Regulations in place

Protecting consumers and companies

Regulations and standards are part and parcel of doing business around the globe. Technology can help India Inc comply with these. We take a look at how CIOs are tackling this issue. by ***Deepali Gupta***

Regulations are meant to guard the interests of consumers and to reassure associates across borders that an industry complies with standard, acceptable norms. This becomes pertinent in light of the trend towards global and local mergers. In the banking industry for example, analysts at IBM predict that all Indian banks will consolidate into three or four large groups. For the sake of smooth mergers it is important for every bank to be aligned in the same direction.

To ensure that an enterprise is complying, with regulations, the company has to find a controlled self-assessment tool

Sunil Chandiramani, Partner, Ernst and Young

The rationale behind regulations

Regulations are also put in place to mitigate threats posed by any one element to related components. In the business world, this process enforces open governance and ensures that risk management measures are in place within organisations. It also prevents any domino effect when a business fails (for instance, if a rural bank fails, people may pull out their money from other rural banks, causing them to fail as well).

As business depends on IT and the data stored, analysed and managed by the IT team, the onus of ensuring regulatory compliance falls upon the IT Head or CIO's shoulders. A lot of today's regulations and standards pertain to data security and integrity. So, let's start with what Indian law sets down as mandatory.

Acting it out

Regulations pertaining to IT and information integrity are still developing in India. As of now MNCs impose a foreign rules or standards upon their Indian partners.

"What a company needs to comply with in India is split over many Acts and Regulations," says Sunil Chandiramani, Partner, Ernst and Young. Depending on a company's sphere of operations, the regulations that it needs to comply with can be found in Acts such as the Excise Act, the Companies Act, the PF Act.. it is a long list. Identifying what is applicable to an organisation and what is not becomes a difficult task. Worse, the Indian IT Act 2000 does not clearly spell out the regulations concerning IT management or security.

The Indian IT Act 2000 broadly dictates that an e-transaction should have a digital signature to be accepted in court. "The Act has no regulations for data protection, and there is no corporate governance act in India," says Vivek Kathpalia, Associate, Nishith Desai Associates.

Listed companies have to abide by the requirements listed by Stock Exchange Board of India (SEBI). For the greater part, SEBI regulations are built on the law, and attempt only to ensure that listed organisations are within the parameters of the law. SEBI's Clause 49 refers to good corporate governance. The disclosure norms issued by SEBI attempt to ensure that the confidentiality of customer data is maintained. However, the implementation of these regulations is not audited by a third-party and the compliance is left to the company. "To ensure the enterprise is complying, the company will have to find a controlled self-assessment tool," says Chandiramani.

A possible solution would be to deploy corporate reporting tools that must be intelligently populated with knowledge. A number of corporate governance tools that are available in the market can be used to generate intelligent reports. The catch, however, is that these tools need clean and sizeable data, a resource that few Indian companies possess.

The Reserve Bank of India imposes certain restrictions upon Indian Banks. While many regulations govern the way a bank is set up there are a number that involve complex reports that have to be submitted to the RBI at regular intervals. For example, a bank's balance sheet must always reflect adequate capital. As far as IT is concerned, the RBI has set up guidelines for network encryption and risk management. At present this is still a recommendation, it may become compulsory in the long run. If the banking system is online, and a set of best practices is in place, a number of Business Intelligence tools are available to help a bank with this kind of reporting, and running audits becomes extremely easy. Unfortunately, the majority of Indian banks are yet to go live with core banking implementations. "That's where most banks are investing time and money," says Ravi Trivedi, Partner Financial Services, Strategy & Technology Consulting, IBM Business Consulting Services, India. In a nutshell, the regulations imposed by Indian authorities only enforce the bare essentials. That is why BPO outfits, MNCs and conglomerates have aligned themselves to foreign standards to gain the confidence of their international partners.

Internationally accepted

The UK Data Protection Act (DPA) and EU-US Safe Harbor (SH) are accepted in many countries. The DPA is applicable in UK and it is also accepted in the US. SH was approved by the EU in 2000 to smooth business between US companies and EU markets, without legal repercussions in either territory. The principles of both the DPA and SH are:

- The individual must be aware of the purpose and use for which personal information is collected.
- There must be documented evidence of customer consent before such information is shared with third-parties.
- Individuals must have access to information pertaining to them so that they can update it.
- Sufficient security precautions must be taken to ensure that the information provided to the organisation is not lost, tampered with or misused.
- Personal data must not be transferred outside the EU that unless a country can ensure an adequate level of protection of the consumer's rights.
- Should there be any problem, a mechanism for addressing complaints must be in place.

Apart from this, there are regulations pertaining to specific industry verticals. Health Insurance Portability and Accountability Act (HIPAA) is a globally accepted norm for protecting patient information. Its aim is to standardise the way patient information is collected, obtain higher continuity of health insurance, prevent frauds and abuse of the system as well as maintain the confidentiality of individually identifiable records. BPO companies hosting medical information such as Wipro Spectramind have to comply with HIPAA.

Pertinent Regulations And Standards

Generally applicable

- The Indian IT Act 2000
- The Data Protection Act
- Safe Harbour
- BS7799, ISO7799 - Security standard
- BS15000, ITSM - Standards for good corporate governance

Specific to verticals

- HIPAA - For healthcare and related insurance
- Sarbanes-Oxley Act, Gramm Leach Bliley Act, SAS 70 - For financial services institutions

Upcoming Standards

- COPC - For call centers and BPOs
- CISP - For holders of creditcard related information

For financial services companies there are the Sarbanes-Oxley Act and the Gramm, Leach, Bliley Financial Modernization Act of 1999. These acts enable commerce without barriers while ensuring protection of privacy and personal rights of individuals who are involved with the system. Encryption and other security measures are needed and record maintenance should be impeccable. The recommendations made by these Acts mostly pertain to practices that need to be implemented.

For security compliance, there are a number of standards such as BS7799 or ISO17799. The 7799s cover information security risk management, information security governance, physical security, IT security and business continuity. To test the robustness of IT service delivery, and to assist with corporate IT governance a standard called BS15000 has been built atop the IT Information Library (ITIL) framework. SAS 70, which still in it's teething stages, is another standard that is aimed primarily at the financial services industry seeking as it does to validate control policies and procedures. It defines Type I and Type II reporting. Type one mandates an external auditor's opinion and a description of existing controls while Type II adds the auditor's testing procedure to the list.

For these regulations there are few third-party auditors and most companies allow their partners abroad to inspect their premises and the measures taken to comply with these. A third-party audit may be a better investment as it can be used for all clients, but auditors are few, and auditing is expensive. So apart from the widely accepted BS7799, companies that certify for any of the other standards are hard to find in India.

You may perhaps have noticed, that India does not have many regulations in sectors other than banking and finance. Therefore, the only companies that have to comply with standards right off the bat are BPO outfits, MNCs and service companies. Our next cover story will look at the challenges faced and methods adopted by BPO companies as they attempt to comply with regulations. As for the banking industry, there are several mandates that IT can help them comply with.

A SOX-GLBA primer

Although the Gramm Leach Bliley Act 1999 (GLBA) and the Sarbanes-Oxley Act (SOX) both aim to protect data regarding customers and companies (for financial institutions), they take different approaches to the problem.

GLBA lists the security and consent requirements at the time any information pertaining to customers or employees of the institution is used, stored, updated or circulated. It is very similar in nature to Safe Harbour.

SOX lists requirements and qualifications of the company board and its audit criteria. Here are some of the key tenets of the Act:

- The company must have a five member board, two of whom must be certified accountants
- The board must have at its disposal at least seven years of audit record
- The auditing firm must be a public listed accounting firm
- Should there be any leakage of information the board may be punished unless it was used for a good cause and was done with prior consent of the concerned parties.
- Directors, officers and ten percent owners must report any transaction they commit in under two working days from the moment of completing the transaction

RBI sets the pace

As Ravi Trivedi, Partner - Financial Services Sector, IBM Business Consulting Services says, "The RBI makes recommendations that have to be treated as regulations." This means that Indian banks need to look at norms such as Basel II to manage Credit, Market, Operational and Settlement risk. Centralised banking applications as well as data warehousing solutions can help with data analysis and issue alerts when a bank's transactions cross the RTGS (Real-Time Gross Settlement) limits, or when it fails to comply with any other pre-set condition.

A number of Indian banks are considering solutions to address anti-money laundering regulations. These solutions are trained to track the movement of money, and they alert the management of any suspicious transactions. The order of activities for functional anti-money laundering solutions is--data cleaning, alerts, investigation (done by means of ranking based upon a series of parameters), discovery (uses an ad-hoc query analysis to discover new testing parameters), and identifying patterns.

For now banks are fulfilling the bare requirements that have been mandated by regulatory authorities. Banks are not investing heavily in intelligent solutions because most of these products require a sizeable amount of clean data. For Indian PSU banks the process of converting their existing data into usable knowledge will take time and effort. This is perhaps why Jitendra Jethanandani, Analyst-Software Infrastructure Asia Pacific, Gartner, says, "The majority of the Indian banking industry is not ready for BI, and probably will not be for another year."

An attempt to centralise data is displayed in the Credit Information Bureau (India) Limited (CIBIL) initiative. India does not have any citizen database equivalent to the American social security system. Bank frauds, particularly when loans and credit card borrowings are concerned, become possible in such an environment. RBI has now mandated the sharing of all banking information with CIBIL. CIBIL, based on this information, has created a system that records the credit history of each individual. Banks subscribing to this facility can use this database to check on the credit status of a customer when they apply for a specific service. The solution met with some conflict with the Privacy Act, but that has been cleared now, and according to Trivedi, the database will prove to be vital for risk management in the future.

The Future of indian regulations

Although the amendment in the Evidence Act is a step forward, the government needs to add data protection clauses to the IT Act

Vivek Kathpalia, Associate,

Anantha Sayana, General Manager of Larsen & Toubro Infotech Limited said that regulations always follow the industry trend. Hopefully, the time lag for Indian regulations to become active will not be too long. The need for Indian regulations is pressing, even as CIOs, and companies align themselves to universally accepted norms. According to Chandiramani weak laws are a major

Nishith Desai Associates

deterrent for FDI, global business and the establishment of research and development parks in the pharmaceutical industry.

Kathpalia believes that although the amendment in the Evidence Act is a step forward, the government needs to add data protection clauses to the IT Act. In fact Kathpalia predicts that eventually Media, IT and communications will have to be controlled by a single regulator. Till then the CIO has to increase his or her interaction with other business personnel, to identify the regulations IT can help with, and implement solutions to keep the organisation clean.

Deepali Gupta can be reached at deepali@networkmagazineindia.com