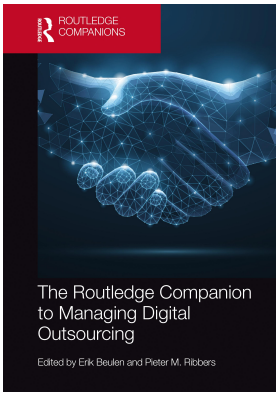

The Routledge Companion to Managing Digital Outsourcing

Erik Beulen, Pieter M. Ribbers

Governing Cloud computing services

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9781351037785-19
Mathew Mertens, Steven De Haes, Tim Huygh
Published online on: 28 Jul 2020

16

GOVERNING CLOUD COMPUTING SERVICES

Risks and mitigating controls

Mathew Mertens, Steven De Haes and Tim Huygh

16.1 Introduction

The increasing shift towards agile enterprises has led to the augmented application of IT outsourcing. To realize this, several options can be applied. Cloud services can be considered as one of the most applied options and has therefore led to a fundamental change in the IT landscape throughout the last decade. Despite that the use of Cloud services is often perceived as an IT-driven choice, it should be seen as an IT-based business model realizing the agile business strategy [1].

The adaptation of the new IT operating model will continue to increase as evident from recent Gartner research, stating that within the next five years a total of approximately one trillion dollars will be spent on the implementation and use of Cloud services [2]. Although the use of Cloud services will continue to be key to realize organizational agility, several organizations remain reluctant to the adoption of Cloud services, due to the risks such adoption might entail [3]. To mitigate or minimize these risks, a formal Cloud governance approach needs to be defined.

This chapter will contribute to these aspects by elaborating upon the potential risks and the corresponding mitigation controls. Before deep-diving into the required governance mechanisms, an overview of the associated risks and benefits will be provided. Based on a risk analysis, the required IT governance mechanisms (i.e. structures, processes and relational mechanisms) to enable risk mitigation will be identified and discussed.

16.2 An overview of Cloud computing services

As defined by NIST (2011), Cloud computing services enable simple and on-demand network access to a shared pool of configurable computer resources, such as servers, applications and services [4]. These resources can be utilized with minimal effort and management involvement and minimal interaction with the service provider. In the following sections, the benefits and risks associated with Cloud services adoption are discussed.

16.2.1 The benefits of using Cloud services

As defined by the 'Technology Business Management methodology', transparency and cost performance are two core elements for realizing business value [5]. Even though technology innovations have led to increasing capabilities and lower costs of IT infrastructures, the increasing complexity of organizations has resulted in increasing costs of information management [6].

Shifting internal control towards an external service provider can therefore reduce IT complexity. This change will realize a transfer from required capital investments towards operational expenditures and will enable cost transparency due to the predefined costs per use [3,7].

Cloud computing can therefore be considered as a next step, realizing scalability and availability by decoupling the performed business services and the required IT infrastructure to support the services by using distributed resources [6,8,9].

Outsourcing datacentre management will moreover significantly impact the required IT staff and other resources and will moreover enable a substantial effect on the cost structure and internal operations of the organization. The adoption of Cloud services should therefore be initiated as a strategic choice enabling the value realization of the business units by reducing complexity, enabling flexibility and reducing time-to-market for new innovative initiatives [6,10].

As illustrated, the adoption of Cloud services can lead to several (IT-related and organizational) benefits. It is however required to identify all potential risks and take them into account.

16.2.2 The associated risks of using Cloud services

Despite the increasing adoption rate of Cloud services, several organizations remain resistant to the use of Cloud services due to the existence of several risks. As defined in COBIT 5, an enterprise governance and management of IT framework developed by ISACA (2012), both the internal context, including management and IT-related capabilities, and the external context need to be considered to evaluate risk [11].

The risks associated with Cloud services can be divided into four categories, namely technical risks, operational risks, organizational risks and compliance risks. The impact and nature of these risks depends on the organization, the used Cloud service model (IAAS, PAAS, SAAS) and the applied deployment model (private, public, community, hybrid) [12].

As illustrated in Figure 16.1, the Cloud service model defines the nature of control and therefore directly impacts the risk level.

16.2.2.1 Technical risks

Recurring scepticism on Cloud services is mainly related to data security and privacy. Privacy is a part of security and solely relates to the content and communication of personal information. To fully cover *data security*, the CIA (confidentiality, integrity, availability) principles need to be managed and controlled efficiently and effectively.

Confidentiality is ensured when the data is only accessible to those who are authorized to access the data. When using Cloud services, data can be made accessible through the Internet everywhere around the world. Therefore, the risk of unauthorized access increases significantly. Moreover, the application of a multi-tenancy model, leading to shared data storage facilities, can result in an increased risk in unauthorized access to data and could also result

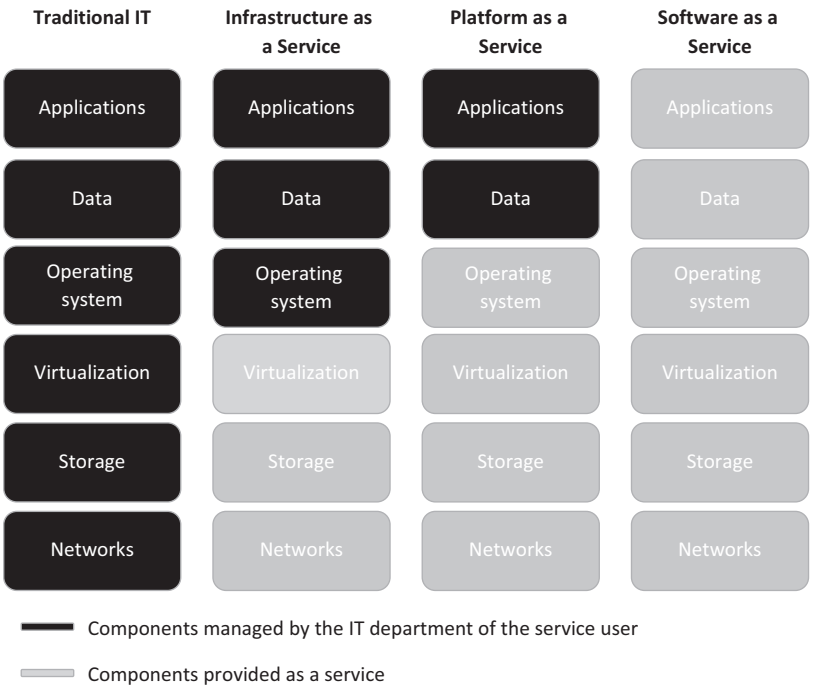

Figure 16.1 Components of Cloud services [13]

in data remanence when the data is not properly deleted [14, 15]. *Integrity* refers to the secure state of the data, meaning that no unauthorized users should be able to change and delete the stored data. The data must comply with all states of the ACID characteristics and therefore needs to be atomic, consistent, isolated and durable. When requesting and transferring the data, these states should remain unchanged [14]. Cloud computing services should have a positive impact on the *availability* of the stored data and applications. Cloud services enable worldwide availability of data and applications on all supported devices connected to the Internet. The increased accessibility could however result to unauthorized network attacks, such as DDOS, spoofing and snipping.

The efficiency of the Cloud service is dependent on the *architecture and networks* provided by the service provider. The scalability and processing requirements should be assessed to ensure all required CPU power is available at all time. Due to the dependency on a steady Internet connection, the risk of an unstable or inaccessible network connection could lead to latency, resulting in major operational impact [16, 17].

Due to outsourcing of responsibilities, the Cloud user will become dependent on the Cloud service provider. Therefore, the lack of efficient *datacentre management* by the provider will have a direct impact. These inefficiencies could relate to lack of updates and patch management, an inefficient service desk and inefficient or non-existing disaster recovery procedures. The service provider can also be dependent on a third party, such as an infrastructure provider. Therefore, a lack of contractual transparency could lead to a turmoil of accountabilities [14, 18].

Investing in Cloud services to enable flexibility can have a positive impact on the strategy execution of the organization. The success will however be dependent on the *compatibility*

between the Cloud service and the existent legacy systems. Lack of integration can lead to duplication and a lack of data transparency, leading to increased data management costs [19].

16.2.2.2 Operational risks

Several risks can have an immediate impact on the operational processes of the organization, resulting in increased operational costs. Business processes are dependent on information, which should be managed by the business units in cooperation with the IT department. *Information management* should focus on data in use, in transport and at rest. To fully cope with all risks regarding information management, the information lifecycle model can be used, which illustrates all five phases of data management.

1 Data collection

   Although Cloud services can enable new data collection techniques (e.g. using internet of things), the use of Cloud services as such will not impact the collection of data [20].

2 Data storage

   When using infrastructure as a service, the user will remain in charge of the content of the data, but will outsource the physical storage of the data. This could lead to fragmentation and lack of transparency about the location of the data. The use of distributed databases will moreover lead to increased complexity and increased risk of data redundancy. When the user is subject to data privacy regulations, the lack of data location transparency could lead to non-compliance [21, 22, 23, 24, 25].

3 Data usage

   The use of the data is dependent on the performance and accessibility of the Cloud service. Direct operational impact will be realized whenever the data is crucial for the continuity of the business processes.

4 Data retention

   Because data under retention requirements will not be accessed frequently, data fragmentation will arise. The data will moreover relate to sensitive information for which no flexible capacity is required [26].

5 Data deletion

   Whenever data does not have to be retained, it needs to be either deleted or anonymized. Because data is stored on hardware, which is being managed by a third party and is shared with other organizations, the risk of improper deletion could lead to the recovery of data using forensic techniques [20, 26, 27, 28].

Because the availability of the data, which is stored in a Cloud environment, is dependent on the actions performed by the service provider, the risk of *data lock-in* occurs. As discussed, technical issues regarding the network and hardware can lead to inaccessibility of data. More risks regarding inaccessibility can occur whenever the service provider suddenly stops the support of the service or whenever discussions occur and the service provider blocks the access to the data servers [21].

Using Cloud services can enforce cost transparency due to the pay per use model. The use of this service can however lead to an increase in users and therefore usage, leading to an increase in the required data transfer capacity, which will be reflected in augmented costs. When using platform as a service, lack of control could lead to the installation of illegal software or the violation of license agreements, which could result in financial penalties.

The use of Cloud services can then lead to a lack of *use transparency*. Therefore, it is required to define the distinction between core and non-core data and define which elements can safely be stored in a Cloud environment [12, 29]. This lack of transparency could moreover result in a *lack of control*, relating to the relationship between the service user and the service provider [12].

16.2.2.3 Organizational risks

Lack of control can have an impact on the governance mechanisms throughout the organization. Specifically, the lack of transparency and control on the physical storage of the data will complicate the risk analysis, which can lead to inefficient *decision-making*, resulting in inefficient governance [8]. While the service provider is responsible for ensuring appropriate security measures, the service user will remain owner of the data stored in a Cloud environment and will therefore be accountable for security breaches. To cope with the risk and impact of security breaches, the service user is therefore required to implement efficient *incident management* procedures. The dependency on the service provider could lead to improper follow-up and escalation of incidents leading to inefficient incident management, which could result in reputational damage of the organization [30].

Organizations might opt for a Cloud service to realize cost reductions. These cost reductions could be achieved by reducing the IT staff, due to the outsourcing of IT responsibilities. When reducing the number of FTEs of the IT department, the organization needs to take all required *knowledge and skills* into account to ensure business continuity. Furthermore, the selection, implementation and follow-up of the Cloud service will require new expertise [12].

Although Cloud services enable flexibility, each service provider will provide a specific service, which can be incompatible with other services. Switching services and service providers can therefore become very complex and lead to *vendor lock-in* [22].

16.2.2.4 Compliance risks

Even though not all organizations are entirely data driven, each organization is dependent on data. To regulate the use of this data, organizations are subject to national, international and industry-specific data regulations. Because the physical location of the stored data is subject to *data privacy and security regulations*, using Cloud computing services has a major impact for the user of these services. Organizations need to comply with these regulations to ensure the confidentiality and integrity of personal, medical and financial data. Several regulations already exist that regulate the communication, storage, access and confiscation of data [6].

Due to the differences in data privacy regulations worldwide, remaining compliant to all specific regulations is a challenge for organizations that operate globally. To provide an overview of these differences, three geographic areas are discussed, namely Europe, the USA and Asia.

The European data privacy regulation (EU Directive 95/46/EC) has, in comparison to the USA and Asia, a specific focus on personal data, because privacy is perceived as a fundamental right. The American privacy regulation only focuses on personal data regarding medical information (HIPAA). The European privacy law moreover defines the user of the data as responsible to ensure data privacy, which implicates the accountability of the Cloud service user. Because the above-mentioned EU Directive focuses on the internal communication of data between two parties, this regulation is no longer sufficient to regulate the use

and privacy of data stored and shared in Cloud environments. Therefore, the 'General Data Protection Regulation' was defined by the European Union in 2015 with 25 May 2018 as enforcement date. This new regulation fully regulates the use and storage of personal data to assure data privacy.

The new GDPR harmonizes all existing European privacy regulations and focuses on the responsibilities of the data controllers and data processors and incorporates financial sanctions for non-compliance up to 4% of the global yearly income of the organization [31, 32, 33].

When inspecting the American privacy regulation, three main acts can be defined to which the contractual agreements between the service user and the service provider need to comply. First, the USA PATRIOT Act (UPA) incorporates the potential access and confiscation of the data by the FBI, based on a court order. Second, certain domain-specific acts, such as the Electronic Communications Privacy Act (ECPA) and the Fair Credit Reporting Act (FCRA), regulate the potential involvement of the Government. Lastly, the well-known Sarbanes-Oxley Act (SOX) is implemented to protect the data of investors and regulate the storage and communication of financial data. All American public companies and public companies listed in the USA need to be compliant to SOX [34].

The 'Asia Pacific Economic Corporation (APEC) Privacy Framework' is built based on best practices to ensure flexibility regarding the transition towards Cloud environments. In comparison with the GDPR, the Asian framework is defined as a guideline rather than a mandatory regulation [35]. Next to the international privacy regulations, several industry-specific regulations are defined, for instance relating to health (HIPAA, HITECH) and finance (GLBA).

The risks that can be associated with compliancy are not limited to privacy and security regulations. The involvement of intellectual property, related to data stored in a Cloud environment, and the discontinuation of contractual agreements can be identified as compliancy risks as well. Cloud services should be used for the storage of non-critical data. Whenever the organization opts to store data relating to intellectual property in the Cloud environment, discussions could occur regarding the ownership of the *intellectual property*. The increased availability could moreover potentially lead to violations of copyright or the loss of competitive advantage. When using a platform as a service Cloud environment, several licence-based applications can be installed. The lack of use transparency, due to the increase in users, could lead to the use of this software by unauthorized users, which could result in substantial fines.

Both the service user and the service provider are responsible for maintaining security and compliancy. Since the service provider has no insight on the nature of the data and the service user does not know the physical location of the data, discussions regarding the accountability could occur. Therefore, it is required to define clear *contractual agreements* to predefine the responsibilities and accountabilities. The lack of follow-up of the service level agreements could moreover lead to insufficient datacentre management and the failure to comply with the agreed upon contractual agreements throughout the contractual lifecycle. The discontinuation of the contract could also have an operational impact whenever the termination procedures are not clearly defined [35, 36].

16.2.3 The impact of the identified risks

Risk analyses need to be performed to select the appropriate service and service provider and monitor the service throughout the lifecycle. Note that the impact of these risks is dependent on the service model and therefore impacts the required management practices [37].

Although the selection of the service type impacts the risk level, all mechanisms listed underneath need to be considered for all services types. The degree and implementation of specific controls, to optimize the limited control over the data and resources, will however be dependent on the chosen service type.

To perform a risk analysis, the organization needs to outline its risk appetite, which illustrates the risks the organization is willing to take to realize its strategy. The risks can be defined based on the standardized ISO 27005 method and 'COBIT 5 For Risk' including the focus on probability and the business impact [28]. Based on the risk analysis, one of the four risk measures (i.e. accept, transfer, avoid, mitigate) needs to be selected.

Because responsibility and accountability regarding Cloud services are contractually defined, it is not possible to shift the risk to the service provider. Moreover, several risks are inherent to the storage and use of data. Choosing or neglecting a Cloud service will therefore not entirely enable the avoidance of the risk. Mitigating the risks by implementing control measures will consequentially be the optimal solution. The effectiveness of these control measures will be dependent on the governance mechanisms as defined and implemented by the organization.

16.3 IT governance mechanisms for Cloud computing services

Governance relates to the decision rights, the accountability and the responsibilities that need to be fulfilled by the management team and the board of directors to realize the strategic goals and optimize the risk profile [17]. Efficient and effective IT governance is required to realize business-IT alignment and can be realized by focusing on three types of mechanisms [19]. These IT governance mechanisms relate to the structures, processes and relational mechanisms and are therefore part of the Governance enablers as defined by ISACA in COBIT 5.

Because the use of Cloud services can be perceived as the implementation of a new IT provisioning model, it will have a direct impact on the organizational governance, due to the outsourcing of control. To realize a successful Cloud implementation and realize agility, the current IT governance mechanisms will have to be adapted and new mechanisms will have to be implemented.

The focus on the required structures, processes and relational mechanisms to realize a clear governance approach is therefore obligatory to optimize the value creation and minimize the associated risks [3, 39].

16.3.1 Structures

It is crucial to have effective Cloud leadership to govern and manage the selection, implementation and follow-up of the Cloud service. Outsourcing responsibilities also leads to a decentralization of the decision-making and control. Therefore, several structures or roles with the required expertise need to be allocated to manage the Cloud service in order to realize the desired agility and achieve the anticipated business goals [17, 40, 41].

COBIT 5 clearly states the need for the *involvement of the board of directors* to clarify the difference between governance and management. Because the use of Cloud services should be based upon strategic initiatives, the board of directors needs to be involved in the selection procedure and the definition of the risk appetite.

To define centralized Cloud leadership, a *Chief Cloud Officer (CCO)* needs to be appointed, who has the required expertise to manage the Cloud service. Note that the CIO can fulfil this role, if he/she has the necessary expertise [40, 42].

Because the decisions regarding the implementation and follow-up of the Cloud service should not be made by one individual, a *Cloud management committee (CMC)* needs to be established, which will consist of members of both the top management team and the middle management team so that the service can be comprehensively managed. To fully manage the follow-up of the Cloud service, the service provider should also be represented in this committee, which separates this committee from the IT steering committee. This committee needs to define what the Cloud service needs to realize and is therefore accountable for creating alignment between the service and the strategic goals as defined by the board of directors [6, 40].

To properly manage the operational follow-up of the Cloud service, a *Cloud service facilitation centre (CSF)*, which could be headed by a *Cloud service manager*, should be established as an internal single point of contact. The operational follow-up involves the monitoring of required data capacity and the execution of the decisions taken by the CMC and therefore entails how the implementation and use of the service will take place.

Due to the dependency on the service user, a transparent and trustworthy relationship will be the key to a successful Cloud implementation. A *Cloud relationship centre (CRC)* should therefore operate as a single point of contact with the service provider and should be responsible for the follow-up of internal policies and the service level agreements [40]. For small- and medium-sized organizations, these roles could be aggregated into a single role, known as the *Cloud service broker*. This internal broker is appointed as single point of contact and is responsible for the entire coordination and support of the Cloud service [43].

The implementation of a Cloud service does not only require new structures, but also impacts the current organizational structures. As discussed, the *Chief Information Officer (CIO)* can occupy the role of CCO, when he/she has the required knowledge and expertise. Otherwise a new CIO/CTO or CCO should be appointed. Due to the regulatory impact of Cloud services, the *Data Protection Officer (DPO)* should be involved in the selection and follow-up of the Cloud service regarding the regulatory impact.

The presence of a DPO is moreover required when the organization is subject to the GDPR [44]. The implementation of a Cloud service moreover impacts the responsibilities of the Security Officer, Risk Officer, Legal Advisor, Portfolio Manager and Infrastructure Architect. These individuals all need to be involved in the Cloud service selection process to ensure an optimal organizational fit [45].

16.3.2 Processes

IT governance processes relate to the formalization of strategic decisions and the follow-up of the predefined procedures. To identify the required IT governance processes, 'COBIT 5 Enabling processes' as part of ISACA's COBIT 5 framework can be used, which provides 37 IT governance and management processes [11, 46].

Within the COBIT 5 framework, the process enabler is further structured in process categories. This also enables a clear separation between IT governance and IT management processes. The first process category, 'Evaluate, direct and monitor' (EDM), bundles the IT governance processes and therefore illustrates the need for appropriate selection and monitoring of the Cloud service to achieve benefits realization. The remaining four COBIT 5 process categories all contain IT management processes. The management team needs to be involved in the planning and monitoring processes, as defined in the process category 'Align, plan and organize' (APO). The categories 'Build, acquire and implement' (BAI) and 'Deliver, service and support' (DSS) illustrate the need for defining and implementing clear requirements and the need for continuous operational support of the service to ensure

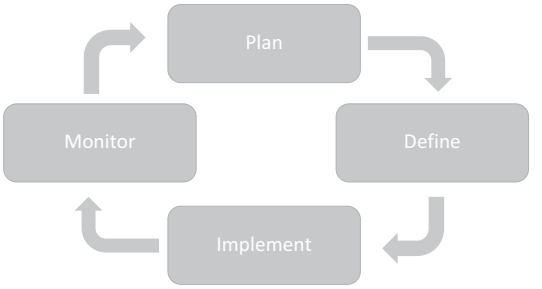

Figure 16.2 Governance lifecycle [47]

business continuity. Monitoring procedures need to be in place to prevent incidents and assess whether the anticipated goals are achieved. COBIT 5 therefore defines the need for the process category 'Monitor, evaluate and assess' (MEA) to indicate the need for clear measures to evaluate the success and effectiveness of the Cloud service [11].

The four COBIT 5 management process categories are required to realize effective and efficient IT Governance and can be allocated to the four phases of the Cloud governance lifecycle [47, 48] (Figure 16.2).

First, the strategic goals and requirements need to be identified during a planning phase. Based on these strategic goals, the specific functional and technological requirements can be defined, resulting in the selection of a specific Cloud service and service provider. After that, the service needs to be integrated with the systems in use. Before initiating a go-live, several test stages need to be conducted to assure the correct implementation of the Cloud service regarding usage, security and compliancy. After the successful implementation of the service, these elements and the accompanied risks need to be evaluated on a continuous basis.

16.3.3 Relational mechanisms

Relational mechanisms relate to the need for participation and communication between all stakeholders involved. The organizational culture and ethics have a severe impact on the effectiveness of the organizational governance. To assure that employees comply with the defined policies and standards, internal communication and transparency is required to generate insight on the need and impact of these requirements. When implementing a Cloud service, users need to be aware of the license agreements and potential security harms by clarifying the potential impact of these incidents. Training and awareness campaigns focused on security and compliancy should be organized to create awareness and assure the optimal behaviour of all users [48, 49, 50, 51].

16.3.4 Mitigating controls for the identified risk categories

When mapping the COBIT 5 processes to the governance and management of a Cloud environment, it is clear that all processes are crucial to realize the anticipated benefits of the Cloud service. It is however not possible to assign each process to a specific risk, since several processes have an organization-wide impact and will therefore impact the entire selection and monitoring process of Cloud services.

The COBIT 5 process '*Manage strategy*' is one of the essential starting points of a Cloud implementation and has an organization-wide impact. Organizations choose to implement

a Cloud service to realize flexibility or minimize costs. This choice is therefore based on the anticipated optimizations that need to be realized to achieve the strategic goals of the organization. Choosing for a Cloud service could also depend on the external environment, including the competition and the client portfolio. Benchmarks and SWOT analyses can be used to identify and evaluate the opportunities and threats. The selection of the Cloud service model and the service provider will be based on a portfolio analysis and the service level agreements as defined by the service provider [11].

The impact of the organizational change realized by a Cloud implementation will be dependent on the implemented service model. Effective *change management* will however be required to make sure that stakeholders are aware of the risks and benefits that can be realized by this change so that change resistance can be minimized.

Risk management is a process with an organization-wide impact, as it relates to both the identification and follow-up of the risk profile. Risk assessments need to be performed by the Risk Officer on a periodic basis to evaluate the current impact of the Cloud service on the risk appetite [34, 52]. The risk management framework for Cloud computing [53] defines five phases that need to be executed to structurally perform risk management based on the predefined risk appetite:

- Assessment of user requirements
- Assessment of the Cloud service provider
- Risk evaluation
- Independent assessment by an external party
- Continuous monitoring.

By applying the CSA, NIST, ENISA and ISACA frameworks, the remaining governance and management processes can be directly assigned as mitigating controls to specific risk categories.

16.3.4.1 Mitigating technical risks

16.3.4.1.1 ENSURING DATA SECURITY AND PRIVACY

The required measures to assure security can be identified using the NIST Cyber Security Framework [54]. This framework identifies five functions that need to be managed to mitigate potential security risks, by referring to the related COBIT 5 management processes.

1 Identification of security threats

   The first function relates to the identification of security threats by performing asset management and risk management processes. The effectiveness of the performed measures will be dependent on the service provider. A careful selection based on CSA and ISO certificates and the use of SOC 2 reporting mechanisms will therefore be elementary selection criteria.

2 Realize protection by implementing the required security measures and controls

   To realize data integrity and confidentiality, encryption, firewalls, authentication and authorization mechanisms need to be integrated by both the service user and the service provider. Data encryption should be applied to data at rest, data in use and data in transport, to assure data confidentiality and integrity in a multi-tenancy environment. The encryption standard 'Transport Layer Security' (TLS) can be applied to ensure a secured

bilateral connection between two parties. Single sign on procedures can be integrated to increase the ease of use.

To assure a successful implementation of these security measures, one of the following best practices could be used [22]:

- Security Assertion Markup Language (SAML)
- Open Authentication (OAuth)
- OpenID.

Next to data encryption, several identity and access management controls need to be implemented to assure data integrity. A login procedure needs to be implemented to assure authorized access. The service user moreover needs to define authorities for each user or user type based on certificates and attributes. Only when the user possesses the required authority, access will be granted and decryption of the data will be performed [14, 22].

The service user moreover needs to apply end-point security measures in case of single sign-on and could opt for the implementation of a remote access and lockdown mechanism to block unauthorized access. Because no physical isolation can be achieved in a multi-tenant environment and public networks, implementing local networks and firewalls can achieve virtual isolation [55]. The service provider or infrastructure provider will be responsible for the physical security of the infrastructure and needs to ensure efficient patch management to monitor and test code changes and realize data integrity.

Availability of the data will be dependent on the used infrastructure and networks. Continuity can therefore be realized by applying duplication and geographical fragmentation of the data, by taking the regulatory requirements into account. Next to these technical implementations, awareness needs to be created to assure appropriate use of the Cloud service.

3 Perform continuous monitoring to detect security breaches

Although security breaches cannot be completely prevented, service providers and users should implement intrusion detection and prevention systems. These systems will register the used IP address and ports and will block those if required [56, 57]. The service user could moreover opt for additional firewalls to prevent unauthorized access or key loggers. Next to the implementation of technical solutions, the service user needs to create awareness on the use policies to prevent negligence.

4 Perform incident management to timely resolve and mitigate incidents

The effectiveness of these detection systems is crucial to timely escalate occurred incidents and undertake the appropriate actions to minimize the impact of the incident. Clear communication between the service provider and the Cloud relationship centre is therefore essential to achieve efficient incident management.

5 Recover and realize continuity

Finally, to ensure incidents do not develop into long-term problems of discontinuity, appropriate monitoring procedures need to be established. To optimize continuity, the organization should moreover opt for duplication and geographical fragmentation of the data, for which the regulatory requirements need to be taken into account [55]. The organization could moreover opt for a public network rather than a VPN connection to reduce the single-point-of failures, for which the organization should consider the required security measures [30, 58].

16.3.4.1.2 ENSURING SYSTEM PERFORMANCE

The service provider will perform the maintenance and monitoring of the Cloud infrastructure for a public Cloud service. The selection procedure, including test phases, and the establishment of clear contractual agreements are therefore essential for the assurance of continuity. The service user could opt for internal backup servers for the stored data to assure continuity. This will however negatively impact the anticipated scalability benefits. The service user needs to monitor the agreed upon performance levels based upon predefined benchmarks [56].

16.3.4.1.3 MONITORING DATACENTRE MANAGEMENT

The service provider is responsible for managing the virtual machines, physical security and service requests through a service desk. The service user therefore needs to be able to rely on external audit validations and the disaster recovery procedure, as defined by the service provider. The service user needs to assign the Cloud relationship centre to clearly communicate and follow up the service requests [59].

16.3.4.1.4 ENSURING COMPATIBILITY

The use of a Cloud service will incur the outsourcing of data storage and maintenance to achieve scalable IT resources. The selected service model will therefore impact the complexity of the compatibility with the internal IT resources. The implementation of a private or hybrid Cloud solution will require the adaption of the current configurations and IT architecture. To avoid unanticipated costs, the Cloud user needs to estimate the required adjustments that need to be performed to integrate the Cloud service and provide a cost buffer. When using a public or hybrid Cloud solution for application management, the implemented architecture model needs to be integrated into the existing architecture of the service user to realize compatibility.

16.3.4.2 Mitigating operational risks

16.3.4.2.1 MANAGING THE INFORMATION LIFECYCLE

To mitigate the risks regarding the control on data use and storage, full transparency is required. The Cloud user therefore needs to focus on the three phases of data usage, namely data at rest, data in use and data in transport. To assure security, encryption of data needs to be applied to all three data phases. Because data in use directly impacts the continuity of the operational processes, backup and data recovery procedures need to be in place to ensure business continuity. These procedures need to be contractually defined in the service level agreements. Because the business units are owner of the data stored, the appropriate business representatives need to be involved in the determination and follow-up of these service level agreements [21].

All organizations are dependent on certain legal requirements, including data retention policies. When this data needs to be kept for several years, without further use, cost calculations might prefer internal storage. When opting for a Cloud storage solution for retention data, fragmentation will be applied due to the lack of usage and will result in complexity and the lack of transparency. Further contractual agreements regarding the storage location

will therefore be required for the data that is bound to legal requirements. Whenever the required capacity will be time-based, the Cloud user needs to timely estimate the required capacity in cooperation with all business process owners to ensure continuity. Clear manuals and procedures need to be defined to ensure data in a Cloud environment is properly deleted and to avoid that other users of the shared infrastructure can retrieve the data by applying forensic techniques.

16.3.4.2.2 PREVENTING DATA LOCK-IN

To ensure business continuity, the discontinuation of the service provider needs to be anticipated to prevent data lock-in. Lack of anticipation might moreover lead to increased migration costs and augmented complexity regarding configurations. Selecting a service provider with a strong market position and strict compliancy procedures regarding privacy regulations and license agreements is therefore essential. To prevent access to the data being blocked by the service provider due to mutual disputes, complete and consistent service level agreements need to be defined.

16.3.4.2.3 ENSURING USE TRANSPARENCY

The scalability and availability features realized by a Cloud environment will result in an increase of users. Insufficient estimations regarding the required data capacity will therefore result in unforeseen costs and will negatively impact the perceptions on the Cloud benefits. The initial budgeting process, which will impact the Cloud decision, therefore needs to contain a certain budget buffer to anticipate the potential increase of data usage.

To ensure use transparency and prevent the exponential increase of data usage, the number of users needs to be limited. Afterwards, the number of users can be gradually increased under strict supervision. Because the number of users needs to be defined by the business units, effective business-IT alignment is required to appropriately estimate and anticipate the required data transfer capacity [17].

The violation of license agreements can result in substantial fines. Defining clear use policies and creating awareness regarding these policies is therefore crucial to ensure appropriate use of the service and licensed applications.

16.3.4.2.4 ENSURING CONTROL

The success of outsourcing responsibilities is dependent on the mutual trust relationship between the two parties involved. Because the service provider only disposes of partial control, reasonable assurance on security and compliancy needs to be obtained by performing external audits. Since every Cloud user wants to obtain assurance on those topics, Cloud providers can obtain audit certifications to prevent a specific internal audit for each individual client [60].

When selecting a service provider, the organization therefore needs to base its decision on the possession of one of the following audit standards for Cloud security and data privacy:

- CSA Star certificate: Cloud security assurance
- ISO/IEC27018: ISO standard for Cloud privacy
- ISAE 3402: IT Outsourcing standard as an update of the SAS70 standard
- SOC 2 and SOC 3: Data security and privacy.

SOC 1 reporting should also be implemented to create transparency on the impact of the implemented control measures on the financial reporting [61].

Audits can be performed in two specific areas, namely security and compliancy. Whenever a security-based audit is performed, events, logs and monitoring procedures need to be evaluated [55, 62].

The 'Cloud computing management Audit/Assurance program' of ISACA can be applied to ensure a standardized approach.

The service user needs to monitor the effectiveness of the implemented controls on a continuous basis so that the quality of the service can be assessed, shortcomings of the predefined service level agreements can be identified and the risk appetite can be monitored [63].

16.3.4.3 Mitigating organizational risks

16.3.4.3.1 OPTIMIZING DECISION-MAKING

Ensuring transparency and control on the used Cloud service is required to realize the benefits. But to realize and govern this control, the listed governance structures and processes need to be implemented. First, clear use policies need to be defined based on the organizational processes. The identified inefficiencies and shortcomings need to be identified by the business process owners and need to be reported to the CIO and/or the CCO. This cooperation between the business end users and the IT department will positively impact the mutual alignment and cooperation [11]. The effectiveness of the decisions taken by the executive management and the board of directors is dependent on the adequacy and quality of the delivered data. The data therefore needs to be available for internal and external audits, which should be based on the COBIT and ISO frameworks [64].

Implementing a Cloud service will severely impact the investment portfolio due to the required implementation costs and the shift towards periodic variable costs. The portfolio therefore needs to be evaluated on a periodic basis by business and IT representatives to identify potential synergies. The implementation of a private Cloud solution will result in optimized transparency regarding costs, but will increase the variation of the costs whenever the infrastructure is managed internally [3].

Because there are no capital investments regarding IT infrastructure, no sunk costs will have to be considered for the implementation of a public Cloud service. To define an overview of the return on investment, the organization needs to take all future cash flows into account. To compare the cash flows for Cloud services with the current IT model, the net present value method needs to be applied [30, 57]. Shifting towards a Cloud environment can realize quick wins and will therefore positively impact the change process, if the project is effectively managed.

16.3.4.3.2 ENSURING INCIDENT MANAGEMENT

As the service user remains accountable for the data-related risks, the service user needs to implement incident management procedures and define an incident response plan to ensure timely and effective resolution management based on the predefined risk appetite [63]. Because the service user is dependent on the service provider, the incident management process needs to be adapted to incorporate the cooperation with the service provider into the escalation and resolution process. The Cloud relationship centre and service facilitation centre therefore need to be involved to realize efficient escalation [63].

16.3.4.3.3 ENSURING THE REQUIRED KNOWLEDGE AND SKILLS

Outsourcing IT responsibilities will lead to a potential reduction of the required FTEs for IT maintenance and support. When reducing the IT staff, the organization needs to consider all required skills and knowledge to ensure business continuity. The implementation of a new service will moreover lead to the need for additional knowledge and skills, which can be realized by hiring new experts or providing training to the current IT staff and IT management team. Shifts in responsibilities could therefore be realized to implement a Cloud relationship centre and service facilitation centre with the appropriate number of experts.

16.3.4.3.4 PREVENTING VENDOR LOCK-IN

Next to the compatibility between the Cloud service and the internal systems, the service user needs to evaluate the potential compatibility between several Cloud services. Whenever an organization opts for a Cloud solution that is not compatible with other services provided by other service providers, vendor lock-in could occur. Switching from provider could then lead to substantial migration costs. The organization therefore needs to take the compatibility with other services into account when selecting a provider. The service user moreover needs to define an exit strategy to assure a smooth Cloud migration if required [63]. The complexity regarding the migration of data will however be limited when using an infrastructure as a Cloud service based on standardized virtual machines [65].

16.3.4.4 Mitigating compliance risks

16.3.4.4.1 COMPLYING TO DATA PRIVACY AND SECURITY REGULATIONS

Even though both the service provider and the service user are responsible for complying with the data security and privacy regulations, the service user will remain accountable for the data stored in a Cloud environment. The selection procedure of the service provider should therefore incorporate the evaluation of ISO and SOC reports. To ensure continuity regarding compliancy, the organization needs to monitor national, international and industry-specific requirements on a continuous basis. To be compliant with the GDPR, the organization needs to assign a Data Protection Officer who will be responsible for the privacy assessments. To appropriately comply with the GDPR, organizations can invoke the assistance of third parties with juridical, technological and audit expertise [17, 21, 31].

Whenever the data is bound to national borders, the storage location of the data needs to be contractually defined and agreed upon in the service level agreements. To prevent inappropriate usage of the data leading to compliancy violations, the organization needs to create awareness on the use policies and the impact of these violations.

The government is authorized to seize the data whenever an organization violates certain regulations. When the data of a co-tenant of the Cloud infrastructure is seized due to compliancy violations, the government might seize the entire server infrastructure. Data backups will therefore prevent data lock-in.

16.3.4.4.2 SAFEGUARDING INTELLECTUAL PROPERTY

Cloud data storage should only be used for non-critical data to ensure business continuity, prevent data breaches and avoid the loss of intellectual property. Whenever the organization opts to store sensitive data in a Cloud environment, the contractual agreement clearly needs

to state the ownership and accountability regarding the content of the data to avoid mutual disputes and maintain intellectual property and knowhow. The contractual agreement should furthermore incorporate clauses regarding compensations for agreement violations. Safeguarding intellectual property moreover relates to the monitoring of the license agreements. These agreements need to be followed up to prevent unauthorized use and avoid financial penalties [65].

16.3.4.4.3 MANAGING THE CONTRACT LIFECYCLE

To ensure clear and complete contractual agreements, all stakeholders with legal, financial and IT expertise need to be involved in the development process. These agreements should incorporate the required resources, configurations, network requirements, data security and privacy measures, the location of the data storage and compensations for violating the agreements. The complete contractual lifecycle needs to be monitored on a continuous basis to timely anticipate violations and potential contractual terminations. Therefore, a clear exit strategy needs to be defined, which incorporates the backup and migration of data.

The main Cloud service providers (e.g. Microsoft, Amazon and Google) do however contain a strong market position and will therefore shift several responsibilities towards the service user. The defined SLAs need to be specific, measurable, assignable, realistic and time-related (SMART). To ensure the completeness of the defined service level agreements, the WSLA framework for web services can be used. This framework defines three requirement categories that need to be incorporated in the service level agreements, namely [66]:

- The roles and responsibilities of all parties involved need to be clearly defined.
- Guaranties need to be defined based on clear SLA parameters, based on specific measurable metrics.
- Next to the goals of the service, the contract needs to entail financial parameters relating to compensation whenever the SLA parameters are not realized.

16.4 Conclusion

A Cloud migration can enable the strategic goals of an organization by facilitating scalability and cost transparency whenever the service is appropriately selected and managed. To ensure proper Cloud governance and management, the organization needs to implement the required structures, processes and relational mechanisms to mitigate the following risks:

- **Technical risks**, incorporating data security and data privacy, technical shortcomings and failures of the used IT infrastructure and networks, inefficient datacentre management and the lack of compatibility between the service and the legacy systems.
- **Operational risks**, relating to data lock-in and the lack of control and transparency.
- **Organizational risks**, incorporating vendor lock-in, ineffective incident management, lack of skills and expertise and inefficient decision-making.
- **Legal risks**, relating to the lack of compliancy on data privacy regulations, violations of intellectual property and contractual shortcomings.

Both new structures (CCO, CMC, CSF, CRC) and changes to current structures will have to be implemented to achieve effective Cloud governance. The required processes can be

identified using the COBIT 5 framework, which includes governance and management processes related to the planning phase, the definition phase, the implementation phase and the monitoring phase. As illustrated, additional frameworks (CSA, NIST, ENISA) will have to be applied to achieve the required control measures to mitigate and monitor the identified risks.

References

1. Madhavaiah, C., Bashir, I., Shafi, S. I. (2012). Defining Cloud Computing in Business Perspective: A Review of Research. *The Journal of Business Perspective*, 16(3), 163–173.
2. Gartner. (2016). *Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending.* Consulted from http://www.gartner.com/newsroom/id/3384720
3. Zhang, Q., Cheng, L., Boutaba, R. (2010). Cloud Computing: State of the Art and Research Challenges. *Journal of Internet Services and Applications,* 1, 7–18.
4. NIST. (2011). *NIST Cloud Computing Standards Roadmap.*
5. Tucker, T. (2016). *Technology Business Management: The Four Value Conversations CIO's must have with their Businesses.* Washington, DC: TBM Council.
6. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A. (2011). Cloud Computing – The Business Perspective. *Decision Support Systems*, 51, 176–189.
7. Peiris, C., Balachandran, B., Sharma, D. (2010). Governance Framework for Cloud Computing. *International Journal on Computing*, 1 (1), 88–93.
8. Rimal, B. P., Choi, E., Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing Systems. *Proceedings of the Fifth International Joint Conference on INC, IMS and IDC* (pp. 44–51). IEEE Computer Society, Washington, DC.
9. Bhardwaj, S., Jain, L., Jain, S. (2010). Cloud Computing: A Study of Infrastructure as a Service (IAAS). *International Journal of Information Technology and Web Engineering*, 2 (1), 60–63.
10. Son, I., Lee, D. (2011). Assessing a New IT Service Model: Cloud Computing. In *Proceedings of Pacific Asia Conference on Information Systems*, Queensland, Australia.
11. ISACA. (2012). *COBIT 5 Enabling Processes.*
12. Dutta, A., Peng, G. C. A., Choudhary, A. (2013). Risks in Enterprise Cloud Computing the Perspective of It Experts. *Journal of Computer Information Systems*, 53 (4), 39–48.
13. Wang, C., Wood, L. C., Abdul-Rahman, H., Lee, Y. T. (2016). When Traditional Information Technology Project Managers Encounter the Cloud: Opportunities and Dilemmas in the Transition to Cloud Services. *International Journal of Project Management*, 33, 371–388.
14. Zissis, D., Lekkas, D. (2012). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems,* 28, 583–592.
15. Kesavaraj, G., Anitha K., Divya, R. (2016). Addressing Cloud Computing Security Issues. *International Journal of Innovative Research in Computer and Communication Engineering*, 4 (6), 11478–11483.
16. Aich, A., Sen, A. (2015). Study on Cloud Security Risk and Remedy. *International Journal of Grid Distribution Computing*, 8 (2), 155–166.
17. Bannerman, P.L. (2010). Cloud Computing Adoption Risks: State of Play. In *Proceedings of the 17th Asia Pacific Software Engineering Conference*. Sydney, Australia, 30 November–03 December.
18. Soundararajan, V., Anderson, J. M. (2010). The Impact of Management Operations on the Virtualized Datacenter. *ISCA'10*, Saint-Malo, France, 19–23 June.
19. ISACA. (2011). *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud.*
20. Shin, Y. N., Chun, W. B., Jung, H. S., Chun, M. G. (2011). Privacy Reference Architecture for Personal Information Life Cycle. *Advanced Communication and Networking: International Conference,* Brno, Czech Republic, 15–17 August.
21. Caroll, M., van der Merwe, A., Kotzé, P. (2011). Secure Cloud Computing: Benefits, Risks and Controls. *Information Security South Africa Conference*, IEEE Computer Society, Johannesburg, South Africa, 15–17 August.
22. Ertaul, L., Singhal, S., Saldamli, G. (2010). *Security Challenges in Cloud Computing.* California State University, East Bay.
23. Goyal, P. (2010). Enterprise Usability of Cloud Computing Environments: Issues and Challenges. *Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* (pp. 54–59). IEEE Computer Society, London.

24. Reddy, S. R., Mohan, Y. R., Naik, J. S. (2015). An Overview of Cloud Computing and Security Issues. *International Journal of Scientific Engineering and Applied Science*, 1 (3), 159–161.
25. Yang, H., Tate, M. (2012). A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems*, 31 (2), 35–60.
26. Swire, P., Ahmad, K. (2012). *Foundations of Information Privacy and Data Protection*. International Association of Privacy Professionals, Portsmouth, NH.
27. ISACA. (2013). *COBIT 5 Enabling Information*.
28. ISACA. (2013). *COBIT 5 for Risk*.
29. Armbrust, A., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., … Zaharia, M. (2009). *Above the Clouds: A Berkeley View of Cloud Computing*. Electrical Engineering and Computer Sciences University of California, Berkeley.
30. Enslin, Z. (2012). *Cloud Computing: COBIT-Mapped Benefits, Risks and Controls for Consumer Enterprises* (Master Thesis). Consulted from Stellenbosch University Library, Stellenbosch.
31. Bartolini, C., Gheorghe, G., Giurgiu, A., Sabetzadeh, M., Sannier, N. (2015). *Assessing IT Security Standards against the Upcoming GDPR for Cloud Systems*.
32. Kuner, C. (2012). *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*. Privacy and Security Law Report, Bloomberg, New York.
33. O'Donovan, C. (2016). On *Security Intelligence*. GDPR Compliance Regulations: The New Challenge for the Cloud Operations Manager. Consulted from https://securityintelligence.com/gdpr-compliance-regulations-the-new-challenge-for-the-cloud-operations-manager
34. Ahmad, R., Janczewski, L. (2011). Governance Life Cycle framework for Managing Security in Public Cloud: From User Perspective. In *4th International Conference on Cloud Computing*, IEEE Computer Society, Washington, DC.
35. Mather, T., Kumaraswamy, S., Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly, Sebastopol.
36. Hon, W. K., Millard, C., Walden, I. (2012). Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now. *Stanford Technology Law Review*, 16 (1), 79–129.
37. Zhang, X., Wuwong, N., Li, H., Zhang, X. (2010). Information Security Risk Management Framework for the Cloud Computing Environments. In *International Conference on Computer and Information Technology* (pp. 1328–1334). IEEE, Washington, DC.
38. De Haes, S., Van Grembergen, W. (2015). *Enterprise Governance of Information Technology; Achieving Alignment and Value, featuring COBIT 5*. Springer, Switzerland.
39. De Haes, S., Van Grembergen, W. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, 27 (1), 307–324.
40. Prasad, A., Green, J., Heales, P. (2014). On Governance Structures for the Cloud Computing Services and Assessing their Effectiveness. *International Journal of Accounting Information Systems*, 15 (4), 335–356.
41. Prasad, A., Green, J. (2015). Governing Cloud computing services: Reconsideration of IT governance structures. *International Journal of Accounting Information Systems*, 19, 45–58.
42. Block D. (2012). *Governing the Cloud as Cloud-based services evolve, so must today's governance functions*. KPMG, Amstelveen.
43. Grivas, S. G., Kumar, T. U., Wache, H. (2010). Cloud Broker: Bringing Intelligence into the Cloud. In *3rd International Conference on Cloud Computing*, Miami, 5–10 July.
44. IAPP. (2016). *Top 10 Operational Impacts of the GDPR: Part 2 – The Mandatory DPO*. Consulted from https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-
45. Joha, A., Janssen, M. (2012). Transformation to Cloud Services Sourcing: Required IT Governance Capabilities. *ICST Transactions on e-Business*, 12 (7–9), 1–12.
46. Mohapatra, S., Lokhande, L. (2014). *Cloud Computing and ROI a New Framework for IT Strategy*. Springer, New York.
47. Bounagui, Y., Hafiddi, H., Mezrioui, A. (2016). COBIT Evaluation as a Framework for Cloud Computing Governance. *International Journal of Cloud Applications and Computing*, 6 (4), 1–18.
48. Karkoskova, S., Feuerlicht, G. (2016). Cloud Computing Governance Lifecycle. *Acta Informatica Pragensia*, 5 (1), 56–71.
49. De Haes, S., Van Grembergen, W. (2009). An Exploratory Study into IT Governance Implementations and Its Impact on Business/IT Alignment. *Information Systems Management*, 26, 123–137.

50. Peterson, R. R. (2003). Information Strategies and Tactics for Information Technology Governance. In W. Van Grembergen (Ed.), *Strategies for Information Technology Governance*. Idea Group Publishing, Hershey, PA.
51. Weill, P., Ross, J. W. (2005). A Matrixed Approach to Designing IT Governance. *MIT Sloan Management Review*, 46 (2), 26–34.
52. Khrisna, A., Harlili. (2014). Risk Management Framework With COBIT 5 And Risk Management Framework for Cloud Computing Integration. *International Conference of Advanced Informatics: Concept, Theory and Application* (pp. 103–108). IEEE, Washington, DC, 20–21 August.
53. Xie, F., Peng, Y., Zhao, W. Chen, D., Wang, X., Huo, X. (2012). Risk Management Framework for Cloud Computing. In *Proceedings of 2nd International Conference on Cloud Computing and Intelligent Systems*, IEEE, Hangzhou, 30 October–1 November.
54. NIST. (2017). *Framework for Improving Critical Infrastructure Cybersecurity (Update).*
55. Zhou, M., Zhang, R., Xie, W., Qian, W., Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. *Sixth International Conference on Semantics, Knowledge and Grids* (pp. 105–112). IEEE Computer Society, Washington, DC.
56. Ardagna, C. A., Asal, R., Damiani, E., VU, Q. H. (2015). From Security to Assurance in the Cloud: A Survey. *ACM Computing Surveys*, 48 (1), 2.
57. Benali, F., Bennani, N., Gabriele, G., Cimato, S. (2010). A Distributed and Privacy-Preserving Method for Network Intrusion Detection. *Lecture Notes in Computer Science book series*, 6427, 861–875.
58. Enslin, Z. (2012). Cloud Computing Adoption: Control Objectives for Information and Related Technology (COBIT) – Mapped Risks and Risk Mitigating Controls. *African Journal of Business Management*, 6 (37), 10185–10194.
59. Srivastava, H., Kumar, S. A. (2015). Control Framework for Secure Cloud Computing. *Journal of Information Security*, 6, 12–23.
60. Ko, R. K. L., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., Lee, B. S. (2011). TrustCloud: A Framework for Accountability and Trust in Cloud Computing. *2nd IEEE Cloud Forum for Practitioners*, Washington DC, 7–8 July.
61. ISACA. (2014). *Controls and Assurance in the Cloud.*
62. Mateescu, M., Sgârciu, V. (2015). Cloud Computing Audit. In *9th International Symposium on Applied Computational Intelligence and Informatics*, (pp. 31–42). IEEE Computer Society, Timisoara, Romania, 15–17 May.
63. Horwath, C., Chan, W., Leung, E., Pili, H. (2012). *Enterprise Risk Management for Cloud Computing.* Committee of Sponsoring Organizations of the Treadway Commission, Chicago, IL.
64. Brender, N., Markov, I. (2013). Risk Perception and Risk Management in Cloud Computing: Results from a Case Study of Swiss Companies. *International Journal of Information Management*, 33 (5), 726–733.
65. ENISA. (2009). *Cloud Computing: Benefits, Risks and Recommendations for Information Security.*
66. Patel, P., Ranabahu, A. R., Sheth, A. P. (2009). *Service Level Agreement in Cloud Computing.* 9e Ohio Center of Excellence in Knowledge – Enabled Computing, Dayton, OH.