Unrealistic or feasible from a risk perspective?

Running business application workloads in the Public Cloud

25 juli 2018

Rada Machluf and Delil Akdeniz

Many enterprises face a number of challenges as they are moving their application workloads to the cloud. What are the most relevant associated risks, and how can they be mitigated? This article gives IT Auditors some pointers in this area.

Cloud computing emerged around the end of the previous century with Software as a Service (SaaS) solutions. One of the biggest players at the time was Salesforce, a company that developed web-based enterprise applications that could be reached via the internet. Not too long after that, other – currently well-known cloud players such as Amazon Web Services (AWS), IBM, Google and Microsoft [MOHA09] – entered the market. They extended the existing cloud services offering with Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) services. Today, the cloud market is still dominated by these same players, with AWS being the biggest by far. Based on figures presented by Gartner, AWS market share in 2017 was almost 50 percent. Microsoft Azure (hereafter: Azure) came in second with a 10 percent market share.

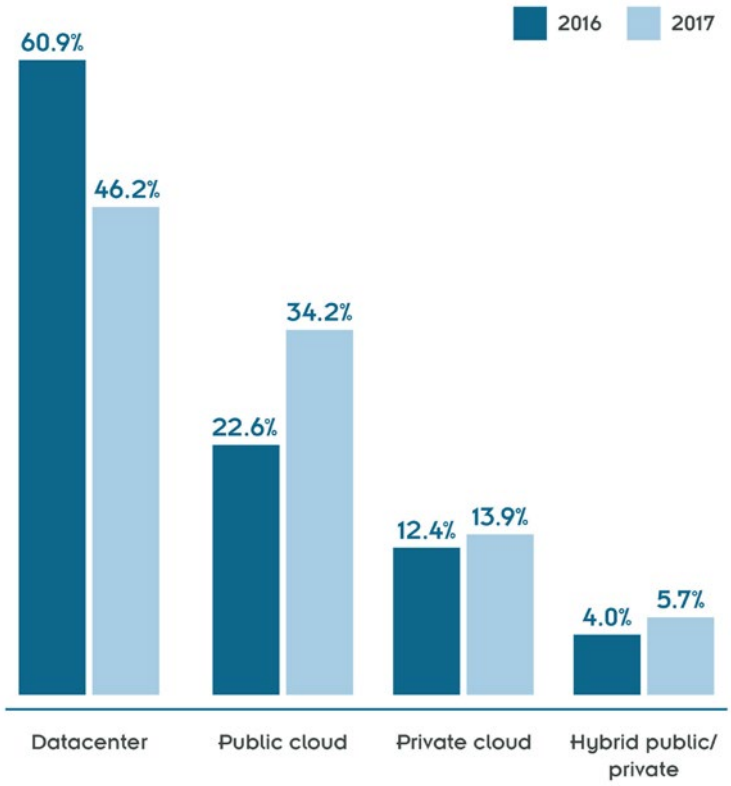

Figure 1: Hosting environments of application workloads [CSA17b]

Today, evermore enterprises are moving application workloads from their data centres to (especially) the AWS and Azure clouds. Based on Cloud Security Alliance research results, almost 35 percent of application workloads were hosted on a public cloud infrastructure by the end of 2017 (figure 1). The question 'why organisations move to the public cloud' will not be answered in this paper, as multiple articles have already been written for this purpose. This paper will also not focus on private cloud implementations, as these have been discussed in earlier published articles for IT auditors, like in 'Auditen in de cloud'. [CARL16] Here we describe the main challenges that a professional organisation will face when implementing application workloads on a public cloud infrastructure, from an IT auditor's perspective. Our aim is to inform IT auditors on this open audit area, assist in outlining the most relevant associated risks, and provide them with recommendations on how to mitigate those.

Configuring a public cloud infrastructure

Moving application workloads to a public cloud environment will immediately raise one of the most burning questions from IT auditors' perspective: How can the data's security and privacy be ensured in a multi-tenant environment? To answer this question, one should be aware of the different cloud services that can be used in a public cloud deployment model.

Dedicated physical systems for storage of customer data is not what a typical cloud customer should be seeking for when considering a move to the public cloud. While this might be an option to be considered for highly classified systems and/or data, it would be rather expensive and is therefore not frequently considered by the average organisation. As a side mark, it should be noted that if a dedicated environment is deemed required, the organisation should reconsider whether a move to public cloud is desirable at all.

In some cases, cloud customers can select a dedicated environment in the cloud, physically segregated from other customer's environments. Usually however, the more affordable logical isolation of environments suffices. Logical isolation refers to a configuration that blocks any communication between environments. This can be set up in detail by using specific cloud services. The setup first starts with the network setup.

A cloud customer can configure its own virtual 'data centre' in the public cloud. For example, AWS gives the option to configure a virtual private cloud (VPC) that is logically separated from other AWS customer environments[1]. The customer can then deploy his workloads in the VPC and has full management control of network technicalities, such as IP addresses, subnets, routing and gateways configuration. As an example, the cloud customer can configure front end (internet-facing) servers by assigning them to a public IP address range and assign the back-end storage systems to a private IP address range within one VPC. Furthermore, the customer can securely connect the back-end (private

subnets) of the VPC to its on-premise data centre and in this way create an extension to its on-premise data centre. This results in a hybrid network. It should however not be considered as a 'plug and play' service that a customer can simply use after purchase. Before the customer can use the cloud service, a hardware connection should be set up between their on-premise data centre and the VPC. This can either be done by using a service from the cloud provider (e.g. AWS's Virtual Private Network) or by using third party direct connect services (e.g. Verizon's Secure Cloud Interconnect). Next, the customer should configure their own network to enable communication with the VPC.

The VPC takes care that organisational data is logically segregated from other cloud customer data, ensuring that only the customer concerned is in control of all management issues, such as networking and operating system management, application and data management – depending on the IaaS/PaaS/SaaS services being deployed within a VPC – and the monitoring of their VPC on all these levels. Their virtual infrastructure will run on the cloud provider's pooled resources, in other words the physical configuration of servers and the network and storage infrastructure.

Both the organisation and the auditor must consider the risks related to a hybrid network. From a security perspective the maturity levels of the interconnected networks should match. Connecting a secure network in the cloud to significantly less secure other networks – on premise or otherwise – will affect the entire environment: 'security in a chain is as strong as its weakest link'. Also, configuring hybrid connections between old (hardware based) and cloud (software defined) environments increase network management complexity. [MOGU17] To mitigate part of the security risk from an identity and access management (IAM) perspective, a customer might implement a federation service. This allows to federate user identities and authorisations to the cloud environment, while identity management remains centralised on premise IAM systems, such as Windows Active Directory.

In general, the security controls an IT auditor should consider regarding isolation, segregation, firewalling, monitoring et cetera, do not change in a public cloud environment. The IT auditor must still consider any required network segregation and monitoring requirements from business or regulatory perspective. What does differ is the fact that segregation and monitoring techniques are software defined and highly automated in a public cloud environment. From an IT auditor perspective, in most cases this will impact the test approach rather than the control settings. When performing an IT audit, the monitoring information, provided through native cloud services, enables the auditor to collect most of the required information from within his own organisation. Surely, information related to any layer down from the virtual machines (hypervisor, servers, storage, networking and physical data centre environment) is stored at the cloud provider's side and not accessible by cloud customers. The only sources of information on these layers are third party assurance reports, which have limited value as audit evidence (see also section 'Shared responsibility model').

In the next section we will describe new ways of developing and deploying cloud systems in a virtualised environment and their impact on traditional control testing.

DevOps and Continuous Integration / Continuous Delivery

DevOps and Continuous Integration / Continuous Delivery (CI/CD) emerged with the rise of 'agile' working and new automated techniques provided by public cloud services. Both methodologies are becoming the new standards for developing and operating systems and applications (in the cloud). What are DevOps and CI/CD pipelines and what is their link with public cloud?

DevOps

DevOps is a new method and way of working to enable automated system and application development and deployment. [MOGU17] In the traditional world the two activities, development and operations, are physically separated, as both require different abilities and segregation of duties to maintain adequate control over operational systems. When development activities are completed, the software is handed over to the business, and then managed by the operators and administrators. In the DevOps world there is no handover anymore, as both the development and operations activities are performed by the same team, with a high focus on automation. This requires real combined abilities within the DevOps team and a new operating model.

CI/CD

Continuous Integration (CI) is a software development method used by DevOps teams to enable multiple daily integrations of new code into a single piece of software. The integrated code is validated by an automated test to detect possible integration errors and verify that the new functionality meets the agreed quality levels. This shortens feedback loops and decreases time and cost to correct software errors. Continuous Delivery (CD) is a method to ensure every new coded functionality is ready for release. Because the delivered piece of code is relatively small, compared to traditional software development, and is delivered in an automated and repeatable way, customer feedback can be followed up faster. This considerably speeds up the software delivery process and enhances development efficiency if done correctly. Continuous Delivery should not be confused with Continuous Deployment. The latter means that a piece of software can be directly used by end-users with no (manual) intervention needed and all required service management processes integrated. This differs from Continuous Delivery, where the business ultimately decides on when to release the new functionality to their end-users. [ABNA17] See figure 2 for an overview of the CI/CD process.

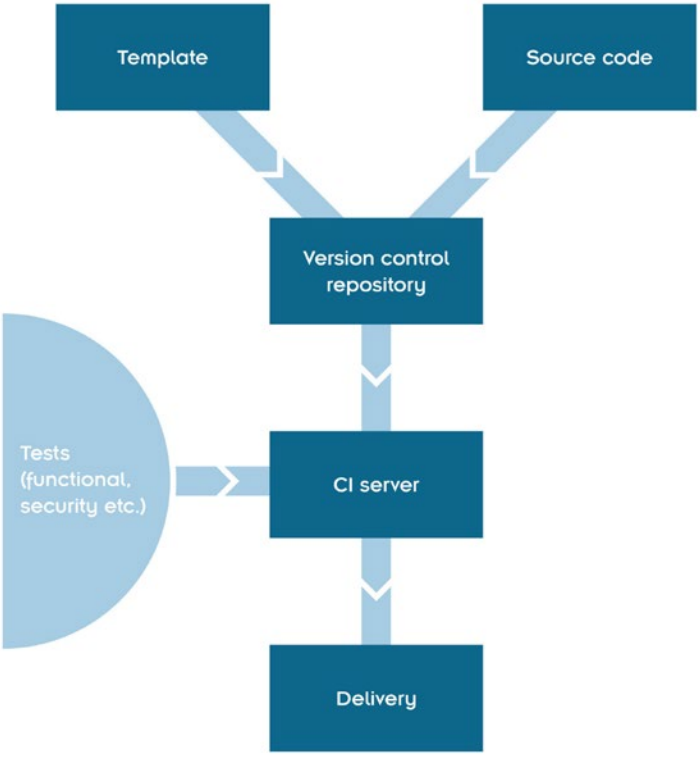

Figure 2: CI/CD pipeline [MOGU17]

DevOps and CI/CD are not exclusive to public cloud environments, but they integrate seamlessly with automated cloud services and are heading to become the most applied cloud application delivery model. [MOGU17]

In the public cloud, both infrastructure (servers, network components) and applications can be coded and delivered via automated CI/CD pipelines. Once a specific deployment template for an infrastructure system is approved, e.g. a Windows server, it can be used as a master template to quickly deploy multiple servers into the cloud environment. Developers can code any required settings in the template, based on the organisation's security requirements, such as hard disk encryption, backup settings, subnet settings et cetera. They may also choose using vendor-provided pre-hardened images in their template, to ensure that the systems deployed comply with the required security standards. Such images are based on industry best practices like Center for Internet Security baselines. In such an environment no individual changes are made to virtual machines. All changes are implemented in the master template and/or associated image, then tested and next deployed to all machines simultaneously.

Risks and opportunities to consider

A developer must translate business requirements in the best possible way into automated functionality, while an operator or administrator traditionally focuses more on maintaining confidentiality, integrity and availability of the functionality. For example, traditionally, it is the server administrator who is familiar with the processes of patch

management, configuration management, incident management, problem management, backup and recovery et cetera. The question is whether this knowledge is sufficiently available in a DevOps team. In our experience, the first DevOps teams mostly comprise traditional developers that lack experience in applying and maintaining traditional IT controls.

Furthermore, secure development of cloud systems should be a main attention area for both the DevOps teams and IT auditors. Secure development of cloud applications and infrastructure systems in public cloud requires organisations to design coding standards and to educate and train their employees to adhere to these standards. Like application code, infrastructure code can be affected by security flaws. As a result, quality and security of both application and infrastructure code must be properly tested during the development phase. While it is possible to do this manually, this testing should be automated as much as possible, as this enables organisations to optimise the advantages of public cloud capabilities. Automating the tests can be done by integrating required code quality/security tests into the CI/CD pipeline.

The traditional types of testing (static, unit, functional and dynamic) should be integrated with security tests to validate if security features built into the infrastructure and/or application work adequately. Also, integrating vulnerability scanning in the CI/CD pipeline is recommended. This allows, for example, to validate that no outdated software is used, no insecure encryption mechanisms are applied or insecure (application) interfaces are programmed.

Lastly, management of access rights to the CI/CD pipeline, including code configurations is another important risk area to take into account. This does not differ from traditional control testing, as the IT auditor must ensure that, just like in the traditional environment, segregation of duties is implemented. Only a limited number of authorised personnel must be allowed to update code configurations and even less should be authorised to deploy code to production. Furthermore, the pipeline must remain in a dedicated client environment, to minimise the risk of code disclosure to third parties. Surely, even when changes are controlled and applied via a tight CI/CD pipeline, monitoring of the production environment for baseline deviations remains necessary.

Auditors are also able to reap the benefits from this new way of working, as the CI/CD pipelines can log any activity, including any change to code configuration files on the user level, and retain full history of developed software in a version control repository. This can be used as evidence for testing purposes, if of course the general IT controls regarding the CI/CD pipeline are operating effectively.

Hereafter, we will shift focus to the shared responsibility model. Where does the demarcation in control responsibility start between a cloud customer and a cloud

provider? This model, if clarified between both parties, forms the basis for maintaining continuous compliance.

Shared responsibility model

The root cause of many public cloud concerns is a lack of clarity over the shared responsibility model. [MUNC17] To prevent any misconceptions it is important to understand the shared responsibility model before moving to the cloud. Cloud providers offer considerable advantages for security and compliance efforts, but these advantages do not absolve the customer from taking their own measures to protect their users, applications, and service offerings. Organisations can use tools like the CSA Cloud Controls Matrix [CSA17a] to assess and document cloud project security and compliance requirements and controls, as well as who is responsible for each.

Compliance in the cloud, similar to security, is achieved by design and by adherence to a shared responsibility model. The demarcation of responsibilities between the cloud provider and the cloud customer, highly depends on the selected service model (IaaS, PaaS, SaaS), deployment model (public, private, community, hybrid), and to a lesser extent on the particular cloud provider. To be clear, final responsibility of the security of customer data, always rests with the cloud customer. The customer should ensure that their data is continuously controlled and secured in line with the data classification and its organisation's policies and standards. Technical and/or organisational risk mitigating measures will have to be taken by both the provider and the customer. In this article the demarcation of those tasks will be referred to as 'responsibilities'. We will explain the shared responsibility model by comparing all three service models (IaaS, PaaS, SaaS), see table 1.

In general, with cloud service models, the customer's responsibility increases the lower you go down the IT stack. Most of the responsibilities for the cloud customer lay with the IaaS model. As a cloud customer, you can outsource the lowest computing level elements to a cloud provider, from the physical data centre environment up to the virtualisation layer. From here, the cloud customer must design, develop and implement its own systems and controls. In this model, it is the customer's responsibility to install, configure, patch, update, and maintain the operating system, and any middleware and application software installed. The cloud provider will typically bill the customer for computing power by the hour and the amount of resources allocated and consumed, as per its service level agreement (SLA).

With the PaaS model, customers receive a core hosting operating system and optional building block services that allow them to develop and run their own applications or third-party applications. Customers will not have to deal with lower level elements of infrastructure such as network topology and load balancers, as all this is covered by the

cloud provider. The provider provides them with a fully functional operating system with major platform software.

With the SaaS model, customers consume (business) applications as a service. The SaaS provider manages the entire cloud infrastructure, while in most cases the customer is required to manage some minor application level (IAM) controls only. [KUMA13]

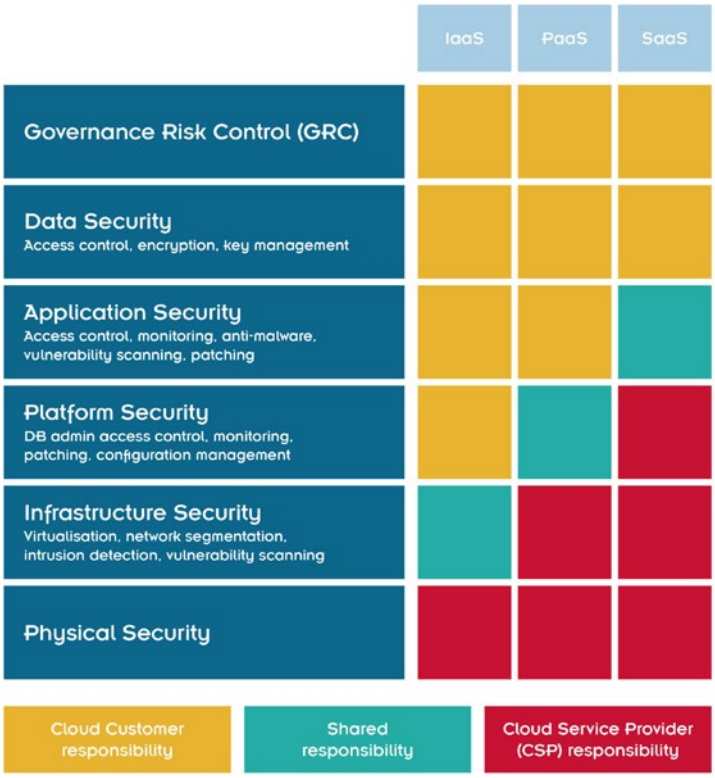

Table 1: Shared responsibility model

In the next section, we will outline some specific risks and controls to consider as part of the shared responsibility model, from the compliance, legal and regulatory perspectives.

Compliance, legal and regulatory considerations

Compliance requirements cannot be outsourced. Because a cloud customer remains responsible for its data at all times, he also remains accountable for ensuring compliance with legal and regulatory requirements. It is essential that all areas that are unclear be clarified prior to signing the contract between the customer and provider. It is important to involve all internal stakeholders (e.g. legal, compliance, risk, audit) to identify potential compliance gaps while negotiating the contract. Analysing compliance gaps in an early stage with subject matter experts from the customer's first and second line of defence, will give the organisation time to decide whether to mitigate the gap or accept its risk.

Right to audit

A fundamental compliance discussion, especially for regulated financial institutions, is the inclusion of the right to audit clause in (public) cloud contracts. Several laws, regulations and guidelines are applicable and address this and other requirements for financial organisations when services are outsourced. The general rule that applies is that outsourcing of important operational functions may not be undertaken in such a way as to impair materially the quality of its internal control and the ability of the supervisor to monitor the firm's compliance with all obligations. The most recent and most applicable guidelines on outsourcing to cloud service providers were released by the European Banking Authority (EBA) in December 2017. [EBA17] The EBA recommendations [EBA17, section 4.3] explicitly state that a written agreement with a cloud service provider should contain provisions for:

- Full access to business premises, including the full range of devices, systems, networks and data used for providing the outsourced services (right of access).
- Unrestricted rights of inspection and auditing related to the outsourced services (right of audit).
- The effective exercise of the rights of access and audit should not be impeded or limited by contractual arrangements.
- The outsourcing institution should exercise its rights to audit and access in a risk-based manner. Where an outsourcing institution does not employ its own audit resources, it should consider using at least one of the following tools:
  - pooled audits;
  - third-party certifications and third-party or internal audit reports – acceptable only under specific conditions regarding scope, coverage of key controls, aptitude of the certifying organisation, use of widely recognised standards, right to request the expansion of scope of the certifications.

As such, regulated financial institutions should have effective audit rights included in the agreement with their cloud service provider. However, where in traditional outsourcing agreements a right to audit clause used to be rather easy to include, public cloud providers will usually reject this. This changed attitude results from fundamental differences between traditional outsourcing as compared to outsourcing to a public cloud provider. Table 2 outlines the main differences between the two types of outsourcing.

Traditional Outsourcing	VS	Outsourcing to a public cloud provider / Consuming a cloud service
Outsourcing of process /system 'as is'.	——	Standardised (cloud) service, process/system.
Vendor is only allowed to change the outsourced service after approval from/notification to client.	——	CSPs can change their services at their own discretion. Clients are not necessarily involved or informed.
Bespoke contract, tailored to the needs of both parties.	——	Standard contracts without tailor-made arrangements.
Client has negotiating power.	——	CSPs have negotiating power.
Client's policies and standards apply.	——	Policies and standards of the CSPs apply.
Client has negotiating power.	——	CSPs have negotiating power.
Client's policies and standards apply.	——	Policies and standards of the CSPs apply.
Right to audit/examine can be agreed upon.	——	No right to perform audits/inspections.
Bespoke service delivery reports.	——	Standard reporting facilities.
2nd Line of Defence can perform its oversight and risk control duties.	——	2nd Line of Defence are not allowed the access to perform its regular oversight and risk control duties.

Table 2: Traditional outsourcing versus outsourcing to public cloud providers

Major cloud providers will provide their customers with third party assurance reports or industry attestations such as PCI DSS, SOC1, SOC2, HIPAA, as a means to cover the right to audit gap. These reports however, need to be understood by the cloud customer within their boundaries [MOGU17]:

- These reports are a statement 'over a period of time' and will not be valid at any future point;
- They certify that the provider is compliant with the framework that was audited against;
- Any service that a customer builds on top of the provider's compliant infrastructure/ platform should be assessed separately;
- The scope is limited; cloud customer should assess which specific features/services are covered in which locations and jurisdictions;
- What set of controls are in scope, are these controls sufficiently aligned with customer's compliance needs;
- The possibility to disclose and review evidence of test work performed by the third-party auditor.

In the end the fundamental question remains: Can an organisation's internal audit department or their external accountant fully rely on the third-party reports? And if not, what additional activities can be taken to fill any identified assurance gaps? Taking these

questions and limitations into consideration, the IT auditor may never solely rely on the fact that an assurance report has been made available by the cloud provider. The report contents must always be reviewed, and additional means must be used to fill any applicable assurance gaps. Examples are performing a separate audit either individually or in a pool with other cloud customers, reviewing evidence of test work performed by third party auditor, and performing an interview with the third-party auditor.

Legal concerns

Typically, cloud providers and cloud customers are operating across multiple jurisdictions. Data in the cloud means that it is constantly in motion and to ensure high availability it is being stored in multiple locations concurrently. [CART17] As a result, different data protection regulations might apply depending on the region where the data is stored. These different data protection regulations can pose a risk for organisations if local legal and regulatory requirements are not met. Legal concerns like these regarding cloud usage have also been discussed earlier in articles published in the IT-Auditor. [SMIT16] To secure its data, organisations should understand not only the legal implications of where the cloud provider physically operates and stores data, but also which relevant regulatory frameworks and restrictions apply in a country where its business headquarters is based. To avoid many of these legal implications, most cloud customers will prefer using data centres of cloud providers in the same jurisdictional region.

The General Data Protection Regulation (GDPR), which came into force on May 25, 2018 for all EU member states, as well as members of the European Economic Area (EEA), is the most prominent regulation. The GDPR introduces numerous obligations for organisations that process personal data. [MOGU17] For example, the GDPR requires organisations to keep records of their data processing activities. Organisations are expected to develop and operate their products and services in accordance with 'privacy by design' and 'privacy by default' principles. The transfer of personal data outside the EU/EEA to a country that does not offer a similar level of protection of personal data and privacy rights is prohibited. To prove that it will be offering the 'adequate level of protection' required, an organisation may use one of the different optional legal mechanisms. In addition, GDPR requires organisations to report that they have suffered a security breach within 72 hours of the organisation becoming aware of the incident. Because the violations of the GDPR expose an organisation to significant sanctions, cloud customers should understand the legal implications of using particular cloud providers and check those against their legal requirements.

As opposed to managing traditional data centres, the concept of multi-tenant cloud computing adds an extra layer of legal complexity. The concept that different cloud customers share the same physical hardware, makes the cloud provider contractually bound not only to your organisation, but also to other organisations. Potentially, any of the cloud providers or one of its customers could be subject to an e-discovery process,

carried out by law enforcement authorities, in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. [CATT12] In some cases, storage media or other hardware might be seized as evidence. A loss of control over access to organisational data should be addressed not only in a contract with the cloud provider, but also in the organisational incidents response and business continuity plans.

Lastly, exit strategy and system portability are two important aspects to consider in the early stage. These allow a cloud customer to easily move between cloud providers at any later stage during the production lifecycle. This requires the cloud customer to take into account and assess the characteristics and features of a system or application that can lead to a vendor lock-in.

Conclusion

We ended our article with an outline of how to ensure compliance with regulations when considering running business workloads in a public cloud environment. This entails the most important aspects that professional organisations should consider, especially regulated organisations such as financial institutions. After the move to public cloud, the adequate implementation of the shared responsibility model within the cloud customer's organisation, defines the level of success in remaining compliant with its regulatory, legal and security requirements. IT auditors should consider these compliance requirements, both up front and during the production lifecycle. They should be aware of risks and opportunities that arise with changing methodologies and ways of working in a public cloud environment. The opportunities to securely implement a public cloud environment are there. The question remains whether organisations will dare to make the move and change their way of working in order to obtain full advantage of public cloud services.

Final note

Just before the publication of this paper the US federal government implemented the Clarifying Lawful Overseas Use of Data Act, also known as the CLOUD Act. This act enables US law enforcement agencies to warrant US cloud and communication companies and obtain electronic stored (customer) data, regardless of the physical storage location. As a result, any European institution that makes use of cloud services provided by US companies like Microsoft, Amazon, IBM, and Google is affected by this act, even if both contractual and logical controls have been implemented to preserve the storage of data in EU-based data centres. [CLOU18], [DECH18]

This development certainly impacts our conclusion regarding the secure use of (public) cloud services, as data privacy (e.g. storage location and access by external parties/foreign authorities) is considered to be one of the primary concerns of (regulated) institutions in relation to the use of the cloud. Current and potential cloud customers must closely monitor the further developments in this area and consult with their legal and compliance professionals in assessing the exact (potential) impact for their institution. Just as the cloud companies were moving towards pole position in onboarding especially regulated European institutions, this development might lead to an interesting turn in the way cloud services will be used and/or implemented by non-US based companies. Perhaps the idea of national or regional clouds will start to rise again – or will we further break the principles of territoriality by allowing US authorities to enforce their laws over European (and other continents') companies and their data?

Literature

[ABNA17] ABN AMRO CI/CD internal Wiki, 2017.

[CARL16] A. Carlier-Algoe, X. Bordeaux, S. Scheuller. Auditen in de Cloud. De IT-Auditor, 2016: https://www.deitauditor.nl/business-en-it/auditen-in-de-cloud/ (retrieved on 12 July 2018).

[CART17] D. Carter. *All-In-One Certified Cloud Security Professional Exam Guide.* McGraw-Hill Education, 2017.

[CATT12] D. Cattedu, G. Hogben, T. Haeberlen, L. Dupré. *Cloud Computing risks and recommendations for information security*. ENISA, 2012.

[CLOU18] *Bill 'Clarifying Lawful Overseas Use of Data Act' or the 'CLOUD Act'*, 115th US Congress 2nd Session: https://www.hatch.senate.gov/public/_cache/files/6ba62ebd-52ca-4cf8-9bd0-818a953448f7/ALB18102%20(1).pdf (retrieved on 11 june 2018).

[CSA17a] *Cloud Controls Matrix v3.0.1*, 2017 update: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/ (retrieved on 11 june 2018).

[CSA17b] *Custom Applications and IaaS Trends*. Cloud Security Alliance, 2017: https://cloudsecurityalliance.org/download/custom-applications-and-iaas-trends-2017/ (retrieved on 11 june 2018).

[DECH18] Dechert, *Forecasting the Impact of the New US CLOUD Act.* Dechert LLP, 2018: https://www.dechert.com/knowledge/publication/2018/4/forecasting-the-impact-of-the-new-u-s–cloud-act.html (retrieved on 11 june 2018).

[EBA17] *Recommendations on outsourcing to cloud service providers.* European Banking Authority, 2017: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers (retrieved on 11 june 2018).

[GALI16] I. Galic, D. Schmitt. *Hitchhiker's guide to testing infrastructure as/and code — don't panic!*, 2016: https://puppet.com/blog/hitchhikers-guide-to-testing-infrastructure-as-and-code (retrieved on 11 june 2018).

[KUMA13]. A. Kumawat. *Cloud Service Models (IaaS, SaaS, PaaS) + How Microsoft Office 365, Azure Fit In*, 2013: https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php (retrieved on 11 june 2018).

[MOGU17] R. Mogull, J. Arlen, F. Gilbert, A. Lane, D. Mortman, G. Peterson, M. Rothman. *Security Guidance for Critical areas of Focus in Cloud Computing v4.0. Cloud Security Alliance*, 2017.
[MOHA09] A. Mohamed. A history of cloud computing. *Computerweekly.com*, 2009: https://www.computerweekly.com/feature/A-history-of-cloud-computing (retrieved on 11 june 2018).
[MUNC17] Phil Muncaster, *Shared Responsibility? Barracuda Study Reveals Public Cloud Customers Just Don't Get It*, 2017: https://blog.barracuda.com/2017/07/04/shared-responsibility-barracuda-study-reveals-public-cloud-customers-just-dont-get-it/ (retrieved on 11 june 2018).
[SMIT16] A. Smit. Besluitvormingscriteria bij een cloudbeslissing. De *IT-Auditor*, 2016.

Notes

[1] Other main public cloud providers offer similar services to facilitate logically isolated environments within a public cloud environment. For simplicity reasons we will not elaborate further on this and keep to the AWS example for our explanations.

Rada Machluf CPA

After multiple years of IT auditing experience in the private sector in Israel, Rada has joined ABN Amro Group Audit in May 2016. Her main specialisation in Group Audit was in departmental and IT process audits. Since March 2018, Rada works as an information security expert at ABN Amro CISO.

Delil Akdeniz RE CISSP CCSP

Delil used to work as an information security consultant/auditor at PwC for more than five years before switching to ABN Amro Group Audit in November 2016. His core focus areas within ABN Amro are IT infrastructure and cloud computing.