order to reduce the time spent on and complexity of their customers' administration. Besides hyperscalers, specialised providers (e.g. meshcloud.io) are offering modules for the main challenges posed by operating in a multicloud environment. Nevertheless, it is important to emphasise here that it takes more than simply introducing a tool to be able to implement a successful multicloud strategy.

5 Conclusion

Doing without cloud services results in foregoing excellence in one's own key skills

Cloud is already a commodity. Well, at least the typical delivery models XaaS à la IaaS, PaaS and SaaS. Those who have not yet understood this no longer have any excuse for operating their own hardware; they have another problem on their hands, notably: the ecosystems provided by hyperscalers cannot be used. And it is, indeed, these that bring true added value from migration to cloud. The excellence of tools in terms of quality and number cannot be achieved by third parties. Consequently, the excellence of the company's own core competence cannot fully unfold its effect as it is abruptly thwarted by the mediocrity of the in-house IT unit that is responsible for it.

There is no point in investing in own resources such as money, time and hardware expertise because digitisation is converting everything into software. Indeed, it is those who master software that dominate the market. And the cloud is the machine that transforms hardware into software. It is also the foundation, engine room, laboratory and development department for digitisation. The foundation is built by the XaaS nucleus – the classic computing data centre of a company, i.e. server, hard drives, appliances, networks. Many companies are, if not overburdened, so heavily committed that fewer resources are available for the actual core business. And for most of the companies out there, IT is not their core business. For instance, the engine room comprises tools for integration, virtualisation, security, governance, IoT and identity management. The laboratory in the cloud is made up of tools, e.g. for data, analysis, databases and blockchain. And the development department can draw on tools for, say, artificial intelligence (AI), machine learning (ML), DevOps, web apps and mobile apps.

Increasing regulation is forcing hyperscalers to put more effort into compliance in order to always provide a compliant and non-disruptive platform for their customers' core business; non-disruptive in the sense that customers – in the best scenario – no longer need to worry about the compliance of their IT-based business. There are now also tools on the market for this, in varying numbers and covering regulatory requirements on the topics of money laundering prevention, prevention of financing terrorism, data protection and information security, including IT security. There are far more measures for the last two aspects than for the other topics. As far as information security is concerned, a cloud platform such as Azure, for example, can implement some or all of 71 of 136 security objectives of the ISO 27001 standard by means of technical measures. In terms of the above example, this basically means that a cloud user only needs to fulfil less than half of this test criteria using their own means. Compliance-as-code is becoming increasingly reality, at least for cloud users.

'Software eats the world' is meanwhile a relative common mantra used to describe digitisation. The cloud is a huge machine that transforms hardware into digitisation via software. In this respect, the cloud is democratising the availability of IT resources and, via the ecosystem of cloud tools, is also democratising development and production technologies, including artificial intelligence.

The cloud does not hold the future, it holds the present. There is no future without being aware of the past. In terms of the cloud, there is no future without the present.

Bibliography

@DKB.de. (24 March 2020). *twitter.com/DKB_de.* Retrieved from https://twitter.com/DKB_de/status/1242417794303606785

Amazon Web Services. (24 August 2006). *Announcing Amazon Elastic Compute Cloud (Amazon EC2) –beta*. Retrieved on 2 February 2021 from https://aws.amazon.com/de/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/

Amazon Web Services. (2015). *AWS-Fallstudie: Stripe.* Retrieved on 17 March 2021 from aws.amazon.com: https://aws.amazon.com/de/solutions/case-studies/stripe/

Amazon Web Services. (2018). *AWS-Fallbeispiel: Home24.* Retrieved on 17 March 2021 from aws.amazon.com: https://aws.amazon.com/de/solutions/case-studies/home24/

Official Journal of the European Union. (06 July 2016). *Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Retrieved on 8 April 2021 from EUR-Lex: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148

Beiersmann, S. (24 February 2016). *Spotify zieht in die Google Cloud um.* Retrieved on 17 March 2021 from zd.net: https://www.zdnet.de/88260948/spotify-zieht-in-die-google-cloud-um/

Bitkom. (2020). DS-GVO und Corona – *Datenschutzherausforderungen für die Wirtschaft (GDPR and COVID-19 Data Protection Requirements for Business)* Retrieved on 19 02 2021 from https://www.bitkom.org/sites/default/files/2020-09/bitkom-charts-pk-privacy-29-09-2020.pdf

Bitkom Research, KPMG. (2020). *Cloud Monitor 2020.* Retrieved on 2 February 2021 from https://www.bitkom.org/sites/default/files/2020-06/prasentation_bitkom_kpmg_pk-cloud-monitor.pdf

Federal Office for Information Security (BSI). (October 2020). *Cloud Computing Compliance Criteria Catalogue – C5:2020.* Retrieved on 8 April 2021 from https://www.bsi.bund.de: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

Federal Financial Supervisory Authority (BAIT). (26 October 2020). *Banking Supervisory Requirements for IT (in German).* Retrieved on 8 April 2021 from the mailshot 10/2017 (BA) dated XX.XX.2020: https://www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2020/dl_kon_13_20_BAIT.pdf?__blob=publicationFile&v=4

Federal Financial Supervisory Authority. (14 September 2018). *BAIT Bankaufsichtliche Anforderungen an die IT (Banking Supervisory Requirements for IT).* Retrieved on 8 April 2021 from the mailing 10/2017 (BA) dated 14.09.2018: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=9

Federal Financial Supervisory Authority. (01 October 2019). *Kapitalverwaltungsaufsichtliche Anforderungen an die IT (Supervisory Requirements in IT for German Asset Managers).* Retrieved on 8 April 2021 from the mailing 11/2019 (WA) dated 1.10.2019: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1911_kait_wa.pdf;jsessionid=1AE63BF6AD0868C106685ACF039322D9.2_cid383?__blob=publicationFile&v=3

Federal Financial Supervisory Authority. (20 March 2019). *Versicherungsaufsichtliche Anforderungen an die IT (Supervisory Requirements in IT for Insurance Undertakings).* Retrieved on 8 April 2021 from the mailing 10/2018 (VA): https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1810_vait_va.pdf?__blob=publicationFile&v=5

Federal Ministry of the Interior. (17 June 2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS Strategy).* Retrieved on 8 April 2021 from https://www.bmi.bund.de/: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf;jsessionid=9C09997EB074A0C40F94809302B1297A.1_cid295?__blob=publicationFile&v=3

Buski, M., Dymala, M.-A., & Dr Grudzien, W. (June 2020). *Leverage Data Protection - Time to End the Debate.* Retrieved from CORE.SE - Technmonitor: https://core.se/fileadmin/WhitePapers/20200616_CORE_Whitepaper_Das_Ende_der_Karenz-Datenschutz_nutzen_DE_v1.0.pdf

Caumanns, V. (April 2020). *Geheimnisschutz mit ISO-Normen und DSGVO.* Retrieved on 18 March from dialog.dqs.de: https://dialog.dqs.de/acton/attachment/40656/f-bd8bc3d8-a17f-4325-b9f2-88f3dccdd02f/1/-/-/-/-/Geheimnisschutz%20mit%20ISO-Normen%20und%20DS-GVO.pdf

Cloudride LTD. (07 January 2021). *CI/CD as a Service: 10 Solutions for Continuous Integration and Delivery in the Cloud.* Retrieved on 2 February 2021 from medium.com: https://medium.com/@cloudride_il/ci-cd-as-a-service-10-solutions-for-continuous-integration-and-delivery-in-the-cloud-c57e1a74562b

European Commission. (24 September 2020). *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors.* Retrieved on 8 April 2021 from EUR-Lex: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0595&from=DE

Francke, S. (27 August 2020). *Vertrauen der Finanzdienstleister in die Cloud wächst.* Retrieved on 8 April 2021 from Springer Professional: https://www.springerprofessional.de/en/bank-it/datenschutz/vertrauen-in-die-cloud-unter-finanzdienstleistern-waechst/18316182

Gartner. (23 July 2020). *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020.* Retrieved on 2 February 2021 from https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

IDG Research Services. (2020). *Studie Cloud Native 2020.* Deutschland. Retrieved on 2 February 2021 from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/industry-operations/CloudNative_IDG-Studie_Deloitte_2020.pdf

IDG Research Services. (2020). *Studie Cloud-ERP 2021.* Retrieved on 2 February 2021 from https://whitepaper.cio.de/uploads/files/03f246457d0b42b7474bb53bcc0b3ae6eec2dfb0.pdf

interxion. (14 May 2019). *Fast alle Unternehmen in Deutschland beschäftigen sich mit der Multi-Cloud.* Retrieved on 8 April 2021 from https://www.bsi.bund.de: https://www.interxion.com/de/whitepapers/cloud-trends--wege-aus-dem-cloud-chaos

ISO (International Organisation for Standardisation). (October 2013). *Information technology — Security techniques — Information security management systems — Requirements.* Retrieved on 8 April 2021 from ISO/IEC 27001:2013: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Kirchner, C. (25 March 2020). *Das Online-Brokerage der DKB geht erneut in die Knie.* Retrieved on 2 February 2021 from https://finanz-szene.de/digital-banking/das-online-brokerage-der-dkb-geht-erneut-in-die-knie/: https://finanz-szene.de/digital-banking/das-online-brokerage-der-dkb-geht-erneut-in-die-knie/

Lemos, R. (15 April 2010). *Cloud Computing: Early Adopters Share Five Key Lessons.* (Published by cio.com) Retrieved on 17 March 2021 from cio.com: https://www.cio.com/article/2418957/cloud-computing--early-adopters-share-five-key-lessons.html

Lünendonk & Hossenfelder. (2020). *Cloud Transformation – Strategien und Maßnahmen von Banken und Versicherungen auf dem Weg in die Cloud.* Retrieved on 2 February 2021 from https://www.luenendonk.de/produkte/studien-publikationen/luenendonk-trendstudie-2020-cloud-transformation-strategien-und-massnahmen-von-banken-und-versicherungen-auf-dem-weg-in-die-cloud/

Lünendonk & Hossenfelder. (2020). *Digital Outlook 2025: Financial Services.* Retrieved on 19 February 2021 from https://www.luenendonk.de/produkte/studien-publikationen/luenendonk-studie-2020-digital-outlook-2025-financial-services/

National Institute of Standards and Technology. (September 2011). *The NIST Definition of Cloud Computing.* (Published by U. D. Commerce) retrieved on 2 February 2021 from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Netflix. (11 February 2016). *Completing the Netflix Cloud Migration.* Retrieved on 17 March 2021 from Netflix.com: https://about.netflix.com/en/news/completing-the-netflix-cloud-migration

Reckwitz, A. (2019). Das Ende der Illusionen. Politik, Ökonomie und Kultur in der Spätmoderne. Berlin: Suhrkamp Verlag (Publisher).

Authors

Nicolas Freitag is a transformation manager at CORE. Nicolas uses the experience gained from training as a a banker, studying economics and long-term development of career networks throughout Germany for his clients in the preparation of corporate strategies, development of digital business models as well as the management of agile software developments.

Nicolas Freitag
nicolas.freitag@core.se

Markus Frik is a transformation associate at CORE. After graduating as an economics engineer at Karlsruhe Institute of Technology (KIT), he was able to gain experience in various cloud transformation projects. Markus assists customers from the financial services industry in implementing applications – from specifications to 'go live' – and builds information security and anti-financial crime (AFC) management systems.

Markus Frik
markus.frik@core.se

Waldemar Grudzien is an expert director at CORE. He has more than 26 years of consulting experience and is well-versed in the special challenges posed by IT transformations driven by compliance. His main area of responsibility is information security and data privacy – in theory and practice, including operational activities as an ISO and DPO for various customer structures.

Dr Waldemar Grudzien
waldemar.grudzien@core.se

Nadine Hofmann is an expert manager at CORE. She studied aerospace engineering in Braunschweig (Lower Saxony) and Dresden. Her main area of management consultancy concentrates on technical data protection and information security (main areas are IAM, managing risks, ISO 27001 and GDPR). She supports clients in structuring and setting up financial compliance systems.

Nadine Hofmann
nadine.hofmann@core.se

Author team

Christian Böhning is a managing director at CORE. He has many years of experience in carrying out digital transformation projects in industries that are permanently changed by IT. His work focuses on programmes for modernising IT architecture, implementing compliance initiatives and realignment of IT organisations.

Christian Böhning
christian.boehning@core.se

Philipp Gampe is an engineering manager at CORE. He studied informatics in Bonn and Potsdam. As a specialist in cloud infrastructures and architectures, he implements new projects in the cloud and assists in the migration of existing applications. Furthermore, he assists in automating the deployment and development processes as well as extensive automated testing.

Philipp Gampe
philipp.gampe@core.se

Calvin Klee is a transformation manager at CORE. He graduated from the Royal Holloway University of London with a BSc degree in management. Calvin has experience in the migration of core banking systems and implementing payment platforms. His main areas of activity are in coordinating project management and orchestrating business cases.

Calvin Klee
calvin.klee@core.se

Ronny Raschkowan is an expert manager at CORE. He studied business administration and international relations. Ronny manages the IT department at CORE and assists clients with cloud migrations, focussing on infrastructures, the modern workplace and mobile device management. His security expertise is rounded off with experience in ISO 27001 certification and as Deputy ISO at CORE.

Ronny Raschkowan
ronny.raschkowan@core.se

About COREresearch

As an independent technology think tank, we research the systematics of technology-driven transformations in industries with a high degree of IT involved in the value creation process. As part of our research activities, we analyse markets and technologies, address the structures, causes and mechanisms of change and curate results for clients and the public. Furthermore, we make selected results of our interdisciplinary research available to a broader Chapter of the public in the form of comprehensive publications, case studies as well as lectures.

CORE

https://core.se

https://core.se/publications/white-paper

Disclaimer

CORE SE
Am Sandwerder 21–23
14109 Berlin| Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21–23
14109 Berlin| Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se