Moore’s Law has been operating for decades without signs of slowing down, which leads to new technologies and, thus, new challenges for IT auditors. In recent months, cloud computing and Software as a Service (SaaS) have led the “bleeding edge” of IT. Therefore, IT auditors need to understand these technologies, establish an approach for identifying the key risks and develop effectual audits of the technologies for those risks. However, the risk-based approach (RBA) process for cloud computing is complicated by the fact that all of the technologies and controls are housed outside the entity being audited.¹,²,³

A key to IT audits of cloud computing and SaaS is to choose a framework for the components that assist an effective risk assessment of those technologies. Once a proper risk assessment is produced, the IT audit becomes a natural extension of auditing for the identified risks, especially where controls have not adequately mitigated the risk. This RBA is the common approach for audits of various types today.

COMPONENTS OF CLOUD COMPUTING

Much has been written about cloud computing, SaaS, and data centers, but often those technologies are melded as a composite service referred to as cloud computing. Actually, there is a simple framework for thinking about cloud computing that should help IT auditors in performing a risk assessment. The components are Infrastructure as a Service (IaaS) and Software as a Service (SaaS)—almost identical to the way we think of the body of technologies internal to an entity.

CLOUD COMPUTING: IAAAS

Services of IaaS components replace or supplement the internal infrastructure. The key decision factors for management in deciding to move to IaaS (outsourcing part of its infrastructure) and choosing the appropriate vendor are usually efficiency-related. For instance, it takes one full-time employee (FTE) “blank amount of time” per year to manage about 70 servers. If the entity has a server farm, it can outsource those costs to an effective data center and reduce costs significantly. In addition, when the entity needs to upgrade its software, or acquire a new software application, the consideration of infrastructure is probably an insignificant consideration regarding cost, assuming the choice in IaaS provider was sufficiently sophisticated, and requires little to no changes to its own infrastructure.

There is also the accounting consideration. Usually, infrastructure costs are substantial and, according to the Generally Accepted Accounting Principles (GAAP), are treated as a capital expense (CAPEX). However, if the infrastructure is outsourced, the expense associated with the IaaS infrastructure usually becomes an operating expense (OPEX). In the US, this leads to a tax advantage regarding income taxes.

Thus, some of the key factors for management when choosing the IaaS provider are flexible performance (including scalability) and availability while achieving physical and virtual security needs.

There are various ways to break down IaaS, but here is one way:

- Connectivity
- Network services and management
- Compute services and management
- Data storage
- Security

Connectivity obviously refers to reliable access to the Internet and connectivity to associated systems and technologies, for instance, data storage to application servers. Examples of risks would be availability/downtime and speed of access.⁴ The average entity experiences one day per annum of downtime.

Network services and management includes not only providing network capabilities, but managing the network, monitoring the network and providing for efficient access through aspects such as load balancing. Examples of these risks...
are scalability for new technologies or expanding the level of transactions, availability, secured transmissions, and the level of access (e.g., load balancing).

Compute services and management include appropriate resources such as core, processors, memory and managing the operating system (OS). Examples of the risks are availability (including system failure) and scalability.

There has been significant growth in data centers over the last few years, and data centers are becoming more sophisticated in the scope of services. Examples of the risks for data storage include the obvious: security of data, recovery, availability and scalability. The security and recovery issues are particularly important. Management should ensure that the data storage aspect of IaaS can provide an appropriate level of physical and logical security and an appropriate recovery methodology to ensure a timely recovery if the data center is involved in a disaster.

Security issues are more or less ubiquitous for IaaS and include physical security, especially data storage, and logical security. They include security from unauthorized access by malicious intruders and rogue employees of the IaaS provider. In fact, the latter is an increased risk to the user entity that needs to be addressed via adequate controls by the service entity.

Risks are always determined within contextual circumstances to the entity—for example, the industry, its own business processes, the current economy and other circumstances peculiar to the entity at that time. Some of the other issues that may be risks are ownership, insurance, project management and performance reporting.

Mitigating controls could be discoverable from a SAS 70 Type II audit report. If one exists for the IaaS provider, the IT auditor should certainly read it to see what level of assurance can be gained for the specific, identified risks. Controls the provider should be employing include best practices in security, support (e.g., IT Infrastructure Library [ITIL] v3) and business recovery.

**CLOUD COMPUTING: SAAS**

Some of the key points in deciding to use SaaS, or a particular vendor, are the complexity of the environment, the need to buy smaller pieces/modules, compatibility with existing systems and IT (including programming platform), ease of purchase, ease of integration, project management, scalable infrastructure, and billing/costs (metering).

There are various ways to break down SaaS, but here is one framework:

- Business process modeling
- Evaluation and analysis
- Process execution

Business process modeling involves the need to fit together workflow/business process structure, applications and data, organizational structure, and the integration of existing systems. Evaluation and analysis includes process cost accounting, balanced scorecards, service level agreements (SLA), process warehouse and optimization. Process execution includes workflow control, applications integration (Enterprise Application Integration [EAI]), service orchestration (Service-Oriented Architecture [SOA]), populating databases/conversion and business activity monitoring. Other issues include document and content management, collaboration, systems management and administration, and various aspects of management of SaaS.

Examples of risks would be related to these areas. Some examples include an improper fit of the business process to the application, inadequate connectivity between applications and data, improper integration with existing systems, and inadequate monitoring of SaaS business processes and events. Obviously, the SLA is a key audit objective. There is also a risk of cost control and estimates; that is, it is possible that the move could end up costing the entity more rather than less. One example of cost control is the metering/billing aspect of SaaS, which presents an area of potential risk.

**IT ASSURANCE FRAMEWORK**

ISACA’s IT Assurance Framework™ (ITAF™) includes a section (3630.6) on outsourcing and third-party activities (see figure 1). Cross-references are included—ConIT® PO4, PO7, PO8, PO9, AI2 and AI5, and ISACA IT Audit and Assurance Guidelines (formerly IS Audit Guidelines) G4, G18, G32, and G37. These referenced documents provide useful technical assistance in conducting an IT audit for cloud computing.

Obviously, the fact that a third party is involved means direct auditing of the service entity may not be practical or
even possible. ITAF also supplies a list of potential documents that could provide service audit information that should be relevant (see figure 2).

CONCLUSION
Auditing cloud computing in one sense is like auditing any new IT—understand the IT, identify the risks, evaluate mitigating controls and audit the risky objects. The understanding and risk assessment can be enhanced with a good framework to think about the IT and risks and, thus, assist the IT auditor in conducting an effectual risk assessment. The IaaS/SaaS framework described here is intended to assist IT auditors in performing their duties associated with cloud computing.

ENDNOTES
2 Ross, Steve; “Cloudy Daze,” ISACA Journal, ISACA, USA, vol. 1, 2010
4 Each IT audit has its own context (e.g., financial audit, internal audit, special IT audit). Each IT audit has its basic objectives. Thus, the scoping aspects of a particular IT audit would review all of these risks for various aspects of cloud computing and determine whether they are applicable and relevant.

![Table 1](image1)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A report that provides:</td>
<td>No assurance</td>
<td>Assurance</td>
<td>No assurance</td>
<td>Assurance</td>
<td>Assurance based on predefined criteria</td>
</tr>
<tr>
<td>A report that will be available for:</td>
<td>Restricted use to a predefined audience</td>
<td>General distribution</td>
<td>Restricted use to those who have agreed to the procedures</td>
<td>Restricted use to current customers and their auditors</td>
<td>General distribution</td>
</tr>
<tr>
<td>A report that will disclose:</td>
<td>Detailed information</td>
<td>Limited information</td>
<td>Specific procedures and factual findings</td>
<td>Detailed information</td>
<td>Specific information that may be in summary or detailed form</td>
</tr>
</tbody>
</table>


![Table 2](image2)