Total Information Assurance Framework for Health Care Industry

(TIAF4HC)
By
Naavi

Founder www.naav.org : Managing Director: Ujvala Consultants Pvt Ltd (www.ujvala.com)

Health Care industry world over is concerned with the need to protect the Privacy of patient information. While there is a focus on the Privacy and Information Security requirements of Health Care industry in USA in the form of HIPAA-HITECH acts, in India the health care industry is yet to develop the required focus.

Indian Health Care industry is in the initial stages of adopting IT into its operations and very few of the hospitals have gone beyond the first stages of implementation of IT. At the current stage the managements are more interested in the functional aspects of IT and are not providing the right priority to Information Security.

It is however necessary to remind the Indian Health Care industry that India has a law that is similar to HIPAA in the form of Information Technology Act 2000 as amended in 2008 (ITA 2008). Under the provisions of this act and the rules notified under Section 43A on April 11, 2011, information relating to “Physical, Physiological and Mental Health condition” (Health Information) is considered as “Sensitive Personal Information” and requires to be protected by a “Reasonable Security Practice”. Failure in meeting this obligation will place a civil liability for payment of compensation under Section 43A of the Act. It may also result in criminal liability under Section 72A in certain cases.

In view of this provision of ITA 2008, it is essential for Indian Health Care industry to implement an information assurance program that may be considered as “Reasonable Security Practice”.

Naavi who has developed a general information security framework IISF-309 for ITA 2008 compliance and LIPS1008 framework for legal information protection in India has now developed a separate framework tailored for the Indian Health Care industry. This adopts the best practices of HIPAA and ISO 27001 already reflected in IISF309 and LIPS 1008 but is customized for the requirements of the Health Care industry. It takes into account the present status of the industry where the information security adoption is at a preliminary stage as compared to industries such as the banking industry. Though this framework is presented for the Health Care industry, it is also suitable for other industries where the use of IT is yet to mature.

The framework is tentatively recognized as ‘Total Information Assurance Framework for Indian Health Care industry” (TIAF4HC). It is recommended for consideration by the industry for adoption as the industry standard.

The inaugural version of the framework would be referred to as TIAF4HC (v1/1112).

The detailed specifications will be developed by Ujvala Consultants Pvt Ltd and explained through these columns in a series of articles.

The Background

Information Security is normally recognized with three parameters namely

a) Confidentiality

b) Integrity

c) Availability

This is the CIA approach which is used in the basic ISO 27001 approach.

The “Techno Legal Information Security” principle that Naavi has been suggesting extends the above three pronged approach to two other parameters such as Authentication and Non Repudiation that is recognized as an “Information Assurance” approach. With legal compliance comes an assurance of mitigation of the “Liability Risk”. Mitigation of “Liability Risk” arises both from the ability to defend against being held liable for a breach as well as the ability to recover compensation for the breach from another. Hence in this approach the end objective extends from DRP-BCP to DLS-OLS. (DLS=Defensive legal shield and OLS=Offensive legal sword).

The COBIT approach is often associated with the term “Information Assurance” rather than Information Security.

Considering the practical difficulties in implementation of Information Security, Naavi has been advocating a “Three Dimensional” model which extends the “Techno legal” approach further to include “Behavioral Science”. In this approach the importance of the “People factor” is recognized not merely by the need for awareness training but from the point of view of making them behave in a secure manner.

Naavi has tried to codify these thoughts in the “Theory of Information Security” and the Indian Information Security Framework.

The “Theory of Information Security” is built around a “Pentagon Model” where implementation of Information Security in an organization is considered as bound by five aspects namely

a) Awareness

b) Acceptance

c) Availability

d) Mandate

e) Inspiration.

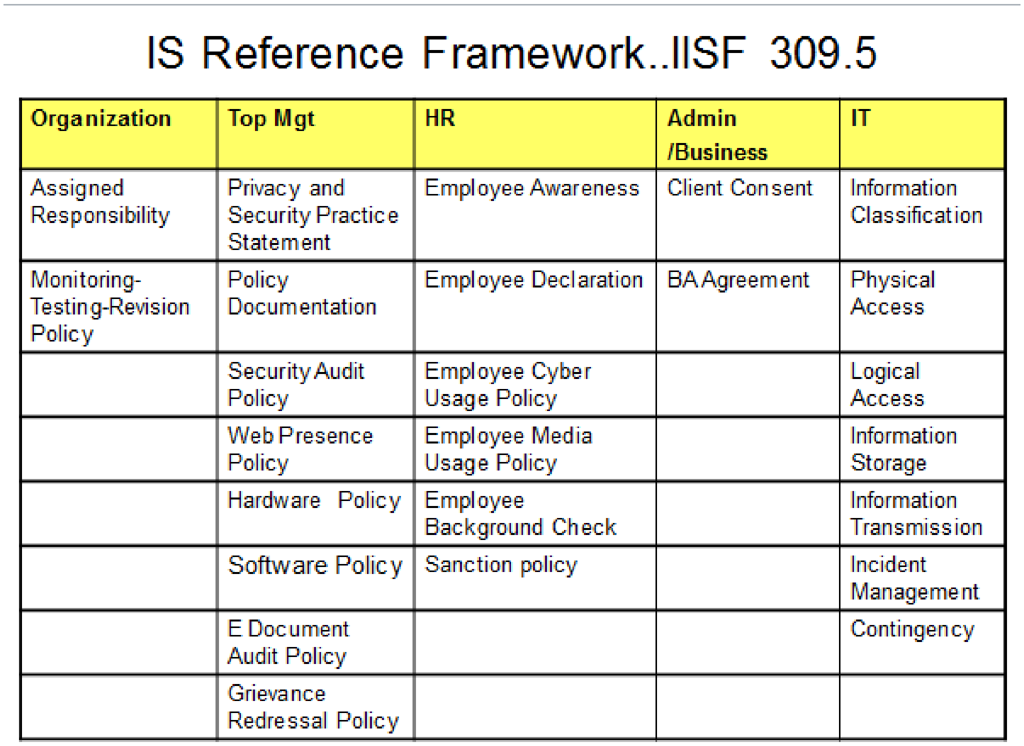
The theory postulates that for achieving a satisfactory implementation of Information Security in an organization, the users should first be “Aware” of the threats, vulnerabilities and security aspects. However mere “awareness” does not lead to implementation and the users need to “accept” the need for security. This requires a change to be brought in the minds of the users. In view of the “human” factor involved in this conversion the term “Control” used in other frameworks are used as “Strategies” in this approach.

“Availability” refers to all aspects of security that are within the control of the organization such as placement of appropriate software tools necessary for the information security.

“Mandate” recognizes both the existence of external legal compulsions but also the strategic value of internal sanctions that support the legal impositions and security objectives.

While “Availability” and “Awareness” are controlled by the organization, “Mandate” is imposed by the law and can be supported additionally as a strategic internal policy, “Acceptance” and “Inspiration” is predominantly controlled by the users themselves. The Organization can only facilitate “Acceptance” or ”Inspiration” by appropriate strategies but the user has the greater say in the end result.

Based on the above thoughts, Naavi presented the IISF 309 framework to provide the necessary guidance to the organization for implementation of Information Security.



IS Reference Framework..IISF 309.5

Organization	Top Mgt	HR	Admin /Business	IT
Assigned Responsibility	Privacy and Security Practice Statement	Employee Awareness	Client Consent	Information Classification
Monitoring-Testing-Revision Policy	Policy Documentation	Employee Declaration	BA Agreement	Physical Access
	Security Audit 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
	E Document Audit Policy			Contingency
	Grievance Redressal Policy			

The IISF 309 was an attempt to zero in on the responsibilities of different parts of an organization towards achieving the Information Assurance objectives. In the version 5 of the framework, 25 different steps have been identified. This includes top management decisions, policy formulations as well as requirements to be fulfilled by the different departments such as the HR,IT or General administration. Detailed specifications have also been drawn on each of the 25 steps to be implemented for three different levels of implementation.

While working on the IISF framework which was based on the TISM, for the purpose of "measurability" , certain suggestions have also been made similar to CMMI model of identifying the level of maturity capability reached in an organization at a point of time and how it can be monitored over a period of time.

It may be said that these suggestions are subject to a need for further refinement through research both at the academic and industry level.

In the light of this background, Naavi looked at the requirements of the Health Care industry in India and the outcome has been the industry specific suggested framework "TIAF4HC".

TIAF4HC is an "Information Assurance Framework" specifically designed to meet the requirements of Indian Health Care industry such as the Hospitals. Companies engaged in medical transcription or insurance billing or providing other services to the US clients are already having the mandatory framework of HIPAA-HITECH.

While HIPAA-HITECH framework is a good framework for adoption by any Health Care or other companies, it was felt that there was a need to provide a compliance path with gradual implementation of security measures rather than providing one large framework such as HIPAA-HITECH and determine whether a company is "Compliant" or "Non Compliant".

Though we say that "Security is as strong as the weakest link" and there are no "half measures", in practice, no organization can jump to the highest level of information security in one step. Auditors are therefore confronted frequently with the question of whether the suggested framework is commensurate with the nature and size of activity of the organization. In the absence of proper guidance to break the compliance into smaller achievable steps, auditors were forced to compromise on their reports stating that certain controls were considered "Not Necessary". This involved a subjective assessment often under unavoidable pressure from the management. While some auditors stood their ground and dubbed a client "Non Compliant" for reasons they considered reasonable and fair, the management felt that the auditor was needlessly rigid in his approach.

While a rigid approach of the auditor is acceptable in the case of a "Mandatory Audit" conducted by a regulatory agency, when a progressive management initiates an audit as an improvement measure of its own volition, the rigidity of the auditor could be considered misplaced and dysfunctional.

Naavi has been an advocate of “Self Regulation” and hence even where ITA 2008 compliance audit has not been mandatory, he has strongly favoured such an audit as good corporate governance.

However many managements feel that they are not “Big Enough” for ISO 27001 or COBIT or ITA 2008 audit and hence end up not doing anything at all towards security.

Similarly Indian health care industry at present may not be ready for a full HIPAA implementation and hence they are not considering any structured approach to information assurance.

Instead of just lamenting on the non compliance, Naavi therefore felt the need to put in place a suggestion which can be implemented by most organizations who would like to achieve acceptable levels of Information Assurance in smaller steps. The feeling of having achieved “Level 1” or “Level 2” would act as a motivation for the organizations to start an information assurance program which they would otherwise not begin at all.

This approach which is generally referred to as TIAF4MI (Total Information Assurance Framework for modular implementation) is referred to as TIAF4HC as a health care industry specific framework.

Though the approach originated in the light of the felt need of the Health Care industry in India, it is Naavi’s considered opinion that the approach may also be found suitable for other organizations trying honestly to achieve greater levels of information assurance competence but are not ready to take a single large leap to “satisfactory zone of safety”.

TIAF4MI/TIAF4HC tries to achieve this objective of “Satisfactory information assurance through small doses” rather than attempting an over dose which may be rejected by the system altogether.

Breaking the “Satisfactory Information Assurance” into achievable sub goals and the manner in which this classification is made in the framework is considered the USP of this framework.

The end result of achieving say all levels of assurance under IAF4MI may be same as or should be better than a faithful implementation of assurance under COBIT or under HIPAA or under ISO 27001.

But IAF4MI is designed to assist a voluntary compliance program better than the other formats.

Let’s look deeper into the concept of Information Assurance through modular implementation in the next part of the article.

Modular Approach to Information Assurance

Information Assurance (IA) is an augmented concept of Information Security and extends the three core principles of IS namely Confidentiality, Integrity and Availability (CIA), to Authentication and Non Repudiation, and incorporates Legal compliance as the second dimension.

For each of these aspects of information assurance, the management need to ensure “Availability of the tools” and impose necessary “Mandates”.

The “People Factor/Behavioural Science aspect” which is referred to as the “Third Dimension of Information Security” cuts across all dimensions of Information assurance such as Confidentiality, Integrity, Availability, Authentication and Non Repudiation.

At each of these levels the stake holders need to be made “Aware”, their “Acceptance” need to be obtained and steps to be taken to “Inspire” them into implementing the security requirements.

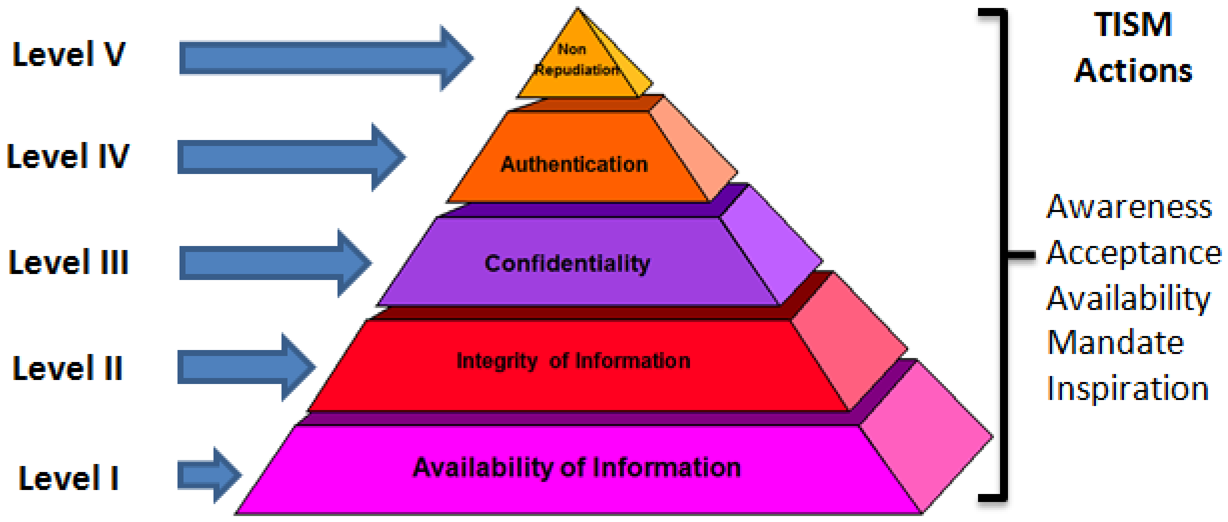
Under the Modular approach to Information Assurance, it is suggested that we re-order the Information Security/Asssurance objectives into different levels as follows.

Level	Assurance Objective	Actions
I	**Availability** of required information to users	Create **Awareness***, Obtain **Acceptance***, Make tools **Available***, **Mandate*** requirements Promote **Inspiration***
II	**Integrity** of information across time and space	
III	**Confidentiality** of information on a need to know basis	
IV	**Authentication** of information to fix ownership for all information events	
V	**Non Repudiation** of action by any user	

(* Refer Theory of Information Security Motivation)

It may be observed that the usual depiction of CIA +Authentication and Non Repudiation has been put under a hierarchy with priority of achievement moving from Level I to Level V.

The above chart can also be presented in the more familiar Pyramid form as follows:



The TIAF4MI model ensures that most organizations which adopt IT for business can achieve Level I. This level is basically functional and most managements address this issue in the first phase since this is directly responsible for the conduct of business. DRP and BCP is part of this level at the simplest form. At level II, the data integrity aspects need to be taken into account At level III confidentiality aspects need to be addressed. Level IV normally has a close relation to Level III and has to be addressed more or less together. Level V addresses the legal aspects of non-repudiation including evidence management.

A further sub division of A, B and C can be made at each level to distinguish between different levels of implementation maturity such as “Implemented”, “Implemented and tested for functionality”, “Implemented, certified as sustainable” etc.

A more detailed specification would be developed for each level and to some extent will have to be customized for different industries and different organizations.

The objective of the “Framework” is to provide a direction to an organization to start implementing information security step by step and reach an acceptable level over a period of time. Each level will be a sort of a milestone to mark their journey. For an auditor, the framework provides a guideline to measure the compliance and provide its certification on whether the organization has reached a given level of compliance.

Further refinement of the framework will be done in due course based on the feedback received and the experience of Naavi and Ujvala Consultants Pvt Ltd. I welcome the views and suggestions from the public in this respect.

Naavi