I. J. Computer Network and Information Security, **2020, 4, 30-40**
Published Online August 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2020.04.03

Information Technology Risk Management Using ISO 31000 Based on ISSAF Framework Penetration Testing (Case Study: Election Commission of X City)

I Gede Ary Suta Sanjaya
Department of Information Technology, Faculty of Engineering, Universitas Udayana, Indonesia
E-mail: suta.arry@gmail.com

Gusti Made Arya Sasmita and Dewa Made Sri Arsa
Department of Information Technology, Faculty of Engineering, Universitas Udayana, Indonesia
E-mail: aryasasmita@it.unud.ac.id, dewamsa@unud.ac.id

Received: 03 April 2020; Accepted: 02 May 2020; Published: 08 August 2020

Abstract: Election Commission of X City is an institution that serves as the organizer of elections in the X City, which has a website as a medium in the delivery of information to the public and as a medium for the management and structuring of voter data in the domicile of X City. As a website that stores sensitive data, it is necessary to have risk management aimed at improving the security aspects of the website of Election Commission of X City. The Information System Security Assessment Framework (ISSAF) is a penetration testing standard used to test website resilience, with nine stages of attack testing which has several advantages over existing security controls against threats and security gaps, and serves as a bridge between technical and managerial views of penetration testing by applying the necessary controls on both aspects. Penetration testing is carried out to find security holes on the website, which can then be used for assessment on ISO 31000 risk management which includes the stages of risk identification, risk analysis, and risk evaluation. The main findings of this study are testing a combination of penetration testing using the ISSAF framework and ISO 31000 risk management to obtain the security risks posed by a website. Based on this research, obtained the results that there are 18 security gaps from penetration testing, which based on ISO 31000 risk management assessment there are two types of security risks with high level, eight risks of medium level security vulnerabilities, and eight risks of security vulnerability with low levels. Some recommendations are given to overcome the risk of gaps found on the website.

Index Terms: ISO 31000 Framework, ISSAF Framework, Penetration Testing, Risk Management, Website.

1. Introduction

The use of the website as an information system service has been widely applied by agencies in Indonesia, one of which is the Election Commission of X City. Election Commission of X City is an institution that has the duty to hold elections in X City. The website has a website as a medium for delivering information to the public and as a media for managing and organizing voter data at the domicile of X City. The website stores data with 421,789 voter data, 412 files in the data bank, and 849 data about the news. These data are highly crucial and cannot be published to public, so it is vulnerable from network or website attacks. For an example case that has quite an impact on the website is a deface attack carried out on July 22, 2014 (published on media) and the latest attack occurred in December 2019. Based on these problems, it is necessary to prevent cyber-attacks that can harm website X. One of the prevention efforts that can be done is to identify security holes and treat security holes against dangerous security risks.

Security holes on a website can be obtained through 2 ways, namely vulnerability assessment and penetration testing [1]. Vulnerability assessment is the process of scanning the system or software or a network to find out the weakness and loophole in that. These loopholes can provide backdoor to attacker to attack the victim. A system may have access control vulnerability, Boundary condition vulnerability, Input validation vulnerability, Authentication Vulnerabilities, Configuration Weakness Vulnerabilities, and Exception Handling Vulnerabilities etc. Penetration testing is the next step after vulnerability assessment. Penetration testing is to try to exploit the system in authorized manner to find out the possible exploits in the system. In penetration testing, the tester has authority to do penetration testing and he intently exploit the system and find out possible exploits. Comparing both ways, vulnerability assessments search systems for known vulnerabilities, which penetration test attempts to actively exploit weaknesses in an environment. Both are complimentary strategies to each other and proactive. But it is recommended to use penetration testing regularly [2].

Several methods can be used to do penetration testing. The Information System Security Assessment Framework (ISSAF) is a penetration testing framework that has several advantages of security control, which has a clear and intuitive structure that guides testers through complex steps [3]. This methodology explains the optimal penetration testing process to help testers carry out testing completely and correctly, avoiding errors that are commonly associated with randomly chosen attack strategies [3]. However, the results of penetration testing are only in the form of security loopholes on the website being tested, without analyzing the level of risk and impact that could result from such a vulnerability. Overcoming this, it is necessary to have a risk management of website security, which is assessed based on security loopholes on the website. ISO 31000 provides a generic guide, this standard is not intended to homogenize risk management across organizations, but is intended to provide a supporting standard for the application of risk management in an effort to guarantee the achievement of organizational goals [4].

Management of security risks on website information systems need to be done to determine the level of security vulnerability of a system and preventive actions that can be taken. In this study, we proposed a two stages assessment method. On the first stage we analyze the weakness of the website using penetration testing. We use The Information System Security Assessment Framework (ISSAF) as penetration testing method because it has several advantages over existing security controls against threats and security gaps, and serves as a bridge between technical and managerial views of penetration testing by applying the necessary controls on both aspects. On the second stage, we use ISO 31000 Framework as website's risk management. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

The purpose of this study was to determine the level of security risk of Election Commission of X City's site, which obtained through the ISSAF framework penetration test with an assessment using ISO 31000 risk management. The research focuses on the issuing framework through ISO 31000 risk management, with recommendations based on test results which is a limitation of this research. With this research, we are expected to be able to improve security on Election Commission of X City's site to prevent cyber-attacks by outsiders

This paper written as follows. On section II, we provide supporting theories related to our study. Then, we present our methodology on section III. The result of the assessment and recommendation that can be given will be present on section IV. Furthermore, we conclude our findings in section V.

2. Literature Study

2.1. Penetration Testing

The application of security systems aims to overcome all problems and constraints, both technically and non-technically which can affect the performance of the system such as availability, confidentiality and integrity factors so that the level of security [5]. Penetration testing is an emerging method to test the vulnerabilities in the system, identification of poor and improper system configuration, hardware & software flaws and operational weaknesses in the process or technical countermeasures [6]. Penetration testing is a comprehensive method for testing a complete, integrated, operational, and trusted computing base consisting of hardware, software, and the people involved in it [7]. Penetration testing is increasingly used by organizations to assure the security of Information systems and services, so that security weaknesses can be fixed before they get exposed [8]. Penetration testing process approach audit web application security, also can be used to secure associated layers and includes to audit system for finding vulnerabilities, which may be existing in the system [9]. Penetration testing helps the developers to find security flaws in their application and maintain their application secure. Performing real-time tests on web applications has proven to be helpful in hardening the security of the website [10]. The main purpose of penetration testing is to identify system security weaknesses. In addition, it can also be used to test organizational security policies, awareness of organizational employees on security requirements, and the ability of organizations to identify and respond to security incidents [4, 5]. Penetration testing process consists of information gathering, identifying penetration points, and reporting the results of testing [9]. Implementation of security testing with the penetration testing method is recommended to use related framework so that the stages of attack carried out towards the system have standardization that has been developed and recognized by certain organizations that are experts in the field of security testing [12]. Penetration testing provides detailed information about actual security threats, which can be exploited if covered by the organization's security doctrine and process. This will help the organization to identify quickly and accurately, the potential vulnerability and real vulnerability [13]. By providing the information needed to effectively and efficiently isolate and prioritize vulnerabilities, penetration testing can help refine and change test organization configurations or patches to proactively eliminate identified risks.

2.2. Risk Management

Risk management is the process of carrying out management activities to cope with the emergence of risks, both faced by the company and those faced by the community. So it can be concluded that the management functions that are carried out to cope with risk include the process of managing, measuring and assessing risk [14]. Proper information system risk management makes it possible to reduce the frequency and intensity of risk-related incidents in the system. Incidents include bad events that have occurred in the operational parts of information systems and information assets [15]. The ISO 31000 framework gives only generic standard guidance. Therefore, to implement it the company must fit the implementation with their needs and circumstances [16]. Some functions of information technology risk management are providing guidance to help executives and management ask key questions; help save time, money and effort with tools to deal with business risks; integrating IT management related to business risk into overall enterprise risk management; help leadership understand company risk and risk tolerance; provide practical guidance driven by the leadership needs of companies throughout the world.

2.3. ISSAF Framework

The Information System Security Assessment Framework (ISSAF) is a penetration testing framework developed by OISSG (Open Information System Security Group). The ISSAF penetration testing methodology is designed to evaluate network, system and application control [17]. ISSAF Framework explains the optimal penetration testing process to help testers carry out testing completely and correctly, avoiding mistakes that are generally associated with randomly chosen attack strategies [18]. There are three steps in ISSAF framework; planing and preparation, assessment, and reporting, clean up, and destroy artifacts. Planning and preparation phases consist of the steps to exchange initial information, plan and prepare for the test. Then, in the assessment process, we have to follow nine steps as shown in Fig. 1.

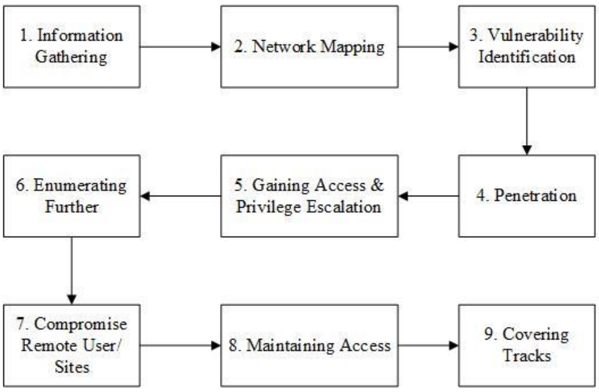

Fig.1. ISSAF Framework Methodology

The assessment phase begins with Information Gathering, which is the stage of gathering general information about the target website. The second stage is Network Mapping, which is the stage of gathering specific information about the target website network. The third stage is Vulnerability Identification, which is the stage of scanning vulnerabilities on the target website. The fourth stage is Penetration, which is an attack simulation stage that aims to find security holes on the website. The fifth stage is Gaining Access and Privilege Escalation, which is the stage of testing access into the target system. The sixth stage is Enumerating Further, which is the stage of finding information related to passwords from the target website. The seventh stage is Compromise Remote User / Sites, which is the stage for remote to the target system. The eighth stage is the stage of planting a backdoor into the target system. The last stage is Covering Tracks which is the stage of removing the attack log that has been done on the target system. After penetration testing is done, next phase is reporting, clean up and destroying artifacts. In this phase, all stored information on the tested systems should be removed, and reporting of test results is carried out.

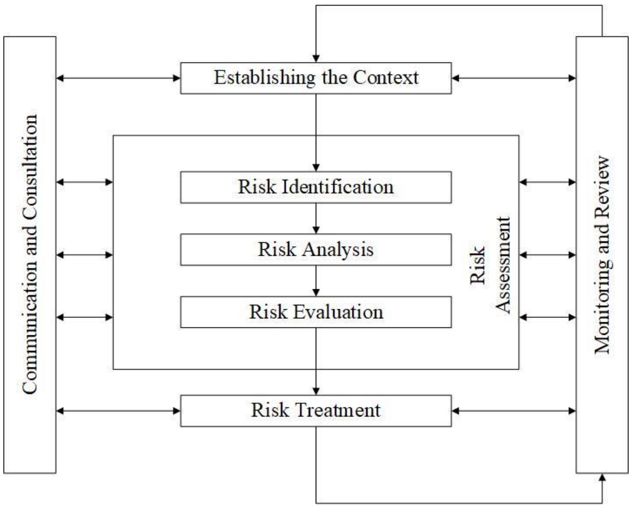

Fig.2. ISO 31000 Risk Management Process

2.4. ISO 31000 Framework

The ISO 31000 Risk Management Standard is one of the risk management standards which is a family of international standards for implementing risk management guidelines issued by the International Organization for Standardization. The standard, published on 13 November 2009, is a development of the AS / NZS 4360: 2004 standard issued by the Australian Standards. Like most other ISO management standards, ISO 31000 provides a structured framework that is intended to meet the needs of all types of organizations or situations [11, 12]. One thing that distinguishes ISO 31000 from other risk management standards is that the ISO 31000 perspective is broader and more conceptual than the others. This is indicated by the existence of a risk management framework which is an implementation of quality management principles and is known as "Plan-Do-Check-Action" [21]. ISO 31000 risk management contains 5 steps which can be seen in Fig 2. Those activities are communication and consultation, establish the context, risk assessment, risk treatment, and monitoring and review [12, 14]. More details about the ISO 31000 risk management process are as follows:

A. Communication and Consultation

This process runs internally within organizations, divisions, and business units or externally aimed at external stakeholders.

B. Establish the Context

Establishing context aims to identify and disclose organizational goals, the environment in which the objectives are to be achieved, stakeholders concerned, and the diversity of risk criteria, where these will help reveal and assess the nature and complexity of risk.

C. Risk Assessment

Risk assessment consists of risk identification, risk analysis, and risk evaluation. Risk identification is identifying what risks can affect the achievement of organizational goals. Risk analysis, namely analyzing the likelihood and impact of the risks that have been identified. Risk evaluation is comparing the results of risk analysis with risk criteria to determine how risk management will be applied.

D. Risk Treatment

Risk treatment is an effort to choose prevention that can reduce or negate the impact of and the likelihood of the risk occurring, then apply the choice

E. Monitoring and Review

Monitoring and Review is part of risk management that ensures that all stages of the process and risk management function are running well [9].

3. Research Metodology

The flow of this research includes literature study, penetration testing and risk management on the Election Commission of X City’s site, as well as providing recommendations based on test results as shown in Fig. 3.

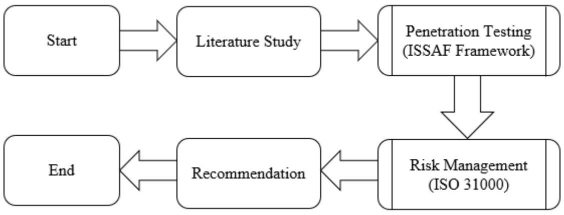
Start
Literature Study
Penetration Testing (ISSAF Framework)
Risk Management (ISO 31000)
Recommendation
End

Fig.3. Research Progress Diagram

Fig. 3 is the stages carried out in the study. Fig. 3 shows the stages of research, which started with the study of literature, with the aim of learning attack techniques on the testing to be carried out as well as risk management on the Election Commission of X City's site. The next step is to do penetration testing, using the ISSAF Framework. The purpose of this test is to obtain security loopholes, so that later it will become a security risk on Election Commission of X City's site. After conducting the penetration testing stage, the next step is to carry out risk management using the ISO 31000 framework on Election Commission of X City's site, based on the results of the previous penetration testing. The purpose of risk management is to determine the level of risk that has been identified, and know the dangers and impacts of the risk so that later it can be given treatment to reduce or overcome the risk. The last stage of this research is the provision of recommendations which is the purpose of this study. The recommendations given are based on the results of risk management that have been carried out, so that treatment can be carried out on these risks.

In penetration testing using the ISSAF Framework, there are four stages of testing, since the permits granted by the related parties only reach the penetration stage. Meanwhile, the sub stages of penetration testing using the ISSAF Framework include four stages which can be seen in the Fig. 4.

Fig. 4 shows stages of penetration testing conducted on research based on ISSAF Framework. Penetration testing begins with the information gathering stage, where this stage aims to gather information in general on Election Commission of X City's site. The second stage is the network mapping stage, which is the information gathering stage, but specifically regarding network mapping on Election Commission of X City's site. The third stage is vulnerability identification, which is the stage of scanning for vulnerabilities using scanning tools to obtain vulnerabilities on Election Commission of X City's site. The last stage is the penetration stage. This stage is the simulation stage of the attack on Election Commission of X City's site through the Cross-Site Scripting and SQL Injection attacks that aim to find security holes on Election Commission of X City's site.

After conducting penetration testing, the risk management process is then carried out using ISO 31000. Meanwhile, the sub stages of risk management using the ISO 31000 Framework include three stages which include risk identification, risk analysis, risk evaluation, which can be seen in the Fig. 5. In the risk management process using ISO 31000, the stage begins with risk identification, which is the stage of identifying the risks contained on Election Commission of X City's site by knowing the description of the risks and impacts of the risks obtained. Meanwhile, the results of penetration testing conducted previously will be a security risk that will be identified at the risk identification stage. The next stage is the risk analysis stage, which is the stage of determining the likelihood and impact value of the identified risks. The last stage in risk management is the risk evaluation stage, which is the stage of determining the level of risk based on the product of the likelihood value and the impact value of a risk.

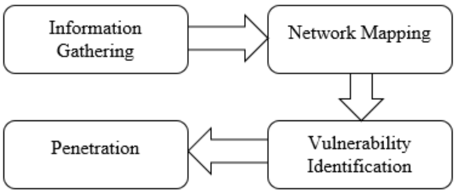

Fig.4. Penetration Testing Progress Diagram

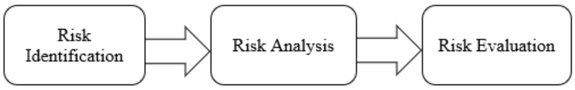

Fig.5. Risk Management Progress Diagram

4. Experiments and Result

4.1. Experiment Setup

In this study, there were two stages: penetration testing and risk management. This aims to obtain a security hole on the website that will become a risk, so that later it can be done with the handling of security risks on Election

Commission of X City's site. In the penetration testing phase using the ISSAF framework, this study uses the Windows 10 and Kali Linux operating systems, and several penetration tools as software requirements. The process of risk management is based on ISO 31000.

4.2. Penetration Testing using ISSAF Framework

The stages used based on the ISSAF framework such as Information Gathering, Network Mapping, Vulnerability Identification, and Penetration stages. Information gathering is the stage where information is collected about the website to be tested. The result of Information Gathering stage can be seen in the Table 1.

Table 1. Information Gathering Test Result

Content	Tools	Result
Locate the target web presence	Whois Domain	✓
Find Out domain registration info and IP block owned	Whois Domain	X
Check for the Authoritative Name Servers	Whois Domain	X
Check for Reverse DNS lookup presence	Dig	✓
Check for Reverse IP lookup presence	Reverse IP Lookup Scanner	✓
Check Spam/ Attackers databases lookup	Spamhaus, Spamcom	X
Check to change whois information	Whois Domain	X
Search System/Network Survey Sites	Netcraft	✓
Search on Internet Relay Chat	-	X
Search Underground Sites	NMap	✓

Table 1 shows that there are 10 types of information that collected on Information Gathering stages. Based on Table 1, there are five information that was successfully obtained and five information that failed to be obtained. information collected at this stage is general information about the website which can later be used as information in carrying out attacks.

Network Mapping is the stage of taking specific information about the network from the previous section taken and expanded to produce a network topology that is possible for the target. The result of Network Mapping stage can be seen in the Table 2.

Table 2. Network Mapping Test Result

Content	Tools	Result
Identify Live Host	NMap	✓
TCP Port Scanning	NMap	✓
UDP Port Scanning	NMap	X
Banner Grabbing	Netcat	X
ARP Discovery	Arping	X
Identify Perimeter Network (Tracerouting)	Traceroute	X
Perform FIN/ ACK Scan	NMap	✓

Table 2 shows that there are seven types of information that collected on Network Mapping stages. Based on Table 2, there are three types of information that can be obtained based on the tools used at the Network Mapping stage. In testing, all TCP ports on the website are open, different from UDP ports that have been closed as a whole. This is a loophole that is quite vulnerable for outsiders to do hacking.

Vulnerability Identification is a stage of vulnerability scanning performed using a specific vulnerability scan tools, where in this study using the Vega Vulnerability Scanner. The test was conducted on three domains which included one main domain and two subdomains related to Election Commission of X City's site. The result of Vulnerability Identification stage using Vega can be seen in the Table 2.

Table 3 shows that there are three domains regarding the Election Commission of X City's site which include the main website, subdomain *datapemilih* and *bankdata*. Based on the results of the scan, there are five high level vulnerabilities, two medium level vulnerabilities, and one low level vulnerability.

Penetration is the stage where the testers carry out a series of types of attacks on the target website. In this test, two types of attacks include Cross-Site Scripting and SQL Injection and tested on the main domain and two subdomains that are related to the Election Commission of X City's site. Result can be seen in Table 4.

Table 3. Vulnerability Identification Test Result

Domain	Vulnerability	Level
xyz.go.id/	Session Cookie Without Secure Flag	High
	Directory Listing Detected	Low
datapemilih.xyz.go.id/	Session Cookie Without Secure Flag	High
	Local Filesystem Path Found	Medium
bankdata.xyz.go.id/	Session Cookie Without Secure Flag	High
	Shell Injection Vulnerability	High
	SQL Injection Vulnerability	High
	Local Filesystem Path Found	Medium

Table 4. Penetration Test Result

Domain	Attack Method	Vulnerability Location	Result
xyz.go.id/	XSS	Input Form “No. Identitas/ KK” on homepage	✓
	SQL Injection	-	X
datapemilih.xyz.go.id/	XSS	-	X
	SQL Injection	datapemilih.xyz. go.id// home /get_warga/ 51xxx12101xxxxxx/	✓
bankdata.xyz.go.id/	XSS	Input Form “Kata Kunci”	✓
	SQL Injection	-	X

Table 4 shows that on the site's main domain, a cross-site scripting attack was successfully carried out on the "*No. Identitas/ KK*" input form on the main page. Similar to *bankdata* subdomain, a Cross-Site Scripting attack was successfully carried out on the "*Kata Kunci*" input. In the *datapemilih* subdomain, the SQL Injection attack was successfully carried out, by adding the injection query to the location of the vulnerability based on Table 4.

4.3. Risk Management using ISO 31000

Risk management is carried out through stages including risk identification, risk analysis, and risk evaluation. The security gap that has been obtained at the next stage of penetration testing will be used as an identified risk. Table 5 shows the risks that have been obtained based on the results of penetration testing using the ISSAF Framework, along with descriptions and impacts of these risks. The identified risks are further analyzed by determining the likelihood and impact value of each risk based on predetermined criteria. ISO 31000 determines that the risk assessment in Risk Analysis is carried out by giving a value of 1-5 in the likelihood value (frequency of occurrence of risk) and impact (the impact caused by risk). The likelihood and impact criteria used for the analysis can be seen in Table 6 and Table 7. Table 6 shows the criteria for each likelihood value that will be assigned to each risk. It can be seen that the likelihood assessment is divided into rare, impossible, possible, likely, and almost certain criteria.

Table 7 shows the criteria for each impact value that will be assigned to each risk. It can be seen that the likelihood assessment is divided into insignificant, minor, moderate, major, and catastrophic criteria.

Next, the risks that have been identified will be given a value of likelihood and impact value. The grading of each risk is done by brainstorming the website manager of Election Commission of X City based on the situation and environmental conditions at Election Commission of X City, attacks that have occurred before, and the results of literature that has been done about the impact that will be caused at any risk. The result of likelihood and impact value for each risk are shown in Table 8.

Table 5. Risk Identification Result Table

Risk Code	Risk Source	Risk Description	Impact
R1	Check for Reverse DNS lookup presence	Information regarding the website IP and domain hosting used was successfully obtained	Attackers can obtain an IP from the website and use it for further attacks and gathering information about the hosting service used
R2	Check for Reverse IP lookup presence	Information about the website domain and subdomains relating to the main website was successfully obtained	Attackers can find out other domains (subdomains) related to the website, both subdomains that are used for users and subdomains that are confidential
R3	Search System/ Network Survey Sites	Information regarding the target IP, operating system and web server used was successfully obtained	Attackers can obtain the website IP and information about the operating system and web server used. This information is important enough for the attacker to know the scope of the attack to be determined.
R4	Search Underground Sites	Information about opening FTP and telnet ports	The attacker gets information about the FTP and telnet loopholes so that further attacks can be carried out.
R5	Identify Live Host	Obtained information about the hosts connected to the website.	Attackers can limit the number of systems that must be tested on the website
R6	TCP Port Scanning	All TCP ports on the website are open	Attackers can take advantage of all open port loopholes to carry out various types of attacks on the system and the website server
R7	Perform FIN/ ACK Scan	Filtered TCP packets that were tested were trying to send to several open ports on the website	Attackers can find out information about the existence of a firewall by utilizing the FIN / ACK gap. The process is done by sending a TCP packet and see whether the shipment is filtered or not.
R8	Session Cookie Without Secure Flag	There is no security on the Session cookie website of the so information on ci_session can be obtained easily	Attackers can obtain ci_session on the website. Session cookies are authenticating credentials. Attackers who get it can get unauthorized access to the target web application
R9	Directory Listing Detected	The directory on the website can be seen by accessing /public and /uploads on the website	File location in /public and /upload directories. However, some folders have been granted security in the form of access, so the attacker cannot open the contents of the folder in the / public or upload directory
R10	Local Filesystem Path Found	There is a vulnerability that is the possibility of getting a file system path, which is open in the URL / home/tambahdata/ and /home/get_data_ model /	Attackers can utilize file system path information by looking at the contents of all file directories on the website
R11	Shell Injection Vulnerability	Vulnerability to shell injection attacks can be obtained through the POST method with the id_category parameter in the URL bankdata / search	Attackers can exploit shell injection security holes by running commands on the website server. Exploitation obtained based on shell injection vulnerability can lead to unauthorized remote execution.
R12	SQL Injection Testing	The SQL Injection attack test was successfully carried out on the website	Attackers can exploit SQL Injection loopholes by retrieving important information in the database, or running queries that can endanger data in the database
R13	Cross-Site Scripting (XSS) Testing	Testing of the XSS attack was successfully carried out on the website	Attackers can exploit XSS loopholes to obtain cookies on the website user account (administrator) and use the script execution for manipulation of the website.

Table 6. Likelihood Criteria Table

Likelihood		Description
Rating	Criteria	
1	Rare	Almost never happens
2	Unlikely	Possible but rare
3	Possible	It might happen sometimes
4	Likely	Most likely to occur (often)
5	Almost Certain	Almost always happens

Table 7. Impact Criteria Table

Impact		Description
Rating	Criteria	
1	Insignificant	General information is obtained, does not cause damage to system security
2	Minor	Information about system security is obtained but has no impact on system damage and leakage of sensitive data
3	Moderate	Some sensitive data is obtained, security holes for unauthorized access are difficult to obtain, and have no impact on system damage
4	Major	Some sensitive data is obtained, security holes for unauthorized access are easily obtained, causing little damage to the system
5	Catastrophic	All sensitive data is obtained, most systems can be damaged so that it interferes with system information services

Table 8. Risk Analysis Result Table

Risk Code	Likelihood	Impact
R1	Possible (3)	Insignificant (1)
R2	Unlikely (2)	Insignificant (1)
R3	Possible (3)	Minor (2)
R4	Rare (1)	Minor (2)
R5	Rare (1)	Insignificant (1)
R6	Possible (3)	Minor (2)
R7	Unlikely (2)	Minor (2)
R8	Possible (3)	Moderate (3)
R9	Unlikely (2)	Minor (2)
R10	Unlikely (2)	Moderate (3)
R11	Possible (3)	Moderate (3)
R12	Almost Certain (5)	Major (4)
R13	Almost Certain (5)	Major (4)

Table 8 shows the likelihood and impact values that have been assigned to each identified risk. Determination of likelihood and impact criteria as shown in Table 6 and Table 7 is done based on agency conditions, environment, and literature in previous studies.

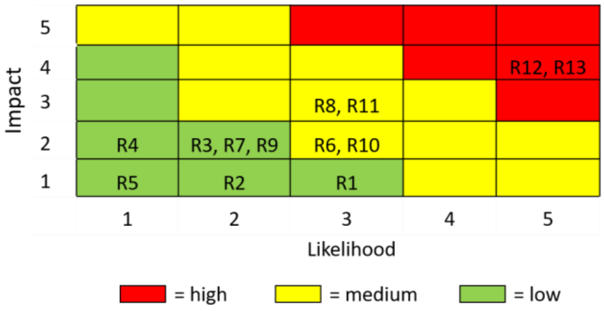

Fig.6. Risk Evaluation Matrix Result

Risk Evaluation stage is the stage of determining the level of risk vulnerability based on the results of a Risk Analysis conducted at the previous stage. Determination of risk levels is based on a risk matrix that refers to the ISO 31000 standard. Risk levels are divided into three types which include high level, medium level, and low level. The results of the risk evaluation can be seen in Fig. 6. Determination of the level of risk is done by multiplying the likelihood value with the impact value, where the likelihood value and the impact value have been obtained previously at the Risk Analysis stage. The results of the multiplication of the likelihood value and the impact value are mapped to the matrix based on Fig. 6, so obtained that there are two risks with a high level, four risks with a medium level, and seven risks with a low level.

After obtaining the risk level based on Risk Evaluation assessment, next step is giving recommendation on the security of the Election Commission of X City's site for prevent security risks. Recommendations are given for the risks that have been identified by considering the situation and conditions in the environment of the Election Commission of X City. The prioritized for treatment are risks with high and medium level, since low level risks do not significantly affect the security of sites based on situation and conditions in the environment of the Election Commission of X City. Recommendations that can be given to Election Commission of X City for identified risk can be seen in Table 9.

Table 9 shows the recommendations that can be given for handling each risk with a high level and risk with a medium level risk. Giving recommendations for handling each risk is done by learning about each security gap that becomes the risk and considering the conditions and situations on the ground, so that appropriate steps are obtained to handle the risks obtained to improve security on the Election Commission of X City's site.

Table 9. Recommendation for Risk Prevention

Risk Code	Level	Recommendation
R12	High	The validation process should be done at the php level, not the query. Validation of the php level used ensures that there is no query inject, so that when the validation script detects a query string (select, #, -, from, where) the system will reject the request. Another prevention that can be done is to encrypt all POST parameters so that the attacker will be quite difficult to find SQL Injection loopholes.
R13	High	Form input on the website is used to check voter data based on KTP and information search on the *bankdata*. The developer can provide validation of the use of symbols (such as "<>", "/") on the input form
R6	Medium	Close all open TCP ports on the system
R8	Medium	Set the secure flag to 'true' on the source code that functions as a cookie
R10	Medium	Output errors such as the file system path must not be sent via the remote client. Aministrator can send the error output to another place, for example in the error log
R11	Medium	Execution of system commands via the command interpreter, such as with system () must be avoided. The developer must be careful with validating the input before passing it to the interpreter

5. Conclusion

This study uses the ISSAF framework penetration testing stage and ISO 31000 risk management as a method for security risk analysis on Election Commission of X City’s site and the treatments that can be provided to improve future security. The ISSAF Framework is a penetration testing method that can be used as an application security control. In penetration testing, there are four stages instead of nine, which are the results of an agreement with the manager of Election Commission of X City’s site. These stages include the Information Gathering stage, the Network Mapping stage, the Vulnerability Identification stage, and the Penetration stage. The overall penetration test results are obtained 13 security holes found on Election Commission of X City’s site. More about the research process is to carry out risk management to determine the security risks on the website and overcome the existing risks. This study uses ISO 31000 as a risk management method, which includes three stages, namely the risk identification stage, the risk analysis stage, and the risk evaluation stage. The results of penetration testing were previously used as data in the risk management process, namely at the risk identification stage. Meanwhile, the results of risk management are obtained by two high-level risks which include vulnerabilities to attack SQL Injection and Cross-Site Scripting, four medium level risks which include TCP ports, session cookies, file system paths, and shell injection, and four risks with levels low which includes general system information, FTP information, firewall information based on TCP filters, and directory access. Providing recommendations is given for risks that have a high level of risk and medium level of risk, where risks with low levels have little impact on the security of Election Commission of X City’s site.

For future studies, other methods of penetration testing or risk management can be used with other frameworks to compare the results of security gaps obtained and the results of risk management. So that later it can be known the better penetration testing methods and risk management that can be used for other website security testing.

References

[1] J. N. Goel and B. M. Mehtre, “Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology,” *Procedia Comput. Sci.*, vol. 57, pp. 710–715, 2015.

[2] J. Doshi, “Comparison of Vulnerability Assessment and Penetration Testing,” no. June 2017, 2015.

[3] F. R. Mahtuf, P. Hatta, and E. S. Wihidiyat, “Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan,” *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 4, no. 1, p. 17, 2019.

[4] U. Nugraha and R. Istambul, “Implementation of ISO 31000 for information technology risk management in the government environment,” *Int. J. Innov. Creat. Chang.*, vol. 6, no. 5, pp. 219–231, 2019.

[5] I. Riadi, S. Sunardi, and E. Handoyo, “Security Analysis of Grr Rapid Response Network using COBIT 5 Framework,” *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 10, no. 1, p. 29, 2019.

[6] M. Z. Hussain, M. Z. Hasan, M. Taimoor, and A. Chughtai, “Penetration Testing In System Administration,” *Int. J. Sci. Technol. Res.*, vol. 6, no. 6, pp. 275–278, 2017.

[7] A. G. Bacuido, X. Yuan, B.-T. B. Chu, and M. Jones, “An overview of penetration testing,” *Int. J. Digit. Crime Forensics*, vol. 6, no. 4, pp. 50–74, 2014.

[8] M. Mirjalili, A. Nowroozi, and M. Alidoosti, “A Survey on Web Penetration Test,” *Adv. Comput. Sci.*, vol. 3, no. 6, pp. 107–121, 2014.

[9] A. Wiradharma and A. Sasmita, “IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study : X Company),” no. December, pp. 17–29, 2019.

[10] K. Nagendran, A. Adithyan, R. Chethana, P. Camillus, and K. B. Bala Sri Varshini, “Web application penetration testing,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10, pp. 1029–1035, 2019.

[11] E. Pratama and A. Wiradharma, “Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study : X Company),” *Int. J. Comput. Netw. Inf. Secur.*, no. July, pp. 8–12, 2019.

[12] A. Lubis and A. Tarigan, “Security Assessment of Web ApplicationThrough Penetration System Techniques,” *Jend. Gatot Subroto Km*, vol. 4, no. 100, pp. 296–303, 2017.
[13] B. V. Tarigan, A. Kusyanti, and W. Yahya, “Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 3, pp. 206–214, 2017.
[14] N. Z. Firdaus and Suprapto, “Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT . Petrokimia Gresik),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 1, pp. 91–100, 2018.
[15] H. Očevčić, K. Nenadić, K. Šolić, and T. Keser, “The impact of information system risk management on the frequency and intensity of security incidents,” *Int. J. Electr. Comput. Eng. Syst.*, vol. 8, no. 2, pp. 41–46, 2017.
[16] P. Sukapto, J. D. . Desena, P. K. Ariningsih, and S. Susanto, “Integration of Risk Engineering by ISO 31000 and Safety Engineering: A Case Study in a Production Floor of Sport Footwear Industry in Indonesia,” *Int. J. Simulation, Syst. Sci. Technol.*, pp. 1–12, 2008.
[17] B. Ratore *et al.*, *Information System Security Assessment Framework (ISSAF) Draft 0.2.1B*. OISSG, 2005.
[18] R. H. Hutagalung, L. E. Nugroho, and R. Hidayat, “Analisis Uji Penetrasi Menggunakan ISSAF,” *Hacking Digit. Forensics Expo.*, pp. 32–40, 2017.
[19] C. Lalonde and O. Boiral, “Managing risks through ISO 31000: A critical analysis,” *Risk Manag.*, vol. 14, no. 4, pp. 272–300, 2012.
[20] Nice and Imbar, “Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000,” *J. Inform. dan Sist. Inf. Univ. Ciputra*, vol. 2, no. 2, 2016.
[21] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, “Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.
[22] A. N. Rilyani, Y. AW Firdaus, and D. D. Jatmiko, “Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000,” *e-Proceeding Eng.*, vol. 2, no. 2, pp. 1–8, 2015.

Authors’ Profiles

I Gede Ary Suta Sanjaya, is a student and currently studying on information technology major in the Engineering Faculty of Udayana University. His research interests are mostly about computer network and network security management topics. Such as Network Centric Principles, IT Security Audit, IT Risk Management, and Network Security Applications.
Email: suta.arry@gmail.com

Gusti Made Arya Sasmita., is a lecturer at the Department of Information Technology, Faculty of Engineering, Udayana University Bali, Indonesia. Arya Sasmitha obtained his bachelor's degree in Electrical Engineering, Udayana University, Bali in 1997 and he obtained master's degree in Informatics Engineering, Gadjah Mada University in 2003. His research interests are Audit and Network Security
Email: aryasasmita@it.unud.ac.id

Dewa Made Sri Arsa, is a lecturer at the Department of Information Technology, Faculty of Engineering, Udayana University Bali, Indonesia. Sri Arsa obtained his bachelor's degree in Computer Science, Udayana University, Bali in 2014 and obtained his master's degree in Computer Science, Indonesia University in 2016. Currently, he actively doing research in Image Processing, Machine Learning, and Optimization
Email: dewamsa@unud.ac.id

How to cite this paper: I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, Dewa Made Sri Arsa, "Information Technology Risk Management Using ISO 31000 Based on ISSAF Framework Penetration Testing (Case Study: Election Commission of X City)", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.4, pp.30-40, 2020. DOI: 10.5815/ijcnis.2020.04.03