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 is director, information security, at Flipkart, an online marketplace entity. Previously, he worked with Microsoft India and Accenture, as well as PricewaterhouseCoopers, Ernst & Young and a UK-based mortgage institution while living in the UK. Subramaniam is an international conference speaker and columnist.

Q Privacy is one area that has never been audited in my enterprise. Please provide your point of view on how privacy compliance can be assessed?

A Though some standard security controls can ensure protection of sensitive information, including those that can be deemed as private, security and privacy are not synonymous. Privacy requirements vary from country to country, depending on national and regional laws and regulations. However, there are some common principles on privacy based on which such laws/regulations are created. Examples of such principles include, but are not limited to, the following:

> "Security and privacy are not synonymous."

- Notice
- Choice
- Purpose specification
- Collection limitation
- Access and rectification
- Retention
- Disclosure to third parties

Depending on the country/continent, there are multiple data protection models such as:

- Comprehensive laws of the European Union
- Sector-specific laws in the US
- Co-regulatory model, found in Australia and Canada
- Self-regulatory model, found in US, Japan and Singapore

Compliance with regulations is mandatory and nonnegotiable.

This is an indicative list to outline the assessment approach; only a lawyer can provide legal advice.

The privacy policy of your enterprise (assuming one exists) must serve as the basis of your audit. The privacy policy must be reviewed for its comprehensiveness. Operationalizing such principles is essential so that the policy is adopted both in letter and in spirit:

- Adequate notice must be provided to the consumers whose data get collected.
- The notice given must explicitly state how the information collected will be processed.
- Choice must be provided to the consumers. In other words, does the enterprise provide for the consumers to either opt in or opt out?
- The purpose for which data are collected must be disclosed to the consumers at the point of collection. Any change in purpose must also be disclosed.
- The data collected must not be unlimited information. It must be clearly predefined, limited information.
- Personal information (PI) collected must be protected against threats such as unauthorized access, modification impacting the integrity of the data and deletion.
- Consent must be obtained from the data subjects or the consumers from whom the data are collected.
- Consumers whose data are collected must be given the facility to view the information held about them. In addition, they must be given the facility to amend or delete information that is not complete, relevant or accurate.
- An identified individual must be designated to be accountable for ensuring compliance toward the above principles.
- What constitutes a breach must be clearly identified. Processes and controls to handle any breach must be defined and must be in place. In some cases, notification has to be done to external regulators and the data subjects/consumers whose data have been compromised. Disclosure as stipulated by laws and regulations will not constitute a breach.

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:

- Transfer of data outside the EU, for example, for processing purposes can be done subject to certain conditions. If your enterprise were to transfer data from the EU to the US, it must ensure that the conditions laid out by regulations are clearly met.

Figure 1 provides a comparative analysis of the various privacy principles as elucidated in various laws/regulations.

Figure 1— Privacy Principles Comparison

Asia Pacific Economic Cooperation (APEC)	EU Data Protection Act	US Federal Trade Commission Fair Information Practice Principles
• Preventing harm • Notice • Collection limitation • Choice • Usage • Access controls and correction • Accountability	• Purpose specification • Collection limitation • Security controls • Usage • Accountability • Participation by individuals	• Notice • Choice and consent • Access to participate • Security controls to ensure accuracy of data • Enforcement