HelpSource Q&A

We invite you to send your information systems audit, control and security questions to:
HelpSource Q&A
bgansub@yahoo.com or
publication@isaca.org

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Ganapathi Subramaniam heads the information security function at Flipkart *(www.flipkart.com)*, India's leading e-commerce marketplace. An accomplished professional with 24 years of industry experience, Subramaniam's passion and profession has always been information security. Until recently, he was employed at Microsoft Corporation India as its chief security officer, performing the role of a security evangelist within its sales and marketing support group. He's previously worked at Accenture and big 4 firms such as Ernst & Young and PricewaterhouseCoopers. As a conference speaker and columnist, he has addressed numerous gatherings of chief information officers and chief information security officers risk worldwide.

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.

Go directly to the article:

Q My company has outsourced call center operations. Both inbound and outbound call services are provided by the outsourced vendor. My team is planning to conduct an audit of the security controls with respect to the outsourced call center operations.

What are the key controls that we must consider for assessing the third-party vendor?

A Using a framework such as COBIT® or a standard such as ISO 27001:2013 is a good option. Using one or a combination of these, you may choose the relevant controls. Because business continuity is a key component of any outsourced arrangement, it can be audited using international standards that are available.

Given that the call center staff may have access to a lot of sensitive data or personally identifiable information (PII), one of the big risk factors is potential data spillage.

The following is an indicative list of controls that require assessment (This list assumes that the contract with the vendor provides for an independent audit as a matter of right and not as an optional obligation. If the contract does not provide for an independent audit, recommend an amendment to the contract for inclusion of a right-to-audit clause.):

- The contract must provide for a liability clause in which the vendor agrees to compansate the company for any losses generated due to any data breach.
- Depending in which country/continent the company operates, there may be local legal and regulatory requirements that forbid transfer of data outside of the country. In some countries, such transfer may be permitted if certain conditions are met. Obtain a clear understanding of the local laws/regulations and assess whether the outsourced arrangements meet such tenets. Additional controls may require assessments if such data are to reside in a public cloud.
- Access to data, in particular to sensitive data, must be restricted and must be provided on a need-to-know basis as dictated by the business need. A data classification policy will help determine how to bucket the data into groups so that a granular level of access can be provided. An access control policy must exist to govern data access.
- The outsourced vendor must complete background checks of all new employees and contractors prior to gaining access to live data. This is one of the weakest links and must be made strong. If the agents were to deal with any credit-card-related information, they must not locally store such information for potential abuse later.
- USB ports must be disabled for use with removable storage media. For example, in some of the major business process outsourcers [BPOs] in India, no one, including visitors, employees and contractors, is permitted to bring any memory sticks onsite. An Internet access policy must be reasonably restrictive. There is no point in governing Internet access internally while allowing unrestricted access at the third-party vendor end.
- Desktops/laptops must follow certain baseline security standards. Such baseline standards must include a number of controls such as local administrator disablement. Granting of local administrator rights to all users will enable anyone to install any software, which, in some cases, may be inappropriate. Thus, such unwarranted rights must be curtailed.
- The network and applications must be regularly tested for vulnerabilities; there must be a patch management regime to ensure that the right patches are applied at the right time to plug the holes. Any third-party, vendor-supplied applications must also be patched appropriately.
- All connectivity must be clearly documented. Such documentation must be current.
- Disaster recovery arrangements and properly tested, well-documented continuity plans are

also a must. The absence of such tested plans implies a lack of adequate recovery arrangements in the event of a disaster. The crisis management group must be comprised of individuals representing both organizations—the outsourcer and the outsourced—with roles and responsibilities clearly defined.

- In the event of any security breach, a well-defined incident management framework must help handle it. A clear communication process must exist with proper escalation mechanisms. A root-cause analysis (RCA) is a must for all incidents in order to prevent recurrence.
- There must be regular, periodic internal assessment of controls. While an auditor cannot place complete reliance on such work, internal assessment will definitely contribute to identification of key issues.

Additionally, please refer to the *ISACA Journal* volume 1, 2015, HelpSource Q&A on privacy audit. Most of the privacy control requirements included there will also apply.