Cloud computing has come a long way from being a mere buzzword to a meaningful tool with a lot of potential for consumers of technology products and services. The adoption of cloud computing has accelerated in the last few years, and it continues to undergo phenomenal growth. Just as in the early days of the Internet, there are many unknown variables in cloud computing. Due to its nebulous nature, it is important to understand the risks associated with utilizing cloud computing. It is not just a new technology; it is a different way of doing business.

**CASE STUDY**

Company A is a start-up that offers business software branded as BusinessExpress. Company A offers BusinessExpress as a Software as a Service (SaaS) solution. The demand for SaaS solutions is expected to grow rapidly. With SaaS, customers enjoy all the benefits of cloud solutions such as not having to host their software in-house (figure 1).

Company A’s core competency is performing software development, not providing hosting solutions. Infrastructure as a Service (IaaS) cloud service providers (CSPs) specialize in providing hosting solutions. Leveraging an IaaS CSP for hosting has allowed Company A to remain focused on its core competency. There are several other benefits of utilizing an IaaS CSP, such as:

- The ability to offer the software solution on a variety of hardware platforms such as Windows, UNIX and Linux
- Rapid scalability
- Pay-as-you-go capabilities
- Resource availability

Due to the numerous benefits of IaaS, Company A leapt into a cloud computing arrangement. The cloud’s economies of scale and flexibility are both a friend and a foe from a security point of view. The chief information officer (CIO) of the company engaged an information systems (IS) auditor to conduct a

---

Figure 1—Example of an IaaS Cloud Hosting BusinessExpress Software That Is Offered As a SaaS Solution

Cloud Express Application User (via PDA)

Customer’s BusinessExpress Application Administrator

BusinessExpress Application User (Desktop)

Company A’s BusinessExpress Release Manager

Company A’s BusinessExpress Testing Manager

Company A’s Network Administrator

Company A’s Database Administrator

---

Do you have something to say about this article? Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.
review and assess the risks of offering a SaaS solution and adopting IaaS cloud computing for this arrangement. The following paragraphs describe the steps followed by the IS auditor to conduct the exercise. This exercise will help the CIO in determining what Company A needs to protect, prioritizing the risks and determining a response.

To conduct a risk-based assessment of the cloud computing environment, there are generic risk frameworks such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management—Integrated Framework. There are also IT domain-specific risk frameworks, practices and process models such as ISO 27001 and IT Infrastructure Library (ITIL). Bottom-up guidance specific to cloud computing also exists from various bodies such as the Cloud Security Alliance (CSA), European Network and Information Security Agency (ENISA), and the US National Institute of Standards and Technology (NIST). The Cloud Controls Matrix released by CSA is designed to provide security principles to guide cloud vendors and assist prospective cloud clients in assessing overall security risks of a CSP. The NIST guidelines on security and privacy in public cloud computing (NIST Special Publication [SP] 800-144), which are currently in draft form, contain the guidelines required to address public cloud security and privacy. The Risk IT: Based on COBIT® framework from ISACA fills the gap between generic risk management frameworks and domain-specific frameworks based on the premise that IT risk is not purely a technical issue.

The IS auditor of Company A chose the Risk IT framework, supplemented with an understanding of the Cloud Controls Matrix, ENISA’s cloud computing risk assessment and the NIST guidelines.

Risk IT provides a list of 36 generic high-level risk scenarios, which can be adapted for each organization. Starting with the set of generic risk scenarios helps ensure that the IS auditor does not overlook risks and attains a more comprehensive view of IT risk. Further, Risk IT offers an extensive mapping between the generic risk scenarios and the COBIT control objectives that are customizable for each situation. Figure 2 illustrates the mapping between the high-level risk scenarios and the corresponding COBIT control objectives created by the IS auditor for the cloud computing arrangement.

Leveraging Risk IT in conjunction with a widely accepted IT governance and controls framework such as COBIT makes the risk identification robust and the risk assessment process

<table>
<thead>
<tr>
<th>Risk IT Reference No.</th>
<th>High-level Risk Scenarios</th>
<th>Plan and Organize (PO)</th>
<th>Acquire and Implement (AI)</th>
<th>Deliver and Support (DS)</th>
<th>Monitor and Evaluate (ME)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Technology selection</td>
<td>P03.2</td>
<td>A1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Selection/performance of third-party suppliers</td>
<td>P05.5</td>
<td>A15.2</td>
<td>DS2.4</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Logical attacks</td>
<td></td>
<td>A12.4</td>
<td>DS5.3, DS5.10</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Information media</td>
<td></td>
<td></td>
<td>DS5.11</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Data (base) integrity</td>
<td></td>
<td></td>
<td>DS11.6</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Logical trespassing</td>
<td></td>
<td></td>
<td>DS5.4, DS5.5</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Contractual compliance</td>
<td></td>
<td></td>
<td></td>
<td>ME3.4</td>
</tr>
</tbody>
</table>

the user organization needs to add compensating controls. The organization must understand the state of controls at the CSP and whether
need to be reviewed. A review of the report would help the user
In future years, an independent auditor’s report (e.g., ISAE 3402/SOC
impact on Company A’s ability to meet its obligations to its customers.
Degradation in the QoS may have a significant
Monitoring of the quality of service (QoS) provided by the CSP needs
Findings
The cloud provider contract does not include certain critical elements
to help protect security and privacy requirements. The contract does not include a nondisclosure agreement or a right-to-audit clause.
There is no process for the monitoring of potential vendor failure.
An independent auditor’s report (e.g., ISAE 3402/SOC 1/SSAE16/
SAS 70 report, WebTrust report, SysTrust report) was not reviewed. A review of the report would allow the user organization to understand the controls at the service provider and the nature and extent of controls required to implement.

Relevant COBIT Control Objective
A15.2 Supplier contract management—Set up a procedure for
establishing, modifying and terminating contracts for all suppliers. The
procedure should cover, at a minimum, legal, financial, organizational,
documentary, performance, security, intellectual property, and
termination responsibilities and liabilities (including penalty clauses). All
contracts and contract changes should be reviewed by legal advisors.
Audit Procedure
Confirm, through interviews with key staff members, that the policies and standards are in place for establishing contracts with suppliers. Contracts should also include legal, financial, organizational, documentary, performance, security, auditability, intellectual property, responsibility and liability aspects.

Findings
The cloud provider contract does not include certain critical elements
to help protect security and privacy requirements. The contract does not include a nondisclosure agreement or a right-to-audit clause.
There is no process for the monitoring of potential vendor failure.
An independent auditor’s report (e.g., ISAE 3402/SOC 1/SSAE16/
SAS 70 report, WebTrust report, SysTrust report) was not reviewed. A review of the report would allow the user organization to understand the controls at the service provider and the nature and extent of controls required to implement.

Relevant COBIT Control Objective
ME3.4 Positive assurance of compliance—Obtain and report assurance
of compliance and adherence to all internal policies derived from internal
directives or external legal, regulatory or contractual requirements,
confirming that any corrective actions to address any compliance gaps
have been taken by the responsible process owner in a timely manner.
Audit Procedure
Inquire whether procedures are in place to regularly assess levels of compliance with legal and regulatory requirements by independent
parties.
Review policies and procedures to ensure that contracts with third-party service providers require regular confirmation of compliance
(e.g., receipt of assertions) with applicable laws, regulations and
contractual commitments.
Findings
Monitoring of the quality of service (QoS) provided by the CSP needs to be strengthened. Degradation in the QoS may have a significant
impact on Company A’s ability to meet its obligations to its customers.
In future years, an independent auditor’s report (e.g., ISAE 3402/SOC
1/SSAE 16/SAS 70 report, WebTrust report, SysTrust report) would
need to be reviewed. A review of the report would help the user
organization understand the state of controls at the CSP and whether
the user organization needs to add compensating controls.

Relevant COBIT Control Objective
DSS.3 Identity management—Ensure that all users (internal, external
and temporary) and their activity on IT systems (business application,
IT environment, system operations, development and maintenance)
are uniquely identifiable. Enable user identities via authentication
mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job
requirements are attached to user identities. Ensure that user access
rights are requested by user management, approved by system
owners and implemented by the security-responsible person. Maintain
user identities and access rights in a central repository. Deploy cost-
effective technical and procedural measures, and keep them current
to establish user identification, implement authentication and enforce
access rights.
Audit Procedure
Determine whether access provisioning and authentication control
mechanisms are utilized for controlling logical access across all
users, system processes and IT resources for in-house and remotely managed users, processes and systems.
Findings
Generic user identifications (IDs) are used to access the virtual servers
in the cloud. Multi-factor authentication is not utilized for the cloud
management console.

Relevant COBIT Control Objective
DS5.10 Network security—Use security techniques and related
management procedures (e.g., firewalls, security appliances, network
segmentation, intrusion detection) to authorize access and control
information flows from and to networks.
Audit Procedure
Inquire whether and confirm that a network security policy (e.g.,
provided services, allowed traffic, types of connections permitted) has
been established and is maintained.
Inquire whether and confirm that procedures and guidelines for
administering all critical networking components (e.g., core routers,
DMZ, virtual private network [VPN] switches) are established and
updated regularly by the key administration personnel and that
changes to the documentation are tracked in the document history.
Findings
Application teams currently manage the configuration of the cloud
firewall instead of relying on the network engineering team.
represents a summary of the specific risks and gaps after conducting the audit.

The auditor created a heat map of risks (figure 12) that shows the impact/magnitude and likelihood/frequency of key risks relevant to Company A. The combination of higher (negative) impact/magnitude and higher likelihood/frequency of the incident leads to a higher level of business risk. The darker shade indicates unacceptable risk. This level of risk is far beyond Company A’s normal risk appetite. (There may be other risks unique to the ultimate end users/customers of Company A, but that is out of scope for this case study.)

Due to competing resources, the prioritization of risks related to cloud computing needs to occur, and appropriate action should be taken based on the risk appetite of the company. Appropriate action includes a combination of the following:

• Implement controls.
• Transfer risk(s).
• Avoid risk(s).
• Accept risk(s).

The audit highlighted that Company A needs to mitigate several risks. However, implementing too many controls may
not be the best risk-mitigation approach because the benefit from implementing controls should outweigh the cost. Other risk-mitigation measures such as transferring, avoiding or accepting the risk are worth considering as well.

Once the company aligns IT risk with the organization’s overall business risk and remediates unacceptable security controls, the company is better prepared to harness the power of cloud computing.

CONCLUSION
Businesses are realizing the power of cloud computing, and its use is increasing. This case study represents a one-

<table>
<thead>
<tr>
<th>Risk IT Reference No.</th>
<th>High-level Risk Scenarios</th>
<th>Specific Risks and Gaps</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Technology selection</td>
<td>The cloud provider contract does not include certain critical elements to help protect security and privacy requirements and lacks a technology infrastructure plan and a cost/benefit analysis (CBA). An independent auditor’s report was not reviewed.</td>
</tr>
<tr>
<td>16</td>
<td>Selection/performance of third-party suppliers</td>
<td>Monitoring of the QoS, including availability, needs to be improved. Service level agreements (SLAs) are vague.</td>
</tr>
<tr>
<td>27</td>
<td>Logical attacks</td>
<td>The business owner of the IaaS arrangement has not been defined yet. IaaS firewalls are managed by the application team instead of the network administrators. Multifactor authentication is not utilized to administer the cloud.</td>
</tr>
<tr>
<td>28</td>
<td>Information media</td>
<td>SSL is not used to exchange sensitive information with the CSP.</td>
</tr>
<tr>
<td>31</td>
<td>Data(base) integrity</td>
<td>PIi is stored in clear text at the cloud provider.</td>
</tr>
<tr>
<td>32</td>
<td>Logical trespassing</td>
<td>Company A’s network diagrams have not been updated to reflect the IaaS arrangement.</td>
</tr>
<tr>
<td>34</td>
<td>Contractual compliance</td>
<td>The CSP does not go through an independent service auditor’s examination.</td>
</tr>
</tbody>
</table>

**Figure 11—Summary of Risks and Gaps**

**Figure 12—Heat Map**
time attempt at risk assessment of the cloud computing arrangement. The risk assessment helped uncover some of the key risks, prioritize those risks and formulate a plan of action. Given the evolving nature of risks in cloud computing, no longer can one-time risk assessments suffice. As newer risks emerge, risk assessments need to evolve and the mitigation approach needs to innovate. A risk assessment needs to occur before an enterprise enters into a cloud computing arrangement—to help avoid surprises and minimize the costs of implementing and maintaining controls.

REFERENCES


ITGI, IT Assurance Guide: Using COBIT, USA, 2007


ENDNOTES


5 IT Governance Institute (ITGI), COBIT® 4.1, USA, 2007