Total Information Assurance Framework For Modular Implementation

(TIAF4MI)

By

Naavi

Information Security is a concept reasonably well understood in the IT circles. It is defined as "Protecting the "Confidentiality", "Integrity" and "Availability" of Information"

BS7799 practitioners adopted this definition (CIA model) and worked towards checking the measures adopted by an organization to achieve this objective of protecting the confidentiality, integrity and availability of information. This was continued in the practice of ISO 27001 practice.

Over the years ISO 27001 has evolved and a section on "Compliance of Regulatory Aspects" has been added to the traditional ISO 27001 specifications. However there is a lack of proper guidance on defining the scope of an ISO 27001 assessment and hence ISO 27001 does not fully meet the requirements of an assessment of risks arising out of non compliance of ITA 2008 or similar laws addressing Computer misuse/abuse or digital contracts/signature or E Commerce activities.

As a result the IS community evolved a new term "Information Assurance" which extended the scope of IS. Information Assurance (IA) was defined as "Measures for protecting the "Confidentiality, Integrity, Availability, Authenticity and Non Repudiation of information".

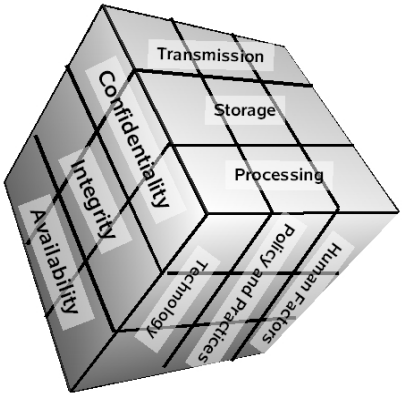
The risk assessment and mitigation policies of IS practitioners correspondingly moved from the CIA model to this CIA++ model.

IA did recognize that IS was a management responsibility and not limited to IT. In this respect it did recognize the need for IS to go beyond "Technical Security aspects" to "Management of Security". Hence IA was an improved concept though in many circles IS and IA are terms used synonymously. The COBIT framework of IA appears to address this issue effectively and distinguish itself from the ISO 27001 framework.

Though this CIA++ model used the term "Non Repudiation" as an essential goal of securing information, it was not however clear if "Non Repudiation" was strictly a "Technical" aspect or a "Legal Aspect".

Hence even the term IA appears to be not fully reflective of what Naavi has been advocating as "Three Dimensional Approach to Information Security" which is inclusive of Technical, Legal and Behavioural Science aspects.

The concept which is nearest to Naavi's approach is the model framework for establishing and evaluating information security/information assurance programs by John Mccumber, introduced in 1991 and often referred to as the "Mccumber Cube" which is depicted below.



The concept of this model is that, in developing information assurance systems, organizations must consider the interconnectedness of all the different factors that impact them.

It propounded that to devise a robust information assurance program, one must consider not only the **security goals** of the program, but also how these goals relate specifically to the various **states** in which information can reside in a system and the full range of available **security safeguards** that must be considered in the design.

The McCumber model is said to help one to remember to consider all important design aspects without becoming too focused on any one in particular (i.e., relying exclusively on technical controls at the expense of requisite policies and end-user training).

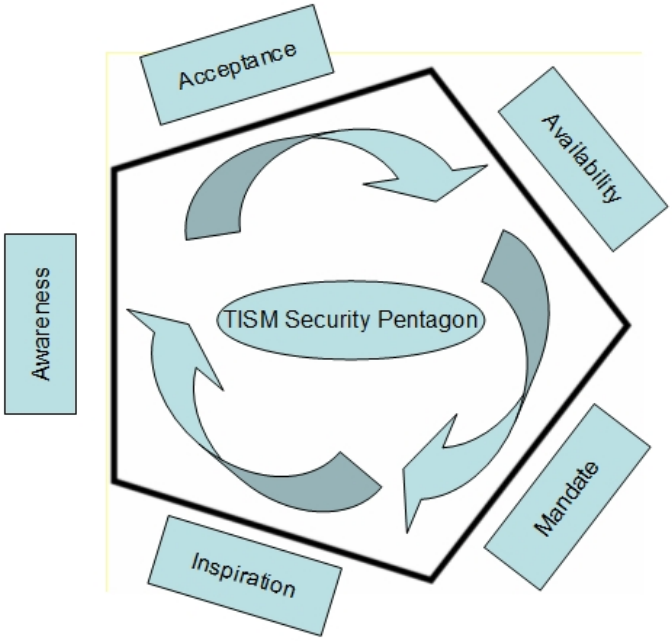
Naavi's approach has been to redefine the end objective of Information Security by stating the goal as

"Protecting the Information Owner" which is inclusive of but beyond "Protecting the Information".

It recognizes that the Information owner by virtue of possessing the information is exposed to certain risks of "liability" and "Security" should mean "Protecting the information owner" from such liability. The liability arises because the information was not secured properly and hence "protecting the information owner from liability" includes "Protecting the information".

Hence Naavi's approach adds an additional layer to IS approach. Since "Liabilities" arise because of laws applicable to information handling, this approach was recognized as "Techno Legal Information Security".

After pursuing this "Techno Legal Approach to Information Security" for several years, Naavi realized the importance of motivating people in an organization to adopt information security as a culture. It was no use to have the best of technical tools and the law of the land. People still had to be motivated. Hence Naavi adopted the "Three Dimensional Model" of Information Security incorporating "Behavioural Science" as the third dimension of information security implementation in an organization.



In order to provide clear guidance to IS practitioners, Naavi postulated that IS Motivation needs to be addressed over five different elements namely "Awareness", Acceptance", "Availability", "Mandate" and "Inspiration". These five elements were placed as walls of a Pentagon that was required to be completed for a good IS implementation program.

The "Theory of IS Motivation" and the "Pentagon Model" gave a new direction to the IS approach.

The model went beyond employee training (Awareness) into obtaining employee commitment (acceptance) and creating an environment where employees would feel

inspired. Similarly the "Mandate" included both external legal mandate as well as internal HR mandate. The internal mandate and inspirational promotion suggested a "Carrot and Stick" approach to ensure that the people used the security tools made available (Availability) to achieve the security objectives. All technical aspects of the CIA++ approach to security were codified as "Tools" which are made "Available" by the organization. (P.S: The term "Availability" is used both in TISM as well as in CIA principle but with different meanings)

The three dimensional approach of Naavi to IS therefore presented a different approach to the existing approaches which included "people" as a factor of IS implementation policy.

In all the above approaches the offer from the IS community to an organization was that *"Here is an IS/IA framework. If you comply, you are compliant. If not, you are non compliant".*

This either 1 or 0 approach meant that before an organization embarked on an IS audit, they should be reasonably sure of their readiness. Otherwise there was a definite risk of an audit which would end in a negative report which the management would find a waste of resources as well as an additional risk of documentation of the "awareness of non compliance". Many managements were therefore hesitant of undertaking an "Audit" or looked for "Pliable auditors".

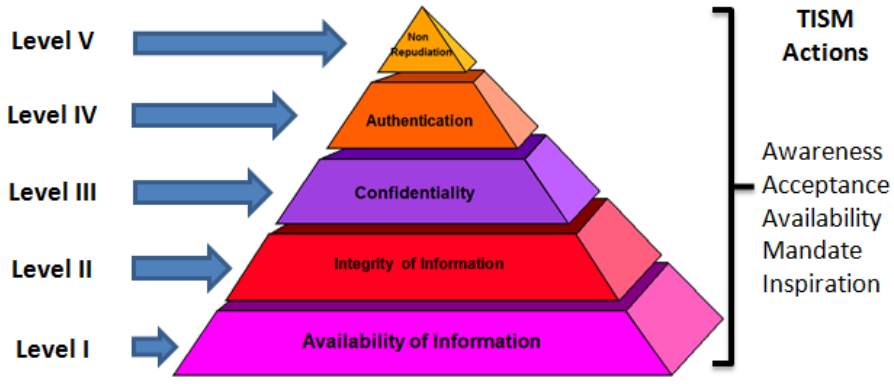
There was therefore a need to find a method by which one could break up the ideal information security implementation into smaller implementation milestones. In other words like in the CMMI approach there had to be "Levels" in IS implementation. However purists in IS found this concept of "Levels" in information security unacceptable since we accept the old adage "Security is as weak as its weakest link".

While there is no two thoughts about the efficacy of this old adage, Naavi still felt the need to find a method of breaking up the security implementation into small dozes for companies which cannot make a one single leap to IS compliance. The thought was inspired by observing the difficulty of applying HIPAA-HITECH framework to an Indian hospital which is in the nascent stage of IT implementation.

HIPAA compliance is not mandatory for Indian hospitals but reasonable information security is a legal compulsion under Section 43A of ITA 2008. However Reasonable Security for a hospital under ITA 2008 cannot be much farther from HIPAA-HITECH framework.

Rather than suggesting the hospitals, that they should adopt the entire HIPAA framework in one single step or remain non-Hipaa compliant Naavi has now tried to find a way to sub divide the IS implementation by creating levels based on the IS objective..

The **Total Information Assurance Framework (TIAF)** developed by Naavi now is depicted as the "Naavi Pyramid" as follows:



Naavi Pyramid

The Naavi Pyramid divides the Total Information Assurance based on the three dimensional pentagon model of IS motivation into five progressively implementable levels based on the well known five principles of Information Security accepted by the current IS and IA practitioners.

The five principles of Information Assurance have been placed in this model as five hierarchial levels starting from "Availability" through "Integrity","Confidentiality", Authentication" and "Non Repudiation". The hierarchy of levels move from the easiest to the more difficult aspects of IS/IA implementation. The five elements of the TISM pentagon run through all the five levels but with different objectives.

To explain the concept further, at level I, the organization is only addressing "Availability of Information at the right time" as the objective. Denial of Access prevention as well as DRP and BCP are parts of this Level. However "Digital Signature" or "Two factor authentication" is not within the objectives of this level.

At Level II, organization will implement measures to maintain "Data Integrity" by introducing version controls, hash tables etc. However "E-Audit" under Section 7A is still not the objective under Level II.

Level III addresses the "Confidentiality" objectives which may include "Privacy Policy" and "Privacy Training".

At Level IV, privacy policy is secured by "Authentication Control". For example, HIPAA privacy belongs to Level III while HIPAA security belongs to Level IV.

At Level V, all the technical, legal and HR measures are benchmarked to the legal requirements and every transaction needs to be capable of standing the test of judicial scrutiny. The evidentiary management requirements as well as managerial responsibilities such as the due diligence responsibilities under Section 85 of ITA 2008 belong to this level.

At each of the five levels the five TISM elements (Awareness, Acceptance, Availability, Mandate and Inspiration) will also undergo changes since the objectives change.

At the end of the Level V, the organization would have achieved a level of security which will also pass the test of a HIPAA-HITECH audit or ITA 2008 audit or ISO 27001 audit or the COBIT Audit.

It may be necessary to consider a further sub division of each level into perhaps A/B/C stages indicating "Adoption", "Implementation" and "Achievement" as the stages of achievement within each level. The fine distinction between these sub divisions may be left to the auditor to judge from the "Commitment" shown by the management, the "Ability" of the work force and "Sustainability" of what has been implemented.

This hierarchial approach to Information Assurance provides the management with some realizable goals and a perceivable return on investment at each level. It makes a "Modular Approach" to Information assurance possible. Hence this approach is titled Total Information Assurance Framework For Modular Implementation (TIAF4MI) This is a huge motivational factor for any management and hence has a better probability of adoption.

For actual implementation, there is still a need for different parameters to be identified as a check list. This is done through a list of IA specifications on the lines of IISF 309 suggested by Naavi. This specification list is still relevant under the Total Information Assurance Framework but the objectives of each specification changes from level to level.

Detailed specification list under TIAF4MI is being developed by Ujvala Consultants Pvt Ltd for its own implementation.

The TIAF4MI is therefore an approach which incorporates the best practices inherent in the current IS and IA practices and increases the acceptability amongst corporate managers. Hopefully the industry will respond positively to this new approach to Information Security and Information Assurance.

Naavi

19th Nov 2012

Download PDF Version of this article

[Comments welcome]