Sec 43A compliance Framework from Naavi

After the notification of the rules under ITA 2008 on April 11, 2011, there has been a sudden realization in the IT industry about the existence of a law called Information Technology Act 2000, with amendments of 2008 (ITA 2008) and the need to comply with it. Though the Act has been in place since 17th October 2000 and the amendments of 2008 have been in place since 27th October 2009, it was only after the April 11, 2011 notification that it has been taken seriously by the industry. The magic has been in the words "Privacy Protection" which Section 43A rules is meant to clarify.

Naavi continues to advocate an ITA 2008 compliance regime for all companies, IT and Non IT, and has already developed an Information security framework IISF-309 to address the requirements of Behavioural Science based Techno Legal Information Security Compliance under ITA 2008.

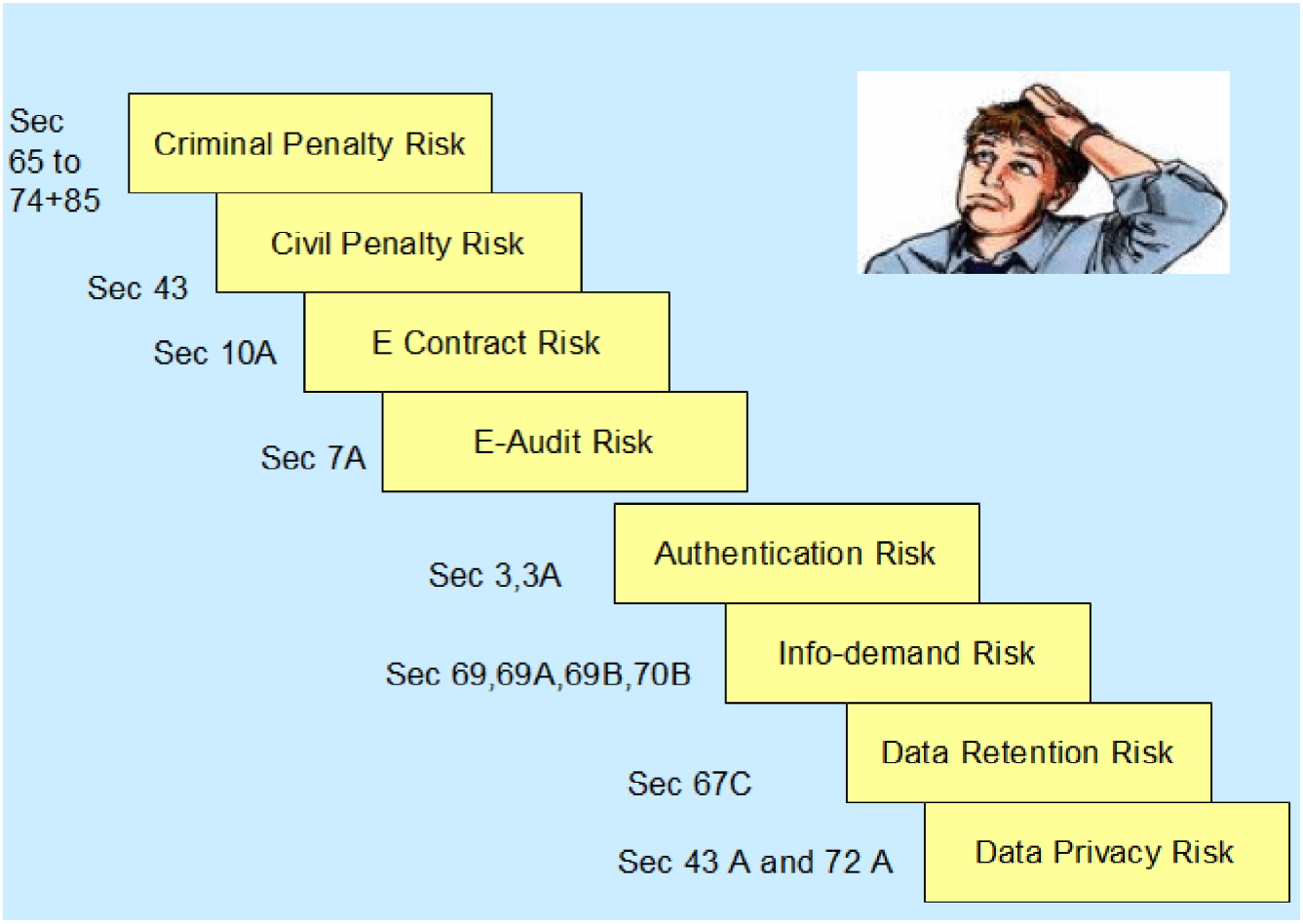
IS Reference Framework..IISF 309.3

Organization	Top Mgt	HR	Admin /Business	IT
Assigned Responsibility	Privacy and Security Practice Statement	Employee Awareness	Client Consent	Information Classification
Monitoring-Testing-Revision Policy	Documentation Policy	Employee Declaration	BA Agreement	Physical Access
	Audit/Self Certification Policy	Employee Cyber Usage Policy		Logical Access
	Web Presence Policy	Employee Media Usage Policy		Information Storage
	Hardware Policy	Employee Background Check		Information Transmission
	Software Policy	Sanction policy		Incident Management
	Grievance Redressal Policy			Contingency-DRP/BCP/other

24 Point IS Framework for Compliance of ITA 2008 developed by Cyber Law College

In order to address the specific requirements of Banks, Naavi has provided a simplified model as indicated below.

ITA 2008 Compliance Steps for Banks



Now in order to address the specific requirement of Section 43A compliance, Naavi provides another specific framework which is briefly explained below.

The most important aspect of Section 43A compliance is the appointment of a "Grievance Officer" to handle the complaints that may be received from the data subjects. Naavi advocates that the person so designated may be called the "Sec 43A Compliance officer" and be expected to take the responsibility for the compliance of all aspects of Privacy Protection as envisaged in the Act. It must be remembered that ITA 2008 mandates that for several aspects of compliance officials need to be designated. Hence if the Company is working on an overall ITA 2008 compliance regime under IISF-309, under "Assigned Responsibility", one official will be designated as an ITA 2008 compliance official. Such a person would also be a compliance official under Section 43A.

The second most important aspect of Sec 43A compliance is to ascertain the applicability of the section to the organization and identification of the information that is subject to protection under the section. This requires information classification to determine what is "Personal Information" and "Sensitive Personal Information" within the information domain of the Company. It is also necessary to identify what is the role of the organization in handling these information. Does the company handle it as an "Intermediary" under the Act ? or as a "Owner" ? or as a "Business Associate"?. The applicability of the section has to be determined based on the role. It is possible that an organization can be an "Intermediary", "Owner" and a "Business Associate" all at the same time for different sets of information that it may come to generate, store or transmit. Sec 43A applies when a data provider and the Company has a direct relationship through a lawful contract. It must be also recognized that the rules of April 11 are subordinate to the Sec 43A in the parent act and hence provisions of the Act override the rule to the extent there could be alternatives available for compliance. The rule may therefore be redundant in many cases.

If a Company is liable under Sec 43A, then it is necessary to develop a set of three policy

documents namely, "Privacy Policy", "Disclosure Policy" and "Sensitive Personal Information Security Policy" taking into account the detailed requirements under the Section including their dissemination to the employees, data providers, associates and other stake holders as may be relevant.

Based on the prescriptions under the rule, the Company needs to set up technical and non technical controls to comply with the Privacy, Disclosure and Security policies adopted by the Company. It is necessary to appreciate that controls of "Techno Legal Nature" cannot always be accomplished completely only by technical measures. There needs to be human intervention from time to time and documentation of such interventions. The compliance official will be the key person to provide such human intervention and depending on the specific needs may have to take the assistance of other functional executives of the company.

As a final step, the Company needs to get an audit conducted to ensure that its documentation of compliance is completed. The notification under the Section makes a clear statement under rule 8(4) that

> *"The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government.*
>
> *The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource."*

It is necessary to draw the attention of the Companies however to the rule 8(1) which states:

> *"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 comprehensively 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.*
>
> *In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies. "*

Following this general comprehensive definition of what is "Reasonable Security Practice" under rule 8(1), sub rule 8(2) states that

> *"The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements"*

is one such standard referred to in sub-rule (1)."

A combination of rule 8(2) and 8(4) gives an impression that ISO 27001 is a necessary and sufficient compliance of Section 43A of ITA 2008.

Rule 8(3) however provides that there is scope for alternate security frameworks to be adopted by industry associations or an entity formed by such associations whose members wants to develop a self regulatory policy.The rule states

> *"Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation"*

It is to be noted that such frameworks have to be however approved as a code of best practice and notified by the Central Government just as the current rules have been approved through a Gazette Notification.

Since at present there are no approved frameworks of any such association and also that the procedure for approval requires the MCIT to give its nod, it is evident that the rules have been so framed as to make it appear that all Companies need to undertake an annual ISO 27001 audit.

While companies who have already undergone ISO 27001 audit may feel comfortable and may quote rule 8(4) whenever there is a question as to whether the company has complied with Sec 43A or not, it is necessary to point out that "Compliance under Section 43A needs to stand the test of rule 8(1) where it is necessary for the Company to demonstrate when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies".

Companies who intend to rely on existing ISO 27001 audits as a sufficient compliance measure need to take note that it is unlikely that the current audits have covered Sec 43A compliance. Though ISO 27001 mandates that *"The organization must comply with applicable legislation such as copyright, data protection, protection of financial data and other vital records, cryptography restrictions, rules of evidence etc."* most ISO 27001 auditors rely on the list of local applicable laws as declared by the management of the Company and proceed to issue ISO 27001 compliance certificates. Also any audit which has been done prior to April 11, 2011 cannot be considered to have considered the law which came to be known only on April 11, 2011 and hence no audit conducted prior to April 11, 2011 can qualify as sufficient to establish compliance of Sec 43A. Only future audits where the ISO 27001 auditor has specifically taken into consideration the implications of Sec 43A rules and incorporated them in his audit will qualify to be considered as a sufficient audit. Such auditors may use the framework suggested here to certify the Sec 43A compliance.

If any company tries to defend a legal claim for damages under this section using an imperfect ISO 27001 audit, the victim may challenge their defense in the Court of law stating that an "ISO 27001 audit done prior of April 11 2011" or any other "SO 27001 audit which does not specifically demonstrate that the auditor has considered the compliance of Sec 43A" may be considered as invalid.

Naavi has raised serious objection to the department introducing an ambiguity into the April 11 rule to give an impression to unsuspecting public that ISO 27001 is a necessary and sufficient compliance of Sec 43A.

Naavi's objections were on the following three grounds.

a) By mentioning that ISO 27001 is one such framework which satisfies the rules, the Government of India is providing a Certificate" to ISO 27001 through a document which has statutory significance. Since ISO 27001 organization is not an Indian Government entity, promotion of such an organization by law is ultra vires the constitution.

b) By mentioning ISO 27001 as a part of the rule, the Government of India has made the specifications under ISO 27001 as part of the Indian legislation. However, specifications under ISO 27001 being a proprietary specification and costs around US $160/- for acquisition, the Government's move suggests that 1.2 billion Indian citizens who have a right to know the law of the land have to spend US $160/- each or remain ignorant of the finer provisions of law. This is a tax on the community and DIT has no authority for the same.

c) If all stakeholders under Sec 43A need to undergo ISO 27001 audit annually, there are not sufficient number of auditors available in the globe and hence most companies will remain non compliant. The cost of even 10 lakh stake holders going in for ISO 27001 audit each year will involve investments of the order of money involved in 2G scam and hence Parliament needs to review this departmental decision.

The DIT has admitted in an RTI reply that the department did not collect any information on the status of ISO audits in India before the rule was framed nor assessed the cost of compliance by the industry.

Further the Director of DIT Mr Prafulla Kumar in his letter dated 11th July 2011 has clarified as follows:

4. Rule 8 do not mandate implementation of ISO 27001 standa exclusively. Body corporate are free to adopt and implement other codes of be practices agreed by the Industry Associations or an entity formed by Indus Association. Thus the presumption that body corporate will have to necessar procure ISO27001 document is not in order. They can adopt other codes of be practices suiting to their nature of business.

Naavi has however continued his efforts to ensure that the DIT modifies the rule under Sec 43A by deleting sub rules 8(2), 8(3) and 8(4). Action is awaited from DIT.

Naavi's Sec 43A compliance framework therefore does not consider that ISO 27001 audit per-se is sufficient and recommends companies to super impose their ISO 27001 audits with a specific ITA 2008 audit conducted under the framework such as IISF-309 which includes and recognizes technical compliancy measures undertaken and approved under the ISO 27001 audit.

It is open to industry associations to take all the relevant facts into consideration and ideally come up with a framework suitable for the specific industry and seek Government approval for the same.

Indian BPO industry which processes information of foreign nationals as a business associate of a data collector abroad needs can therefore develop a separate framework suitable for them. Similarly, companies which are foreign owned and have back office data processing centers in India primarily directed to processing of data of non Indian citizens may also consider a modified framework suitable for them. Banking industry needs to follow the GGWG guidelines and a framework based on GGWG is therefore more appropriate to the Banking industry and they may consider getting the same endorsed by DIT.

Naavi shall be pleased to clarify on the above views and also work along with any interested industry body to develop a customized Security framework for compliance of Sec 43A in particular and ITA 2008 in general.

Naavi

August 3, 2011

Comments may be sent to naavi@vsnl.com

You can share this article by downloading the PDF Version