The silver lining: 
Getting value and mitigating risk in cloud computing

Frequently asked questions

The cloud is here to stay. And given its decreased costs and increased business agility, organizations are moving more of their IT processes and capabilities to the cloud environment. But when you hand over control of your IT systems to a cloud provider, you need to be ready to address the risks involved and plan your internal audit accordingly.

Below are some of the frequently asked questions posed during a webcast hosted by the Institute of Internal Auditors (IIA), where Grant Thornton was invited to present. Our professionals provided answers and tips related to cloud computing, IT security and SSAE 16.

Cloud computing

Q: Won’t cloud service providers be reluctant or even unable to respond to numerous audit requests from user organizations?

A: It is very likely that cloud service providers will be reluctant to respond individually to numerous audit requests from user organizations. One of the key benefits derived from engaging an audit firm to issue a Service Organization ControlSM (SOC) 1 report is that this type of report may be provided to satisfy those requests. Moreover, with the release of new guidance concerning SOC 2SM and SOC 3SM reports, additional controls such as those related to security and privacy can be addressed within separate attestation engagements.
Q: What is a general price range for audits of controls at cloud computing providers and what are the drivers that increase costs within that price range?

A: The biggest driver of costs is the complexity of the user transaction processing system (consisting of people, processes and technology) that is in place at the service organization. The complexity of the services that are provided drives the number of risks to a user organization’s internal controls, and the number of risks drives the number of control objectives and activities identified in the report. Pricing for a SOC 1 audit, for example, can range from $20,000 to well over $400,000.

Q: What are some of the major risks of hacking and data compromise in cloud environments?

A: One of the main risks is that the cloud provider's security approach might not meet the user organization’s requirements. This could result in additional vulnerabilities that a hacker could exploit, putting the user organization at risk for unauthorized data disclosure. Companies should talk to their cloud provider to understand how their data will be protected, who will have access to that data, and what will happen if there is a security breach at the provider.

Q: Right now, our IT department is audited as part of our yearly financial statement audit. If we don’t have our own IT department and use the cloud instead, how will an external audit be conducted?

A: The external auditor will still need to confirm that adequate controls are in place to meet the company’s control objectives. The existence and operation of controls that satisfy the relevant control objectives should be documented in a SOC report that has been obtained and provided by the cloud provider.

Q: If our organization has paid for a high resource priority during emergencies/data recovery, what is the risk of the government appropriating cloud resources for its own use during an emergency?

A: This is a valid concern that you should discuss with the cloud provider.

Q: Do we have to stay in a captive environment? That is, how difficult is it for a user organization to terminate the services of an unsatisfactory cloud provider?

A: This is a valid concern that you should discuss with the cloud provider before you agree to engage its services. Specific provisions related to terminating business with the provider should be included in the contract.
Q: What are the top two risks to manage in a private cloud application?
A: The private cloud might not meet the company's data security requirements and the system might not be available when the company needs it.

Q: What is the most common risk related to cloud computing for a financial institution?
A: One of the most common risks is ensuring that the financial institution continues to meet regulatory requirements. The institution must be able to demonstrate to examiners that those requirements are being satisfied.

Q: How will cloud computing affect IT jobs?
A: Companies that use cloud solutions will need a specialized IT employee who is skilled in vendor management, systems analysis and cybersecurity. Additional jobs will likely be created by cloud providers.

Q: Would you recommend a cloud environment for electronic workpapers in governmental audit organizations?
A: This will depend on the type of governmental organization that you work for, the kind of information included in the electronic workpapers, and the cloud provider's ability to meet your organization's cybersecurity requirements. Each organization will have specialized needs.

Q: Are there any ratings bodies that assess the status of security at any given cloud provider?
A: The Cloud Security Alliance, cloudsecurityalliance.org, has several certification and audit programs. These are all very new, and they apply criteria that are evolving.

Q: How suitable is cloud computing for health care organizations, which face HIPAA and HITECH regulations and risks related to PHI?
A: Health information exchanges are cloud services that exist to transmit patient health records between providers (e.g., from the laboratory to the physician). The National Institute of Standards and Technology (NIST) has proposed a health information exchange security architecture; for details, see www.nist.gov/healthcare/security/hiesecurity.cfm. Surescripts is a resource that provides a secure platform for exchanging patient data between laboratories; additional information is located at www.surescripts.com/clinical-interoperability.aspx.
Q: Does the client have any choice when it comes to firewalls and other security features?

A: Yes, in some situations. However, it will depend on the specific cloud solution.

Q: Does change management in the cloud differ from change management of on-the-ground processes?

A: No. However, the group responsible for the change management processes is normally different (i.e., the cloud provider versus the company's internal IT group).

Q: What are your thoughts on the appropriateness of pre-Internet encryption (PIE) of all data assets as a means of protecting corporate information before moving it to the cloud?

A: It depends on the risk appetite and regulatory requirements for each company. Companies with a lower risk appetite and tighter regulatory requirements will be more likely to need encryption both when their data is at rest and when it is in motion.

Q: How do we gain the skills needed to audit a cloud provider?

A: You will first need a basic understanding of IT auditing. We recommend that you review the IIA’s Global Technology Audit Guides (GTAG®). Next, you will need to understand the unique risks associated with cloud computing.

Q: How does cloud computing affect disaster recovery planning (DRP), also known as business continuity planning (BCP)?

A: One of the risks associated with cloud computing involves disaster recovery. Unlike on-premise computing, off-premise computing does not give the company the ability to recover its IT systems or business data. However, the company still has control over its BCP processes. We recommend that these processes be updated to address short- and long-term outages at the company's cloud provider.

Q: Does a cloud provider present a more attractive target for an attack, since a person may gain unauthorized access to multiple companies’ data versus just one company’s?

A: Yes. However, some cloud providers have advanced security tools to protect the data. User organizations with on-premise computing don’t always have access to these tools.
Q: Are there any audit strategies that would be particularly effective for a company limited by size and resources?

A: The approach to mitigating these risks will depend on how each company is using the cloud solution. The audit objectives and approach should be similar to the way each company addresses its on-premise IT environment.

Q: Data security would be our largest concern; the impact of a data breach would be devastating. How can a cloud service provider assure customers that all their data is secure?

A: One of the first steps a company can take is to ensure that its IT group has communicated its data security standards to the cloud provider. In addition, internal audit should work with the IT group to confirm that these standards have been implemented. Confirmation could come from reviewing a Statement on Standards for Attestation Engagements (SSAE) report or a SOC report and/or from performing internal audit testing at the cloud provider (the latter option would require a right-to-audit clause in the contract). While a cloud provider cannot give assurance that performing these activities will prevent a data security breach, doing so will help reduce the risk.

SSAE 16

Q: Is it sufficient to obtain a SOC report from our cloud provider?

A: The procedures that an internal audit function will need to perform should tie directly to the risks that have been identified for the services provided, including control activities at the user organization. Because SOC 1 and SOC 2 reports provide the user organization with a description of the service organization's transaction processing system, the controls in place to mitigate risks related to the control objectives, and the testing performed by the service auditor (as detailed in Type II reports), a review of these reports should be coupled with an examination of the risk assessment performed by the internal audit function to determine whether all identified risks have been mitigated to an adequate level. If internal audit reaches a tentative conclusion that the service organization's procedures or controls are not sufficient, the internal audit function should inquire of the service organization regarding the areas of concern and consider the sufficiency of the user organization's control activities. Internal auditors at the user organization may determine that it will be necessary to perform additional procedures at the service organization if allowed to do so by the contract. In addition, internal audit should test the user organization's controls.
Q: I often see prospective clients asking for not only SOC 1 reports, but also ISO 27000 certification. In your view, are both of those required to mitigate risk? What is the advantage of having an ISO 27000 certification?

A: Unfortunately, the determination of how many reports or certifications will be needed is going to be specific to the relationship that will be established between the service organization and its user organization. If the services provided will affect a user organization’s internal control over financial reporting, a SOC 1 report will likely be necessary. ISO/IEC 27001 is part of the ISO 27000 family of standards. It is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27001 formally specifies a management system that is intended to bring information security under the control of management. Organizations that have adopted ISO/IEC 27001 can be formally audited and certified as being compliant with the standard.

Q: Are SOC reports generally available to the public upon request or only to clients of the service organization?

A: The three types of SOC reports have slightly different use provisions. The most restrictive provision applies to the SOC 1 report. This report is intended solely for user organizations and their auditors as long as user transactions were processed by the service organization’s system during the reporting period. The SOC 2 report is intended to be used by a slightly broader audience. This audience may include prospective customers that have sufficient knowledge and understanding of the user transaction processing system in place at the service organization. This audience may also include the Assurance Services Executive Committee of the AICPA and certain other parties with knowledge of matters related to SOC 2 reports. The SOC 3 report has the broadest audience; SOC 3 reports are not restricted as to use and may be posted to the service organization’s website, provided that they include the appropriate seal.

Q: How comparable is ISO 27001 with SOC 2?

A: The similarities between these two reports center on the subject matter they cover. Because the scope of many SOC reports includes general IT controls, it is possible that controls identified within a SOC report will also need to be in place for an ISO 27001 report. However, these reports are very different with respect to the final product. Because the SOC 2 report is built upon the Trust Services Principles and Criteria, service organizations are able to adapt the scope of applicable controls and criteria to their services, and in some cases,
certain criteria will not be applicable. Moreover, the service organization will have to describe the controls it has implemented to satisfy the criteria, and this additional information may provide valuable information to user organizations. The ISO certification is based upon a standardized set of requirements, all of which must be satisfied in order for the certification to be granted. The requirements are not flexible; that lack of flexibility ensures that a baseline of controls has been established and tested.

Q: If you are a user organization, what can you do if a cloud provider does not obtain a SOC 2 report?

A: Most service providers are not required to provide user organizations with a SOC 2 report, but most of them do so anyway given the competitive nature of business. If user organizations negotiate a right-to-audit provision within their contract, they can conduct an internal review of the cloud provider, hire an outside party to perform the audit, or use the right-to-audit provision to require the service organization to provide a SOC 2 report on relevant controls. If a right-to-audit provision does not exist, user organizations need to determine how critical it is for them to examine relevant controls at the service provider. Under these circumstances, user organizations should evaluate whether they need to renegotiate the terms of the contract to be able to conduct a review of the cloud provider's controls.

Q: Since the risks and controls may vary depending on the type of service — such as software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS) — will there need to be a separate SOC report for each type of service?

A: An organization need not obtain multiple reports unless the nature of the risks that will be addressed within the scope of the engagement or the type of subject matter to be covered by the report is different. For example, a service organization may have very similar change management controls for its entire suite of transaction processing platforms. Under those circumstances, a single report may be sufficient to satisfy the needs of user organizations.

Q: What role will internal auditors working at service organizations have in defining the controls to be tested when SOC reports are a requirement for a company?

A: The role of the internal audit function will certainly differ from organization to organization, but management will usually be well-served by including internal auditors on the team that works to define the applicable criteria and control activities. Internal auditors will understand the subject matter and may have a useful perspective on identifying better control activities. Also, under the new
AICPA guidance, a service organization must prepare an assertion letter that will accompany the service auditor's opinion. The guidance stipulates that management must have a reasonable basis for its assertion. Within many organizations, the internal audit function may help management support that assertion. As a result of the testing processes that are normally associated with it, the internal audit group may be in the best position to assess the controls, including the monitoring controls, that have been placed in operation by the service organization.

Q: Can you tell me whether SOC 2 reports are commonly used within banks and financial services organizations?

A: The SOC 2 report is still quite new to the marketplace and does not have the broad acceptance that SOC 1 reports have. We believe that SOC 2 reports will become much more popular within the financial services industry, because organizations in this industry are very concerned with the privacy and confidentiality of information — two subjects that are at the heart of SOC 2 reports.

Q: In my understanding, a SOC 1 and SOC 2 audit cannot be performed by the same firm. Is that correct?

A: No, the same firm can perform both a SOC 1 and a SOC 2 engagement. In fact, we have found that in many instances, a single service auditor is able to leverage its knowledge of the institution and its controls across both audits. The reports can’t be combined into a single report, but they can be provided together.

Q: Under international standards, is there a service auditor's report equivalent to SOC 2?

A: The International Auditing and Assurance Standards Board has issued a general attestation standard that can be used to report on controls that would be covered in the United States by a SOC 2 report.

Q: What organizations provide independent assessments of controls?

A: Licensed CPA firms are able to provide SOC reports.

Q: Did I hear correctly that SaaS providers are expected to obtain and provide SOC 1 reports to their user organizations?

A: SaaS is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. It is probable that most SaaS providers will need to obtain and provide a SOC 1 report given the nature of the services that they offer.
IT security risks

Q: How do you view the emerging trend of security as a service? Does it make sense to entrust a high degree of management of the enterprise’s IT landscape to a third party?

A: We are starting to see a few companies using security as a service. Yes, some companies do benefit, such as smaller companies that do not have the infrastructure or resources to manage information security themselves. However, this service offering creates additional risks that need to be taken into consideration by the user organization.

Q: With VPN access becoming popular, are there any IT security strategies or points that you can suggest?

A: One best practice related to a VPN solution is to have strong user access authentication. For example, some companies that are subject to strict regulation have implemented tokenization technology that requires a one-time password. Other companies use digital certificates for authentication.

Q: If a cloud provider is using a proprietary software configuration, how much value is gained by retaining backups of the provider’s files?

A: While you might not be able to easily move the data to another provider, you should be able to extract specific information from the provider’s database.

Q: How do you obtain independent validation that encryption is in place?

A: Given the nature of data encryption, validating its effectiveness is a complicated process. Looking at the problem from a very high level, you should verify that the file is encrypted either by accessing it from the hard drive and viewing it there (when the data is at rest) or by using a networking tool to view the data on the network (when the data is in motion).