Doing Business in India Requires Digital Compliance

Anil Vaidya, DBA, CISA, CISM, has been an IT management professional for the past three decades. He is the professor of information management at S. P. Jain Institute of Management & Research in Mumbai, India. He can be reached at *anvvaidya@gmail.com.*

The Information Technology Act in India is an ever-evolving document, progressing on all fronts. Business must be in sync with it.

The proliferation of digital media in every aspect of business has been changing the way businesses run. The spread of networks and easy access to the Internet has brought a common denominator to the world. Companies have gone global with business partners and customers spread around the globe. This has resulted in newer compliance requirements and, consequently, legal implications in the case of shortcomings. Over the last decade, Asian countries have emerged as major contributors to globalized businesses. With one-third of the world's population living in Asia, it also offers an opportunity to tap a bigger customer market.

Much has been said about the growth of India's IT service sector—from 1.2 percent in 1998 to 8 percent of its gross domestic product (GDP) in 2012-13.[1] Outsourcing to Indian companies has been popular for several years. In addition to outsourcing, many firms have set up their own shops in India for back-office services, development, health care and engineering, among others. Furthermore, many enterprises have joint ventures and subsidiaries doing business in India.

It is important to know that India has been progressing on the cyberfront in many ways. E-commerce has been provided legal recognition. The governments—central and state—have offered e-filing facilities for businesses and individuals. Copyrights, patents and trademarks have been officially supported through international cooperation. All of this has become possible because of the legal framework of India's Information Technology Act 2000 and other allied Acts.

This article addresses the vital components of this structure and brings forth the compliance requirements.

THE LEGAL FRAMEWORK AND ITS AIM

The legislation that encompasses cyberspace in India is the Information Technology Act, 2000. It came into force on 17 October 2000 and has since been updated by the Information Technology (Amendment) Act 2008 and further rules, orders and notifications issued from time to time. Together these are referred to as the Information Technology Act 2000 (ITA-2000). Internationally the Act aligns with the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, 1996.

ITA-2000 seeks to:

- Provide legal recognition for electronic records and digital/electronic signatures, thus facilitating e-commerce
- Facilitate e-governance and encourage the use and acceptance of filing of electronic records with government agencies
- Identify cybercrime and provide penalties

ITA-2000 covers e-commerce, e-governance, e-records, digital signatures and electronic signatures. In keeping with this, the following Acts were amended:

- Indian Evidence Act
- Bankers Books Evidence Act
- India Contract Act

With electronic records granted legal recognition, the Indian Government has also amended the Indian Penal Code, thus bringing the offences against electronic records within the purview of ITA-2000. Further, considering the significance of digital assets, those are now covered under the following acts (amended):

- The Copyright Act 1957
- The Patents Act 1970
- The Design Act 2000
- The Trade and Merchandise Marks Act 1958

SCOPE OF ITA-2000—ITS JURISDICTION

ITA-2000 is applicable to the whole of India, i.e., all states and union territories. All acts committed using computer resources in India are covered by this Act. The term "computer resource" includes, for example, all computers,

cell phones, mobile devices, databases and networks. Any action committed by a person located outside the geographical boundaries of India also falls under the jurisdiction of this Act if the action involves a computer resource located in India, per section 75 of the Act. However, one may argue that extension of jurisdiction beyond Indian geographical boundaries poses additional challenges.

THE LEGAL FRAMEWORK—SALIENT FEATURES

In India, three sections of society are involved in the enactment of cyberlaws: the legislators, the judiciary and the government. The primary cyberlaw in India is the legal framework provided by ITA-2000 and allied amended laws. The legislations award necessary powers to the judiciary to rule on various matters as required. The Indian legal system also follows precedents established by prior decisions—the principle of *stare decisis*. The decisions of higher courts are binding on the lower courts. Rulings of peer courts and lower courts also carry persuasive value though they are not binding. This implies that any precedent may be cited while arguing the case.

Following the legislature and the judiciary, the central and the state governments are required to ensure that the laws are enforced as required. Four major steps are required for a statute to come into force in India. First, the government has to prepare a draft bill and present it to Parliament. The bill is discussed and, if accepted, is passed in both houses of Parliament. The passed bill is sent to the president of India for approval. On receiving the assent, the government provides notification in the official gazette of India. The Act comes into force on the date of notification. As an example, a cyberoffense committed prior to 17 October 2000 (the date on which ITA-2000 was notified) cannot be tried in the court of law under ITA-2000.

E-COMMERCE

ITA-2000 provides protection to electronic transactions by legalizing the digital and electronic signatures. IT introduced digital signatures and the necessary provisions for certifying authorities. While digital signatures were the first step toward promoting e-commerce, it was not enough to get the common consumer on the Internet. The electronic signature recognized in the amended Act in 2008 was instrumental in allowing customers to perform electronic transactions on the Internet. The e-payment facility is the central aspect of e-commerce. Entities intending to provide a payment system in India need to obtain authorization from the Reserve Bank of India (the central bank) under the Payment and Settlement Systems Act 2007. The Reserve Bank publishes a list of authorized prepaid payment instruments on its web site. In the same vein, the Reserve Bank has also approved four card payment networks as of April 2013.

INTELLECTUAL PROPERTY

The Copyright Act 1957 has been amended from time to time—the latest being the International Copyright Order 1999 and the Copyright (Amendment) Act 2012, effective 21 June 2012. The Copyright Act 1957, section 40, protects the rights of member countries of the Berne Convention, Universal Copyright Convention, World Trade Organization and Phonograms Convention. In effect, a program developed in any of the treaty countries becomes copyrighted material in India. Computer software registered as a "literary work" under section 2 enjoys protection under the Copyright Act in India. Similar to the Copyright Act, the Trade and Merchandise Marks Act, the Patents Act, the Geographical Indications of Goods Act, the Designs Act and the Semiconductor Integrated Circuits Layout-Design Act are in force to protect intellectual property rights.

LEGAL REMEDY

The complainant may seek remedy through civil or criminal courts. The secretary of information technology of the state is the adjudicating officer to hear cases relating to chapter 9 (ITA-2000) contraventions. The secretary carries powers equal to those vested in a civil court. In the event of an unsatisfactory outcome, the complainant or defendant may appeal to the Cyber Appellate Tribunal. Further recourse is available to both parties: to approach the High Court. For more serious offenses under chapter 11 of ITA-2000, the complainant may approach the cybercrime cell of the local police. The cybercrime cell carries out necessary investigations and then the trial is held in the relevant criminal court. The parties may appeal to a higher court in case of an unacceptable outcome.

HIERARCHY OF COURTS IN INDIA

The Supreme Court is the highest court of law in India. The courts have varying powers to grant sentences. The Judicial Second Class Magistrate can sentence up to one-year jail terms for criminal offenses. Going up the hierarchy are the

Metropolitan Magistrate/Judicial First Class Magistrate, Chief Judicial Magistrate/Chief Metropolitan Magistrate, Assistant Sessions Court and Sessions Court/District Court/Additional Sessions. The next two levels are High Court and then Supreme Court. For civil cases falling under chapter 9 (ITA-2000), the adjudicating officer is the first level. The Cyber Appellate Tribunal is the next level, followed by High Court and then Supreme Court. Depending on the size of the claim and the offense committed, one has to approach the appropriate court.

In 2012, Google and Facebook faced criminal trial in Patiala House Court (District Court in Delhi) for allegedly hosting objectionable material on their sites. While the case was still in progress, both respondents petitioned the High Court to terminate the criminal proceedings against them. The Delhi High Court exempted heads of both companies from appearing at the trial; however, it did not stay the trial in the lower court.

COMPLIANCE REQUIREMENTS

It is imperative that companies doing business in India, by themselves or through their partners, meet certain compliance requirements. Closer attention is required if the business involves collecting customer information. Such information may be personal and sensitive in nature, which if disclosed, misused, modified or lost, may carry severe legal repercussions—even for the parent company located outside India. Data protection is clearly described in sections 43, 43A, 66 and 72 of ITA-2000. Furthermore, the government of India may ask for cooperation of a company or individual in accessing information when required. The company and its officials are obliged to provide all possible cooperation if asked. The government and its agencies have powers to block/intercept data or order the company to remove contents from hosted sites. The company must make necessary provisions to meet all such demands.

The employees and the directors of the company are liable for punishment in case of wrongdoing. The complaints, notices and other communication received from customers, employees, partners or the general public offer clues of such wrongdoing; they need to be addressed. Section 85 of ITA-2000 states that in case of failure to protect sensitive information, all persons responsible to the company for conduct of its business shall be held guilty, barring certain exceptions. Section 43A in the amended ITA-2000 spells out the responsibility of corporate bodies handling sensitive personal information in a computer resource. The corporate bodies have an obligation to ensure adoption of reasonable security practices.

A process for prompt investigation and resolution is required. Furthermore, there should be a well-maintained record of such issues and their resolution. It is vital to put in place a robust security policy, safety practices and precautions. The privacy code needs to be published and made known to all concerned. A regular audit and review can help to bring out issues to be addressed and corrective measures to be put in place.

REASONABLE SECURITY PRACTICES

Section 43A of ITA-2000 brings in corporate responsibility of data protection. Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules 2011 specifies the compliance expected of a corporate body.

> *A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.*

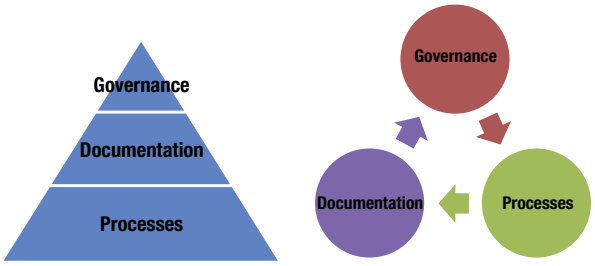
The Rules 2011 also makes a mention of ISO/IEC 27001 as one such standard. In case of breach, the body corporate and all personnel concerned with data protection are considered liable under ITA-2000. For banks, the Reserve Bank of India has published its guidelines for reasonable security practices.[2] The banks are required to adopt practices matching these guidelines and submit regular compliance reports to the Reserve Bank of India.

ITA-2000 does not specifically mention the hardware/software required. Exception has been given for the certifying authorities for whom certain standards have been prescribed. Similarly, the banks may get certain guidelines from the

Reserve Bank of India, specifying certain standards. It is quite clear that no mandate is issued in terms of hardware or software. Electronic transactions are expected to be confidential. ITA-2000 does not specify any reporting on transactions. It only expects that the corporate body maintains adequate security and confidentiality.

All entities that handle personal/sensitive information and/or collect and/or process such information need to comply with the requirements of ITA-2000. Examples of businesses with entities that may engage encompass e-commerce, business process outsourcing (BPO), banking and financial services, and social media. Under section 79, the intermediaries, such as network service providers, are not liable for the third-party information if they provide only access to such information. However, the intermediaries are held liable under ITA-2000 in the case of having received notice of unlawful content and having failed to remove or disable access of such content. Examples of such businesses include network providers, hosting services, marketplace providers and social media. It is imperative that all of these businesses set up appropriate processes to meet the legal requirements. Besides, it is essential to have the governance structure in place to ensure that intended practices are followed in reality. **Figure 1** shows three aspects of compliance: processes, documentation and governance. Adequate documentation provides evidence that underlying processes are followed, while governance provides for monitoring, controlling and updating features of compliance.

Figure 1—Compliance Requirements



Becauses ITA-2000 is a living act, compliance needs to be perpetually attended. Processes need to be updated and followed.

To summarize, digital compliance in an organization can be deployed through:

1. **Processes**—These are used to:
   - Understand the compliance requirements and to gather information from sources such as cyberlaw consultants, legal databases, published reports and newspaper clippings
   - Document and publish expected actions and processes
   - Execute the setup processes
2. **Documentation**—The actions and their outcomes need to be documented (digital documentation is acceptable).
3. **Governance**—It is vital that the organization has a formal structure to monitor the process execution and regular update. As part of such a structure, one would expect to have a cell to coordinate activities and report noncompliance, if any, to the governing body.

EXAMPLES OF VIOLATIONS AND CONTRAVENTIONS

The legal framework and expected compliance discussed in the previous sections can be seen in light of the cases filed in the courts of law. Depending on the severity of crime, the trials are held in different courts. Examples of such court cases presented here underscore the digital compliance requirements.

Penalties

ITA-2000 stipulates varying penalties or punishments, depending on the offense committed. For criminal offenses (chapter 11), such as publishing/transmitting offensive material, cyberterrorism, violating directions of Indian Computer Emergency Response Team (ICERT) or accessing a protected system, the punishment may range from two years imprisonment to life imprisonment in addition to fines. For access-related crimes involving, for example, unauthorized access, copying, damage to computers or fraud (chapter 9), compensation is awarded to the aggrieved party.

Chapter 9 (ITA-2000) contraventions mainly cover crimes related to unauthorized access, pornography, damage and fraud. Chapter 11 offenses deal with, for example, hacking, privacy or cyberterrorism. Even the rights of a nonresident are protected under Indian Law. This can be exemplified by the case of Shri Umashankar Sivasubramaniam vs. ICICI Bank.[3] The case shows responsibility of the corporate body toward expected due diligence for the safety of data and customer

care. The case was heard before the Adjudicating Officer at Chennai for the loss suffered by a nonresident of India, a victim of phishing fraud. The adjudicating officer directed the bank to compensate the victim for the loss suffered.

Role of Intermediaries

The role of intermediaries is examined by the court in the complaint filed by Vinay Raj against 21 companies in Delhi in 2011.[4] The arguments were about the contents on the web sites and whether the intermediaries were responsible for defamatory contents. Facebook and Google were among the defending companies.

In the case of Google India Pvt. Ltd. vs. M/S.Visaka Industries Limited in Andhra, Pradesh High Court issued its ruling on 19 April 2011.[5] Google petitioned that, being a platform provider, it was not responsible for any content hosted on its servers. The court observed that Google failed to remove the defamatory contents when the respondent brought those to the notice of Google. The court dismissed Google's petition saying that Google cannot claim any exemption under section 79 of ITA-2000.

Personal Liability—Employees, Directors, Partners

In the Bazee.com case, the organization's Indian-born, American-citizen chief executive officer was arrested by authorities for objectionable material on the site. Bazee.com was acquired by eBay. The arrest was carried out under section 67 of ITA-2000 for transmission of obscene material. Although he was later released on bail, the case demonstrates the expected responsibility of persons running the company.

Intellectual Property

As an example of legal protection in India, one may cite the cases that Microsoft has won in Indian courts for infringement of copyright.[6, 7] In these cases, the courts granted relief to complainant Microsoft Corp. and ordered injunction restraining further infringement.

Recently Telefonaktiebolaget Lm Ericsson filed a case in the Delhi High Court against Micromax Informatics Ltd. for patent infringement, claiming damages of Rs 100 crore (INR 1 billion or US $18.52 million). Micromax is an Indian manufacturer of mobile handsets and tablets. The court passed an interim order in favor of Ericsson. Micromax was ordered to deposit with the court 1.25 to 2.5 percent of the sale value. In addition, Ericsson officials were authorized to inspect Micromax consignments at customs. If Ericsson gets its way, it may take legal action against more companies.[8]

ROLE OF IT AUDITOR

In the changing environment of businesses in the cyberworld, IT auditors must widen their perspective and get to know the legal provisions of ITA-2000. It is not the aim of this article to consider whether the auditor should play the consultant role or conventional audit role. However, it is clear that auditors must be much more vigilant about the legal aspects of cyberspace in India. They must understand and describe the strengths and weaknesses of the organization with respect to ITA-2000.

Cybercrimes have evolved rapidly, but the legislations also try to curb such acts through newer enactments of rules, guidelines and notifications. In this environment, it is insufficient to provide a traditional checklist for the audit function. The following is suggested:

1. Know the business; get to understand the business involvement in the cyberworld, including:
   - Products/services sold on the Internet
   - Sensitive/personal data collected or processed through computers
   - Remote services provided over the Internet
   - Connections offered as intermediaries
2. Find the relevant processes practiced in the organization.
3. Get to know the current status of ITA-2000 and the guidelines/mandates from any related agency such as the Reserve Bank of India.
4. Check the documentary evidence on processes and governance.
5. Report shortcomings and strengths to the relevant authority in the organization.

Figure 2 provides examples of businesses and related information that an IT auditor must possess.

Figure 2—Examples of Relevant Information

Business Examples	Relevant Notifications/Guidelines
Internet banking	The Reserve Bank of India guidelines issued in 2011 on IT governance, information security, IS audit, IT operations, IT services outsourcing, cyberfraud, business continuity planning and customer awareness programs
Cybercafé	Information Technology (Guidelines for Cybercafé) Rules 2011
Hosting services	Intermediary rules
Distribution/sale of software	The Copyright Act

CONCLUSION

It is of utmost importance that IT auditors keep their eyes and ears open to happenings around the world. The Reserve Bank of India regularly issues guidelines to banks, e.g., for Payment Card Industry Data Security Standard (PCI DSS) compliance to protect cardholder data. These may be important to get a feel of expectations, even if the company does not deal in the financial sector. The government of India and the state governments also issue orders and notifications from time to time. An internal cell may be organized to gather and understand the requirements that may originate from such communiqué. The IT auditor and the company doing business in India need to be abreast of the legal aspects and the adequacy of internal processes.

ENDNOTES

[1] Government of India, *Electronics and Information Technology Annual Report 2012-13*, 2013

[2] Reserve Bank of India, circulars, *www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx*

[3] Shri Umashankar Sivasubramaniam vs. ICICI Bank petition no. 2462, judgment delivered on 12 April 2010

[4] Vinay Raj vs. accused, complaint no. 136 of 2011 in the court of Sudesh Kumar, Metropolitan Magistrate Patiala House Courts, New Delhi, 2011

[5] Google India Pvt. Ltd., vs. M/S.Visaka Industries Limited, on 19 April, 2011, Crl.P.No. 7207 of 2009

[6] Microsoft Corporation vs. Mr. Yogesh Papat and Anr, 22 February 2005

[7] Delhi High Court, Microsoft Corporation vs. Mr. Kiran and Anr, 7 September 2007

[8] Das, S.; J. Philip; "Ericsson Sues Micromax for Patent Infringement, Claims About Rs 100 Cr in Damages," *The Economic Times*, 26 March 2013