

Information Security Risk Management by a Holistic Approach: a Case Study for Vietnamese e-Government

Ha LE Viet¹, On PHUNG Van¹ and Hoa NGUYEN Ngoc²

¹Center of Information Technology, Vietnamese Government Office, Vietnam

²Department of Information Systems, VNU University of Engineering and Technology, Vietnam

Summary

Information security risk management is one of the essential tasks currently in ensuring information security. In particular, for e-Government information systems, the assessment and management of security risks through the exploitation of software vulnerabilities, network equipment, etc., allow us to minimize the loss of data and essential information of organizations in e-Government. In this paper, we introduce a holistic approach to assessing information security risks based on both qualitative and quantitative methods for the Vietnamese e-Government. Our model of security risk management is built according to both international standards (ISO 27005-2018, NIST SP800-30r1, SP800-39, SP800-53r4) and Vietnamese standard (TCVN). For the quantitative risk method, we use both CVSS and OWASP scoring standards to quantify information system risks. Besides, the information security risks of the system can also be determined through vulnerability scanners. We also implemented the proposed model in a Web application, called SoC.UET. The experiments we conducted with UET.SoC allowed proving the ability to manage the information security risks holistically for a Ministry or a Province in the Vietnamese e-Government.

Key words:

Information Security Risks; Security Risk Assessment; Security Risk Control; Security Risk Management.

1. Introduction

e-Government is a place that provides access to government services anywhere and anytime from the Internet. Thus, the risk of being hacked into infrastructure systems and application, infection of viruses, malicious code, revealing state secrets, steal and destroy information and data, gaining control of the system, etc., are significant challenges in ensuring information security for e-Government building today. That requires Vietnam to master technology, propose solutions to ensure information safety and security for e-Government development.

Information security is of great concern to a family of ISO/IEC 27000 standards dedicated to information security management, in which ISO/IEC 27005 focuses on security information risk management [1]. The National Institute of Standards and Technology of the United States (NIST) has also developed many standards to assume the security risk management, including NIST SP800-30r1 described the process and framework of information security risk

assessment, and NIST SP800-39 specified all steps in the framework of information security risk management. By these standards, the security risk management is considered all the coordinated activities to direct and control an organization concerning the security risks. These activities will usually be divided into groups, which must include risk assessment, risk treatment, and risk monitoring [2].

International standards for information security risk management are usually only general guidelines or reference models [3]. They are necessary to customize and establish specific parameters related to a specific organization. Moreover, to manage information security risks, risk assessment processes, methods, and techniques should be tuned to respect the requirements of its information systems. Therefore, in the Vietnamese e-Government, the information security risk assessment and management need to coordinate standards of security risk management and specify a list of possible controls for the information systems of a specific ministry/province.

In this paper, we focus on the proposed model of information security risk management. It is based on the two principal risk management methodologies built by ISO/IEC and NIST. With this proposed model, we have also developed a Web application, called UET.SoC, that allows a ministry/province in e-Government to assess and manage information security risks for its information systems.

The remainder of this paper is organized as follows: Section 2 presents several security risk assessment methodologies. Section 3 describes the quantitative methods for assessing information security risks. In Section 4, we introduce some related work. Section 5 details the mixed approach to assessing information security risks based on both qualitative and quantitative methods. Section 6 presents a summary of our test results to verify and evaluate our approach. The last section comprises some conclusions and future work.

2. Security Risk Assessment Methodologies

Protecting the organization's information security, whether it is commercially sensitive information or customers' personal details, has not been of significant interest to date. International standards such as ISO/IEC 27005:2018 [1],

NIST SP800-39 [4] or AS/NZS 4360 ... will provide guidance and a framework for organizations to effectively manage risks.

Risk management is the identification, evaluation, and handling of risks by the appropriate use of resources to control the probability of occurrence and the effects of risks. The objective of risk management is to ensure that the effects of risks do not divert the organization's business operations. In summary, risk management is a coordinated activity on risk to operate and control the organization. In this section, several common information risk management methodologies will be briefly described.

2.1 ISO 27005-2018

The introduction of ISO/IEC 27001:2005 Information Security Management System (ISMS) marks a development step in the field of information security in the world. Applying ISMS helps organizations architecture an advanced, effective, and appropriate cost management system with overall information security solutions to protect their business operations.

Since 2005, the ISO/IEC 27000 series has been continuously improved to provide international management tools for the process of setting up, operating, monitoring, reviewing, maintaining, upgrading the Information Security Management System.

ISO/IEC 27005:2018 is designed to support the implementation of ISO/IEC 27001 based on a risk management approach. ISO/IEC 27005 provides guidance on risk management that meets the relevant requirements specified in ISO/IEC 27001. In detail, ISO/IEC 27005 provides objectives, tools, and ways in which organizations can effectively manage their information security risks according to ISO/IEC 27001. This standard also helps to demonstrate to customers of an organization or its stakeholders that reliable security risk management procedures are established, giving them confidence that the organization can be trusted to do business and collaborate together.

According to ISO/IEC 27005:2018, the process of managing security risks is, as in Fig.1.

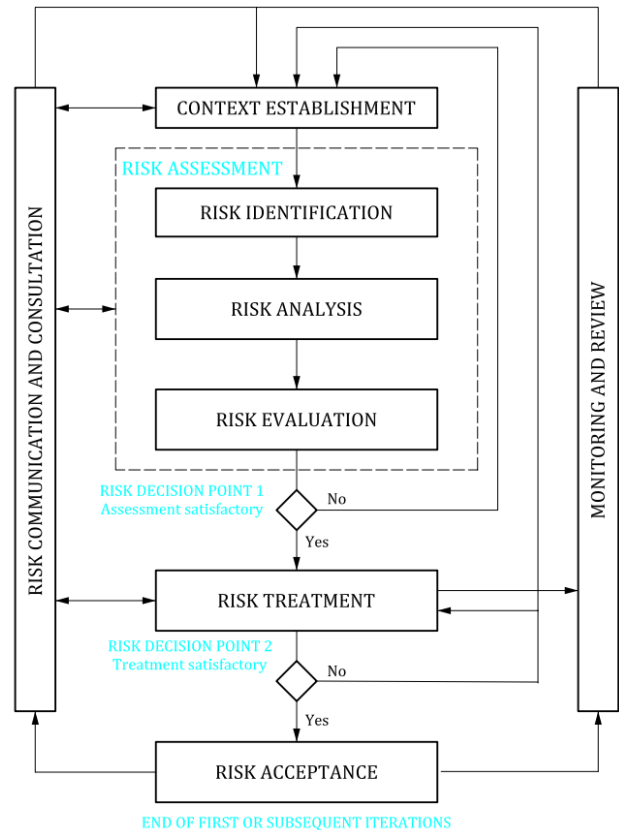


Fig. 1 Process of Information Security Risk Management from ISO/IEC 27005-2018.

The process of information security risk management of ISO/IEC 27005 is a cycle, starting with the "Context Establishment" step. It then follows by the "Risk Assessment" step after the risks are identified, analyzed, and evaluated. They will be addressed at "Risk Decision Point 1" or switch to "Risk Decision Point 2" to accept the risk only if they fully meet the organization's risk acceptance policies and criteria. Once risks are addressed or accepted, they will be monitored, reviewed, communicated, and consulted to finalize a complete cycle.

ISO/IEC 27005:2018 provides procedures for the management, assessment, and handling of information security risks. Furthermore, the annexes also help identify the value of information assets, and assess impacts, identify common threats, weaknesses, and methods to assess weaknesses and some approaches to assessing security risks. However, ISO/IEC 27005 does not provide any specific approaches for managing security risks. The organizations themselves must determine their approach to the management of security risks, for example, depending on the scope of the security management system or based on the context of risk management.

2.2 NIST SP800-39

NIST SP800-39 provides a structured, flexible approach to risk management based on the risk assessment, response, and monitoring provided by NIST security standards and guidelines. The instructions are not intended to replace or include other risk-related activities, programs, processes, or methods that organizations have implemented or intend to implement.

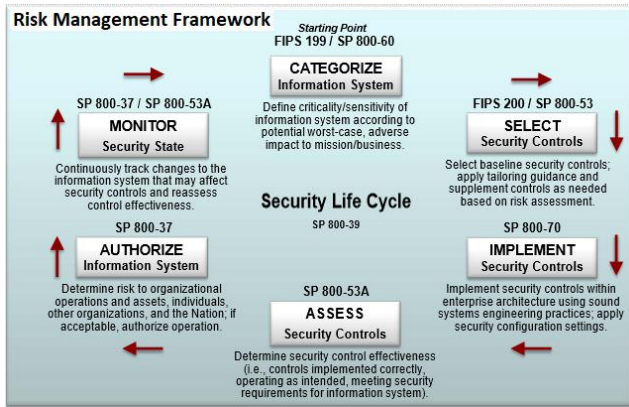


Fig. 2: Risk Management Framework by NIST SP800-39.

According to the NIST SP800-39, Risk Management Framework described in Fig.2, risk management is a comprehensive process that requires organizations to: (i) Develop risk frameworks (set the context for risk-based decisions); (ii) risk assessment; (iii) respond to risks once identified; and (iv) continuous monitoring of risks by using effective communication and a feedback loop to improve the organization's risk-related activities continually.

To integrate risk management processes across the organization, including large scale organizations, NIST proposes a hierarchical approach to manage risks at three levels: (i) organizational level; (ii) mission/business process level; and (iii) information system level. The risk management process is carried out continuously on all three tiers with the common goal of continually improving the effectiveness of coordination between tiers for risk-related activities.

Unlike the standard ISO designed and applicable to managing most types of risks, NIST SP 800 is only most suitable for managing technology-based risks with standard criteria. The risk management approach, according to the multi-tiers, has proved to be many advantages. However, one of NIST's shortcomings is not to consider human resources as one of the organization's assets.

3. Information Security Risk Metrics

For each risk management system, an indispensable component is the risk severity scoring. Currently, for information systems, there are several ways to calculate the risk severity. However, the most common in the world are two methods: (i) Common Vulnerability Scoring System (CVSS), used to calculate risk severity for all information systems in general, and (ii) risk scoring method proposed by the Open Source Foundation for Application Security (called OWASP in this paper), designed specifically for use with web application systems. The following is a summary of these two risks scoring systems for information technology systems.

3.1 CVSS

CVSS [5] is a system that provides a way to classify information security vulnerabilities and methods for scoring vulnerabilities depending on the severity level ranging from lowest 0 to the highest 10. CVSS is divided into three metric groups: Base, Temporal, and Environmental; each of which consists of component metrics with the same group-specific attributes, as shown in Fig.3. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment.

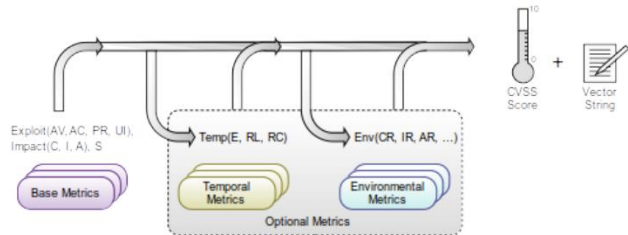


Fig. 3 CVSS Metric Groups.

Base group represents the intrinsic nature of a vulnerability regardless of time or environment. It contains two metric sets: the Exploitability metrics and the Impact metrics. The Exploitability metrics reflect technical attributes, where vulnerabilities can be exploited. Meanwhile, the Impact metrics reflect the direct consequences when a vulnerability is successfully exploited.

Temporal group represents the time-dependent attributes of a vulnerability. For example, when the source code for exploiting a published vulnerability will increase the CVSS score, it will decrease if the vulnerability patch is released.

Environmental group represents the environment-dependent attributes of a vulnerability. These are

vulnerabilities that can only be exploited if they exist in specific technology infrastructure environments.

After the metrics are scored by the analytics tool, they will be used as inputs to the base CVSS scoring formula with a range of values from 0 to 10. However, the Base Score is not entirely fixed; it can be changed depending on the Temporal and Environmental Score to more accurately reflect the level of risk at a given time and for a particular system. Typically, it is not necessary to calculate the Temporal and Environmental Score, but to ensure the exact factor, these values should still be recommended.

3.2 OWASP

The Open Web Application Security Project (OWASP) is a nonprofit organization that works to improve the security of software. OWASP proposed a risk assessment framework, which contains a static application security testing and risk assessment tools. OWASP Risk Rating Methodology is an important component of this framework, which shows how to classify risks and prioritize vulnerabilities. This methodology consists of 6 steps [6]:

1. Risk Identification: the expert should collect and analyze all security vulnerabilities and threats that hackers can use and their impact on the organization if it is successfully exploited.
2. Likelihood estimation: this is determined by four threat agent factors and four vulnerability factors.
3. Impact estimation: divided into two groups of Technical and Business Factor, each group has four factors.
4. Risk severity scoring: The values Likelihood factor and Impact factor are quantified into severity, to determine the severity of risk using the following formula:

$$\text{RiskSeverity} = \text{Likelihood} \times \text{Impact}$$
5. Treatment: Normally, at this stage, high-severity risks will be prioritized, but if the cost is too high, they can be reconsidered depending on the specific circumstances.
6. Risk rating customization: OWASP allows customizing the way of calculating risks to fit specific circumstances in the following three ways: (i) adding factors; (ii) customizing options; and (iii) weighting factors.

4. Related Work

Attempts to address information security pricing and management issues for the Vietnamese e-Government information systems, especially nationally important information systems, we focused on research related to risk assessment and management methods, qualitative and quantitative methods, and their application in specific case studies.

4.1 Security Risk Assessment and Management

According to ABBASS [7] in a study of popular Information System Security Risk Management (ISSRM) methods such as MEHARI, EBIOIS, CRAMM, OCTAVE, ... helps organizations to make accurate decisions about system information security. However, because the results include informal and un-analyzed documents is a disadvantage. To solve this problem, the authors aligned the security modeling language approaches such as SecureUML, Secure Tropos, Mal-Activity Diagrams, Misuse Cases Diagrams with the ISSRM domain model to improve related information. As a result, this study analyzed the advantages and disadvantages of each security modeling language when combined with ISSRM. In another study by Adrián Fernandez [8] also evaluated the flexible and effective use of simple and complex asset modeling approaches for information security risk assessment. One of the properties that determine the model's complexity is the way to characterizes the dependence between assets and is usually represented by dependency graphs. To evaluate the effect of changing dependency graph variables, the author used MAGERIT methodology, a powerful tool for managing graphs of variable complexity and allows qualitative or quantitative asset valuation. Moreover, Yubin Wang [9] developed a methodology and a tool that supported framework for model-based risk assessment that can solute the identifying granularity of risk computation and distinguishing influence level of risk on the asset's importance.

Besides, there is some other research that is specific case studies such as the Brent Sherman group's research on hardware security risk assessment for a large-scale hardware-centric environment. This study has proposed and implemented a particular automation method using quantitative weighted risk ratings of the Security Development Lifecycle (SDL) with acceptable accuracy and labor savings but also dispersed security concerns compared to other approaches using qualitative analysis. Or another case study Hamid Asgari [10] proposed SecRAM risk assessment method to systematically applied the network systems, specifically, to an emerging network architecture called recursive inter-network architecture (RINA), Jason R.C. Nurse [11] introduced a new method to assess the risk of the Internet of Things systems, Jin B. Hong [12] proposed a stateless security risk assessment that combines the security posture of network states at different times to provide an overall security overview, Devin Reeh [13] with the electric vehicle Charging System, ...

Last but not least, there are new approaches but not really getting much attention that is the application of probabilistic [14] or Artificial Intelligence techniques [15] approaches in the problem of information security risk assessment.

4.2. Security Risk Qualitative and Quantitative

Although CVSS is a viral metrics as described above, it still has certain limitations. Firstly, CVSS only guides assessing each individual CVEs and not a complex multi-component system. Second, it does not use information about the source attacks and the attack routes to calculate the risk. To solve this problem, M. Ugur Aksu [16] has proposed a CVSS-Based quantitative model that calculates both the base risk of a system and attack graph-based risks. Besides, this model also allows for calculating the risk of a multi-component IT system.

Another study also based on CVSS is that of Suryadinata [17]. Based on BRO Intrusion Prevention System (IPS) specifications that detect and prevent network attacks, the author will use CVSS and VEA-bility metric to calculate the security level of the system and compare them. VEA-bility only needs a base score from CVSS, while CVSS scores also need environmental metrics. VEA-bility shows how safe the system is from a value between 0 to 10, and CVSS shows how dangerous the vulnerable is.

Going into more detail into a specific case study, Joh [18] conducted a quantitative analysis of security vulnerability two operating systems for well-known network devices, Cisco IOS and Juniper JUNOS using vulnerability discovery model and CVSS. Balume Mburano [19] is directed to Web applications, this study compares some open-source Web Vulnerability Scanners with the OWASP and WAVSEP benchmark, thereby showing some valuable recommendations for the practice of benchmarking web scanners.

In addition to the two general methods of quantifying risks in the information system above, in order to quantify information security risks, there are many vulnerability scanners built and exploited to use today. These scanners can detect security holes in IT systems; scan for vulnerabilities, malware in program source code; manage application patches, ... For instance, Rapid7 with InsightVM vulnerability management tool is capable of real-time analysis, monitoring, and detection of vulnerabilities [20]. Acunetix enables us to scan, detect vulnerabilities, and malicious code in Web applications [21]. Furthermore, Tenable Nessus is now considered as one of the best scanners for detecting vulnerabilities, supporting continuous control mechanisms, establishing, classifying risk levels, advising, and supporting risk mitigation [2].

5. Holistic Approach for the Security Risk Management

Based on both national (TCVN) and international standards (ISO/IEC 27005:2018 [1], NIST SP800-30r1 and NIST SP800-39 [22]), in this paper, we propose a holistic approach for assessing and managing the information

security risks. This approach is proposed within the scope of a national project on information security risk assessment and management in Vietnamese e-Government, code KC.01.19/16-20, funded by the Ministry of Science and Technology of Vietnam. Our proposed model of security risk management is constituted of the experience came from the Information Technology Center, the Government Office, and the Department of Information Security, Ministry of Information and Communications. This model contains both a qualitative method divided by six main steps and a quantitative method by using both CVSS and OWASP risk scoring to determine the security risk severity of an information system in Vietnamese e-Government.

5.1 Information security approach in the Vietnam e-Government

In December 2019, the E-Government Architecture Framework Version 2.0 was published to address shortcomings of the previous version, the most important is the addition of 5 reference models built on the Federal Enterprise Architecture Framework - FEAF: Business reference model (BRM), Application reference model (ARM), Data reference model (DRM), Model Technical infrastructure reference (IRM), Information security reference model (SRM). This framework is illustrated as in Fig.4.

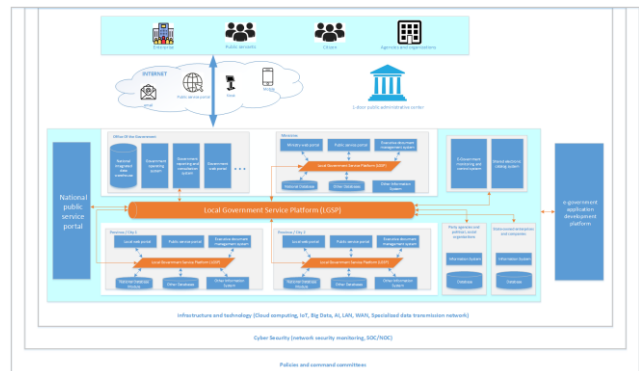


Fig. 4 Vietnamese e-Government Architecture Framework V2.0.

With the approach of ensuring information security by level, e-government systems are classified into five levels from 1 to 5 depending on the type of information system and the importance of information that the system processes. Level 5 is the highest, these are information systems that affect national security, centralized storage of important national data, or national information infrastructure systems. Therefore, the reference model is also built in this approach. The structure of the information security reference model consists of 3 components: Objectives, Risks, and Controls, as shown in Fig.5. These components are then divided into

six sub-components. Each of which has to be addressed at both the organizational and information systems levels.

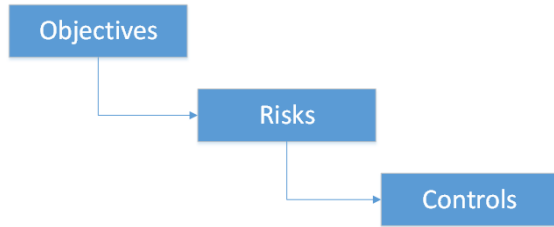


Fig. 5 Three components in information security reference model.

Objectives: requirement that an information system is protected in accordance with the law based on the level of security of that system.

Risks: requirement that an information system should be tested, assessed, identified, and managed risks and control methods to minimize the level of risk.

Controls: regulating the implementation of the protection plan should comply with the provisions of law and evaluate the effectiveness of the protection plan.

5.2 Process of Security Risk Management

With a qualitative assessment approach, we follow the guide provided in the ISO/IEC 27005:2018 standard (fully accepted by the Vietnamese standards organization - TCVN), NIST SP 800-30r1/39, and NIST SP800-53r4 for the security controls. As these standards, our proposed process of information security risk assessment consists of 6 following steps illustrated as the following:

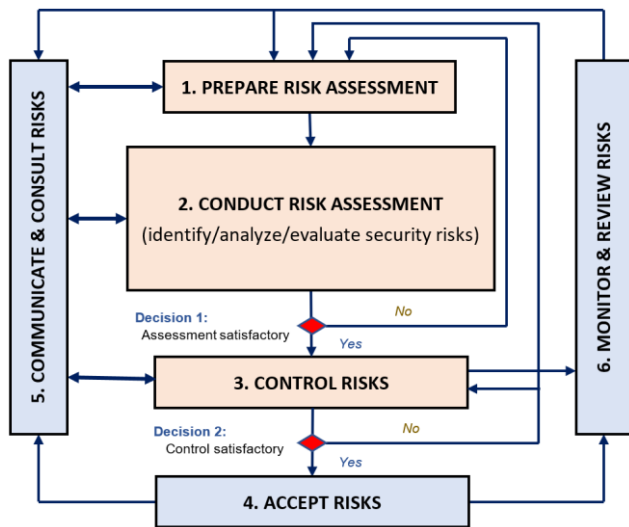


Fig. 6: Proposed Process of System Security Risk Management.

1. Prepare the system security risk assessment

This step is equivalent to the first step of ISO/IEC 27005:2018 related to the context establishment. Thus, we need to identify all information related to the organization's information system security risk assessment. From there, we will establish a plan, the content of information security risk assessment including characteristics of the assessed information system, criteria, standards, and methods of assessment, tools, technical documents for assessment.

2. Conduct the system security risk assessment

In this step, we will emphasize to perform the (i) risk identification; (ii) risk analysis; and (iii) risk evaluation.

Based on the results of Step 1 related to the plan and content of information security risk assessment, in this step, we need first to identify a list of information security risks. This task can be done using vulnerability scanners or using risk estimation tools such as CVSS or OWASP.

Then, the analysis and evaluation have to be performed on that list of information security risks. We need to conduct an analysis and evaluation, both quantitatively and qualitatively, to determine the severity of each security risk.

The result of this step is a list of security risks that have been prioritized according to the risk estimation criteria related to the threat scenarios that lead to those risks.

3. Control the system security risks

This step treats security risks, determined in the previous step, based on the outcome of the risk assessment, the expected cost for implementing these options, and the expected benefits from these options. In general, there are four common options for risk treatment, such as (i) risk modification, (ii) risk retention, (iii) risk avoidance, (iv) risk-sharing. For the e-Government organizations, these options can be substantially combined in order to reduce the likelihood of risks, their consequences, and sharing or retaining any residual risks.

4. Accept system security risks

In this step, we should determine the security risk acceptance criteria. Then, the residual security risks have to be justified based on these criteria.

5. Communicate and consult the system security risks

All security risk information obtained from the risk management activities should be exchanged and/or shared between the decision-maker and other stakeholders in the e-Government. The coordination between major decision-makers and stakeholders may be achieved by the formation of a committee where a debate about risks, their prioritization and appropriate treatment, and acceptance can take place. It is crucial in the case of crisis communication actions, for example, in response to particular incidents.

6. Monitor and review the system security risks

All security risks and their factors (i.e., a value of assets, impacts, threats, vulnerabilities, the likelihood of occurrence) should be monitored and reviewed to identify any changes in the context of the e-Government at an early stage and to maintain an overview of the complete security risk picture. Moreover, the risk acceptance criteria should also be verified to measure the security risk and assumed its elements were still valid and consistent.

5.3 Security Risk Quantification

Conducting information security risk assessments should quantify the risks. In our holistic approach, in order to identify specific security risks, vulnerability scanning tools must be used by both black-box and white-box testing methods. Some of the famous tools currently used in this purpose include Tenable Nessus, InsightVM Rapid7, etc. or our *vScanner* built and customized based on the open-source solution OpenVAS.

In the case of quantifying global information security risks, we use both CVSS or OWASP quantification methods.

a. CVSS Scoring

As described in Section 3.1, the CVSS scoring method is based on three metric groups: base, temporal, and environment metrics. For quantifying the security risk severity, the Base Score should be firstly determined by the Impact and Exploitability metrics. The formula to compute these metrics are defined as follows [23]:

$$ISS = 1 - [(1 - Confidentiality) \times (1 - Integrity) \times (1 - Availability)]$$

$$Impact = \begin{cases} 6.42 \times ISS & \text{if Scope is unchanged.} \\ 7.52 \times (ISS - 0.029) - 3.25 \times (ISS - 0.02) & \text{otherwise.} \end{cases}$$

$$Exploitability = 8.22 \times AttackVector \times AttackComplexity \times PrivilegesRequired \times UserInteraction$$

$$BaseScore = \begin{cases} 0 & \text{if Impact} = 0. \\ \text{Roundup}(\text{Minimum}[(\text{Impact} + \text{Exploitability}), 10]) & \text{if Impact} > 0 \text{ and Scope is Unchanged.} \\ \text{Roundup}(\text{Minimum}[1.08 \times (\text{Impact} + \text{Exploitability}), 10]) & \text{otherwise.} \end{cases}$$

These others metrics are calculated by the simple formula specified in the CVSS manual [5].

b. OWASP Scoring

By the OWASP risk rating method, the security risk severity is determined based on the Likelihood and Impact factors [6]. According to the CVSS method, there are four factors related to an agent (Skill, Motivation, Opportunity, and Size), which are conducted through four vulnerability

assessment criteria (Discovery, Exploit, Awareness, and Detection). To calculate the security risk impact, OWASP proposes to use four factors to determine the technical impact (Confidentiality, Integrity, Availability, and Accountability) and 4 business impact factors (Finance, Reputation, Non-compliance, and Privacy). Security Risk Likelihood and Risk Impact will be classified into three levels, as illustrated below.

Likelihood and Impact Levels	
$0 \leq \text{Mean_value} < 3$	LOW
$3 \leq \text{Mean_value} < 6$	MEDIUM
$6 \leq \text{Mean_value} \leq 9$	HIGH

Fig. 7 Levels of Security Risk Likelihood and Impact.

Based on the security risk likelihood and impact levels, the information security risk severity of an information system will be determined according to the following matrix:

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
Likelihood				

Fig. 8 Metric to Determine the Security Risk Severity.

6. Results and Analysis

Based on the proposed model of information security risk management, we have built a Web application called UET.SoC. The main objective of this application is to allow an IT administrator of a Ministry/Province (namely the Ministry M) to manage all information security risks in its information systems in accordance with the proposed process.

The main functionalities of UET.SoC are illustrated in detail through the six corresponding steps in the information security risk management process described in Section 5.2:

6.1. Step 1: Prepare risk assessment

In this step, we should firstly determine all security risk measurement criteria. For an information system of the Vietnamese e-Government, the impact areas compose in general the reputation, trust, safety & health, financial, productivity, fines and legal penalties. In our context, the areas of impact were prioritized by following scale:

Table 1: Priority Scale of Impact Areas.

Areas of Impact	Priority
Reputation and citizen confidence	5
Financial	4
Fines and legal penalties	3
Productivity	2
Health and safety	1

These impact areas will obviously be established depending on the current context of a ministry or a province in e-Government.

The following table shows our suggested measurement criteria for these impact areas.

Table 2: Risk Measurement Criteria for the Impact Areas of a System

Areas of Impact	Low	Medium	High	Critical
Reputation and citizen confidence	Minimal damage to reputation and citizen confidence	Revokable damage to reputation and citizen confidence	Irrevokable damage to less important citizen confidence	Irrevokable damage to key citizen confidence or public reputation
Financial	Yearly revenue reduction or one-time loss of less than 50 million VND	Yearly revenue reduction or one-time loss of 50-200 million VND	Yearly revenue reduction or one-time loss of 200-500 million VND	Yearly revenue reduction or one-time loss of more than 500 million VND
Fines and legal penalties	Fines, non-frivolous lawsuits or investigations do not exceed 50 million VND	Fines, non-frivolous lawsuits or investigations do not exceed 200 million VND	Fines, non-frivolous lawsuits or investigations exceed 200 million VND	Public investigations of organizational practices is made
Productivity	Less than 1 full-time officer is required for less than one month	Less than 1 full-time officer is required for less than two months	Less than 4 full-time officers are required for less than six months	More than 4 full-time officers are required for more than six months
Health and safety	No significant threats to health and safety	Maximum 4 days of degrading an officer or citizen health	More than 4 days of degrading an officer or citizen health	Permanent degrade in officer or citizen health

After defining the risk assessment criteria, information about the system administrator, technical information about the system, and some other auxiliary information will be collected to prepare for the step conducting the security risk assessment of these systems by our proposed holistic approach as shown in Fig.9.

Name	Comment	Level	Created Time	Updated Time
National E-document Exchange Platform	A system for sending and receiving e-documents between Vietnam Government Office and ministries, agencies, and localities.	4	16:55 14/11/2019	20:38 27/02/2020
National public service portal	The system provides information on administrative procedures and connects public online services nationwide.	4	15:19 27/02/2020	20:47 27/02/2020
System of registration, change driver's license	A public service system that allows the citizens to register and change driving license online	2	21:00 27/02/2020	21:00 27/02/2020
Business registration system	Through this system, business founders can prepare applications and submit business registration documents online.	2	21:17 27/02/2020	21:17 27/02/2020

Fig. 9: Information Systems of an Organization.

6.2. Step 2: Conduct security risk assessment

Before the systems are assessed risks by qualitatively and quantitatively, they will be vulnerability scanned by a scanner (such as our one, namely *vScanner*, or *InsightVM*, ...) or any other software that supports scoring according to the CVSS and OWAPS standards. The

following Fig.10 illustrates the risk assessment results for all three methods that we have installed and implemented in the UET.SoC.

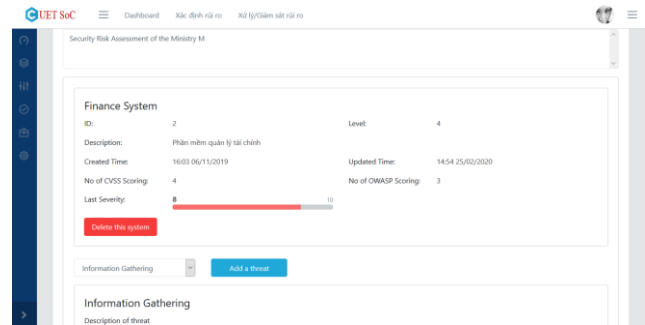


Fig. 10 Security Risk Severity of a System.

Technically, we identify the following threats that may affect an information system:

- Malicious Code: Use of code to perform unauthorized disclosure, adjustment, or destruction.
- Information Gathering: Gather the data/information of the important system.
- Intrusions: Unauthorised access to data, systems, physical documents, or facilities.
- Availability: Unavailability of systems, people, physical documents, or facilities.
- Information Content Security: Unauthorised adjustment of information content.
- Fraud: Fraud is deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right.

Based on these threats, we perform a step of security risk identification. Here, the CVSS or OWAP method will be used to determine the severity of the information security risks. The following figures illustrate both the two methods of risk quantification.

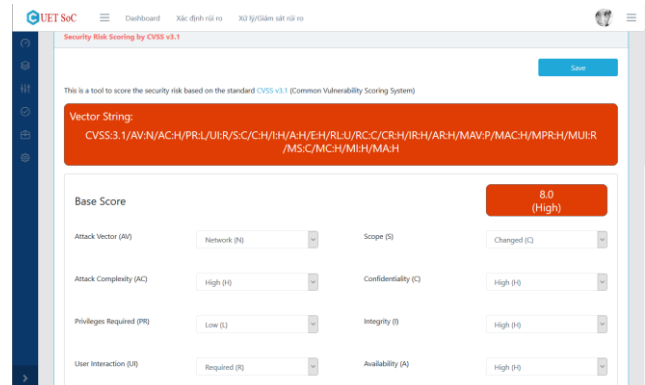


Fig. 11 Security risk quantification by the CVSS method.







Base Score	Temporal Score	Environmental Score	Created Time	Updated Time	
7.7	7.4	5.0	22:58 27/02/2020	22:58 27/02/2020	  
4.9	4.9	4.9	20:54 27/11/2019	00:07 28/11/2019	  

Fig. 12 Evolution of CVSS severity of a system,

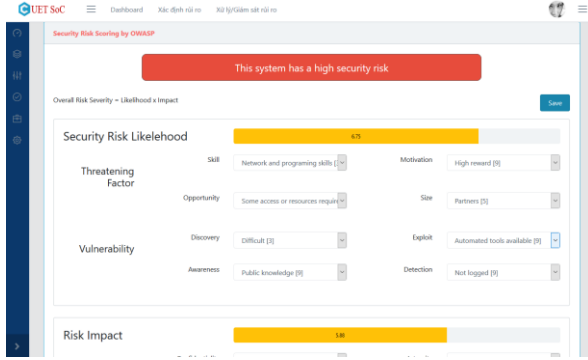


Fig. 13 Security risk quantification by the OWASP method.










Likelihood	Impact	Created Time	Updated Time	
3.4	5.1	23:56 27/11/2019	01:13 28/11/2019	  
4.6	4.1	23:54 27/11/2019	00:03 28/11/2019	  
6.3	6.8	19:27 27/11/2019	00:07 28/11/2019	  

Fig. 14 Evolution of OWASP severity of a system.

After this qualitative step, we obtain a list of systems that have identified the severity of the security risks. This is an important list for security risk analysis.












System Name	Comment	Created Time	Updated Time	CVSS Scoring No	OWASP Scoring No	Severity	
National public service portal	The system provides information on administrative procedures and connects public online services nationwide.	15:19 27/02/2020	20:47 27/02/2020	1	0	6.9	  
System of registration - change driver's license	A public service system that allows the license to register and change driving license online.	21:00 27/02/2020	21:08 27/02/2020	0	1	5.0	  
Business registration system	Through this system, business founders can prepare applications and submit business registration documents online.	21:17 27/02/2020	21:17 27/02/2020	1	0	5.9	  
National e-Document Exchange Platform	A system for sending and receiving e-documents between Vietnam Government Office and ministries, agencies, and localities.	16:51 14/11/2019	22:17 27/02/2020	2	2	7.7	  
System of Academic Formation Management	Managing the Academic Activities	16:03 30/11/2019	08:13 27/02/2020	2	3	6.1	  

Fig. 15 Severity of system security risks.

6.3. Step 3: Control security risks

In this step, our UET.SoC system will allow controlling information security risks for each information system of a ministry or province in e-Government. This treatment will be performed corresponding to each risk scenario (as described above) with containers and controls in compliance with the NIST SP 800-53r4 standard [22]. The following figures illustrate a list of controls selected to treat corresponding threats and to ensure the security for the information system (critical information).

Container	Information Systems	Threat	Controls
Administrators	Finance System	Malicious Code	AC-01 Access Control Policies and Procedures AC-02 Access Management
Administrators - Network	Finance System	Malicious Code	AC-03 Access Enforcement AC-04 Information Flow Enforcement
Employees	Finance System	Information Gathering	AI-01 Security Awareness And Training Policy And Procedures AI-02 Security Awareness
Employees - Finance	Finance System	Information Gathering	AI-03 Security Training AI-04 Security Training Records
Laptops	National e-Document Exchange Platform	Intuition	AU-01 Audit And Accountability Policy And Procedures AU-02 Available Events
Laptops - Finance	National e-Document Exchange Platform	Intuition	AU-03 Content Of Audit Records AU-04 Audit Storage Capacity
Network appliances	National e-Document Exchange Platform	Availability	CA-01 Certification, Accreditation, And Security Assessment Policies And Procedures CA-02 Security Assessments
Network appliances - Firewalls	National e-Document Exchange Platform	Availability	CA-03 Information System Connections CA-04 Security Certification

Fig. 16 List of control selection.

6.4. Step 4: Accept security risks

Basically, those responsible for ensuring information security of systems will make every effort to fully overcome the system's possible risks. But for certain situations, for example, overcoming risks could affect or disrupt system performance, or the cost and time to deal with risks are far above the probability that the system can damage by risk, ... then, the risk assessment expert should choose one or several options from the different risk acceptance criteria, as described in Section 5.2.

6.5. Step 5: Communicate and consult risk assessment results

Based on our system, UET.SoC, all technical risks will be advised on how to fix it. All results of information security risk assessments and treatments will be communicated to relevant people in e-Government. Accurately, these results will be transferred to, such as the Department of Information Security or the Ministry's leader in charge of information security. It can be performed on the UET.SoC system by granting user accounts and setting the appropriate permissions and roles.

6.6. Step 6: Monitor and review security risks

Based on UET.SoC, the risk assessment manager can monitor and review all the security risks. Fig.17 below illustrates a functionality that allows to perform this task.

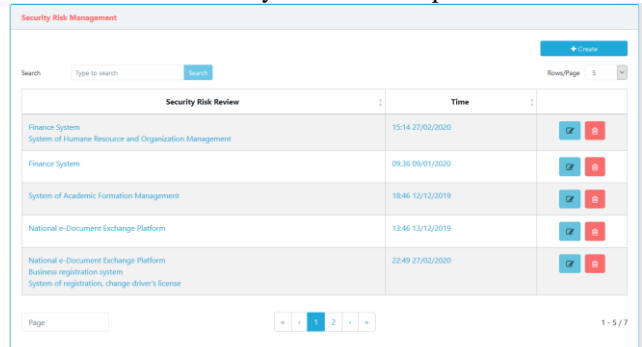


Fig. 17 Monitoring and reviewing the security risks

By following the 6 steps in the process of information security risk management, UET.SoC has allowed us to manage all information security risks in the information systems of a Ministry/Province in the Vietnamese e-Government. Moreover, for each Ministry/Province, UET.SoC provides functionalities for managing information systems; helping to establish a list of threats; conducting security risk quantification; supporting to determine the security risk impacts; and reducing the security risks through strengthening security controls. UET.SoC also allows to monitor and review all information security assessment and treatments.

7. Conclusion and Future Works

With urgent requirements from the task of ensuring information security in the development of Vietnamese e-Government, it is specifically building an information security risk management solution. We have researched and analyzed the standards and approach of security risk management in the world combined with the standards and regulations on information security in Vietnam, thereby proposing a holistic approach that allows assess and manage risks on both qualitative and quantitative aspects in line with the unique characteristics of Vietnam e-Government but still inherit the strengths of global standards.

Based on the proposed process of security risk management, we have implemented and integrated it into the Web application, called Soc.UET. The preliminary experimental results show that its six steps are performed intuitively and allow the IT administrators of a Ministry/Province to manage information security risks in its information systems effectively.

Continuing with other tasks in ensuring information security for e-Government, for future works, we aim to propose methods for handling risks and responding to information security incidents for information systems of the Vietnamese e-Government.

Acknowledgments

This work is supported by the national research project No. KC.01.19/16-20, granted by the Ministry of Science and Technology of Vietnam (MOST).

References

- [1] ISO/IEC 27005:2018 Information Technology | Security Techniques | Information Security Risk Management." <https://www.iso.org/standard/75281.html>, 07 2018.
- [2] I. Chalvatzis, D. A. Karras, and R. C. Papademetriou, "Evaluation of security vulnerability scanners for small and medium enterprises business networks resilience towards risk assessment," in 2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), pp. 52-58, March 2019.
- [3] K. Labunets, F. Massacci, F. Paci, S. Marczak, and F. M. de Oliveira, "Model comprehension for security risk assessment: An empirical comparison of tabular vs. graphical representations," in 2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE), pp. 395-395, May 2018.
- [4] NIST special publication 800-39: Managing information security risk." US National Institute of Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>, 03 2011.
- [5] FIRST, "Common vulnerability scoring system version 3.1." FIRST, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf, 03 2016.
- [6] B. Mburano and W. Si, "Evaluation of web vulnerability scanners based on OWASP benchmark", in 2018 26th International Conference on Systems Engineering (ICSEng), pp. 1-6, Dec 2018.
- [7] W. Abbass, A. Baina, and M. Bellafkih, "Survey on information system security risk management alignment", pp. 1-6, 03 2016.
- [8] A. Fernandez and D. Garcia, "Complex vs. simple asset modeling approaches for information security risk assessment: Evaluation with Magerit methodology," pp. 542-549, 08 2016.
- [9] Y. Wang, W. Wu, and G. Zhan, "An optimized algorithm in risk calculating", pp. 354-357, 12 2016.
- [10] H. Asgari, S. Haines, and O. Rysavy, "Identification of threats and security risk assessments for recursive internet architecture," IEEE Systems Journal, vol. PP, pp. 1-12, 11 2017.
- [11] J. Nurse, S. Creese, and D. Roure, "Security risk assessment in internet of things systems", IT Professional, vol. 19, 09 2017.
- [12] J. Hong, S. Yusuf Enoch, D. Kim, and K. Khan, "Stateless security risk assessment for dynamic networks", pp. 65-66, 06/2018.
- [13] D. Reeh, F. Tapia, Y.-W. Chung, B. Khaki, C. Chu, and R. Gadh, "Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats", pp. 1-6, 06/2019.
- [14] A. Pitto, E. Ciapessoni, and D. Cirio, "A probabilistic risk-based security assessment tool allowing contingency forecasting", 06/2018.
- [15] Y. Azan Basallo, V. Senti, and N. Sanchez, "Artificial intelligence techniques for information security risk assessment," IEEE Latin America Transactions, vol. 16, pp. 897-901, 03 2018.
- [16] M. Aksu, M. H. Dilek, E. Tatlı, K. Bicakci, H. Dirik, M. Demirezen, and T. Aykir, "A quantitative cvss-based cyber security risk assessment methodology for it systems", pp. 1-8, 10/2017.
- [17] I. Suryadinata, S. Nasution, and M. Paryasto, "Analysis security metric on bro ips based on cvss and vea-bility metric," pp. 174-180, 09/2017.
- [18] H. Joh, "Quantitative security analysis of network oses by fitting vdm and examining cvss," pp. 565-570, 01/2018.
- [19] B. Mburano and W. Si, "Evaluation of web vulnerability scanners based on owasp benchmark", pp. 1-6, 12 2018.
- [20] K. Flanagan, E. Fallon, A. Awad, and P. Connelly, "Security analytics on asset vulnerability for information abstraction

and risk analysis," in 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation (UKSim), pp. 9-15, April 2016.

- [21] I. Altaf, F. u. Rashid, J. A. Dar, and M. Rafiq, "Vulnerability assessment and patching management," in 2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI), pp. 16-21, Oct 2015.
- [22] NIST special publication 800-30 revision 1: Guide for conducting risk assessments." US National Institute of Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>, 09 2012.
- [23] M. Aksu, M. Dilek, E. Tatli, K. Bicakci, H. Dirik, M. Demirezen, and T. Aykir, "A quantitative CVSS-based cyber security risk assessment methodology for it systems," in 2017 International Carnahan Conference on Security Technology (ICCST), pp. 1-8, Oct 2017.



Ha LE Viet graduated from the University of Science with a bachelor's and master's degree in applied mathematics and informatics at 2003 and 2011, respectively. After a few years of experience as an embedded programming engineer for mobile devices, settleboxes, ..., since 2011, he has been an specialist of Office of the Government, in charge of information security for Vietnam's e-government

systems. Since 2016, he has been appointed as the Deputy Head of Information Security Department. His research focuses on system information security penetration testing, malware analysis and detection techniques, and their application in Vietnam e-government systems. Currently, he is a member of a number of state-level scientific research projects in the field of information security.



On PHUNG Van has many years of experience working and researching in the leading IT professionals, especially his profound knowledge in e-government development. He completed bachelor and master's programs in applied mathematics and informatics at VNU University in 1980 and 1997. Following that, he, as the associate dean of Information technology faculty -

Vietnam Maritime University, continued his Ph.D. in the same major in 2001. From 2009 to 2015, as the director of the informatics center of the government office, Dr. On Phung Van, together with senior government leaders laid the first foundations for forming e-government Vietnam as successful as today. In his research and teaching career, he has conducted more than 20 national and international scientific research articles, participated in dozens of scientific projects at all levels, instructed about 40 masters and PhD in information technology. Currently, he is a member of a number of national organizations such as vice president of Vietnam Association for Information Processing (VAIP), president of national-level science council,



Hoa NGUYEN Ngoc received her engineer's degree in computer science from Hanoi University of Science and Technology in 1999, and the Ph.D. degree in computer science from Joseph Fourier University, France in 2005. He is currently an Associate Professor at VNU University of Engineering and Technology, and his research interests include big data management, information security, and smart systems.