A Review of Cyber Security Risk Assessment for Web System during Its Deployment and Operation

Manh-Tuan Nguyen, Thi-Huong-Giang Vu
Hanoi University of Science and Technology, Hanoi, Vietnam
Correspondence: Thi-Huong-Giang Vu (giangvth@soict.hust.edu.vn)
Communication: received 05 Oct 2022, revised 16 Feb 2023, accepted 01 Mar 2023
Digital Object Identifier: 10.32913/mic-ict-research.v2023.n1.1089

Abstract: This paper presents the state of the arts in security risk assessment of web systems. The process of assessing security risks and the process of developing and operating information systems in general, web systems in particular, are depicted step by step, showing how the risk assessment is performed during the deployment and the operation of web systems. Based on this analysis, different methods related to the manual and automatic risk assessment are reviewed, focusing on the methods using probability theory and Bayesian networks. The techniques developed for quantitative and qualitative assessment are presented and compared in terms of their objectives, scopes, and results to pick out advantages and limits. Finally, the approaches dedicated to assessing the risks of web systems are presented.

Keywords: *security risk assessment, DevOps, web system, bayesian network*

I. Introduction

In recent years, the explosive development and wide application of web systems in all aspects of life has brought great benefits to organizations, businesses as well as individuals. The richer information and services the web systems deliver through Internet web technologies, the more complex the web systems to be developed and operated become, making securing web systems more difficult.

Security becomes one of the focuses in the processes of developing, deploying, and operating these systems. Security is not an one-time job, it is a continuous process associated with the web system's life cycle. Various security countermeasures have been implemented in organization to control potential security threats. However, web systems still face the security risks that arise from their intrinsic vulnerabilities, particularly when moving them from the development environment (i.e., test environment, staging environment) to the production environment. Successful exploits of such vulnerabilities during the operation of web systems can cause a loss, damage, or destruction of their assets, such as data leaks, service interruptions, or other violations of CIA (confidentiality, integrity, availability) triads. Practical experience in cyber security shows that the effectiveness of security countermeasures is not only based on the technical aspects of these countermeasures, but also depends on the security risk management process, in which the security risk assessment plays the critical role.

The risk assessment process aims to discover possible risks and analyze what might happen if risks arise, including the likelihood of successful intrinsic vulnerabilities exploits and their potential impacts. The risk assessment is performed at different stages of the web system's life cycle and is conducted by different stakeholders of the organizations developing, owning, and using them. Risk assessment in general, security risk assessment in particular is a combination of measurable and quantitative calculations with the in-depth expertise and expert knowledge on uncertain and incomplete data. As a result, the approaches to security risk assessment differ from the business processes, the tools or techniques used for assessment, and the contextual characteristics of the system being assessed.

In the case of web systems, some of their unique characteristics compared to other types of software systems make the security risk assessment more difficult. First, web systems provide functions for both anonymous users and authenticated users with broad accessibility through many different entry points inside or outside the systems. This causes complexities in identifying and modeling threats. Second, web systems often include many software or application components that are developed with diverse technologies and architectures and using different programming languages and frameworks. These expose web systems to a wider range of vulnerabilities in their components.

Third, the technologies used to deploy and operate web systems are now inexpensive and available from third-party vendors. However, the audit reports or declarations of compliance with international standards from these vendors are not detailed enough to their customers to establish an effective security risk response plan for the web systems. Fourth, web systems reside on the network and must deliver their services continuously. For that, the selected security risk assessment approaches in different stages of the life cycle of web systems must be aligned with the business process of the web systems and relevant to the context of the organization developing, owning, and using the web systems. As there have been numerous solutions with different approaches to assess risks of web systems in different application domains, these approaches need to be systematically aggregated from specific perspectives to help organizations select an appropriate security risk assessment strategy.

This paper gives an overview of current approaches in security risk assessment to address the following research question: "How to perform the security risk assessment during the development and operation of web systems?" The aim of the review is to provide a clear description of the risk assessment stages performed by organizations developing the web systems and those performed by organizations operating the web systems. Based on this description, stakeholders from organizations deploying, operating, and using a web system could easily identify the gaps in their security risk assessment results and easily conduct a suitable security risk assessment technique for a web system before its deployment.

Our approach is to conduct a literature search about security risk assessment for web systems, filter and select the 60 most relevant papers according to their titles, abstracts, and keywords. We synthesize data from these selected papers to outline their commonalities and differences according to different perspectives: process, degree of automation, techniques, and web system characteristics. The literature results are classified and explained as follows. First, risk assessment stages are identified through the standardized assessment processes or those defined by security organizations. Then these stages are mapped to different stages of software development and operations processes. Next, the approaches realizing these stages are considered and classified by their degree of automation. These approaches are also classified based on the characteristics of their assessment outputs (whether quantitative or qualitative). Finally, these approaches are classified based on the characteristics of developing and operating web systems.

This paper is organized as follows: Section II introduces different security risk assessment processes and discusses how they are related to the software development life cycle in general, to the web system development life cycle in particular. Section III describes two approaches to manual assessment and automatic assessment of web systems' security risks. Section IV summarizes qualitative and quantitative security risk assessment techniques, with a focus on techniques based on Bayesian networks and their ability of application for assessing web systems' security risks during the phases of their life cycle. Section V is the analysis of the specificity of the field of application in the security risk assessment process of web systems. Section VI suggests a framework for the categorization of risk assessment for web systems. Finally, Section VII presents our conclusion.

II. Process

This section synthesizes studies on security risk assessment from the perspective of web systems development and operations.

1. Security Risk Assessment Processes

Security risk assessment processes could be divided into 2 groups. The first group includes the international standards such as ISO/IEC 27001 and ISO/IEC 27005. The second group is composed of the processes that are defined by security organizations such as NIST 800-30, and the processes that are dedicated for specific application domains. Examples of the latter are HIPAA Security and Privacy Rules[1] for health care systems, PCI-DSS[2] for payment card and banking systems, etc. In this section, we focus on the ISO/IEC 27005 and the NIST 800-30.

a) Standards

ISO/IEC 27005 [1] is a member of the ISO/IEC 27000 standard family, describing the best practices to conduct information security risk management. The intention of ISO/IEC 27005 is to specify recommended processes for organizations to ensure the quality of their risk management methodology. ISO/IEC 27005 provides an iterative process of assessing and monitoring security risks, as is illustrated in Figure 1a. This process contains three stages: risk identification, risk estimation, and risk evaluation, in which risk identification and risk estimation belong to the risk analysis process.

Risk identification: The objective of this stage is to discover and identify risk factors forming the causes of security risks, including the assets of the organization, their vulnerabilities, and their potential threats.

[1]https://www.hhs.gov/hipaa/index.html
[2]https://www.pcisecuritystandards.org/standards/

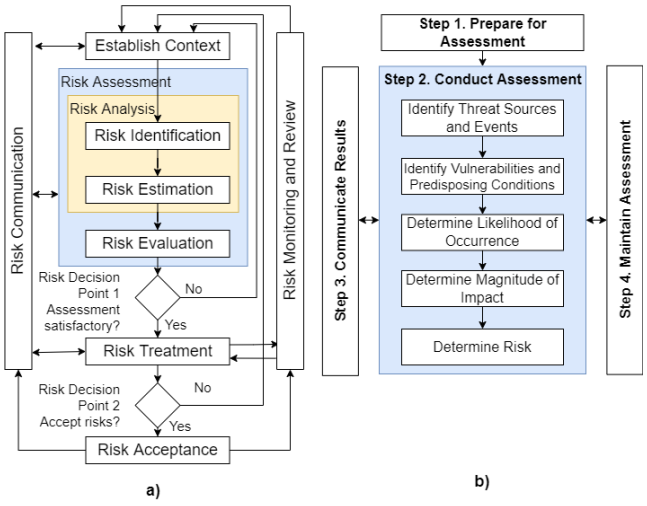

Figure 1. a. ISO/IEC 27005 process [1], b. NIST SP800-30 revision 1 process [2]

Assets. According to [3], assets extend beyond physical goods or hardware, and include software, information, people, and reputation. Examples of assets in web systems include servers (hardware and software), data, and network. To identify assets in a web system, the study [4] proposes a structure of 4 inter-dependent layers: the application's configuration; relationship between network, hardware and software; information; and organization environment (functions inside organizations to justify the application's existence). The value of each asset is then rated using security criteria such as availability, integrity and confidentiality with a specific qualitative assessment scale. This structure allows identifying the main assets of a web system, but does not allow considering assets in different phases of the web system life cycle. The value of assets can also be calculated based on their importance to the organization [5]. The loss in value of these assets can be used to quantify the risk impacts on the organization.

Vulnerabilities. The security risk is defined by the threats that might take advantage of the vulnerabilities of the assets. The work [6] synthesizes approaches to analyze vulnerabilities for web applications. Two popular methods are: (1) building models of known vulnerabilities and matching the models against web system components; and (2) building models of normal web application behaviors in advance and use these models to analyze anomalies that could cause security risks. The former is easier to implement because of diverse sources used to identify vulnerabilities: the result of penetration testing, vulnerability scanning tools, previous risk assessment reports or public vulnerability databases like Common Weakness Enumeration (CWE) [3], National Vulnerability Database (NVD) [4]. Another common approach to detect vulnerabilities in web systems is to analyze the source code of the application. The study [7] combines source code analysis and data mining techniques to predict false positives in candidate vulnerability sets for improving accuracy. Experimental results applied to web applications written in PHP programming language are compared with available tools showing the effectiveness. The challenge of the method is the complete definition of the formal specifications of the programming language used to develop web applications.

Threats. Several methods are made available to analyze threats and match them with related vulnerabilities of the assets [8]. Threats can also be detected through threat classification systems such as STRIDE [9]. STRIDE models threats based on attack attributes but it lacks context information. When applying this threat model to a web system it is necessary to map to the specific functions of the application as well as consider the platforms and technologies in a particular attack scenario. The study in [10] uses the knowledge base to define rules for identifying relationships between concepts of asset, threat, and vulnerability for the efficiency and accuracy of risk assessment.

Risk estimation: In this step, the risk value, i.e., the likelihood of the risk and the impact of the risk, is measured by using qualitative, quantitative, or hybrid methods [11] [12]. The risk estimation is based on the modeling of the relationship between the risk factors identified in the previous step. Risks are estimated either qualitatively using a risk matrix representing both likelihood and impact on a scale of 1 to 5, or quantitatively by numbers representing the risk levels.

Risk evaluation: In this stage, the organizations make decisions of rating risks using the results of the analysis phase. The identified risks are prioritized, and their severity is determined, leading to one of the following decisions on handling the risks:

- Risk avoidance, meaning elimination of threats and vulnerabilities that can negatively affect the assets of the organization.
- Risk mitigation, the consequences of the risk are controlled, and the risk level is reduced to an acceptable level.
- Risk transferring, the risks are shifted to a third party.
- Risk acceptance, the organization understands the consequences of the risk and does not take any measures to avoid the impact of the risk happening.

ISO/IEC 27005 has not focused on technical details of the risk assessment processes. Thus, the standard can be

[3]https://cwe.mitre.org/

[4]https://nvd.nist.gov/

implemented in every type of organization and combined with other standards or methods to fulfill the organization's needs. ISO/IEC 27005 also provides a framework for other security risk assessment studies and approaches to develop standard-compliant products.

b) Organizations

NIST 800-30 rev. 1 [2] has been developed by NIST featuring a step-by-step information risk assessment guideline as is illustrated in Figure 1b. This guideline was designed to assess the risk factors in a straightforward way with simple calculations. NIST 800-30 is consistent with the ISO/IEC 27005 standard. It starts with preparatory work towards conducting assessment steps that can be corresponded to the stages of the standard as in Table I.

TABLE I
ISO/IEC 27005 VS. NIST SP800-30 REVISION 1

ISO/IEC 27005	NIST SP800-30 rev. 1
Risk identification	Identify threat sources and events
	Identify vulnerabilities & predisposing conditions
Risk estimation	Determine likelihood of occurrence
	Determine magnitude of impact
Risk evaluation	Determine risk

NIST 800-30 describes the way risk management processes can be performed in support of each phase of the system life cycle. It was produced as a set of guidelines for the organizations to follow. This enterprise-oriented approach allows customization to suit the complexity of systems and the constraints of security budgets. The decision as to what type of risk assessment should be performed depends on the particular organization. An organization may choose a simplified approach obtaining basic security risk assessments. These results will be the first step to provide an overview for further in-depth assessments. The organizations applying these standards and guidelines to their risk management processes still need a lot of work to develop an appropriate methodology. The combination approaches of ISO/IEC 27005 and NIST SP800-30 are reviewed in several works such as [13], [14]. Other enterprise-oriented approaches include: Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) [15], Factor Analysis of Information Risk (FAIR) [16], COBIT 2019 [17] and OWASP Top 10 [18]. OCTAVE version 2.0 defines a risk-based strategic assessment and planning technique for security to effectively manage operational risks. COBIT 2019 is a framework for the governance and management of enterprise information and technology (I&T). This framework supports enterprise to improve the value they get from all their IT processes and manage risks at the same time. For enterprise, the I&T risk assessment in general, the security risk in particular, is guided in the COBIT core model by considering which I&T-related issues it currently faces. OWASP provides awareness of important security risks for web applications. It is often chosen by organizations and developers to build solutions to reduce the security risks of their web systems.

2. Software Development and Operation Process

Effective security risk management processes must be integrated into the web system life cycle to minimize negative risk impact on the organization. With modern fast-paced software development models, the phases of the web system life cycle are no longer separate, but continuously connected.

As the system life cycle is considered from different perspectives, there are many approaches to integrate the security risk management.

From the technical perspective: ISO/IEC/IEEE 15288 [19] identified 14 technical processes related to the life cycle of a system. There are: business or mission analysis process; stakeholder needs and requirements definition process; system requirements definition process; architecture definition process; design definition process; system analysis process; implementation process; integration process; verification process; transition process; validation process; operation process; maintenance process; and disposal process. NIST 800-160 Volume 1 [20] extended these processes with systems security engineering aspects.

From the system providers' perspective: A System Development Life Cycle (SLDC) typically consists of five stages: initiation, development or acquisition, implementation, operation and maintenance, and disposal. SP800-37 Rev. 2 [21] describes how the NIST's risk management framework relates to system development life cycle processes and stages.

From the consumers' perspective: In general, system life cycles can be described by development and operations processes called DevOps processes. These processes encompass the deployment, i.e., the work of making software work on a test environment, on a staging environment, on a production environment or on a user's device. This work could be attached as the ending stage of the development process or the initial state of the operations process. According to [22], there are 3 ways to consider the DevOps process (c.f. Figure 2). The first way corresponds to the principles of flow thinking, that enables a left-to-right flow of work from development to operations to the customer. The second way refers to the principles of feedback, that amplifies the feedback loops so necessary corrections can be continually made to prevent problems from happening

again, or enable faster detection and recovery. The third way sticks with the principles of continual learning, that fosters continual experimentation, taking risks and learning from failure; and understanding that repetition and practice is the prerequisite to mastery.

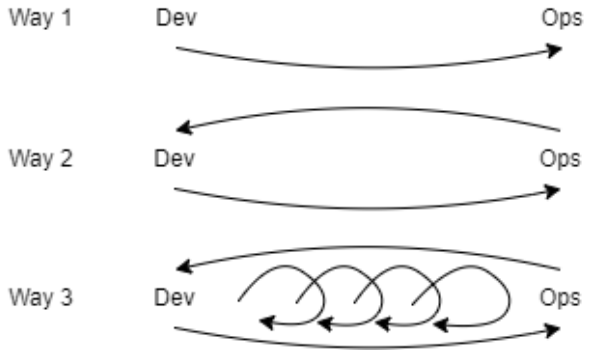

Figure 2. Three ways of DevOps

As the development side and the operation side are distinguished in these 3 ways, the security risk assessment is differently conducted in these sides.

From the development side, the security risk management is integrated into the test phase and is called risk-based testing. The latter uses risk (re-) assessments to steer all phases of the test process in order to optimize testing efforts and limit the risks of the software-based system [23]. This approach is the assessment of the functionalities of the software that has the highest impact on the probability of software failure. Security risk assessment is especially meaningful to consider in security testing as some security requirements can be difficult to design test cases for it. For example, given a security requirement such as "Outside attackers should not be able to change the data of the website". The functional test cases defined for this requirement must be all the trusted ways that an attacker can change the system data. With risk-based testing, only a risk scenario is defined and then tested for each security requirement. Risk-based testing could use security risk assessment results including threat modeling, vulnerability identification to reduce testing efforts. Risk-based testing activities can be integrated into main phases of a normal test process, as in [24]. The vulnerabilities that may exist in the source code of web components during the development process are also one of the main inputs for the security risk assessment. The study [25] has introduced techniques for static analyzing the source code of web components during the programming phase to detect vulnerabilities. The shortcoming of the proposed method is not yet tied to the testing phase to confirm the removal of vulnerabilities. Research [26] has built a secure development paradigm based on a combination of security practices and agile methodology for web applications. The development model allows web developers to reuse defined security goals from previous projects as a basepoint for the development process. However, this approach does not consider the connection to the deployment and operations process of the web system's life cycle.

From the operational side, managing security risks is very important to ensure the business continuity of the organization. Selected risk management strategies must follow the existing risk management practices and standards and consider risks from all the involved stakeholders. They are analyzed and assessed from an operational perspective, such as attacks according to usage scenarios, the risk impact on the reputation and financial aspects of the organization or choosing the countermeasures regarding the available resources of the enterprise. Studies [27] [28] show that security risk management frameworks should be integrated with the organization context proactively.

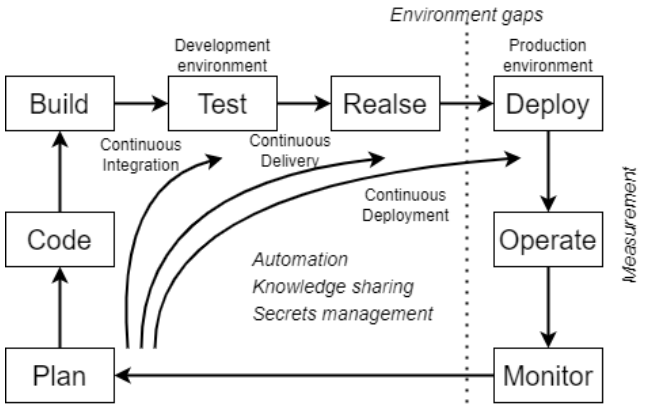

Figure 3. DevOps security risk challenges

As illustrated in Figure 3, the DevOps process also faces new security risks due to the continuous integration of development and operation processes. One of the challenges is the gap or the lag between development and operation activities. Security risks can be introduced by either development or operations process (or both), in which security risk assessment in the deployment phase, a transitional phase as mentioned above, has not received much attention from researchers. Most studies tend to analyze the continuation of the two processes, whereas the results of the security risk assessment of deployment phase allow the combination of developer, vendor, and user perspectives in a comprehensive security risk management strategy. As the DevOps process focuses on speed, it might not give proper attention to security issues or security risk assessment results. It often takes a long time to decide the selection of security countermeasures.

The principle to ensure process continuity is automation,

where the term *Continuous Deployment* (CD) means automatically deploying system changes into the production environment. The difference between the test environment in the development process and the production environment in the operations process makes the CD might not be fully automated. The manual operations might cause security issues including misconfigurations (e.g., opening unused ports, leaving default credentials embedded in configuration files, granting redundant privileges) and dependencies on third parties without evaluating their potential security risks (e.g., reusing codes or installing new tools from unreliable sources). Automated deployment environments with cloud service providers containing malicious or vulnerable container images and repositories are also security risks.

Study [29] has specified a method of risk analysis and assessment in the DevOps process. The targeted method is associated with optimizing DevOps-related criteria including cost, speed and quality of the assessment. In [30], the authors built three case studies for different configurations of DevOps toolchains in order to identify the impacts on security from both positive and negative aspects. The results show that choosing the right tools contributes decisively to ensuring the security of the stages in the life cycle of the system. To deal with the long-time problem in the risk assessment process, the work [27] proposed a lightweight approach, a rapid risk assessment framework, targeting rapid-release cycles and high flexibility.

III. Degree of automation

Risk assessment methods could also be regrouped by degrees of automation. By this way, there are two groups: manual assessment and automatic assessment.

1. Manual Assessment

With manual assessment, information security experts will perform the audits, following standards and detailed procedures mentioned above with the support of automated vulnerability scanning tools such as Nessus [5], OpenVas [6], Nmap [7], etc., vulnerability classifier (CVE - Common Vulnerabilities and Exposures), an information technology product name checker (CPE - Common Platform Enumeration dictionary), and a Common Vulnerability Scoring System (CVSS) [31]. The quality of a manual assessment depends on how systematically this process has been performed and documented. To describe the scope of the assessment and identify a list of critical assets, the experts need clear definitions and criteria in the context of the organization. Manual analysis of security risk factors is also arduous because a complete list of the potential threats and vulnerabilities that would endanger these assets, is rarely available. The support of scanning tools and public vulnerability databases can help the experts reduce processing time, but with large amounts of information, this is still a costly task. The study [32] argued that each tool could report thousands of vulnerabilities, of which only a small number are actually related to security risks. Thus, if this process is repeated for each asset, then it still requires human inspection. In addition to the expert reviews, gathering data for the assessment process from a historical perspective through stakeholder interviews is also an important feedback about security risk. Security incidents occurred and resolved and decisions taken by managers may not be fully documented, causing information shortages for organizations to apply the manual assessment process.

The manual security risk assessment is still very useful when it is used as a high-level risk discovery approach. In [27], the rapid risk assessment framework consists of 4 phases: (i) Gathering information, (ii) Establishing a data dictionary, (iii) Identifying and measuring risks and (iv) Making recommendations. The framework uses a *risk table* to decompose measurements into 3 areas: confidentiality, integrity, and availability. This table is used to consider the risk impact to the reputation, finances, and productivity of the business. Each assessment is conducted with the participation of trained risk analysts and relevant people in an associated meeting which takes between thirty minutes and one hour with well-designed templates of spreadsheets and documents.

2. Automatic Assessment

The second approach is automated security risk assessment. Many frameworks have been proposed to overcome the inefficiencies of the expert-based manual assessment approaches, but the results have not been put into practice as commercial tools [33], [34], [35], [36]. To automatically assess the risks, following approaches are considered:

- *Automatic assets management.* Studies in this group aim to identify and classify assets of the organization into appropriate critical levels. If an asset is not identified or classified as non-critical, it is unlikely that it will be taken into account in a security risk management strategy. [37] has proposed a fuzzy-based framework for classification and labeling information assets according to ISO/IEC 27001 security standard. Assets are classified according to the values of the attributes confidentiality, integrity and availability in a six-phase framework for security risk assessment. Studies [38] [39] have built models to evaluate assets

[5] https://www.tenable.com/
[6] https://www.openvas.org/
[7] https://nmap.org/

value, one of the main parameters used to calculate the risk impact. These models also considered dependencies between assets and business processes.

- *Automatic threats and vulnerabilities analysis.* This includes knowledge-based methods to model and analyze these two essential factors of security risks. The results considered different aspects of threats and vulnerabilities and the relationship between them. For example, [40] presented a novel automated architecture for threat modeling and risk assessment for cloud systems using ontology knowledge bases. [41] introduced an automatic approach for scoring vulnerabilities based on machine learning algorithms. These automated knowledge-based approaches have proven effective when it comes to assessing new security risks that may not yet have sufficient detailed analytical information.
- *Automatic assessment workflow.* Diverse approaches involve determining the likelihood of occurrence and assessing the impact of security risk on the critical assets. It is essential to deal with the uncertainty associated with the assessment results. [33] [35] used probability theory and Bayesian networks - described as an expert system of uncertain facts - to cope with the challenge. [34] and [36] have built the solutions based on fuzzy decision theory.
- *Others.* Some works are geared towards tracking and trending security risk assessment. Risk assessment results will be continuously recorded and monitored throughout the acquisition process, providing the ability to connect to recommendation systems for further risk mitigation. [42] attempts to assess insider threats by technical and behavioral monitoring. The former is built on the principles of need-to-know, least privilege, and segregation of duties. The latter focuses on insiders with malicious intent. [43] provides a model for securing healthcare data confidentiality, where risk monitoring strategy is built on a machine learning approach.

Each approach, whether manual or automated assessment, has its own advantages and disadvantages. Manual methods must find solutions for efficiency. Automated methods face data volume and computational feasibility problems. A combination of the two, where automation is imperative as much as possible, can be a suitable strategy for keeping the organization safe from threats.

IV. Techniques

In the risk analysis phase, the organization needs to choose a particular technique which is used to measure risk factors including the value of assets, the effect of vulnerabilities, the risk likelihood, the risk impact, and so on. The risk likelihood denotes the chance of a prospective risk occurring, whereas the risk impact denotes an estimate of the potential losses connected with a detected risk. Existing risk assessment techniques could be classified into qualitative techniques and quantitative techniques. Qualitative risk assessment is based on subjective analysis of different threat-vulnerability scenarios. Quantitative risk assessment is based on objective processes and metrics of different risk assessment components. Following criteria are used to compare these techniques: their approaches, their hypothesis and constraints, their underlying algorithms, mechanisms or models, and their obtained results.

1. Qualitative techniques

A qualitative approach rates the magnitude of these elements as relative values or ranks. The former are usually represented by numerical ranges (e.g. 0 to 5 or 0 to 10). The latter are usually expressed on a descriptive scale of levels (e.g. low, medium, and high). The risk levels are estimated using a matrix or table with one element represented by the rows and the other element represented by the columns of the table. Figure 4 illustrates the levels of risks in the rapid risk assessment (RRA) framework [27].

Risk		Likelihood			
		LOW	MEDIUM	HIGH	MAXIMUM
Impact	LOW	LOW	LOW	MEDIUM	MEDIUM
	MEDIUM	LOW	MEDIUM	HIGH	HIGH
	HIGH	MEDIUM	HIGH	HIGH	MAXIMUM
	MAXIMUM	MEDIUM	HIGH	MAXIMUM	MAXIMUM

Figure 4. Levels of risks are expressed as ranks [27]

Many organizations use these qualitative approaches for preliminary risk analysis, because the simplicity of these methods can make them less complicated to understand and implement the assessment. CORAS [44], CIRA [45] are model-based methods for conducting security risk analysis using the idea of qualitative assessment. The NIST SP800-30 method [2] is also mainly qualitative because it is described as the guidelines and the processes to assess and mitigate security risks rather than a specialized method. The downside of a qualitative approach is the subjectivity of the assessors because the assessment results depend on their knowledge and experience. Another limitation with the qualitative methods is the lack of measurable detail to support cost-effective decision making for management or

to compare the associated risk assessment results. According to ISO/IEC 27005 [1], a qualitative analysis should be conducted first giving an overall indication of risk levels and major risks. Followed by assessments using actual data that can be measured mathematically or via other computational techniques.

2. Quantitative techniques

A quantitative analysis uses specific formulas and calculations to measure the value of the risk elements. The objective assessment results often require knowledge of mathematics, statistics and probability theory. The ongoing research is interested in computational models for the occurrence probability and the financial impact of security risks. The calculated impact, together with the probability, forms a quantitative risk estimation.

Quantitative methods are also known as "expected loss" analyses where the expected loss to the organization caused by security risk is used to evaluate its impact. There are three classic quantitative security risk nalysis formulas: Annual Loss Expectancy (ALE), Single Loss Expectancy (SLE), and safeguard value [46]. Factor Analysis of Information Risk (FAIR) [16] is a well-known risk assessment framework in academic research and industry. The FAIR framework integrates the FAIR taxonomy structure and quantitative reasoning algorithms to determine the interactions between risk factors and calculate the financial losses. In a different approach, [47] proposes a quantitative methodology utilizing CVSS metrics to define the risk metrics, risk metrics values and the detailed risk assessment formulas for different risk views. Quantitative methods often come with increased complexity and cost in the calculation process. There is also the importance of providing enough data to yield reliable results, such as asset value information and historical security incident data.

Due to the advantages and disadvantages of both quantitative and qualitative methods, several hybrid methods, also known as semi-quantitative methods, have been proposed. Among them, Bayesian network-based methods are receiving more attention because of the effective combination of objective and subjective perspectives (i.e. beliefs are represented by probabilistic values, allowing quantitative risk estimation results to be interpreted). A Bayesian Network (BN) is a graph-based probabilistic model for the representation of an uncertainty domain where each node corresponds to a random variable and each edge of the graph represents a conditional probability. Bayesian networks can be constructed as static or dynamic networks. The studies [35] [48] [49] use static Bayesian network to assess the risk severity following two aspects: the likelihood of a threat exploiting a vulnerability and the impact level of the vulnerability being exploited. [50] uses a dynamic Bayesian network, showing the ability to change network parameters at different points in the risk assessment process. Table II summarizes the main features of risk assessment techniques.

V. Specific web system's features

The works mentioned in Sections II, III and IV allows clarifying information about the stages, the elements and the techniques that could be used to build a security risk assessment process for web systems in general. However, such a process still needs to be refined to adapt to the tactical features of a specific web system in a given developing or operational context of the organization. In this section, features of web systems that are related to their architecture, their development process and their application domain and that need to be considered in security risk assessment are presented.

Web system architecture. In deployment and operation view, this is the skeleton describing how to instantiate the web system components and how they interact with each other. The web servers host network-associable web application modules processing the client's requests. They provide an operational environment including infrastructure, system software and platform services such as operating systems. The web systems with a large number of concurrent users might contain multiple copies mirroring web servers. One of them has the role of load balancer dealing with the scaling requirements. Other servers include database server and optional service servers (e.g. caching service, job queue service, search service) which are not directly visible to clients. These web components interact with each other through a network connection. Web servers and web applications are directly accessed by clients, so they are the most critical sources of security risk to the organization. Study [51] examines the security approaches in four case studies which are industrial and open source projects. The results recommend the adoption of security frameworks from an early stage of system development and deployment. [52] proposes an approach to improve security of web servers in IoT systems by self-monitoring vulnerabilities mechanism. The work [53] addresses the security challenges of service-oriented architecture (e.g. RESTful, Web services) and proposes measures to mitigate security risks regarding business and technical impact. Communication between the client-side web browser and the server-side web components may require the implementation of callback function calls, such as the implementation of AJAX (Asynchronous JavaScript And XML) techniques. The carelessness of the programmers in implementing these functions creates a vulnerability that allows access to

TABLE II
THE MAIN FEATURES OF RISK ASSESSMENT TECHNIQUES

Study	Technique	Hypothesis / Constraints	Contents	Outcomes
CIRA [45]	Qualitative	Stakeholders, strategies, utility factors, initial values	- Focus on the human-related risks - Multi-criteria decision analysis	Strength of stakeholders' incentives or changes in utility that generates risks
CORAS [44]	Qualitative	Asset, vulnerability, threat scenario, risk evaluation matrix, likelihood scale	- CORAS language for risk modeling based on UML models and tools - Security risk analysis is conducted in eight steps	Identify and assess potential risks for strong business and asset orientation
NIST SP800-30 [2]	Qualitative	Overall risk management in information system	- General method and complete guide for defining all aspects of an effective risk management	Identification and evaluation of assets, Identification and evaluation of threats, Safeguard selection
RRA[27]	Qualitative	Small or medium services, associated meeting, well-designed templates	- Four phases - Risk areas: confidentiality, integrity, and availability - Impact areas: reputation, productivity, and finances of the organization	Service notes, data dictionary, threat scenarios, recommendations
Bayesian-based [35], [48], [49], [50]	Quantitative	Causal relationships between risk factors, sample data	- Network structure (construction, update) - Network parameters (conditional and prior probabilities) - Bayesian inference	Integrate risk assessment results with uncertainty ratings
CVSS-based [47]	Quantitative	High level risk metrics, attack graph, CVSS metrics	- Asset and vulnerability centric model - Quantify the risks of both individual assets and the vulnerabilities at the assets	Asset and system risk metrics Product risk metrics Attack path risk metrics
FAIR [16]	Quantitative	Taxonomy of the distinct factors that constitute risk (FAIR taxonomy)	- Analyze, measure and understand cybersecurity and operational risk - Top-down risk approach: assess risks specific to their environment	The assets of business, threat actors and threat vectors, the financial impact of threats

resources via callback function calls without the necessary privileges. Study [54] proposes a framework that supports analyzing the source code of web applications to detect vulnerability in the implementation of callback functions and make suggestions to modify these functions in a more secure way. The experimental results of the framework allow detecting SQL injection attacks on web systems through complex queries.

Web system deployment process. There are many types of deployment: deploying a new web system (for the first time), replacing or upgrading new functionalities for an existing web system. Starting just after the completion of the product testing phase, the deployment process consists of 4 stages: (i) business analysis and identification of technical requirements, (ii) logical design, (iii) architectural design and (iv) implementation [49]. The deployment scenario summarizes the deployment design, deployment activities and the security requirements of the deployed web system. Study [55] supports the selection of a cloud-based web application deployment model that matches security and privacy requirements. Problems arising during the deployment process such as the selection of older versions of software, errors in the configuration of components or default user accounts will pose high security risks to the organization.

Web system application domain. Web-based systems are the basis for different business solutions from e-transport, e-health to many other e-solutions. The security risk assessment process needs to be associated with a specific business solution so that the assessment results are relevant to the context of the organization. The work [56] indicates the need for ensuring optimal security of healthcare web applications, it proposes a security risk assessment approach through adaptive neuro-fuzzy inference system during the development of web application. [57] outlines the four quantitative security risk analysis models for cloud computing systems supporting decision makers to select the suitable models regarding cost and brand of the organizations. The study [58] introduces a secure risk management approach for e-commerce web applications. The security risk management stages follow ISO/IEC 27005 and use the OWASP top 10 list as input. To assess the impact of security risks on e-commerce web systems, this study uses the FIPS 199 impact category scale [59]. Although the approach is aimed at e-commerce web systems, it does not tie the risk management process to the characteristics of these systems.

The security risk management model for e-learning systems in [60] uses the Mean Failure Cost metric to quantify security risks in terms of the losses per stakeholder (system administrator, teacher, student, and course administrator) to bear when a security incident arises. The results can also be extended to make more detailed diagnoses.

Security risk assessment for web systems. A compromised web system can be harmful in many ways, from exposing customer data to a defaced homepage that indirectly damages an organization's reputation. The OWASP Top 10 [18] provides a classification of the security risks associated with web applications. Security risk assessment for web systems also includes basic stages: (1) identifying assets and security objectives, (ii) analyzing vulnerabilities, threats, and countermeasures and (iii) assessing security risks. Web system deployment scenarios provide the necessary input to the assessment process, possibly automating part of the assessment activities, or providing data for quantitative assessment. OWASP also provides a risk assessment framework that could be integrated in the DevSecOps toolchain to help developers to write and produce secure code.

VI. Discussion

We propose a framework for linking the security risk assessment with the deployment and operation (DevOps) of web systems as shown in Figure 5. Two main stages of the ISO/IEC 27005's security risk assessment process (i.e., establish context and risk assessment) could be associated with DevOps' stages. A web system could be assessed either from the development perspective or operational perspective. From the development perspective, the associated stages are plan, test, release. From the operational perspective, the associated stages are deploy, operate, monitor. The assessment could be performed by using either a generalized approach or an in-depth approach to meet the assessment objective and the expected level of details at a given time in the associated stage. The assessment results are fed back to the same associated stage of the DevOps. This means that risk assessment is performed iteratively in the web system's life cycle. The next sections present in detail the web systems' artifacts in each stage of the mentioned security risk assessment process.

1. Establish context

In this stage, the scope and the criteria for the security risk assessment process are defined. The context of the risk assessment includes the factors that can influence the formation of a security risk such as tactical features of a specific web system in a given developing or operational context of the organization.

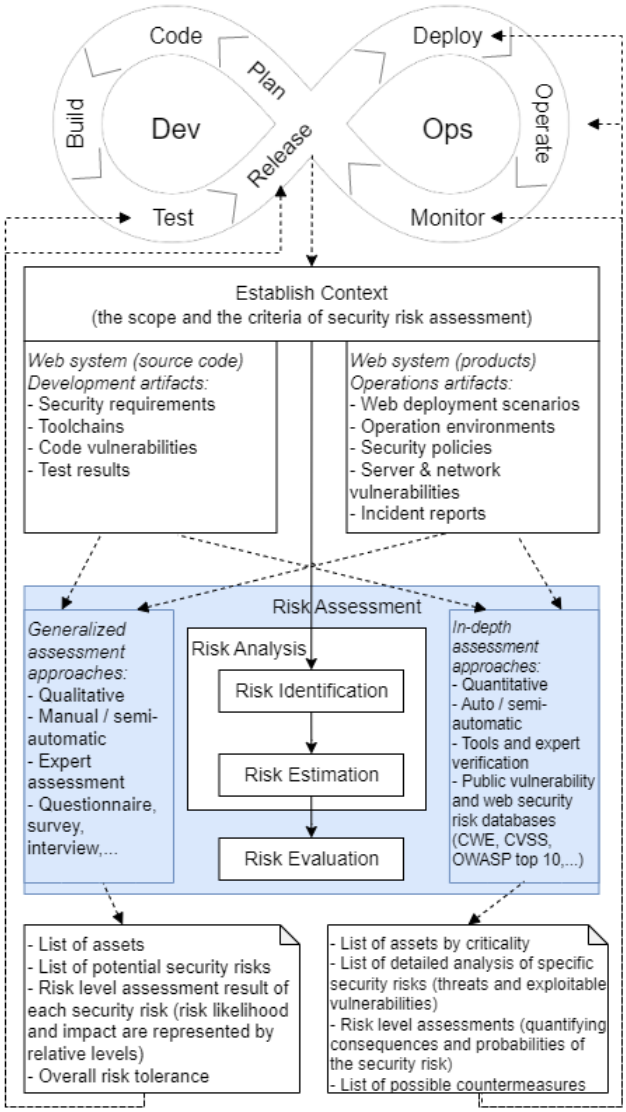

Figure 5. Security risk assessment framework for web systems

Organization-related context: Criteria relevant to the context of the organization including the value of the business process, critical levels of assets, the relationship between information security attributes and the business activities of the organization. Risk acceptance criteria are also defined for risk response in the next phase. These criteria depend on financial and organizational business objectives, security and legal policies, operating requirements and technology of the web system, and social and human factors.

Development-related context: Web systems are characterized by the source code of the web components in development. Software requirements are inputs to the development process. It includes statements about the requirements to ensure the security properties of the web system under development. The test results at the end

of the development process determine the fulfillment of these security requirements. Web component source code is constantly evolving. It is developed by diverse technologies, tools and programming languages. For example, the front-end components use css and javascript libraries, the back-end components are built on java, php, python, or other programming languages. Differences in development technology can yield different results in identifying vulnerabilities of the source code of web components. Artifacts in the web system development process that can be used to provide input for the security risk assessment phase include software requirements, development tools, source code vulnerabilities, and test results.

Deployment-related and operation-related context: Web systems are characterized by finished products operating in a given environment. An operational environment includes infrastructure, platform services and other services. Web systems can be deployed on-premises, i.e., the system is installed and executed on servers on the organization's premises, rather than at a remote site. The operating environment of web systems can also be built on top of cloud infrastructure services provided by third-party vendors. Operational vulnerabilities are identified by analyzing web components combined with operational environment information such as servers, configurations, and networks. Security incident reports during operational monitoring are also an important source to support identifying new threats or update the security risk assessments. Artifacts in the web system operation process that can be used to provide input for the security risk assessment phase include web deployment scenarios, operation environments, security policies, server and network vulnerabilities, and incident reports.

2. Risk assessment

This stage contains three steps: (1) Identify security risks, (2) Estimate potential impact and likelihood of risks, and (3) Evaluate and prioritize risks. There are two approaches with different assessment techniques. The result of the risk assessment is the likelihood and impact of the security risks, from which the risk level is determined.

Generalized assessment approaches: These are used to detect general security risks for web systems. These results can be used to develop a security risk management plan and support identifying groups of protected assets within a web system. The main input sources for assessment are expert knowledge. In addition, the goals of the high level assessment process include both speed and simplicity. Therefore, suitable techniques include qualitative assessment, manual assessment combined with semi-automatic tools and forms.

In-depth assessment approaches: There is detailed analysis of security risks that examine the attack of exploiting specific vulnerabilities of web components. The identified web attack scenarios include relationships between assets and their vulnerabilities. This result allows us to identify the weakest parts of the web system and the specific impact of security breaches. In-depth assessment can select qualitative assessment techniques combined with expert knowledge, automated tools and available vulnerability databases to reduce complexity and implementation time.

VII. Conclusion

There are diverse security risk assessment approaches today, bringing both flexibility and difficulties for organizations in choosing the proper method to assess the security risk of a given web system. This study analyzed security risk assessment methods according to the assessment process, degree of automation of assessment activities and assessment techniques. These methods are applicable to information systems in general, to web systems in particular.

From the process perspective, the selection of a standardized security risk assessment process is the important first step that enables an organization to define the stages, the activities to be performed, and the possible outcomes. An enterprise-oriented security risk assessment process can be developed in accordance with the mentioned standards to achieve compliance. However, the standards are often general and lack detailed guidance for the successful implementation of the assessment process. Therefore, the combination of standards with enterprise-oriented processes will be the solution for adapting to the context of the organization. Beside, the security risk management process is an integral part of the development and operation process of a web system. Security risks can appear at any stage in the web system's life cycle. Early detection and assessment of these risks is critical to a comprehensive security strategy of the organization. Deployment phase, where many changes occur as the system moves from the development environment to the operational environment, is an appropriate stage for performing in-depth security risk assessments.

From the implementation perspective, stages in a security risk assessment process could be performed manually or automatically. The manual assessment focuses on simplicity and coverage, suitable for initial security risk discovery. The automatic assessment is about leveraging knowledge bases and automated computations to reduce time and costs for quick and precise assessments.

From the analysis perspective, security risk assessment techniques could be divided into 2 groups: qualitative and quantitative techniques. These two groups of techniques differ in how they assign values to inputs and outputs

of risk estimation. Qualitative techniques provide relative assessments from the subjective view of the assessors. Quantitative techniques provide the calculation of the risk likelihood or risk impact that are specific numerical values. This allows the organization to use the evaluation results for comparison and improvement. The challenges with these techniques are computational power and uncertainty where probability-based techniques receive much attention.

From the system specific perspective, the results of the analysis about architectural features, deployment and operation models and application domain support the organization to determine the suitable processes and techniques for security risk assessment of web-based systems.

The proposed framework shows the security risk assessment of web based systems during its deployment and operation from all mentioned perspectives.

Further research focuses on (i) tuning the proposed framework so that the security risk assessment is conducted accordingly to detail analysis of features of web system to be assessed, and (ii) dealing with the accuracy and the uncertainty of the risk assessment results.

ACKNOWLEDGEMENT

This research is funded by Hanoi University of Science and Technology (HUST) under project number T2022-PC-045.

REFERENCES

[1] ISO, *ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management*. International Organization for Standardization, 2018.

[2] J. T. F. T. Initiative, "Guide for conducting risk assessments," *NIST Special Publication*, vol. 800-30r1, pp. 1–39, 2012.

[3] ISO, *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements*. International Organization for Standardization, 2013.

[4] H. M. Haddad *et al.*, "Asset assessment in web applications," in *2010 Seventh International Conference on Information Technology: New Generations*. IEEE, 2010, pp. 762–767.

[5] E. Wheeler, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Elsevier, 2011.

[6] M. Cova, V. Felmetsger, and G. Vigna, "Vulnerability analysis of web-based applications," in *Test and Analysis of Web Services*. Springer, 2007, pp. 363–394.

[7] I. Medeiros, N. Neves, and M. Correia, "Detecting and removing web application vulnerabilities with static analysis and data mining," *IEEE Transactions on Reliability*, vol. 65, no. 1, pp. 54–69, 2015.

[8] K. Tuma, G. Calikli, and R. Scandariato, "Threat analysis of software systems: A systematic literature review," *Journal of Systems and Software*, vol. 144, pp. 275–294, Oct. 2018.

[9] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Threat modeling-uncover security design flaws using the stride approach," *MSDN Magazine*, vol. 11, pp. 68–75, 2006.

[10] J.-z. Guan, M.-t. Lei, X.-l. Zhu, and J.-y. Liu, "Knowledge-based information security risk assessment method," *The Journal of China Universities of Posts and Telecommunications*, vol. 20, pp. 60–63, Dec. 2013.

[11] M. U. Aksu, M. H. Dilek, E. I. Tatli, K. Bicakci, H. I. Dirik, M. U. 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)*. IEEE, oct 2017.

[12] A. Behnia, "A Survey of Information Security Risk Analysis Methods," *The Smart Computing Review*, Feb. 2012.

[13] M. A. Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency," *Procedia Computer Science*, vol. 161, pp. 1206–1215, 2019.

[14] S. Tweneboah-Koduah and W. J. Buchanan, "Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study," *The Computer Journal*, vol. 61, no. 9, pp. 1389–1406, Sep. 2018.

[15] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, *Introduction to the OCTAVE Approach*. Carnegie-Mellon University, Software Engineering Institute, 2003.

[16] J. Freund and J. Jones, *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann, 2014.

[17] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, 2018.

[18] D. Wichers and J. Williams, "OWASP top-10 2017," *OWASP Foundation*, vol. 3, p. 4, 2017.

[19] ISO, "ISO/IEC/IEEE International Standard - Systems and software engineering – System life cycle processes," *ISO/IEC/IEEE 15288 First edition 2015-05-15*, pp. 1–118, 2015.

[20] R. Ross, M. McEvilley, and J. Oren, "Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," *Gaithersburg: National Institute of Standards and Technology*, vol. 800-160v1, pp. 1–242, 2016.

[21] J. T. F. T. Initiative, "Risk Management Framework for Information Systems and Organizations," *NIST Special Publication*, vol. 800-37r2, pp. 1–164, 2018.

[22] K. Gene, H. Jez, D. Patrick, W. John, and F. Nicole, *The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations*. IT Revolution Press, 2018.

[23] M. Felderer and I. Schieferdecker, "A taxonomy of risk-based testing," *International Journal on Software Tools for Technology Transfer*, vol. 16, no. 5, pp. 559–568, Oct. 2014.

[24] J. Großmann, M. Felderer, J. Viehmann, and I. Schieferdecker, "A taxonomy to assess and tailor risk-based testing in recent testing standards," *IEEE Software*, vol. 37, no. 1, pp. 40–49, 2019.

[25] A. Masood and J. Java, "Static analysis for web service security-tools & techniques for a secure development life cycle," in *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE, 2015, pp. 1–6.

[26] B. Subedi, A. Alsadoon, P. Prasad, and A. Elchouemi, "Secure paradigm for web application development," in *2016 15th RoEduNet Conference: Networking in Education and Research*. IEEE, 2016, pp. 1–6.

[27] J. Vehent, *Securing DevOps: security in the cloud*. Simon and Schuster, 2018.

[28] H. I. Kure, S. Islam, and M. A. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Applied Sciences*, vol. 8, no. 6, p. 898, 2018.

[29] O. Kolisnichenko, M. Kolomytsev, and S. Nosok, "Software

security risk management in devops methodology," *Theoretical and Applied Cybersecurity*, vol. 3, no. 1, 2021.

[30] N. Wilde, B. Eddy, K. Patel, N. Cooper, V. Gamboa, B. Mishra, and K. Shah, "Security for devops deployment processes: Defenses risks research directions," *International Journal of Software Engineering & Applications*, vol. 7, no. 6, pp. 01–16, 2016.

[31] FIRST, *Common Vulnerability Scoring System version 3.1*. FIRST Org, Inc., 2019.

[32] J. A. Kupsch and B. P. Miller, "Manual vs. automated vulnerability assessment: A case study," in *First International Workshop on Managing Insider Security Threats (MIST)*, 2009, pp. 83–97.

[33] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, Jan. 2012.

[34] X. Wu, Y. Fu, and J. Wang, "Information systems security risk assessment on improved fuzzy AHP," in *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*. Sanya, China: IEEE, Aug. 2009, pp. 365–369.

[35] M. Khosravi-Farmad and A. Ghaemi-Bafghi, "Bayesian Decision Network-Based Security Risk Management Framework," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 1794–1819, 2020.

[36] A. P. Henriques de Gusmão, M. Mendonça Silva, T. Poleto, L. Camara e Silva, and A. P. Cabral Seixas Costa, "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory," *International Journal of Information Management*, vol. 43, pp. 248–260, Dec. 2018.

[37] C. Y. Alonge, O. T. Arogundade, K. Adesemowo, F. T. Ibrahalu, O. J. Adeniran, and A. M. Mustapha, "Information asset classification and labelling model using fuzzy approach for effective security risk assessment," in *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*. IEEE, 2020, pp. 1–7.

[38] I. Loloei, H. R. Shahriari, and A. Sadeghi, "A model for asset valuation in security risk analysis regarding assets' dependencies," in *20th Iranian Conference on Electrical Engineering (ICEE2012)*. IEEE, 2012, pp. 763–768.

[39] S.-C. Cha, L.-T. Liu, and B.-C. Yu, "Process-oriented approach for validating asset value for evaluating information security risk," in *2009 International Conference on Computational Science and Engineering*, vol. 3. IEEE, 2009, pp. 379–385.

[40] P. Kamongi, M. Gomathisankaran, and K. Kavi, "Nemesis: Automated architecture for threat modeling and risk assessment for cloud computing," in *Proc. 6th ASE International Conference on Privacy, Security, Risk and Trust (PASSAT)*, 2014.

[41] Y.-j. Zhang, P. Liao, K.-z. Huang, and Y.-l. Liu, "An automatic approach for scoring vulnerabilities in risk assessment," in *2nd International Conference on Electrical and Electronic Engineering (EEE 2019)*. Atlantis Press, 2019, pp. 256–261.

[42] I. H. Elifoglu, I. Abel, and Ö. Taşseven, "Minimizing insider threat risk with behavioral monitoring," *Review of business*, vol. 38, no. 2, pp. 61–73, 2018.

[43] M. Rizwan, A. Shabbir, A. R. Javed, G. Srivastava, T. R. Gadekallu, M. Shabir, and M. A. Hassan, "Risk monitoring strategy for confidentiality of healthcare information," *Computers and Electrical Engineering*, vol. 100, p. 107833, 2022.

[44] F. Den Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen, "Model-based security analysis in seven steps—a guided tour to the CORAS method," *BT Technology Journal*, vol. 25, no. 1, pp. 101–117, 2007.

[45] L. Rajbhandari and E. Snekkenes, "Using the conflicting incentives risk analysis method," in *IFIP International Information Security Conference*. Springer, 2013, pp. 315–329.

[46] D. Landoll, *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press, 2021.

[47] M. U. Aksu, M. H. Dilek, E. İ. Tatlı, K. Bicakci, H. I. Dirik, M. U. Demirezen, and T. Aykır, "A quantitative CVSS-based cyber security risk assessment methodology for IT systems," in *2017 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2017, pp. 1–8.

[48] M. Frigault, L. Wang, S. Jajodia, and A. Singhal, "Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks," in *Network Security Metrics*. The Capital Region of Denmark: Springer Charm, 2017, pp. 1–23.

[49] V. T. H. Giang and N. M. Tuan, "Application of Bayesian network in risk assessment for website deployment scenarios," *Journal of Science and Technology on Information security*, vol. 2, no. 14, pp. 3–16, Jan. 2022.

[50] J. Wang, K. Fan, W. Mo, and D. Xu, "A method for information security risk assessment based on the dynamic bayesian network," in *2016 International Conference on Networking and Network Applications (NaNA)*. Hakodate, Japan: IEEE, Jul. 2016, pp. 279–283.

[51] H. Cervantes, R. Kazman, J. Ryoo, D. Choi, and D. Jang, "Architectural approaches to security: Four case studies," *Computer*, vol. 49, no. 11, pp. 60–67, 2016.

[52] L. Song and M. García-Valls, "Improving security of web servers in critical IoT systems through self-monitoring of vulnerabilities," *Sensors*, vol. 22, no. 13, p. 5004, 2022.

[53] C. E. Cirnu, C. I. Rotună, A. V. Vevera, and R. Boncea, "Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture," *Stud. Inform. Control*, vol. 27, no. 3, pp. 359–368, 2018.

[54] K. Kubota, W. K. K. Oo, and H. Koide, "A new feature to secure web applications," in *2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW)*. IEEE, 2020, pp. 334–340.

[55] C. Kalloniatis, H. Mouratidis, and S. Islam, "Evaluating cloud deployment scenarios based on security and privacy requirements," *Requirements Engineering*, vol. 18, no. 4, pp. 299–319, 2013.

[56] J. Kaur, A. I. Khan, Y. B. Abushark, M. M. Alam, S. A. Khan, A. Agrawal, R. Kumar, and R. A. Khan, "Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: A design perspective," *Risk Management and Healthcare Policy*, vol. 13, p. 355, 2020.

[57] M. Jouini and L. B. A. Rabai, "Comparative study of information security risk assessment models for cloud computing systems," *Procedia Computer Science*, vol. 83, pp. 1084–1089, 2016.

[58] K.-S. Lin, "Online transaction security risk management for e-commerce web applications," *American Journal of Operations Management and Information Systems*, vol. 2, no. 1, pp. 5–14, 2017.

[59] F. Pub, "Standards for security categorization of federal information and information systems," *NIST FIPS*, vol. 199, 2004.

[60] N. Rjaibi, L. B. A. Rabai, A. B. Aissa, and M. Louadi, "Cyber security measurement in depth for e-learning systems," *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, vol. 2, no. 11, pp. 107–120, 2012.

Manh-Tuan Nguyen is a lecturer of the School of Information and Communication Technology, Hanoi University of Technology. He obtained his Master's Degree in Information Technology in 2016 and his Information Technology Engineering degree in 2007 at Hanoi University of Science and Technology. His research interests focus on web system development and security risk assessment for information systems.
Email: tuannm@soict.hust.edu.vn

Thi-Huong-Giang Vu is a senior lecturer of the School of Information and Communication Technology, Hanoi University of Technology. She obtained her PhD in Information Technology in 2010 at Grenoble INP, France. She obtained her Master's Degree in Information Technology in 2003 and her Information Technology Engineering degree in 2001 at Hanoi University of Science and Technology. She contributes to the construction of ERP software. She conducts fundamental and applied research activities in software project management and non-functional aspects of software such as security and risk management.
Email: giangvth@soict.hust.edu.vn