Cloud Computing Risk Assessment
A Case Study

Sailesh Gadia, CISA, ACA, CPA, CIPP, is a director/senior manager at KPMG's advisory practice in Minneapolis, Minnesota, USA. He has an extensive background in designing, implementing and assessing IT controls in various industries and third-party service organizations. Gadia is also an editorial advisor for the monthly *Journal of Accountancy* from the American Institute of Certified Public Accountants (AICPA). His previous *ISACA Journal* article on cloud computing was published in vol. 6, 2009. Gadia can be reached at *sgadia@kpmg.com*.

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.[1]

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

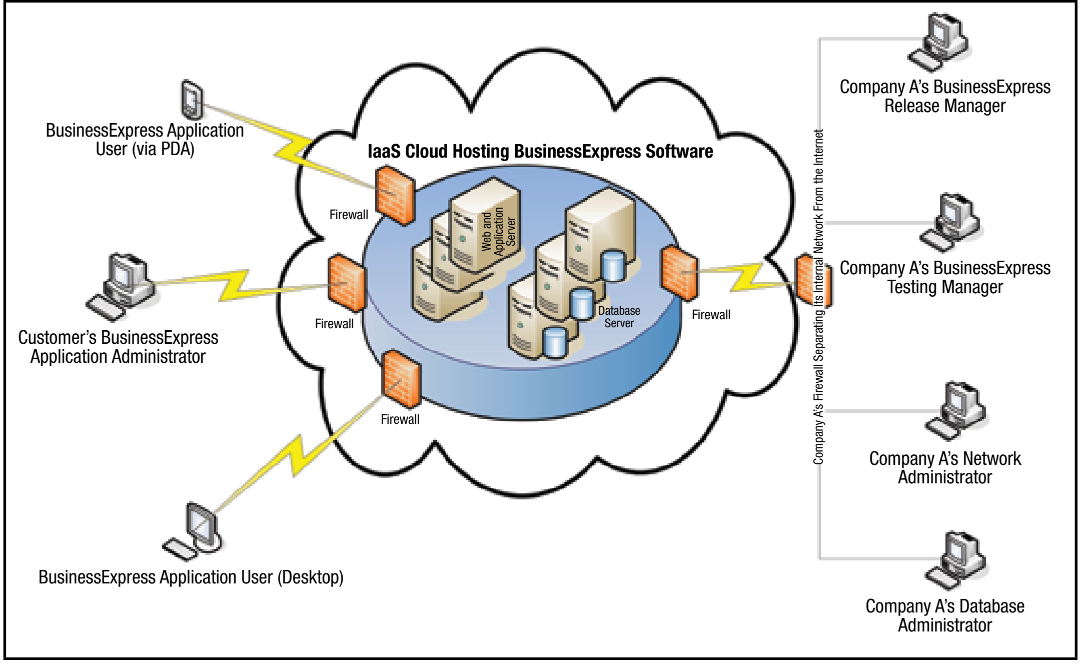
Company A is a start-up that offers business software branded as BusinessExpress. Company A offers BusinessExpress as a Software as a Service (SaaS) solution. The demand for SaaS solutions is expected to grow rapidly. With SaaS, customers enjoy all the benefits of cloud solutions such as not having to host their software in-house[2] (**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:[3]

- 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.[4] 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


BusinessExpress Application User (via PDA)
IaaS Cloud Hosting BusinessExpress Software
Firewall
Web and Application Server
Firewall
Database Server
Firewall
Firewall
Customer's BusinessExpress Application Administrator
BusinessExpress Application User (Desktop)
Company A's Firewall Separating Its Internal Network From the Internet
Company A's BusinessExpress Release Manager
Company A's BusinessExpress Testing Manager
Company A's Network Administrator
Company A's Database Administrator

FORUM

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

Figure 2—Mapping Between High-level Risk Scenarios and Corresponding COBIT Control Objectives

		COBIT Processes and Corresponding Control Objectives			
Risk IT Reference No.	High-level Risk Scenarios	Plan and Organize (PO)	Acquire and Implement (AI)	Deliver and Support (DS)	Monitor and Evaluate (ME)
3	Technology selection	P03.2	AI1.2		
16	Selection/performance of third-party suppliers	P05.5	AI5.2	DS2.4	
27	Logical attacks		AI2.4	DS5.3, DS5.10	
28	Information media			DS5.11	
31	Data(base) integrity			DS11.6	
32	Logical trespassing			DS5.4, DS5.5	
34	Contractual compliance				ME3.4

Source: ISACA, *The Risk IT Practitioner Guide*, USA, 2009, *www.isaca.org/riskit.pdf*, figure 40 effective and efficient. This leads to a model that is extensible and reusable and that can scale up to IT risks affecting the entire company.

Once the risks and COBIT control objectives were defined, they were used by the IS auditor to develop a risk-based audit program. **Figures 3–10**[5] represent a selection of the audit program for the higher-risk areas in **figure 2**. **Figure 11**

Figure 3—Audit Program: Technology Selection (AI5.2)

Relevant COBIT Control Objective
AI5.2 *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.

Figure 4—Audit Program: Selection/Performance of Third-party Suppliers (ME3.4)

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.

Figure 5—Audit Program: Logical Attacks (DS5.3)

Relevant COBIT Control Objective
DS5.3 *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. Multifactor authentication is not utilized for the cloud management console.

Figure 6—Audit Program: Logical Attacks (DS5.10)

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.

Figure 7—Audit Program: Information Media (DS5.11)

Relevant COBIT Control Objective DS5.11 *Exchange of sensitive data*—Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and nonrepudiation of origin.
Audit Procedure Inquire whether and confirm that data transmissions outside the organization require an encrypted format prior to transmission. Inquire whether and confirm that sensitive data processing is controlled through application controls that validate the transaction prior to transmission.
Findings Exchange of sensitive data and administration of cloud instances are done via a regular Internet connection instead of a secure channel such as Secure Sockets Layer (SSL) or Secure Shell (SSH). The organization utilizes an outdated version of Internet Explorer browser software to access and administer the cloud. According to the US Sarbanes-Oxley Act, there need to be proper controls over the initiation, authorization and recording of transactions relevant for financial reporting.

Figure 8—Audit Program: Data(base) Integrity (DS11.6)

Relevant COBIT Control Objective DS11.6 *Security requirements for data management*—Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organization's security policy and regulatory requirements.
Audit Procedure Determine whether a policy has been defined and implemented to protect sensitive data and messages from unauthorized access and incorrect transmission and transport, including, but not limited to, encryption, message authentication codes, hash totals, bonded couriers and tamper-resistant packaging for physical transport.
Findings Personally identifiable information (PII) is stored in clear text at the CSP.

Figure 9—Audit Program: Logical Trespassing (DS5.5)

Relevant COBIT Control Objective DS5.5 *Security testing, surveillance and monitoring*—Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.
Audit Procedure Determine whether the IT security management function has been integrated within the organization's project management initiatives to ensure that security is considered in development, design and testing requirements to minimize the risk of new or existing systems introducing security vulnerabilities.
Findings Network diagrams have not been updated to reflect connectivity with the CSP. As a result, the last network penetration testing did not include this as part of the scope.

Figure 10—Audit Program: Contractual Compliance (ME3.4)

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 The cloud computing vendor does not have an independent auditor's report (e.g., ISAE 3402/SOC 1/SSAE 16 report).

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:

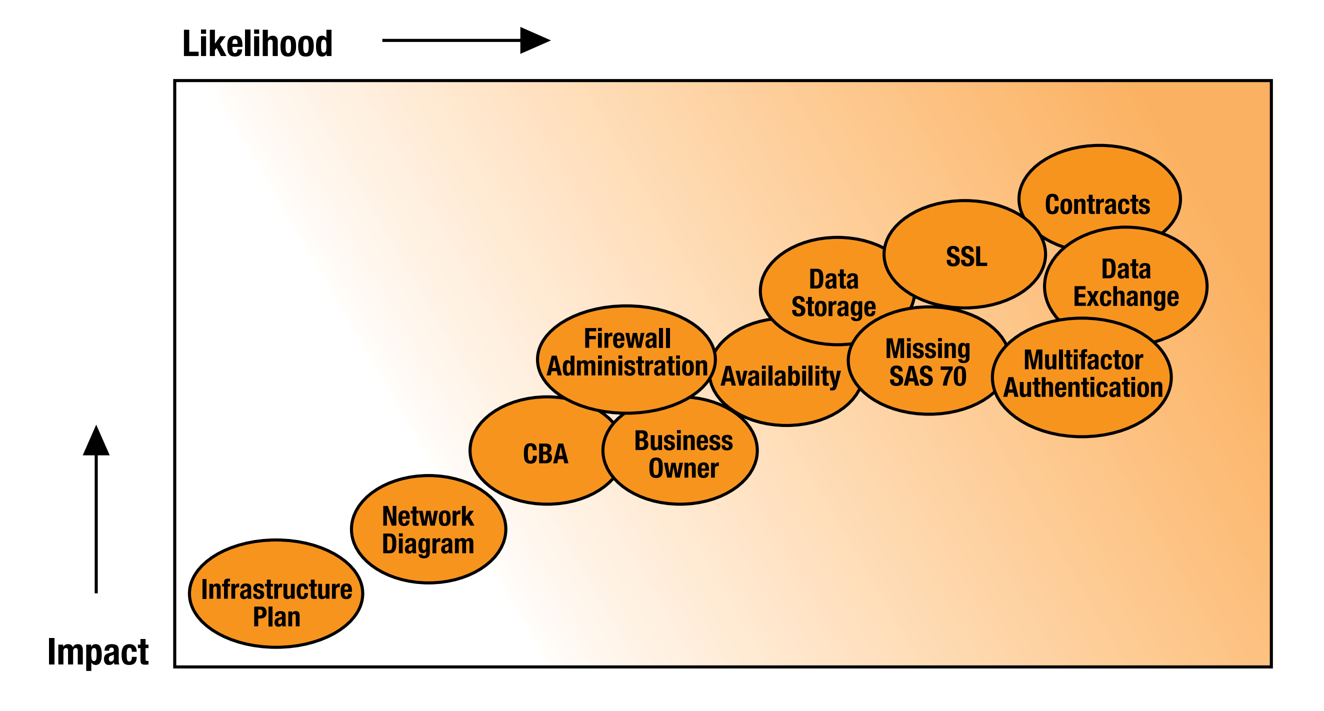
- Implement controls.
- Transfer risk(s).
- Avoid risk(s).
- Accept risk(s).

The audit highlighted that Company A needs to mitigate several risks. However, implementing too many controls may

Figure 11—Summary of Risks and Gaps

Risk IT Reference No.	High-level Risk Scenarios	Specific Risks and Gaps
3	Technology selection	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.
16	Selection/performance of third-party suppliers	Monitoring of the QoS, including availability, needs to be improved. Service level agreements (SLAs) are vague.
27	Logical attacks	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.
28	Information media	SSL is not used to exchange sensitive information with the CSP.
31	Data(base) integrity	PII is stored in clear text at the cloud provider.
32	Logical trespassing	Company A's network diagrams have not been updated to reflect the IaaS arrangement.
34	Contractual compliance	The CSP does not go through an independent service auditor's examination.

Figure 12—Heat Map



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-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

American Institute of Certified Public Accountants (AICPA), Service Organization Control (SOC) reports, *www.aicpa.org/interestareas/accountingandauditing/resources/soc/pages/sorhome.aspx*

Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," December 2009, USA, *https://cloudsecurityalliance.org/csaguide.pdf*

International Organization for Standardization (ISO), ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*, Switzerland, 2005, *www.iso.org/iso/catalogue_detail?csnumber=42103*

International Federation of Accountants (IFAC), International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, *http://web.ifac.org/download/b014-2010-iaasb-handbook-isae-3402.pdf*

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

Office of Government Commerce, IT Infrastructure Library, UK, *www.itil-officialsite.com*

Jansen, Wayne; Timothy Grance; National Institute of Standards and Technology (NIST) Draft Special Publication (SP) 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST, USA, 2011, *http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf*

ENDNOTES

[1] Gartner Inc., "Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010," press release, 22 June 2010, *www.gartner.com/it/page.jsp?id=1389313*

[2] Gadia, Sailesh; "Cloud Computing: An Auditor's Perspective," *ISACA Journal*, vol. 6, 2009, *www.isaca.org/Journal/Past-Issues/2009/Volume-6/Pages/Cloud-Computing-An-Auditor-s-Perspective1.aspx*

[3] Pepitone, Julianne; "Why Attackers Can't Take Down Amazon.com," CNNMoney.com, 9 December 2010, *http://money.cnn.com/2010/12/09/technology/amazon_wikileaks_attack/index.htm*

[4] European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, Greece, 2009, *www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment*

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