# An Assestment Model for Cyber Security of Vietnamese Organization

Le Quang Minh*, Doan Huu Hau, Nguyen Ngoc Tuan,
Cu Kim Long, Nguyen Minh Phuc

*Information Technology Institute, Vietnam National University, Hanoi,*
*144 Xuan Thuy Street, Cau Giay District, Hanoi, Vietnam*

Received 11 April 2017
Revised 07 June 2017, Accepted 28 June 2017

**Abstract:** This article aims to introduce the cyber security assess model (CSAM), an important component in cyber security architecture framework, especially for the developing country as Vietnam. This architecture framework is built up with the Enterprise Architecture approach and based on the ISO 2700x and NIST SP 800-53 Rev.4. From the holistic perspective based on EGIF developed previously by UNDP group and the main TOGAF features, ITI-GAF is simplified to suit the awareness, capability and improvement readiness of the developing countries. The result of survey and applying in countries as Vietnam, Lao affirms the applicable value of ITI-GAF and the CSAM. The comprehensive, accurate and prompt assessment when applying ITI-CSAM enables the organization to identify the cybersecurity strengths and weaknesses, thereby determine the key parts need invested and its effects to the whole organization's cybersecurity, then build up the action plan for short-term and long-term.

*Keywords:* ITI-GAF, Cyber-security architecture framework, assessment model for cyber-security, NIST SP 800-53 Rev.4.

## 1. Introdution

In recent years, along with the explosive development of Internet infrastructure, smart devices and Internet of Things, information services and social networks, cyber security has become a global real challenge. On one hand, the systems must be flexible and use friendly. On the other hand, it must protect our asset and privacy. In reality, the systems become more and more complex as integrations of many systems deployed by different vendors with different views and interests to cyber security.

There must be some architecture to guideline the deployment of information systems while guaranteeing the security. Such an architecture must confront the increasing number of attacks in a variety of forms, tools, environment, at different levels of complexity and severity. It would be a major part of Enterprise Architecture [1-2]. However, in general it is extremely difficult to achieve consensus in Cyber Security. On the other hand, the situation of security is characteristic, as Information System can be designed in a top down approach, while Cyber Security must be designed to adapt to the existing systems. Cyber Security issues are also sensitive to the policy, strategy, top management views and commitments, interpersonal communication.

* Corresponding author. Tel.: 84-989736464.
Email: quangminh@vnu.edu.vn

https://doi.org/10.25073/2588-1116/vnupam.4102

After all, security solutions mainly serve the interests of the organizations, while do not bring new user functionalities, so it is not easy to gain popularity from the beginning.

Thus, the popular architecture frameworks like TOGAF, FEA, DODAF,… [3-5] would be too complicated and expensive for Cyber Security. While those tools are superior from the methodological points of view, in practice, it is not easy to implement. Therefore, most architecture frameworks do not cover cyber security issues. To fill this gap, Viet et al [6] have proposed to apply ITI-GAF [7-9] to construct the Cyber Security Architecture Framework (CSAF) for developing countries. ITI-GAF has an advantage of being simple and easy to adapt to cyber security.

In this paper, we will address the assessment model of CSAF. In the implementation process of cyber security projects, the assessment model plays an important role. Firstly, it can be used to enforce the cyber security standards, which are important in the information systems deployed by several different vendors. Secondly, the assessment model can point out the weaknesses in a prioritised order, which help the organizations to prepare an investment and implementation plan to address them. Thirdly, the assessment model can be used to evaluate and monitor the performance of cyber security projects in order to maximize it.

In this paper we use the ISO and NIST standards to work out the assessment questions. However, this procedure is extendable to adopt other standards as well. We have constructed the assessment schemas with different depths according to various needs of the organizations. Based on these schemas we have designed a web based application to provide assessment services. Although CSAF is constructed for the developing countries, it can be used for more advanced countries as well.

The paper is organized as follows: In Section II., an overview of ITI-GAF and the methodology of our work will be presented. In Section III., CSAF will be presented with a strong focus on the assessment model. In Section IV., a logical design of a cyber security assessment service based on the CSAF's assessment model will be briefly discussed. Section V. will discuss the conclusions, learned lessons and future perspectives.

## 2. Methodology

### *2.1. Overview of EA and ITI-GAF*

EA has been proposed by Zachmann and IBM [1-2] to ensure the interoperability of an information system and to align the business processes, objectives with technology. In 1998, the CIO council and presidential Budget Bureau have constructed FEA to reduce the failure rate of the US government's IT projects [3]. Soon after that, EA has been built in all advanced countries and became an industrial standards, with contributions from more than 350 leading global IT companies and hundreds thousands of projects [4].

ITI-GAF [6-8] have been developed since 2009 by Nguyen Ai Viet and collaborators at ITI-VNU based on the UNDP's E-GIF [5], TOGAF [4] and other architectures [1-4]. It has been simplified to match the needs and conditions of developing countries. It has been applied successfully in the design model of many important real-life projects such as E-parliament of Vietnam, 3-level E-office model of Hanoi City and Vietnam's pharmaceutical and cosmetic administration systems.

ITI-GAF is based on an enterprise model consisting of 3 views which are tightly correlated: Resources, Institutions, and Operations. Each view includes 3 components. The Resources View includes Business Processes, Human Resources and Infrastructures. The Institutions View includes Regulations, Organization and Mechanisms. The Operations View includes External Transactions, Internal Activities and Capability Buildings. With these 3 views, ITI-GAF ensures a fully reflection of all organization's elements and the relationships between them [Fig.1].

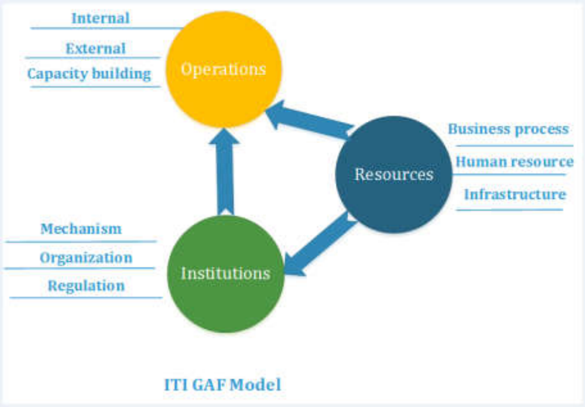

Fig.1. ITI-GAF.

The combination of the 3 views will bring an overall matrix of 27 correlative and interactive blocks, expresses a holistic view of the organization. The most useful feature of this Enterprise model is that the changes in one block always imply changes in other blocks accordingly. This feature guarantees the interoperability. For example the infrastructure must satisfy the business needs and should not be over invested to far beyond the skills of the human resources. Organization functionality and responsibility description must enable the currently applied procedures (mechanism) and must be standardized in regulations. The resources and institutions must be developed to support operations efficiently. All the obstacles and barriers must be removed for the best operational performance.

### *2.2. Cyber security architecture framework*

To assure information security is the biggest concern of all the organizations. In particular, in developing countries [9], new technologies and business investment are being considered and gradually implemented. However, this investment is booming at the moment the cyber risk requires the conjunction with the strengthening of the Cyber Security as a whole development. Some organizations, countries applying the Cyber Security framework as NIST [10] to develop Cyber Security. The approach is very expensive, complex and not directly integrated to the enterprise architecture. Therefore, these methods are not suitable for application in developing countries.

As a characteristic aspect of an information system, cyber security is influenced by Operations, Resources and Institutions as well. Since, the regulations will have a stronger influence, the legal framework for cybersecurity, the habits and the level of people's awareness of cyber security are very different in each country, thus the way these countries face with this issue is very different as well. In that sense, ITI-GAF's generic guidelines turn out to be a very useful and practical tool.

In developed countries, basically, infrastructure was invested properly and synchronized; people are accustomed to high-tech services, have sophisticated consciousness of the cyber risks. Therefore the Cyber Security projects can address directly to its objectives.

In the developing countries, Cyber Security should be developed based on an architecture framework overarching all aspects of an organization. It must be as simple as possible to implement with an appropriate cost, reduce the learning curves and achieve the consensus easily.

## 3. The assessment model

The assessment model based on ITI-GAF should enable organizations to assess the security level of the organizations quickly, accurately and comprehensively. Through evaluations, each organization will identify the strengths, weaknesses of cyber security in their systems, identify key investment needs and its interactive influence to other parts of the organization, then build up an action plan in the short term and long term to develop the organization and enhance its information security. This is one of the most critical steps for building Cyber Security for organizations.

In order to construct the assessment model of CSAF, we use the standards in ISO 27001, ISO 27002 and NIST SP 800-53 Rev.4 [10] and classify the measures and requirements according to the ITI-GAF's blocks. Standard NIST SP 800-53 Rev.4 gives 95 subcategories in 5 security actions: 24 subcategories for Identify, 33 subcategories for Protect, 18 subcategories for Detect, 14 for Respond and 6 subcategories for Recover. ISO 27001 is an international standard for information security management system provides a unified model for establishing, operating, maintaining and improving information security management systems with features such as: risk assessment approach with concentrate on preventative control rather than remedial action, including specifications, application guidelines, requirements, and continuous improvement. ISO 27002 gives guidelines for control practices and implementation of information security for organizations under section 11, 39 control objectives and 133 controls.

The projection ISO 2700x and NIST SP 800-53 Rev.4 in the 3*3*3 model provides a comprehensive model which assesses the organization's information security completely, accurately, fast. Depending on the level of detail required, the model can be applied in 3 forms:

- Basic level: applying the basic model with 3 views: Institutions, Resources, and Operations

- Intermediate level: applying the intermediate model with 9 areas which combine of 3 elements of Institutions (Regulations, Organizations, and Mechanisms) with 3 elements of Resources (Business Processes, Human Resource, and Infrastructure)

- Advance level: applying the advance model with 27 items which combine of 3 elements of Institutions (Regulations, Organizations, and Mechanisms) with 3 elements of Resources (Business Processes, Human Resource, and Infrastructure) and 3 elements of Operations (External transaction, Internal business, and Capability building)

The assessment criteria are also classified into 4 functions:

- Confidentiality: To prevent the information leaks and unauthorized access to the information and devices.

- Integrity: To ensure that the information are not distorted when being stored or transmitted.

- Availability: To guarantee that the information and devices must be ready to access or use as soon as possible, independent of time and location.

- Non-repudiation: To ensure that the people who access the information or devices cannot deny their actions.

The following figure 2 show the high level of cooperation between ITI-GAF, ISO 2700x, NIST SP 800-53 Rev.4 to build up the questionnaire

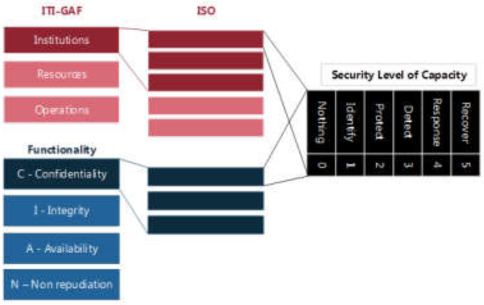

Fig 2. Questionnaire build up diagram.

Our CSAF's assess model has 3 different detailed levels:

- For Leaders: basic model consists 15 questions under 3 views: Institutions, Resources, and Operations

- For Managers: intermediate model consists of 30 questions under 9 areas which combine of 3 elements of Institutions with 3 elements of Resources

- For Implement guys: detail model consists of 60 questions under 29 detail items

Each questions use 6 grades as in Table 1 below

Table 1. grades of assessment

| Grade | Score | Description |
|---|---|---|
| Nothing | 0 | Nothing implemented |
| Identify | 1 | Implemented actions to identify the threats |
| Protect | 2 | Implemented actions to protect against the identified threats |
| Detect | 3 | Implemented actions to detect the threats passing the protection |
| Response | 4 | Implemented respond actions to the detected threats |
| Recover | 5 | Implemented actions to recover the damages |

The result of questions sets gives the basis for a comprehensive review of the organization's cyber security: the strengths, the weaknesses, and correlation between them. Since then the organization can consider critical points need investment and strengthen both in the short term and long term.

## 4. Cyber security evaluation web service design

After a period of applying ITI-GAF, the ITI-EA research team has designed an online cyber security evaluation service to help individuals, organizations get more convenient to use the model to assess, and get preliminary understanding on the cyber security. The service is designed as the following figure:

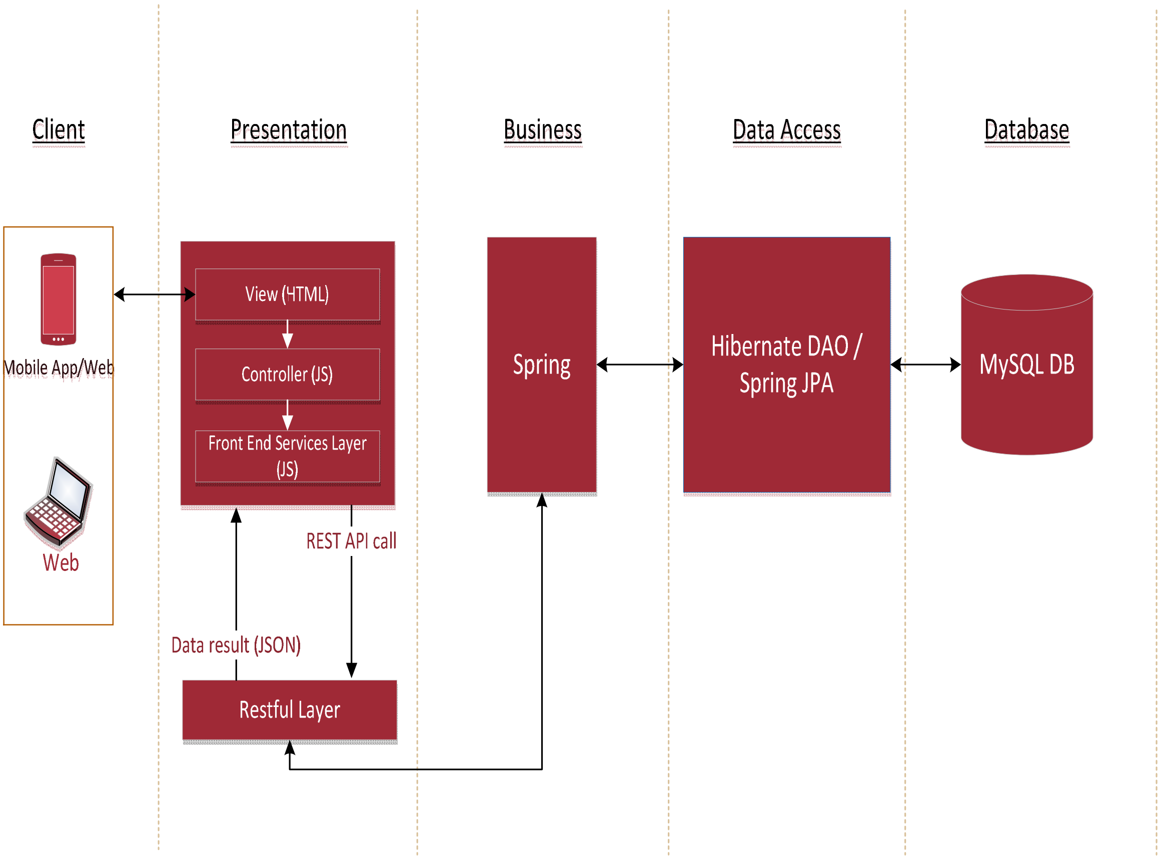

Fig 3. Logical design for online CS service.

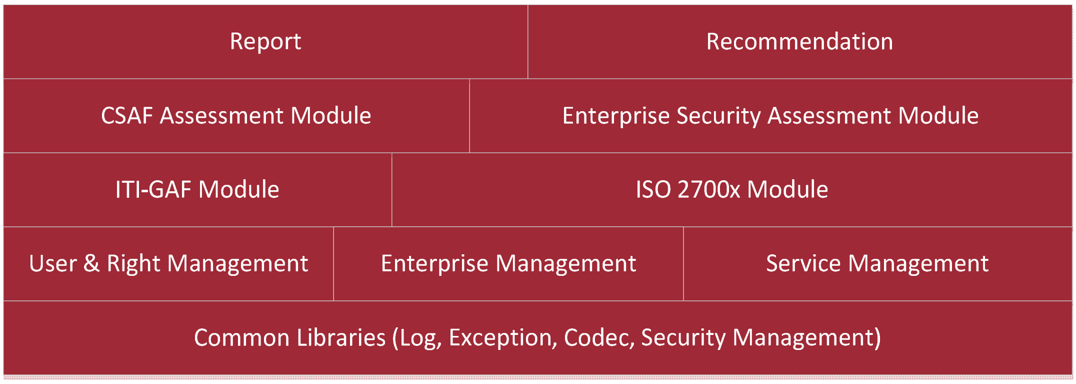

Fig 4. Business diagram for online CS service.

### *4.1. Main functions*

- Give the appropriate question set to the assessment model type (basic, intermediate, or detail) with guideline to answer.

- Give the result of answered question set with some key information as:

• Total score, and general assessment

• Component scores corresponding to selected models (3 views, 9 array, or 27 items) with comments for each component

• Suggestions

• Bend marking the cyber security assessed organization

- Ability to reassessment and check improvement progress

### *4.2. Software modules*

- Common Libraries: Background libraries which needed for a enterprise software such as Log, Exception, Security, Codec Management.

- User & Right Management (Authentication and Authorization): Manage user's information and account, granting the access rights to users.

- Enterprise Management: manage enterprise's information, sector, size of enterprise.

- Service Management: SLA between the Enterprise and the Security Consultant.

- ITI-GAF Module: includes ITI-GAF's information and data

- ISO-2700x Module: includes ISO-27001 and ISO-27002's information and data

- CSAF Assessment Module: contains the configurations and parameters of the Assessment model

- Enterprise Security Assessment Module: assists enterprise users to get corresponding questionnaire, answer them and retrieve the total score after completing the answer sheet. This module allows the user to save and load the current working session.

- Recommendation: give the enterprise users the recommendations on their system's security based on the assessment model.

- Report: necessary reports for enterprise users and administration reports.

**The applying results in practice:** Through practical application at several agencies in Vietnam and Laos, the results showed that:

- In general, developing countries have awareness and certain investments for cyber security. They also are ready for a whole centralized investment (total scores: 79/150, 84/150 and 165/300).

- These organizations have made substantial investments in cyber security for infrastructure, and awareness training and raising for staff .

- However, these organizations do not have regulations, mechanisms and cyber security procedures integrated into business processes

***Preliminary Recommendation:*** Basically, these organizations are willing to invest in new technologies and cyber security. There should be an overall enterprise architecture integrated cyber security for organizations to develop comprehensively.

## 5. Conclusion

Nowadays, the cyber threats are exploded, more complicated and more influence on the performance of organizations, countries. In developing countries, along with the explosion of the cyber-based businesses, the risk is much more serious. On the other hand, the technology platforms in these countries is not strong enough, therefore Cyber Security is a very complex issue. It is necessary to have a method to deploy Cyber Security comprehensively, simple to understand and easy to implement. It is well-known that the technology measures can help to solve at most 10% of the issues.

CSAF is a guidelines for policy measures, while guaranteeing the operability. It can also maximize the benefits of technology.

CSAF based on ITI-GAF is very promising and has been developed to meet those requirements. One hand, it inherits all the good features of the enterprise architecture approach. On the other hand, it has been simplified to match the infrastructure and capacity in the developing countries. The assessment model and the web assessment service designed in this paper can help the organizations, especially in but not limited to developing countries to identify key parts that need improvements. Based on that, it enables those organizations to build up short term and long term action plans and to monitor, reassess and adjust the objectives after each development stage. It is the prerequisites for building a whole comprehensive system.

## Acknowledgements

We would like to express our thankful to the support of “LAN secure“ project 09/2015/CNC-HDKHCN of Information Technology Institute - Vietnam National University, Hanoi.

## References

[1] J. A. Zachman (1987). "A Framework for Information Systems Architecture". In: IBM Systems Journal, vol 26, no 3. IBM Publication G321-5298.

[2] "Business Systems Planning and Business Information Control Study: A comparison”. In:IBM Systems Journal, vol 21, no 3, 1982. p. 31-53.

[3] Chief Information Officer Council (2001) A Practical Guide to Federal Enterprise Architecture. Feb. 2001.

[4] The Open Group Architectural Framework, TOGAF 9.1 Online Documents (2012), URL: http://pubs.opengroup.org/architecture/togaf9-doc/arch/

[5] Nguyen Ai Viet et al, UNDP’s E-GIF (2007)

[6] Nguyen Ai Viet (2016), TOWARD ASEAN-EU COOPERATION IN CYBER SECURITY: An analysis on alignment between EU and ASEAN priorities and objectives – Final Report of CONNECT2SEA project.

[7] Nguyen Ai Viet, Le Quang Minh, Doan Huu Hau, Ngo Doan Lap and Do Thi Thanh Thuy (2014), “E-organisation assessment based on ITI-GAF”, Proceeding of FAIR 2014

[8] Nguyen Ai Viet and EA team of ITI (2013), “Vietnam E-parliament”, Project Report.

[9] Nguyen Ai Viet and EA team of ITI (2012), “Feasibility studies of Vietnam’s National Pharmaceutical and Cosmetic Administration’s Information System”.

[10] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (2014), URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf