Chapter 3:

Cloud Governance

Cloud Governance

3.1 Learning Objectives

After completing this chapter, learners will be able to:

1. Identify the challenges of governance in the cloud.
2. Explain the reasons for implementing and maintaining cloud governance.
3. Articulate the risk involved with cloud implementation.
4. Describe cloud vendor selection processes.
5. Define the need for portability of services in a service level agreement (SLA).

3.2 Overview

Governance is the method an enterprise adopts to evaluate stakeholder needs, conditions and options to ensure that balanced, agreed-on enterprise objectives are achieved. It involves setting direction through prioritization and decision making, and monitoring performance and compliance against agreed-on direction and objectives. Governance in the cloud takes those objectives and activities and focuses them on the cloud environment—especially important in many enterprises, given the strategic contribution of IT and cloud computing toward achieving business goals.

A move to the cloud will cause enterprises to make changes internally to help ensure that they continue to meet performance objectives, their technology provisioning and business are strategically aligned, and risk is managed. For example, the role of the chief information officer (CIO) is transitioning from managing operations to managing IT as a service value chain. Previously, the CIO may have run the internal "IT factory"; now, both enterprises and external service providers have become producers and consumers of services. With cloud computing, the CIO must weave together and optimize this value chain to best support various customers and enable an enterprise's business.

Ensuring that IT is aligned with the business, systems are secure and risk is managed is challenging in any environment and even more complex in a third-party relationship. As with other organizational changes, adoption of cloud computing will necessitate some adjustments to the way business processes are handled. Business processes such as data processing, development and information retrieval are examples of potential change areas. Additionally, processes detailing the way information is stored, archived and backed up will need revisiting.

For enterprises to benefit from cloud computing, a clear governance strategy and management plan must be developed. The governance strategy should set the direction and objectives for cloud computing within the enterprise; the management plan should execute the achievement of the objectives. Cloud computing governance creates business-driven policies and principles that establish the appropriate degree of investments and control around the life-cycle process for cloud computing services.

Just a few reasons enterprises should implement and maintain sound cloud governance are the organization's need to:[12]

- Manage increasing risk effectively, including security, compliance, privacy, projects and partners.
- Ensure continuity of critical business processes that now extend beyond the data center.
- Communicate clear enterprise objectives internally and to third parties.
- Adapt easily. Flexibility, scalability and services are changed in the cloud, enabling the enterprise and business practices to adjust, create new opportunities and reduce costs.
- Facilitate continuity of IT knowledge, which is essential to sustain and grow the business.
- Handle a myriad of regulations.

Governance starts at the top of the organization and, in fact, is unlikely to achieve its mission without complete buy-in from the board of directors. Establishing a clear direction that is aligned with enterprise strategy calls on members of the board to develop a clear understanding of cloud computing benefits and how to maximize them through effective end-to-end governance practices. This requires the board to see cloud computing not as an IT project, but rather as a business technology strategy. This understanding helps ensure that stakeholder needs are considered and met while risk and resource utilization are optimized.

IT, with its particular requirements and terminology, has historically been viewed as a cost center rather than a corporate asset. However, the cloud presents the opportunity to fully align IT with the goals and objectives of the enterprise as a whole. To "sit at the table" of the enterprise's governance programs, IT must adapt to methodologies and the language used in other areas of the enterprise's governance.

3.3 Business Drivers to Cloud Solutions

Cloud computing is viewed as a significant change to the platform in which business services are translated, used and managed. Many consider it to be as large a shift in IT as was the advent of the personal computer or Internet access. However, the rollout of those earlier technologies encompassed a slower development phase, whereas cloud technologies and solutions have come together more rapidly for implementation. This means enterprise decision makers must quickly develop an understanding of the business drivers that may be addressed by adoption of a cloud solution, as outlined in **figure 3.1**.

Figure 3.1—Business Drivers and Cloud Response

Business Driver	Description	Cloud Response
Optimized resource utilization	Organizations are best served by having just the resources they need when they need them. Purchasing hardware and software "just in case" results in extra expense and storage space.	• By using a pay-as-you-go cloud solution, resources become available when needed and are liberated when no longer needed; there is near-to-perfect alignment with actual demand.
Cost savings	Enterprises seek to reduce IT expenses and restructure these expenses to spread them out over time.	• Increased server utilization plus the transition of computational capability from acquired and maintained computers to rented cloud services change the computing cost paradigm from a capital expenditure (CAPEX) to an operational expenditure (OPEX), with potentially significant up-front and total cost savings. • Flexible, on-demand services enable solution testing without significant capital investments and provide transparency of usage charges to drive behavioral change within organizations. • The number of workstations in the office can be reduced and some employees can be allowed to work

		from home to save costs further.
Better responsiveness	In a fast-paced business environment, the ability to respond to developments as they occur provides competitive advantage.	• The cloud offers on-demand, agile, scalable and flexible services that can be implemented quickly, which provide organizations with the ability to respond to changing requirements and peak periods. • Enterprise operations can be monitored effectively, even in real time, enabling improved responsiveness to evolving situations and opportunities.
Faster cycle of innovation	Success in a competitive environment calls for faster development of products and services.	• Cloud computing makes patch management and upgrades to new versions more flexible. • Cloud users can upgrade to a new software version often by doing nothing more than typing a different URL into the web browser. • Staff members can easily share data and collaborate to complete projects even from different locations. Field workers can easily share real-time data and updates with those in the office. • Cloud computing eliminates redundant or repetitive tasks such as data re-entry and scalability.
Reduced time for implementation	New business initiatives brought online in a traditional IT enterprise may require weeks or months to complete (and accrue CAPEX).	• Cloud computing provides processing power and data storage as needed and at the capacity needed, in near-real time.
Resilience	Lack of resilience can increase the potential for a costly, time-consuming and potentially reputation-damaging system failure.	• The failure of one component of a cloud-based system has less impact on overall service availability and reduces the risk of downtime. • By storing data in the cloud, which can be safer than storage on physical servers and in data centers, enterprise data will always be available if users have an Internet connection. • If the enterprise's on-premise data security is compromised, perhaps through the theft of laptops or tablets, the enterprise that has data stored in the cloud can delete confidential information remotely or move it to a different account.

Each cloud opportunity or program has many variables, benefits and risk that affect the decision of whether a cloud application should be adopted from a risk/business value standpoint. The enterprise must weigh those variables to decide whether the cloud is an appropriate solution.

The following questions can help identify the strategic value that cloud services may provide to the enterprise and the impact that cloud could have on enterprise resources and controls. This, in turn, will help identify the cloud deployment required, which will lead to an understanding of the type of CSP needed. Upper management (C-suite) must be prepared to answer these questions in terms that can be easily related to the business benefits cloud computing will provide:

1. Do management teams have a plan for cloud computing? Have they weighed value and opportunity costs? The risk of cloud adoption may be inconsequential when compared to the lost opportunity to transform the enterprise with effective and strategic use of cloud computing—especially if competitors take steps to leverage those same opportunities. From a strategic perspective, cloud computing can be a vehicle to:
   - Gain competitive advantage
   - Reach new markets
   - Improve existing products and services
   - Retain existing customers
   - Increase productivity
   - Contain cost
   - Develop products or services that could not be possible without cloud services
   - Break geographic barriers
2. How do current cloud plans support the enterprise's mission? Cloud services should support efforts to achieve business objectives, which are derived from stakeholder needs (as vetted by the leadership team). Cloud initiatives should have a clear and traceable link to the enterprise strategy so that the value expected from cloud services is clearly defined, accepted and measurable. This link also helps determine the priority assigned to cloud initiatives and supports the development of metrics to measure results against expectations.

   Alignment between cloud objectives and enterprise objectives is critical for effective risk management and cost containment. The potential benefits of cloud services can be enticing, but with reward comes risk. The enterprise must decide whether the potential risk is within acceptable limits.
3. Have executive teams systematically evaluated organizational readiness? Pressure points result when:
   - Cloud computing implementations conflict with enterprise culture
   - Skills that are required to support cloud solutions are not available
   - Cloud-related processes conflict with other established processes
   - Organizational structure does not maximize cloud effectiveness or efficiency

   Evaluating the readiness of the enterprise in anticipation of the adoption of cloud services avoids the need for after-the-fact culture, skill or process changes to remove unanticipated pressure points. A systematic readiness assessment can help management identify additional cost and risk that should be factored into the decision-making process. This readiness assessment should include the following:
   - **Policies and procedures**—New policies and procedures that guide the adoption, management and proper use of cloud computing may be needed.
   - **Processes**—Existing processes using traditional IT services may need to be re-engineered to incorporate new activities that are related to using cloud services.
   - **Organizational structures**—Cloud management may require new organizational capabilities or modifications to existing organizational structures, particularly in IT operations and support.
   - **Culture and behavior**—Organizational culture and behavior can be critical for the successful adoption of cloud solutions.
   - **Skills and competencies**—Procurement, legal, compliance and audit are some examples of functions that may need to develop necessary skills to manage cloud services from evaluation and sourcing to operations and retirement.
4. Have management teams considered what existing investments might be lost in their cloud planning? Cloud computing may not be an immediate and clean fit with the existing technology portfolio of the enterprise. The adoption of a cloud service may, for example, obviate technology investments already made that have not reached their planned end date. The decision about when and how to realize that loss must be considered carefully. Areas to consider include:
   - **Processes**—The IT organization may need to adapt processes such as sourcing and change management.
   - **Culture and behavior**—Cloud services may demand faster turnaround from the IT organization, which may necessitate changes in internal processes and tools.
   - **Services, infrastructures and applications**—The enterprise may need to update data centers, software applications and network infrastructures, which may result in some level of lost investment being realized.

- **Skills and competencies**—The IT organization will need to either develop or acquire the skills required to support users of cloud services if those skills do not already exist within current staffing.

5. Do management teams have strategies to measure and track the value of cloud return vs. risk? Before deciding to adopt cloud computing, the board should give management teams the task of ensuring that proper reporting mechanisms are in place to measure value and risk aligned with enterprise goals.

The enterprise should also consider stakeholders' potential issues when evaluating business drivers for a move to the cloud. Do stakeholders have needs that are beyond the capabilities of the current IT systems? Have stakeholders identified business opportunities that require the support of cloud applications? Do stakeholders anticipate business gains that can be realized only through cloud usage? Are stakeholders concerned about specific compliance issues in the cloud?

Ultimately, cloud is not necessarily the right solution for every organizational need. The most common technical reason enterprises find to not move to the cloud is that the cost of customization outweighs the benefits of the cloud solution. The type of cloud service selected is critical, as is how it is managed. Thinking strategically about benefits, costs and risk is paramount and must be done upfront, before any contract is signed.

3.4 Risk Associated With Cloud Solutions

Just as the benefits associated with the cloud vary based on multiple factors related to the enterprise and the technology, so too does the associated risk. Among the factors that can impact cloud-related risk are:

- **Type of cloud service model**—Each cloud service model (SaaS, PaaS, IaaS, etc.) has varied business purposes and levels of business risk.
- **Robustness of the enterprise's existing IT operations**—Enterprises' current governance, risk management and information security enablers must be well-defined and managed within the existing IT operations. New threats and vulnerabilities may be identified in the cloud, but if the enterprise is prepared and its current IT operations are able to handle these issues, the overall risk to the enterprise may be lower.
- **Current level of business risk acceptance**—The level of risk an enterprise is willing to accept varies among industries and among enterprises within the same industry.
- **Aggregated "street value" of the data to be promoted to the cloud**—Enterprises need to assess the value of the data promoted to the cloud in terms of how tempting the data may be to those with malicious intent.
- **Internal security classification of data being promoted to the cloud**—As with "street value," data have internal value to the enterprise, which provides the enterprise with a vested interest in keeping them proprietary and not releasing data publicly.
- **Identified compliance obligations of the data shared within the cloud**—Personally identifiable information (PII) security controls and financial reporting compliance are two prime examples of compliance obligations that need to be managed in the cloud.
- **CSP risk**—In the absence of commonly accepted cloud security standards, CSPs may take different approaches to cloud security. They should follow best practices and use internationally accepted standards for general information security. Enterprises should exercise due diligence in evaluating and selecting a CSP; having their own well-defined requirements will enable enterprises to reap maximum benefits.

Information assets such as those placed in the cloud can be roughly categorized as data, applications and processes. These assets are commonly subject to the following risk events:

- **Unavailability**—The asset is unavailable and cannot be used or accessed by the enterprise. The cause can be accidental (failure of the infrastructure), intentional (distributed denial-of-service [DDoS] attacks) or legal (subpoena of database holding all data in a case of multi-tenancy architecture where one client's data are subject to legal investigation).
- **Loss**—The asset is lost or destroyed. The cause can be accidental (natural disaster, wrongful manipulation, etc.) or intentional (deliberate destruction of data).
- **Theft**—The asset has been intentionally stolen and is now in possession of another individual/enterprise. Theft is a deliberate action that can involve data loss.
- **Disclosure**—The asset has been released to unauthorized staff/enterprises/organizations or to the public. Disclosure can be accidental or deliberate. This also includes the undesired, but legal, access to data due to different regulations across international borders.

Data are commonly the most valuable assets and the most probable targets of attacks in the cloud. However, the risk related to applications and processes should not be overlooked. The business impact of long DDoS attacks cannot always be absorbed by an enterprise; although no data loss or disclosure is suffered, paralyzing the systems has direct, negative effects on the data. Disclosure of details about how applications handle critical information or about internal enterprise processes could pave the way to more selective attacks with greater consequences.

Figure 3.2 describes at a high level the possible impact of the four risk events on assets.

Figure 3.2—Impact of Risk Events on Information Assets

Type	Unavailability	Loss	Theft	Disclosure
Data	• Disruption of activities • Lack of resources to maintain business as usual • Possibility of data poisoning	• Disruption of activities • Required activation of backup restore procedures (DRP) • Possibility of partial loss of the asset (depending on the recovery point objective (RPO) • Financial loss associated with recovery efforts	• Business competitive disadvantage • Possibility of blackmail • Loss of credibility with customers/clients	• Damage to company reputation or image • Possibility of regulatory sanctions • Financial impact
Applications/ processes	• Disruption of activities • Lack of resources to maintain business as usual		• Higher risk/threat of more selective attacks to data	

Source: ISACA, *Security Considerations for Cloud Computing*, USA, 2012, https://www.isaca.org/bookstore/audit-control-and-security-essentials/scc

Given the multiple and diverse potential areas of risk in the cloud, it is impossible to accumulate an exhaustive list of them all. However, certain risk issues are common to many enterprises and CSP environments. One of the most pressing is information security, which merits a closer look, but other areas of risk can be equally concerning.

3.4.1 Security

Security and privacy must be considered from the moment management considers cloud computing a possibility. Security and privacy requirements should be part of the due diligence, business case studies and vendor selection. Whenever possible, the enterprise should evaluate the provider's control environment to ensure that the enterprise's security and privacy needs will be met satisfactorily. When a close assessment is not possible, the enterprise must request proof that the provider has implemented the necessary controls to protect the enterprise's assets.

Cloud services aggregate data from thousands of businesses. Each new client, bringing a new store of data, increases the value of that CSP as a potential target. This concentrates risk on a single point of failure. A disaster at a cloud provider can affect every one of its customers. A CSP's failure to apply, maintain and monitor the appropriate security measures can result in the commingling of data among clients, compromised data, stolen data and incomplete data deletion. Data breaches can result in diminished customer trust, revenue loss and loss of intellectual property for both the client enterprise and the CSP.

Enterprises may wish to consider securing a Service Organization Control 3 (SOC 3) report, which outlines information related to a service organization's internal controls for security, availability, processing integrity, confidentiality or privacy. Because they are general use reports, SOC 3 reports can be freely distributed. The five areas covered in SOC 3 reports are the focuses of the American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria:

- **Security**—Information and systems are protected against unauthorized access, unauthorized disclosure of information and damage to systems that could compromise the availability, integrity, confidentiality and privacy of information or systems, and affect the entity's ability to achieve its objectives. Security refers to the protection of information during its collection or creation, use, processing, transmission and storage, as well as the systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties; system failure; incorrect processing; theft or other unauthorized removal of information or system resources; misuse of software; and improper access to or use of, alteration, destruction, or disclosure of information.
- **Availability**—Information and systems are available for operation and use to meet the entity's objectives. Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers.
- **Processing integrity** (over the provision of services or the production, manufacturing, or distribution of goods)—Processing integrity refers to the completeness, validity, accuracy, timeliness and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions unimpaired, free from error, delay, omission, and unauthorized or inadvertent manipulation.
- **Confidentiality**—Confidentiality addresses the entity's ability to protect information (all types of sensitive data, including personal information) designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use and retention, and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others.
- **Privacy**—Personal information is collected, used, retained, disclosed and disposed of to meet the entity's objectives. Although confidentiality applies to various types of sensitive information, privacy applies only to personal information. The privacy criteria include notice and communication of objectives; choice and consent; collection; use, retention and disposal; access; disclosure and notification; quality; and monitoring and enforcement.[13] Industry PII regulations such as HIPAA, CCPA and PCI-DSS should also be a consideration for privacy.

Other standards, certifications and frameworks are available, including useful material from ISACA and the Cloud Security Alliance.

It is very important for both the enterprise and the CSP to understand that cloud security is the responsibility of all parties involved in the service contract. Depending upon the deployment model and SLAs, the provider may be responsible for implementing and maintaining the necessary controls to protect its clients' assets. Likewise, the enterprise may be responsible for ensuring that the security and privacy controls are implemented correctly, operate as intended and meet the enterprise's requirements throughout the life of the contract. In some cases, the responsibility to protect information assets can be transferred to the provider, but accountability for the protection of information assets remains with the enterprise.

Cloud access security brokers (CASBs) are tools that the enterprise may wish to investigate relative to cloud security. They are on-premises or cloud-based software or appliances that are positioned between the enterprise's technology infrastructure and the CSP.

As with any product, functionality varies by vendor, but as a baseline, most CASBs enable the enterprise to gain visibility into both authorized and unauthorized cloud application usage throughout the organization, provide a way to discover potential regulatory noncompliance, ensure secure storage of data in the cloud, and offer a degree of threat protection that mitigates to an acceptable security risk level.

Overall, most enterprises use CASBs for three primary purposes:

- **Discovery and analysis of cloud applications**—Most organizations have a significant number of applications, tools or services running in the cloud, most of which are authorized; that is, they are tested, approved, implemented and monitored by the IT department. However, in some cases, employees need enhanced functionality in a hurry and leverage the relatively low cost of and easy access to cloud applications without going through the IT department's approval process. These instances are referred to as "shadow IT." While shadow IT can be beneficial, it also has the potential to expose the organization to significant data leakage and, potentially, a breach, which may result in financial loss, reputation damage and/or other threats such as noncompliance. Many organizations rely on their CASB to discover and catalog all the cloud services being used internally so the risk can be assessed and usage patterns identified that may help them address security issues.
- **Governance and protection of data**—Just as most organizations have an overarching business strategy, they also have a data governance strategy. Among the tactics to support the strategy are policies relating to technology and data, such as security policies, data use policies and data loss prevention (DLP) policies. Communicating awareness of policies and enforcing their compliance pose challenges even on the organization's premises; it becomes even more difficult when dealing with an off-premises third party, such as a CSP. Some organizations use their CASB to extend and enforce the pertinent activity and data security policies to the cloud, to ensure that internal business rules and procedures are applied to cloud resources (files and applications). Most CASBs provide dashboards of pertinent data that enable effective monitoring of risk.

  In addition to support with governing data, CASBs can help protect the data. For example, organizations often integrate their CASB with their authentication solution to set up adaptive access controls that are informed by intelligence generated by the CASB. This enables the CASB to perceive that an employee is trying to access highly sensitive data and to apply appropriate, adapted responses, such as blocking access or sharing ability.
- **Threat detection and incident response**—While valuable, policies are only as good as the actions taken to "walk the walk." Enterprises are looking to CASBs to take a variety of actions that will enable them to identify anomalies in data movement between on-premises and cloud applications and between cloud services—anomalies that may provide early warning of malware, a failure of encryption, or an impending loss or exposure of cloud data. The activities CASBs can support in this area cover the life cycle of detecting and responding to threats—from setting threat detection thresholds, to monitoring all cloud accounts for policy violations or developing threats, to investigating incidents and generating detailed reports. The report and logs created by the CASB—which often cover the type of threat, its causes and responses taken—can also support internal audit reviews and findings, especially when internal audit has the opportunity to help develop the report format.

The CASB is a tool, not the solution; people, capabilities, resources, processing, monitoring and response plans are required to realize the CASB's full potential.

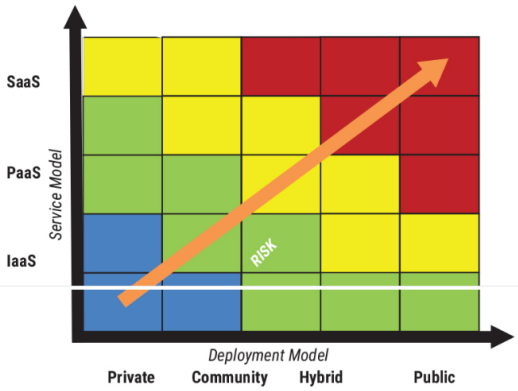
3.4.2 Other Risk Factors

Security is not the only risk factor related to cloud computing. Other areas of concern that merit attention include:

- **Privacy**—Individuals and groups have a strong drive to protect their identity in an online environment. CSPs are responsible for taking measures to protect sensitive personally identifiable data belonging to their clients. Privacy is included in a SOC 3 report, as noted previously, but enterprises that choose not to use such a report must still consider privacy issues.
- **Compliance violations**—Moving data to the cloud does exempt an enterprise from regulations surrounding the protection and use of data. However, the involvement of a CSP in data management may make compliance more difficult.
- **Loss of control**—Transitioning assets/operations to the cloud entails the enterprise losing a degree of visibility and control over those assets/operations. Enterprises must adopt and exercise monitoring and analysis of information about their applications, services, data and users. The ease of adding cloud services can also contribute to a risk-laden loss of control in that employees can provision additional services without IT's review or consent. This can lead to a lack of alignment among in-house applications, introduction of malware, redundancies and cost overruns.
- **Vendor lock-in**—Sometimes a contract with a provider does not easily protect the enterprise from changes to services and products such as supported programming languages or development tools. This becomes an issue when an organization considers moving its assets/operations from one CSP to another (or if the CSP goes out of business). The organization discovers the cost/effort/schedule time necessary for the move is much higher than initially considered, due to factors such as nonstandard data formats, nonstandard application programming interfaces (APIs), and reliance on one CSP's proprietary tools and unique APIs.

The type and degree of risk vary according to the cloud service model and deployment model selected by the enterprise, as illustrated in **figure 3.3**.

Figure 3.3—Cloud Risk by Service and Deployment Models



Source: ISACA, *Controls and Assurance in the Cloud: Using COBIT® 5*, USA, 2014, figure 3, https://www.isaca.org/bookstore/cobit-5/cb5ca

This section discusses just a few areas of cloud-related risk, most of which relate to the IT that supports the service. It is helpful to consider these multiple threats in IT risk categories and keep in mind some pointed questions that should be asked when considering a move to the cloud (**figure 3.4**).

Figure 3.4—Risk Categories and Questions to Consider

Risk Category	Description	Questions
IT benefit/value enablement risk	Associated with missed opportunities to use technology to improve efficiency or effectiveness of business processes or as an enabler for new business initiatives	• Will the cloud program provide a user environment that matches or exceeds the experience offered by competitors? Will current and new users welcome and embrace the experience? • Will the cloud program be completed and then maintained within estimated budgets, providing or exceeding the expected value?
IT program and project delivery risk	Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programs as part of investment portfolios	• Can the enterprise's IT organization execute the planned new cloud program successfully, on budget and on schedule? Will the cloud program provide the expected business benefit? Would not moving to the cloud cause additional levels of risk? • Will the cloud program provide a user environment—for internal, partner and customer users—that is well-thought-out, intuitive and welcoming to use? • Will the environment address the prespecified business

		needs and be able to accommodate requirements identified after implementation?
IT operations and service delivery risk	Associated with all aspects of the business-as-usual performance of IT systems and services, which can bring destruction or reduction of value to the enterprise	• Will the operational support provided by the CSP maintain expected performance and allow for cost-effective scale to support business growth objectives? • Can the new cloud program meet current and future regulatory requirements?

Some enterprises find it useful to consider risk in terms of risk scenarios. A risk scenario is a description of a possible event that, when occurring, will have an uncertain impact—positive or negative—on the achievement of the enterprise's objectives. For example, in considering the selection of cloud technology, a positive risk scenario might be "Optimal technology is selected for implementation" while a negative risk scenario might be "Wrong technologies, in terms of cost, performance, features or compatibility, are selected for implementation." Well-developed risk scenarios support the activities of identifying, analyzing and acting on risk, and help make potential outcomes realistic and relevant to the enterprise.

Risk scenarios can be derived via two different mechanisms:

- **Top-down approach**—This approach, which starts from the overall enterprise objectives and proceeds to an analysis of the most relevant and probable IT risk scenarios impacting the enterprise objectives. If the impact criteria used during risk analysis are well aligned with the real value drivers of the enterprise, relevant risk scenarios will be developed.
- **Bottom-up approach**—This approach, in which a list of generic scenarios is used to define a set of more relevant and customized scenarios, applied to the individual enterprise situation.

These approaches are complementary and should be used simultaneously. Risk scenarios must be relevant and linked to real business risk. Using a set of example generic risk scenarios could assist in identifying risk, reduce the chance of overlooking major/common risk scenarios and can provide a comprehensive reference for IT risk. However, specific risk for each organization and critical business requirements will need to be considered in the organization's risk scenarios.

Simply determining risk, asking pertinent questions and developing risk scenarios are not enough, however, to keep the enterprise at an approved level of risk tolerance. A number of activities must be undertaken to manage risk. A few of those activities, which should constitute part of a fully developed Enterprise Risk Management (ERM) program, include:

- The enterprise must ensure that the results of risk assessments are addressed in risk action plans, which are, in turn, reflected in SLAs.
- A system is established to ensure that risk acceptance is approved by a member of management with the authority to accept the risk on behalf of the organization and who understands the implications of the decision.
- Risk management controls are put in effect in the enterprise and the CSP to manage risk-based decisions.
- The CSP is asked to make available to customers independent third-party assessments to describe the control practices in place at the service provider's operating locations.
- The CSP is asked to submit third-party reviews that certify that the controls have been tested using recognized selection criteria.
- The deployment scenario (SaaS, PaaS, IaaS) defines the data protection responsibilities between the customer and service provider, and these responsibilities are clearly established contractually.

3.5 Cloud Vendor Selection and Management

The selection and ongoing management of a CSP may be the most critical aspects of successful cloud utilization. A CSP that operates in a way that is compatible with the enterprise's needs can ensure a mutually beneficial business relationship. The enterprise plays its part by establishing effective selection and management processes to secure the right vendor, outline performance expected from that vendor, and monitor performance consistently.

3.5.1 Vendor Selection

Once an enterprise has determined that a move to the cloud would be advantageous and selected the most suitable service type and model, it must select a CSP. This is not always an easy task as it entails finding a vendor that best serves the business needs while minimizing potential risk.

A transition to the cloud will be much easier when the CSP has the same industry certifications as the enterprise. This also goes for the business needs of the enterprise: Enterprises that are changing rapidly will want to choose a CSP that is agile and can change quickly as well. If, for example, computing requirements change daily, the enterprise needs a CSP that can accommodate those changes rapidly and fluently. A CSP that can change processor power only biweekly and that also requires the completion of four different forms for each change may not be the best choice for the enterprise.

While there are many suitable CSPs, it is important to choose an established one with the proper references. Established CSPs are potentially more experienced with running cloud infrastructures, adapting to change and generally responding faster to an incident or threat, thus being able to maintain stability more efficiently. However, a larger CSP may also be stricter about its offerings, which could greatly reduce the possibility of fine-tuning services not fully compatible with the enterprise needs.

The following characteristics and challenges can influence the selection of a CSP, depending on the objectives and goals established as part of the governance framework:

- **Vendor expertise**—The enterprise needs expert knowledge or a broader perspective and experience with similar enterprises to effectively and efficiently handle certain activities.
- **Vendor capacity**—If the enterprise does not have the resources to handle the work related to a specific product or service, the vendor can supply the resources to support the entire operation or supplement in-house resources.
- **Vendor assuming risk**—The enterprise wishes to outsource activities to leverage a vendor's experience with operational risk and corresponding risk mitigation services. However, the accountability for the adequate performance of those activities can never be delegated and stays with the enterprise.
- **Vendor leveraging scale**—Vendors can offer services at a lower cost because working for multiple customers allows vendors to leverage scale.
- **Cloud security policy/procedure transparency**—Some CSPs may have less transparency than others when it comes to their current information security policies. The rationalization for this is that the policies may be proprietary. This practice may cause conflict with clients' information compliance requirements. It is important for the enterprise to ascertain whether the CSP has adequate security controls/detection systems in use, such as penetration detection. If such a system is in use, it is important to ensure that it has the required sophistication to monitor all cloud computing activities adequately. It is also important to consider whether a real-time digital dashboard is provided to user managers, along with audit logs and records of security incidents.
- **Legal and regulatory requirements**—For the many compliance requirements, including privacy and PII laws, Payment Card Industry (PCI) requirements and various financial reporting laws, today's cloud computing services can challenge various compliance audit requirements currently in place.
- **Vendor business viability**—As with enterprises in all areas of business, some CSPs will thrive and others will go out of business. Clients need to consider the risk and how data and applications can be easily transferred back to the traditional enterprise or to another CSP.
- **Screening of other cloud computing clients**—By definition, CSPs leverage their cloud computing technology for many clients concurrently to maximize revenue. Clients should consider whether the other clients who share the same servers—and, in the case of SaaS, the same application and data files—are of the same repute as their own enterprises. This degree of due diligence should also apply to vendors that are in the critical path of the CSP. Background checks on these enterprises are important to ensure that data are not being hosted by an organization that is incapable of responding to outages or providing business continuity or that is engaging in malicious or fraudulent activity.
- **Cloud data ownership**—Some CSPs require contracts that provide them ownership of the data placed in the cloud computing environment they maintain. They may also require significant service fees for data to be returned to clients if or when a cloud computing services agreement is terminated.
- **Record protection for forensic audits**—Clients must also consider the availability of data and records, if required for forensic audits. Since data may have been commingled and migrated among multiple servers located widely apart, it may be possible that the data for a specific point in time cannot be located. Furthermore, local authorities may impound a cloud computing server to assess court-warranted data records of a suspect client, taking all the data in the cloud.

Vendor location (storage and processing centers) is of key importance for legal reasons. Laws are applicable locally, which can result in a multitude of different law systems applicable to data or business processes stored in the cloud. The most important applicable laws are:

- **Local law of the enterprise**—Storing data in the cloud does not waive the enterprise from the legal obligations it has toward its customers, employees and shareholders. Therefore, local laws will still apply even if data are stored abroad.
- **Local law of the CSP**—Since the CSP has legal obligations toward its customer (the enterprise), the local laws of the CSP may become applicable to its data centers and its content, including the data or business processes of the enterprise.
- **Local law where data are stored**—Local laws apply to the CSP's storage centers. The country that houses the storage center also imposes the law. This is especially important in relation to privacy. Privacy regulations that the enterprise is bound to may not be applicable in the country where the data are housed, thus potentially compromising the stored data.
- **Local law where data are processed**—In some countries local laws do not merely apply to where data are stored, but also are applicable to the location where data are processed.

More established CSPs will take legal matters into account to avoid legal issues when deploying their data centers and storage centers. It is important, however, to have the CSP's storage regions backed up by an independent organization so it can be assured that data or business processes are in the best possible hands.

Cloud computing requires oversight from the CSP and the client. Enterprises should consider CSPs as partners who share the responsibility of managing assets residing in the cloud. The criticality of these partners will depend on the nature of the assets the enterprise is willing to move to the CSPs environment. The enterprise should remain the sole proprietor of the assets, while the CSP will become a guardian responsible for the activities agreed on in the contract and SLAs.

A CSP is not the only cloud-related vendor the enterprise may wish to research and evaluate. A cloud service broker (CSB) is a third-party provider with access to multiple data centers and cloud service offerings. A CSB integrates and tailors those various services into one service that can be intertwined with enterprise in-house applications and systems. This integration enables the CSB to guarantee interoperability among various cloud services and can make the transition to the cloud more cost-effective.

3.5.2 Vendor Management

An effective vendor management process with goals and objectives can help ensure the following outcomes:

- The vendor selection and management strategy are consistent with enterprise goals.
- Effective cooperation and governance models are in place.
- Service, quality, cost and business goals are clear.
- All parties perform as agreed.
- Vendor risk is assessed and properly addressed.
- Vendor relationships are working effectively, as measured according to service objectives.

These outcomes are critical to the success of the cloud program and involve high-level, coordinated performance of multiple tasks on a consistent basis. Consequently, vendor management is not the work of a single individual or small group. There are responsibilities at virtually every level and function of the enterprise, and they must be performed well to realize the desired outcomes.

The specific responsibilities will vary by enterprise, given different industries, laws, budgets, staffing and organizational structures. However, some general responsibilities can be outlined for various functions, as shown in **figure 3.5**.

Figure 3.5—Responsibilities of Vendor Management Roles

Position	Description	Responsibilities
C Suite	The C-level executive who is accountable for the vendor management process depends on the scale of outsourcing. For involvement of large-scale vendor services covering or impacting the entire enterprise, the chief executive officer (CEO) and chief financial officer (CFO) are closely involved and take on the accountability for the activities described for the CIO. The CEO and CFO should be informed of vendor performance during the operations phase.	CIO: • Often accountable for the execution of the contractual vendor relationship life-cycle phases (when the scope and impact of products and services are limited to IT). • Provides oversight to ensure that contract objectives do not conflict among vendors, products and services; contracts comply with internal policies; contracts are managed properly; and SLAs are met. • Provides oversight and coordination of all responsible parties and supports other C-level executives in the decision-making processes (when the scope also includes the business). CFO: • Responsible for the enterprise budget after it is approved by the board; therefore, should approve the budget available for IT vendors. • Should be at least consulted for drafting the call for tender to validate budget specifications, negotiating with multiple vendors and agreeing on the final vendor contract.
Business process owners	Because the goal of contracting IT products or services is to enable the enterprise to achieve its goals, the business process owners should be actively involved in the vendor management life cycle, in addition to IT and procurement.	• Provide business requirements. • Consolidate stakeholder requirements and make sure they are validated and approved by all parties. • Evaluate potential vendors using specific business knowledge and expertise. • Provide input for contract specifications (e.g., service levels and transition-out specifications).
Procurement	Involving sourcing professionals from the beginning of the process enables them to support business units, IT and compliance during the selection and contract management processes.	• Help business process owners consolidate business requirements from various stakeholders. • Help IT consolidate IT-related requirements. • Prepare and send out the call for tender. • Gather vendor offers. • Facilitate the vendor evaluation process, vendor negotiations and contract management activities.
Legal	To effectively mitigate vendor-related risk, the legal function should be involved throughout the entire vendor management life cycle.	• Provide input regarding service requirements, from a legal point of view. • Consolidate legal requirements and make sure they are validated and approved by the other stakeholders. • Provide boilerplate standard contract language for important legal and compliance provisions. • Evaluate potential vendors using specific legal knowledge and expertise. • Draft the contract, taking into account and reviewing the specifications provided by other stakeholders.
Risk function	The risk function should be consulted throughout the vendor management life cycle to obtain a complete view on risk that is related to the relationship, services or products. After the risk assessment is completed, the	• During the setup and contract phases, provide requirements to mitigate potential risk. • Address potential risk during the operations phase within the enterprise risk framework, based on information provided by the business units and

	enterprise identifies controls required to minimize newly identified risk and updates related documentation (e.g., business impact analyses, BCPs, DRPs, insurance policies and the risk framework).	the enterprise risk appetite. • If the vendor environment, business model, products or services change, initiate an assessment to identify and address new risk.
Compliance and audit	The compliance and audit functions should be consulted throughout the vendor management life cycle to ensure compliance with internal and external laws, regulations and policies.	• Ensure compliance of vendor candidates during the selection process. • Provide compliance requirements to be included in the contract. • Ensure compliance of the selected vendor during operations.
IT	All stakeholders share the responsibility of the vendor management process to ensure that products and services received from the vendor support enterprise goals within risk tolerances. However, the IT role is significant because its members may be more familiar with the products and services and their market availability.	• Identify potential vendors, products and services. • Provide input regarding requirements for products and services from an IT point of view. • Provide input associated with baseline standard requirements and architectural limitations. • Provide expectations associated with good practices and defined architectural boundaries. • Provide information practices, such as information ownership and co-location requirements, partnership arrangements and employee checking. • Consolidate the previous inputs and ensure that they are validated and approved by all stakeholders.
		• Evaluate potential vendors using specific IT knowledge and expertise. • Provide input for contract specifications (e.g., transition-in specifications, transition-out specifications and service metrics). • Monitor, report and manage vendor performance during operations.
Security	Although security is often associated with the IT stakeholder, security is regarded as a separate stakeholder because it does not always reside within the IT function and can be involved with other functions as well as IT.	• Provide input regarding security requirements for products and services. • Provide input associated with baseline security standard requirements. • Provide information practices, such as information accessibility and required assurances of information protection.
		• Verify compliance of the vendor with product, service and information security requirements.
Human resources		• Should be consulted throughout the vendor management life cycle to ensure compliance with the enterprise's worker statutes, local regulations, code of conduct and labor law.

However, the client enterprise may be structured, there are generally two main approaches/techniques the client may use to manage and measure a CSP's quality of service performance:

- Use vendor management, including but not limited to vendor risk assessment, vendor due diligence, vendor-tiering (based on the significance of the process outsourced), and contracting and SLAs (as they apply to a CSP).
- Apply independent assurance by either the CSP's auditors or client personnel outside of vendor management (involves understanding the scope of services provided, obtaining and evaluating third-party assurance reports, evaluating residual risk, and determining whether an onsite visit to the service provider is required).

Service Level Agreement

A key element in any vendor management program is the SLA. A well-designed SLA and mature service level management maximize the effectiveness of the services they target and manage. This improves business performance and fosters a better relationship between the enterprise and the vendor through:

- Better alignment with business objectives
- Ability to manage services proactively
- Greater transparency of service delivery
- Lower service level management overhead
- Better relationships between the enterprise and vendor

An SLA is an agreement between the enterprise and a product or service provider. This service provider may be an external party—in the case of this publication, a CSP; an internal department, e.g., the IT department for IT services; or a combination of both. An SLA is very common in IT contracts and can be an effective tool to create a common understanding between contracting parties regarding services, priorities and/or responsibilities in the framework of an agreement.

The purpose of the SLA is to ensure alignment between IT-enabled services and service levels, enterprise needs and expectations regarding the handling, usage, storage and availability of information, and requirements for business continuity and disaster recovery. It facilitates the relationship between the client enterprise and the CSP by making clear the goals and objectives of the relationship, the expected performance levels, the responsibilities of each party, and actions to be taken in the event of nonperformance or termination.

SLAs must be measurable (using process metrics, which inform the CSP and the enterprise of the effectiveness and efficiency of key actions done while delivering service and technology metrics, which provide efficiency data on the component level), to allow meaningful reporting among the parties—reports that can be used during consultations between parties about the achievement of the SLA. Agreed, realistic terms in the SLA can help eliminate grounds for disputes between parties.

The enterprise must determine in advance the terms to be included in the SLA, keeping in mind that strict or complex SLAs may result in higher maintenance cost. Some terms that should be negotiated

and documented in the SLA include:

- Availability
- Response time for additional computing resources requests
- Response time for incidents
- Backup policies
- Data retention and disposal policies and procedures
- Path management
- Security controls
- Recovery and continuity objectives
- Controls to satisfy legal and compliance requirements

It is also important to address in the SLA the consequences of failure to meet the performance levels specified in the agreement, perhaps by outlining a set of actions to deal with the cause of such failure. The parties could define penalties in case of nonachievement of the levels established (perhaps coupled with incentives for achievement). If a price correction is defined as a penalty, it is important to stipulate that the price correction is not the only compensation that can be claimed in a case of nonachievement of the SLA, so that the right to the payment of full damage is not jeopardized. For continuity of the enterprise, it is recommended to provide a special clause that states that the enterprise can appoint a third-party service provider to deliver the necessary services in case of nonachievement of the SLA by the service provider.

An audit clause can be included in the contract associated with the SLA to grant the enterprise the right to access relevant financial data, accounting information, operational and technical data, safety standards, etc., of the other party. Use of an audit clause is strongly recommended because it allows the enterprise to check, among other areas, the co-contracting party's performances, compliance and achievements.

Service Level Monitoring

Clearly, the enterprise's focus on service levels does not conclude with the execution of the contract. Consistent, thorough monitoring of service levels must take place for as long as the relationship with the CSP is in place, in accordance with the reporting requirements, performance expectations, penalties for shortfalls in performance and rewards for performance that exceeds expectations, as specified in the SLA. The quality of the monitoring depends, in large part, on open and honest communication between the enterprise and the CSP, as well as a shared commitment to meeting objectives measured via specified metrics.

Monitoring may be done by the client enterprise or it can be turned over to a third party that specializes in that activity. In either case, it is likely that one or more of the multiple monitoring tools on the market will be employed. Given the potential need for a third party and the almost certain need for tools, the enterprise must be aware, before entering the cloud space, that there are costs associated with monitoring CSP activities as they endeavor to deliver on the promises made in the SLA.

Identity and Access Management and Vulnerability Management

Many of the risk concerns associated with cloud management were covered in section 3.4. However, two topics merit additional discussion here because, when it comes to risk, security, incident response, etc., clients are limited by the vendor to what the original contracts allow. These same issues arise with cloud-provided IAM and the ability to conduct or receive vulnerability management reports. The enterprise has limited capabilities to mitigate or respond and must rely on what the vendor is willing to provide. This calls for prudent and effective vendor management.

Identity and Access Management

IAM encompasses people, processes and products to identify and management of the data used in an information system to authenticate users and grant or deny access rights to data and system resources.

Its goal is to provide appropriate access (or deny inappropriate access) to enterprise resources. The enterprise should have a strong interest in ensuring that its CSP has developed and implemented adequate user access privilege controls. For example, the enterprise should ensure that user provisioning (on-boarding), deprovisioning (termination) and job function changes of cloud-based applications and operating platforms are managed in a timely and controlled manner, according to internal user access policies.

The increasingly sophisticated applications offered online and available for access by enterprise users, partners and clients call for the use of highly granular and least-privilege-based user access tools. The responsibilities for ensuring an effective IAM system, as categorized by the CSP and the enterprise, are shown in **figure 3.6**.

Figure 3.6—Responsibilities for IAM

CSP	Enterprise
• Manage user identity and logical access. • Manage physical access to IT assets. • Manage roles, responsibilities, access privileges and levels of authority. • Ensure traceability of information events and accountabilities. • Monitor the infrastructure for security-related events.	• Define requirements. • Communicate requirements. • Choose the level or package of service that best meets enterprise goals (based on budget, risk appetite and anticipated benefits delivery). • Document requirements in contracts and SLAs. • Implement internal processes to manage identity and access requests. • Assess control environment. • Report results.

Source: ISACA, *Controls and Assurance in the Cloud: Using COBIT® 5*, USA, 2014, https://www.isaca.org/bookstore/cobit-5/cb5ca

The enterprise's needs and expectations should be spelled out in the contract with the CSP (and managed and monitored consistently thereafter). The agreement should define who can access the enterprise's information, naming specific roles for CSP employees and external partners.

The enterprise should request that the CSP provide detailed technical specifications of its IAM system for the enterprise's chief information security officer (CISO) to review and approve. If the CSP declines to provide such details due to its own internal security policies, the enterprise can request controls and benchmarks, such as the result of penetration testing on the CSP's IAM systems, as an alternative.

An alternative approach is to use the enterprise's IAM systems instead of the CSP's IAM systems. In this way, IAM remains the responsibility of the enterprise, so no access to assets can be granted without the enterprise's knowledge. This approach requires the approval of the CSP and the establishment of a secure channel between the CSP infrastructure and the enterprise's IAM system.

Vulnerability Management

Vulnerability management is another area of special concern to enterprises that use cloud computing services. Information assets could be accessed by unauthorized entities due to faulty or vulnerable access management measures or processes. This could result from a forgery/theft of legitimate credentials or misuse of a common technical practice (e.g., administrator permissions override). The number of new attacks increases regularly and at breakneck speed; it is a constant challenge to stay ahead of the attackers.

Enterprises have a vested interest in ensuring that the CSP is exercising all reasonable efforts to keep the environment in which the enterprise's data are stored and processed free from vulnerabilities that provide opportunities for attackers. Vulnerability management is a key component of a strong information security program, in the enterprise and in the CSP's environment.

However, it is the very nature of the cloud—the fact that organizations do not own and control the infrastructure that provisions the cloud service, nor do they have access to vulnerability data of cloud native services—that make vulnerability management especially difficult. This is coupled with the enterprise's inability to apply security controls or other mitigation to the cloud provider's infrastructure. Ultimately, the enterprise's ability to make informed, risk-based decisions about cloud services is affected.

This is not to say that there is nothing the enterprise can do about potential cloud vulnerabilities. As with IAM, the first step is attention to the contract with the CSP. The enterprise should require the CSP to undertake continuous vulnerability assessment of its infrastructure and provide the enterprise reports that meet the enterprise's specifications for content and frequency.

If the CSP provides the versioning of the software (if there is one), that too may help the enterprise determine whether certain vulnerabilities may exist. The SLA should contain detailed specifications about vulnerability classification and actions taken according to the severity level (and in alignment with the enterprise's policies and procedures for similar events) and clarify who is allowed to access the enterprise's information, naming specific roles for CSP employees and external partners. And, of course, the enterprise should request that the CSP implement application firewalls, antivirus and anti-malware tools. If the request is denied, it may be time to begin a search for a new CSP.

3.6 Portability of Services

Despite the best efforts at vendor selection and management, situations can arise in which it is advisable or necessary to migrate data, applications or platforms from one CSP to another or bring services back in-house. For example:

- The CSP may have applied a price increase the enterprise believes to be disproportionate to a service provided or out of line with marketplace values.
- The CSP may have fallen short of SLA levels of performance or breached enterprise confidentiality.
- The CSP may change its services often, without prior notice to the enterprise.
- The enterprise may have uncovered a new business need that necessitates moving cloud-based resources to a different geographic area, under different jurisdiction.

Portability is a difficult process and can result in business disruption or failure for the client in any case, but especially if the CSP has gone bankrupt, faces legal action or is the potential target for an acquisition (which may entail sudden changes in CSP policies and agreements in place).

This underscores the need to outline clearly in the contract and/or SLA the terms that will trigger the retrieval of the enterprise's assets, the processes surrounding migration, the responsibilities of each party and the time frame for completion of migration as required by the enterprise.

However, even with clear language in the SLA, a smooth, effortless portability process is not guaranteed. Different environments are likely to have compatibility issues, and containers—sometimes touted as a solution to portability woes—cannot always smooth the path. Indeed, some IT experts believe that completely trouble-free portability is an outcome that is unlikely ever to be reached.

For several years, various efforts have been underway to develop standards related to the cloud, including portability. Some activities have been government-led, aimed at creating pertinent legislation. Other efforts have been driven by organizations such as the Institute of Electrical and Electronics Engineers (IEEE) and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), which has produced ISO/IEC 19941:2017 *Information technology – Cloud computing – Interoperability and portability*. As standardization becomes more widely accepted and adopted, it should make portability easier, helping cloud computing enable use of the same applications in different environments.

3.7 Chapter 3 Knowledge Check

REVIEW QUESTIONS

1. One reason to implement sound governance with a cloud implementation is to:
   A. Ensure continuity of critical business processes that now extend beyond the data center
   B. Manage increasing risk while ignoring security and other aspects
   C. Prove to management that migration to the cloud is worth it
   D. Move assets off premise to reduce accountability

2. Governance is likely to achieve its mission without complete buy-in from the board of directors.
   A. True
   B. False

3. What is the **BEST** cloud capability to address the business need of cost savings?
   A. Cloud computing makes patch management more flexible.
   B. Cloud computing can provide on-demand implementation in real time.
   C. Cloud computing is self-healing.
   D. Cloud computing can reduce the number of workstations in the office.

4. All of the following are informational asset risk events, except:
   A. Loss
   B. Unavailability
   C. Manipulation
   D. Disclosure

5. Which of the following reflects a governance objective to consider during vendor selection?
   A. Bandwidth
   B. Culture
   C. Processing capability
   D. Risk assumption

6. What provision can be included in an SLA with a vendor to ensure achievement of proper compliance?
   A. Security controls
   B. Backup policies
   C. Retention of data
   D. Audit clause

7. Which of the following **BEST** describes portability of services?
   A. The ability of the CSP to physically move data from one datacenter to another
   B. How the CSP handles billing requirements
   C. The ease of moving data and services from one CSP to another
   D. The number of mobile data centers a CSP provides

Answers on page 54

Chapter 3 ANSWER KEY

Review Questions

1. **A. Ensure continuity of critical business processes that now extend beyond the data center. Refer to page 34.**
   B. Manage increasing risk while ignoring security and other aspects
   C. Prove to management that migration to the cloud is worth it
   D. Move assets off premise to reduce accountability

2. A. True
   B. False. Refer to page 35.

3. A. Cloud computing makes patch management more flexible.
   B. Cloud computing can provide on-demand implementation in real time.
   C. Cloud computing is self-healing.
   D. Cloud computing can reduce the number of workstations in the office. Refer to page 35.

4. A. Loss
   B. Unavailability
   C. Manipulation. Refer to pages 38-39.
   D. Disclosure

5. A. Bandwidth
   B. Culture
   C. Processing capability
   D. Risk assumption. Refer to page 44.

6. A. Security controls
   B. Backup policies
   C. Retention of data
   D. Audit clause. Refer to page 50.

7. A. The ability of the CSP to physically move data from one data center to another
   B. How the CSP handles billing requirements
   C. The ease of moving data and services from one CSP to another. Refer to page 52.
   D. The number of mobile data centers a CSP provides

[12] Stroud, R.; "Providing Governance in a Rapidly Changing World," ISACA Euro Computer Audit, Control and Security (EuroCACS) conference 2010, Budapest, Hungary

[13] American Institute of Certified Public Accountants, "2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy," March 2020, p. 6-8, www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf