I. J. Computer Network and Information Security, **2019, 12, 17-29**
Published Online December 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.12.03

IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company)

Anak Agung Bagus Arya Wiradarma
Udayana University, Bali, Indonesia
E-mail: 9egungwira5@gmail.com

Gusti Made Arya Sasmita
Udayana University, Bali, Indonesia
E-mail: aryasasmita@it.unud.ac.id

Received: 03 November 2019; Accepted: 23 November 2019; Published: 08 December 2019

***Abstract*—**The major IT developments lead to speed and mobility elevation of information access. One of them is using the website to share and gather information. Therefore, the mobility and information disclosure create a harmful vulnerability. Which is the leakage of information, whether organizational or sensitive information, such as bank accounts, phone number and many more. Security testing is necessarily needed on website usage. One of the website security testing method is penetration testing. Supporting framework that can be used in this method is OWASP Testing Guide Version 4. OTG Version 4 has 11 stages cover all aspects of website protection and security. Security testing is nicely done using tools / software. Tools with the concept of OSINT (Open Source Intelligence) are used to get better access and availability by using the characteristics of open source. The IT risk assessment analysis carried out by ISO 31000 framework and based on the results that have been obtained through penetration testing with OWASP framework. Significance & values of this research is finding the best and effective way to making IT risk management guidelines along with the combination of with OWASP & ISO 31000 framework, by doing website security assessment with penetration testing method based on OWASP framework to get the system vulnerabilities and analyze the risks that appears with the ISO 31000 framework. Also, the IT risk management guidelines consist of system improvement recommendations along with evaluation report which obtained from the collaboration analysis the OSINT concept, penetration testing methods, OWASP and ISO 31000 framework.

***Index Terms*—**Information Gathering, OSINT, OWASP, Penetration Testing, ISO 31000.

I. INTRODUCTION

A. Research Background

The implementation of technology is very helpful in various fields and has a positive impact on everyday life, one of them is sharing through and managing the information within the Internet with a Website. In the presence of positive impact, there are also the negative impact. Information disclosure on a Website can be a weakness point and vulnerabilities of the organization that uses the website as an information access. Security improvements can be done by testing the weak points of the website, existing solutions to have a security assessment is to generate the penetration testing method on the organization website. There are many phases that the examiners have to do in penetration testing processes, one of them is information gathering phase. This phase has purpose to receive as many as possible of system information, architecture, how-to-build, domain names, network mapping, port information, and any other usable information of the target website to get the advanced knowledge for next phase of penetration testing processes. Penetration testing method has several frameworks that can be used by. Based on the previous study about penetration testing frameworks, OWASP Testing Guide is preferred to be the best and compatible frameworks to be used in penetration testing processes. The version of OWASP framework used in this research is OWASP Testing Guide version 4 published on 2015 using the module Testing for Information Gathering. This module has purpose to performing information gathering phases. Definitely, usage of software and tools are must requirements to be fulfilled. Scope of tools that used in this research are in the OSINT (Open Source Intelligence) category. The main OSINT tools used in this research is Maltego. Therefore, in OWASP Testing Guide framework are already have guidelines that suggested to using the tools that have been fixed at every phase. This condition makes the examiners not only to use Maltego as a single and main tool, but also using some other additional tools that have been fixed in the OWASP Testing Guide Framework. However, it is certain that all tools used in this research are open source based. The components of the website will be tested and verified to have a security level to produce an information system with a high level of security and can be used sustainably. The risk management guidelines is produced based on the analysis of the results of penetration test, and then obtains the risk lists that might be received by the organization on the future. Risk management guidelines have functions to provide appropriate actions and system management based on relevant guidelines and stand out to the adoption of ISO 31000 policies. The outputs of this research will produce evaluation report and IT risk management guidelines that will be used as a additional or main reference for preferred recommendations and actions. Problem to be solved is to minimize the level of vulnerability of existing systems and overcome the risks that come within and make the organization website system more secure and protected.

B. *Research Limitation*

There are some points of main limitation of the research, which can be explained as follows.

1. The tools or software used on penetration testing security assessment is limited on OSINT based tools and recommended tools on OWASP Testing Guide version 4 framework.
2. The standardization or framework used in this research is limited to OWASP for penetration testing and ISO 31000 for risk management framework only.
3. The time period of security assessment on the organization is limited span only for 6 months.

C. *Research Achievement Advantage*

There are some points of research advantage and benefits that came along within the research achievement, which can be explained as follows.

1. Providing information about the level of website system security based on the results of security testing and analysis on the website of the organization.
2. Providing recommendations to overcome vulnerabilities and improve security which can be implemented by the organization

II. Literature Study

A. *Open Source Intelligence*

OSINT (Open Source Intelligence) is a part of intelligence disciplines that related and generated by analyzing public data sources. The main source of OSINT is taken from the availability of information for the public that is collected, exploited, and disseminated in a timely manner to the right audience for the purposes of handling certain information and intelligence needs (Benes, 2013; Stiawan et al., 2017). The main function of the use of OSINT is in the functions of national security, law enforcement, and business intelligence and is valuable for analysts who use non-sensitive intelligence in answering classified, non-classified, and proprietary intelligence requirements in all previous intelligence disciplines (Hassan & Hijazi, 2018; Kawakita & Shima, 2018). OSINT is achieved by processing video, image, audio, and text data from public data sources and analyze the processed data to generate major insights from across all data sources. The intelligence products started to be based mostly on open sources thus providing efficient use of the resource capabilities of the intelligence community (Jenter et al., 2014). OSINT grew more important on influencing and growing the advanced progress in communication and encryption technologies. The approach of the Internet, digital interconnected platform and social media platforms have all led to the growing importance of OSINT and the emergence of overlapping jurisdictional areas between other schools of intelligence, but also brought about problems of verification regarding content and news (Edam et al., 2018). The purpose of OSINT in the context of penetration testing is to gather as much information as possible about the attacks that will be carried out. Specific testing agreements that involve organizations and clients allow some information to be released before the testing itself (Hoepman, 2014). Generally, the first phase of OSINT usage on penetration testing process is to analyze the outline up to highly detailed information of the target. This phase could obtain to increase likelihood of success percentage on exploiting the target. The information is typically gained from company websites, social media, public records, and unsuspecting employees. Further activities, OSINT techniques almost like “Google hacking” technique, that often reveal sensitive information from a particular target whom did not realize was publicly available (Young et al., 2017)

B. *Maltego*

Maltego is a software developed by Paterva and is used by professionals and experts in the field of security and digital forensic to collect and analyze open source information for intelligence purposes. Maltego can also be used for handling evidence that is useful because of the large amount of data generated by the method of penetration testing accidentally during the attack on the target (Kawakita & Shima, 2018). A very important feature in Maltego is the ability to search for deeper information using reference information that has been collected regarding OSINT sources. Maltego can easily collect information from various sources and use various kinds of transformations to process and produce results in graphical form so that it is easier for users to understand.

Processing of the information has been embedded in Maltego and can also be adjusted based on user needs (Petersen, 2017). Maltego have a useful graphing software that places an accent on relationships between nodes in the graph and uses a client/server architecture for the purposes of data collection to determine the relationships and real-world links between pieces of data of website infrastructures. In this way, Maltego generates a node graph in which nodes called entities are plotted and relationships between nodes are represented with directional arrows (System & Marx, 2014). Maltego is developed in the Java programming language and runs on the Kali Linux operating system. Users are required to register to be able to use Maltego for free. After registered users, users can already use Maltego to collect targeted digital information on the internet.

C. Penetration Testing

The penetration testing method or often called "pentest" is the practice of computer system, network, or web application security testing to find security vulnerabilities that can be exploited by attackers by providing stages of system attacks to the system (Yeboah-Ofori, 2018). The penetration testing method can be facilitated by using tools or done manually (Ghozali, Kusrini, & Sudarmawan, 2019). The processes contained in the penetration testing method include information gathering, identifying penetration points, and also reporting the results of testing. Implementation of security testing with the penetration testing method is recommended to use a 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 (Lubis & Tarigan, 2017). 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 (Hussain et al., 2017). The results of system security testing evaluations from the penetration testing method that have been successfully identified or exploited will be collected and provided to administrators, organizational owners, or organizational system managers with the aim of giving them recommendations for making decisions and prioritizing efforts to improve system security and protection (Shanley & Johnstone, 2015). Penetration testing process approach audit web application security and also can be used to secure associated layers and includes to audit system for finding vulnerabilities, which may be existing in the system. The tester will find and exploit vulnerability same as an attacker exploit and produce data which represent the risk level of the system (Hasan & Meva, 2018). Penetration testing depend on many kinds of mechanisms or framework for identifying flaws in attacks or tests to get beneficial results when the penetration testing process is going down. A structured work and approach can therefore benefit both the examiners and resources used under the testing processes. An additional benefit is that test results with good and structured mechanism are easier to re-use in the future to ensure that no regressions occur with the penetration testing method (Dahl, 2005).

D. OWASP

OWASP is a non-profit organization that focuses on improving software security (Ghozali et al., 2019). OWASP guideline is applied throughout the software development life cycle (SDLC) phases in application development which are system planning, system analysis, system design, implementation, and testing (Sedek, Osman, Osman, & Jusoff, 2009). OWASP provides many tools, guides and testing methodologies for cyber security under an open source license, specifically the OWASP Testing Guide (OTG) (Dirgahayu et al., 2015). The OTG is divided into three main parts including the OWASP testing framework for web application development, web application testing methodology, and system evaluation reporting. The web application testing methodology can be used independently or can be used as a testing framework. A web application developer can use the framework to build web applications by considering the protection and security aspects followed by security testing with the penetration testing method to test the system security of the web application developed 9 (Pratama & Wiradarma, 2019). The OWASP Testing Guide Framework has a strong focus on the level of security of web applications in all software development lifecycles aspect that different with other penetration testing security testing frameworks, such as ISSAF and OSSTMM, which is both of them are intended to test the security from implementation. The OWASP Testing Guide is specifically targeted to a single scope of domain, which as web applications (Lubis & Tarigan, 2017). OWASP Testing Guide can really help and very important to a security practitioner because it is available completely free of charge and open. Information protection and security must not be an agony that only a few persons can practice. OWASP Testing Guide have an open-access and very detailed penetration testing phase, and because of that, it's should go to the hands of developers and software examiners. There is sufficient security experts applications in the world to make a significant reduction in the security problem, and the responsibility for application security must fall on developers (Mariani et al., 2015).

E. Risk Management // ISO 31000

Risk can be defined as the chance of loss or an unexpected outcome associated with a preferred action. Uncertainty is not knowing what will happen in the future. The greater the uncertainty, the greater the risk will come (Crane, Gantz, Isaacs, Jose, & Sharp, 2013). Risk management has been one of the major concerns considered today. As a rule, effective risk management requires the evaluation of events in a two-perspective approach, on the one hand, from the uncertainty occurrence or probability, and on the other from the viewpoint of the effect result. One of the risk management standards is ISO 31000. Based on the last version of ISO 31000 standard, which is issued on 2018, ISO 31000 summarizes risk management into three main steps. The first step is risk identification with aims to generate a list of risks from different sources, the events, their causes and potential outcome, and the areas affected. The second step is risk analysis with aims to provide an understanding of risk to serve as the core for making decisions on the best reflections and methods. Risk analysis can be carried out at various levels of detail, depending on the risk in question, the purpose of the analysis and the information available. In this paper, the risk analysis will be based on the technical testing results of penetration testing used the combination of OSINT tools and OWASP Testing Guide Version 4 framework. The third step is risk evaluation with aims to provide more support for making decisions and comparing the level of each risk, based on the results of the risk analysis, by evaluating what risks that necessarily need treatment and the priority of implementing the treatment (de Oliveira, Marins, Rocha, & Salomon, 2017). ISO 31000 had established risk management framework that is more flexible and provided more control than the other framework. The flexibility proof of ISO 31000 can be seen on the capability to fit on any organization risk management process (Sukapto, Desena, Ariningsih, & Susanto, 2018). One of the main objectives of ISO 31000 standard is to continually improve risk management in organizations based on a general model that have purpose to adapt to a wide variety of risks. ISO 31000 provides a structured framework intended to meet the needs of any type of organization or situation. The entire risk management process on ISO 31000 will be documented in order to maintain a reporting overview of decision making and will be granted as a periodic review of the entire process of identifying, analyzing and addressing risk in purpose to discover changes in the external and internal environments (Lalonde & Boiral, 2012).

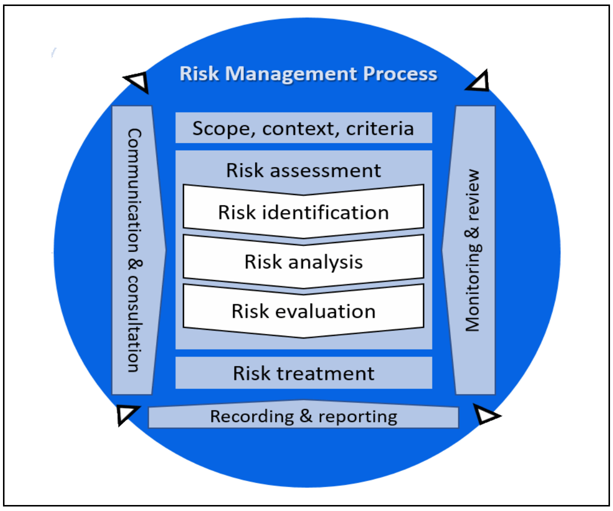


Fig.1. ISO 31000 Risk Assessment Diagram
Source: ISO Official Website

Figure 1. is a illustration of the ISO 31000 based risk management process. The ISO 31000 risk management process includes five activities which can be explained as follows.

1. Communication and Consultation

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

2. Establish the Context

Organizational management determines the limits or internal parameters and external parameters (external that are taken into consideration in managing risk, determining the scope of work, and risk criteria for subsequent processes.

3. Risk Assessment

These stages include Risk Identification, Risk Analysis, and Risk Evaluation. Risk identification is the process of determining risks that have the potential to effect the organization in achieving its objectives. Risk Analysis is an effort to understand risks more deeply. Risk Evaluation is the process of evaluating the likelihood and impact level of each risk using predetermined criteria.

4. Risk Treatment

Risk treatment includes efforts to select options that can reduce or eliminate the impact and likelihood of risks, then implement those choices.

5. 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.

III. Research Methodology

A. Technical Testing Using OTG Version 4 Diagram

Technical testing phase is supported by a flowchart with purpose to simplify the researchers determining the sequence of steps to be taken when finished out the penetration testing process using the OWASP Testing Guide Version 4. Activities begin with planning and preparing the penetration testing processes, which is set up the user's PC, the tools that will be used, and the target website that will be tested. Afterwards, the penetration testing phase with the OWASP framework will be started. There are 11 stages that tested on the target website based on the objectives for each of these stages. The following are figure from the workflow diagram of penetration testing phase using OTG Version 4.

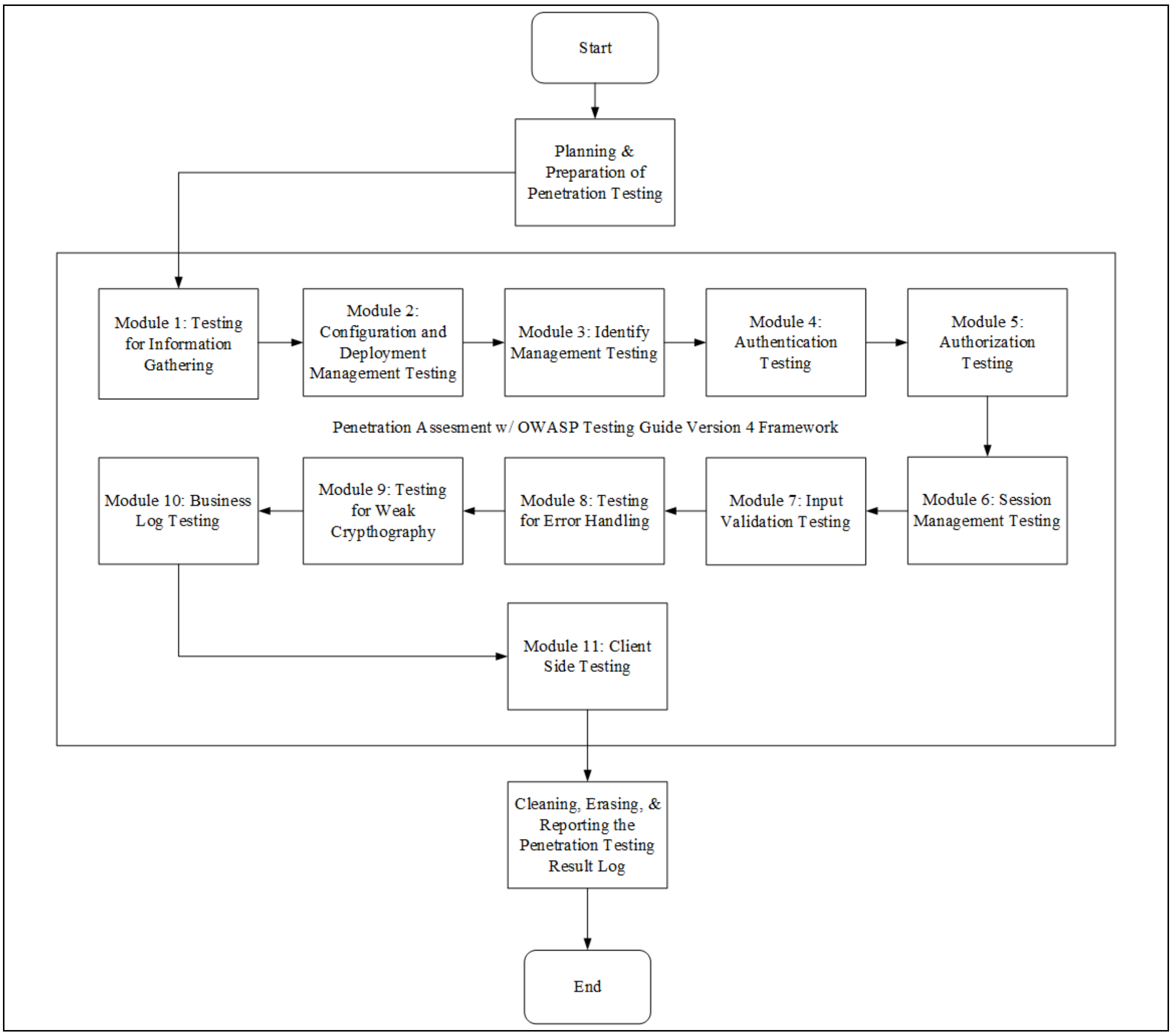

Start
Planning & Preparation of Penetration Testing
Module 1: Testing for Information Gathering
Module 2: Configuration and Deployment Management Testing
Module 3: Identify Management Testing
Module 4: Authentication Testing
Module 5: Authorization Testing
Penetration Assesment w/ OWASP Testing Guide Version 4 Framework
Module 10: Business Log Testing
Module 9: Testing for Weak Crypthography
Module 8: Testing for Error Handling
Module 7: Input Validation Testing
Module 6: Session Management Testing
Module 11: Client Side Testing
Cleaning, Erasing, & Reporting the Penetration Testing Result Log
End

Fig.2. Penetration Testing Diagram
Source: Personal Document

B. Risk Management Analysis Using ISO 31000 Diagram

Testing and analysis of risk management is supported by a flowchart with purpose to simplify the researchers to determine the sequence of steps to be taken when finished out the risk management guide using the ISO 31000 framework. Activities begin with making the agreement for the consultation process with the organization manager. The purpose of this consulting process is to find out and examine the risk management that has already been done before within the company. Afterwards, risk management assessment stage will be started which consist of risk analysis, risk analysis and risk evaluation. The risk assessment stage in the ISO 31000 framework is carried out by including the results of penetration tests for each phase in the assessment stage. The following are figure of the workflow diagram of risk management process using the ISO 31000 framework.

C. Recommendations Analysis Diagram

The results of penetration testing and risk management processes will be combined and collaborated at this stage which will produce IT risk management guidelines. The process of making risk management guidelines will be based on weaknesses and vulnerabilities of target organization website obtained from the penetration testing that has done before. These weaknesses and vulnerabilities will lead to various risks for the organization's whole IT system. The IT administrator will need the risk management guidelines to overcome the risks when the problem appears. The following are figure of the workflow diagram of IT Risk Management decision making process using the OWASP Testing Guide V4 & ISO 31000 framework.

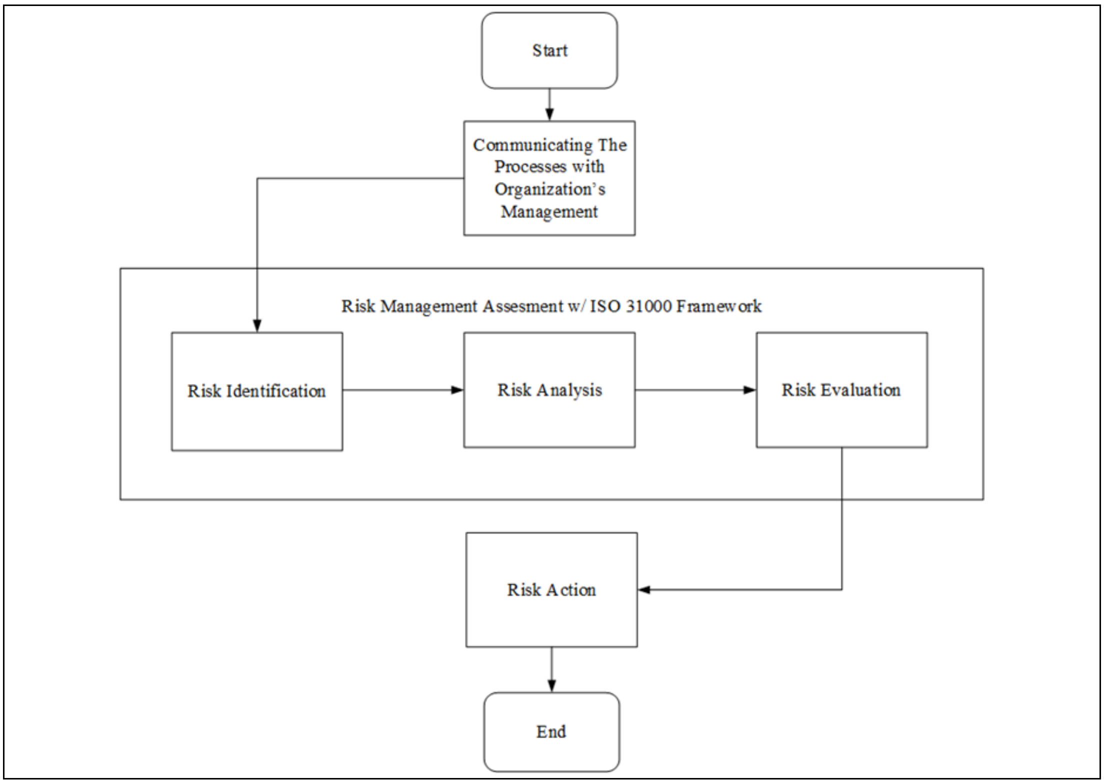

Start
Communicating The Processes with Organization's Management
Risk Management Assesment w/ ISO 31000 Framework
Risk Identification
Risk Analysis
Risk Evaluation
Risk Action
End

Fig.3. Risk Management Processes Diagram
Source: Personal Document

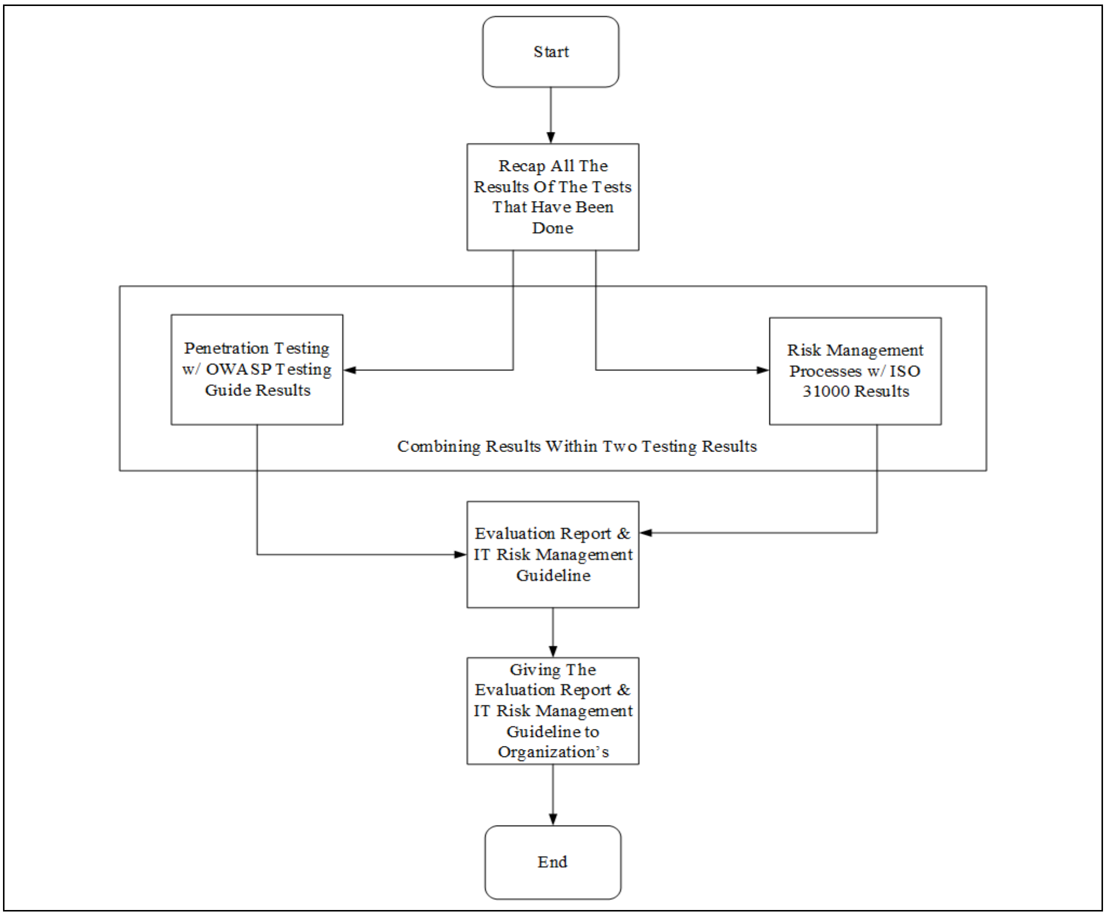
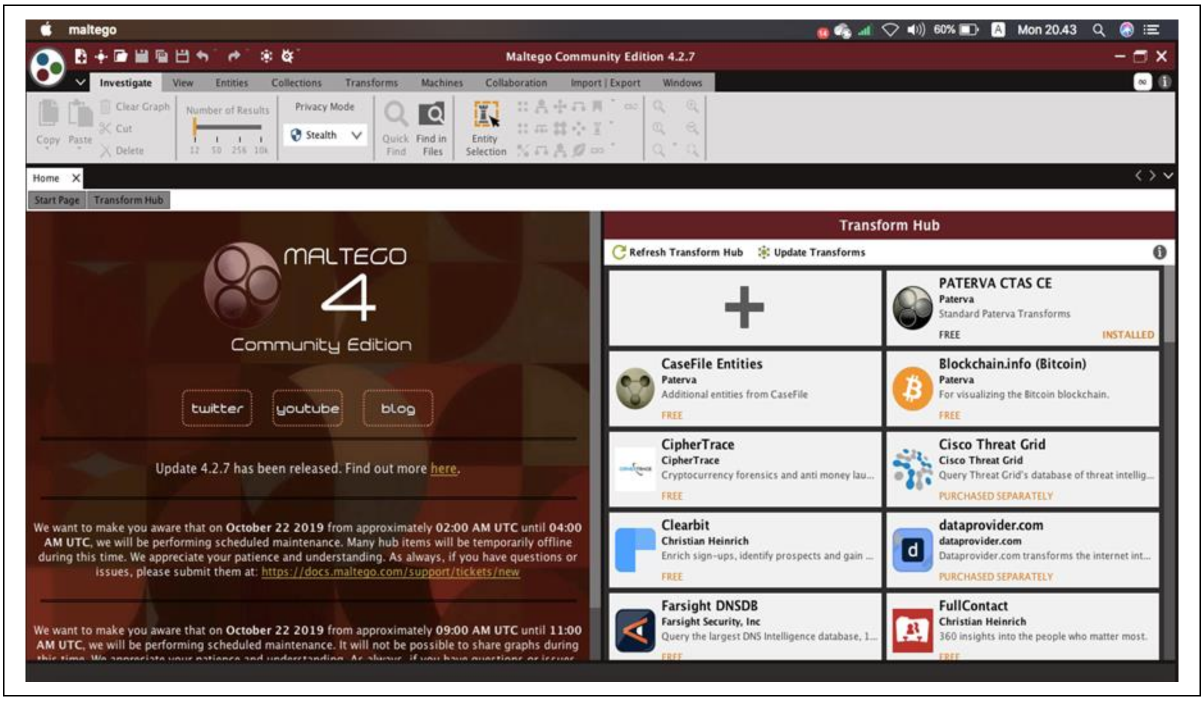

Start
Recap All The Results Of The Tests That Have Been Done
Penetration Testing w/ OWASP Testing Guide Results
Risk Management Processes w/ ISO 31000 Results
Combining Results Within Two Testing Results
Evaluation Report & IT Risk Management Guideline
Giving The Evaluation Report & IT Risk Management Guideline to Organization's
End

Fig.4. Evaluation Report & Risk Guidelines Diagram
Source: Personal Document

IV. Test Results

A. Maltego as OSINT Tool

Maltego is the tools with the purpose to gather all specific and detailed information about how a website deployed and worked on the internet. Open source intelligence (OSINT) concept applied on this software, because of the capabilities to gain the information for the certain intelligence objective with the open source-based program or software. Examination for the information gathering phase, which is the first stage of OWASP Testing Guide Version 4 phases is done by using OSINT tools with a specific function to gather information of the website target. This research paper used Maltego as one of the tools to support the information gathering phase. Maltego version that used on this research is Maltego Community Edition version 4. The following figure is the appearance of the startup from Maltego which runs on Macintosh OS High Sierra, the figure is showed to indicate the example of OSINT tools used in this research.



Update 4.2.7 has been released. Find out more here.

We want to make you aware that on **October 22 2019** from approximately **02:00 AM UTC** until **04:00 AM UTC**, we will be performing scheduled maintenance. Many hub items will be temporarily offline during this time. We appreciate your patience and understanding. As always, if you have questions or issues, please submit them at: https://docs.maltego.com/support/tickets/new

We want to make you aware that on **October 22 2019** from approximately **09:00 AM UTC** until **11:00 AM UTC**, we will be performing scheduled maintenance. It will not be possible to share graphs during

PATERVA CTAS CE
Paterva
Standard Paterva Transforms
FREE INSTALLED

CaseFile Entities
Paterva
Additional entities from CaseFile
FREE

Blockchain.info (Bitcoin)
Paterva
For visualizing the Bitcoin blockchain.
FREE

CipherTrace
CipherTrace
Cryptocurrency forensics and anti money lau...
FREE

Cisco Threat Grid
Cisco Threat Grid
Query Threat Grid's database of threat intellig...
PURCHASED SEPARATELY

Clearbit
Christian Heinrich
Enrich sign-ups, identify prospects and gain ...
FREE

dataprovider.com
dataprovider.com
Dataprovider.com transforms the internet int...
PURCHASED SEPARATELY

Farsight DNSDB
Farsight Security, Inc
Query the largest DNS Intelligence database, 1...
FREE

FullContact
Christian Heinrich
360 insights into the people who matter most.
FREE

Fig.5. Maltego Appearance on Macintosh OS
Source: Personal Document

B. Testing Results of OWASP Testing Guide Version 4 Framework

Testing phases are finished out on the target website using the Testing for Information Gathering module which the first stage of OWASP Testing Guide Version 4 Framework and consists of 10 phases to find every detailed information as complete as possible from the target website as the purpose of the information gathering stage. The following table shown below is a table of testing results on the target website.

The testing of Information Gathering module is conducted by researcher with the skills and knowledge of penetration testing theory, recommended software on OWASP Testing Guide guidelines, and a personal computer with the qualified specifications for supporting and ensuring the reliability of the testing results. On the some phases at this Testing for Information Gathering module there is some website system information that cannot be covered or secured (Example: information of website framework with Wapplyzer). One way to prevent attacks with that uncovered sensitive information is strengthen security technically in developed structures on the website (firewalls, IPS, IDS, etc.) OSINT used: Google Hacking Database, Google Hacking Diggity, Whatweb, Wapplyzer, Netcat, Nmap, robotstxt.org, Whois, reqbin.com, ZAP, Maltego.

Table 1. Objective Table of Testing for Information Gathering Module

Number	Module	Objective	Result
4.2.1	*Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001)*	Discovering the design and configuration information from website/systems/organizations that can be accessed openly either directly (on the organization's website) or indirectly (on third party websites).	Success (Google Hacking Database, Google Hacking Diggity)
4.2.2	*Fingerprint Web Server (OTG-INFO-002)*	Discovering the version and type of web server used by the target to find out the weaknesses and types of exploits when system penetration occurs.	Success (Whatweb, Wapplyzer, Netcat, Nmap)
4.2.3	*Review Webserver Metafiles for Information Leakage (OTG-INFO-003)*	Knowing the leakage of information of directory and folder path of the web application from Robots/Crawler/Spiders analysis.	Success (curl Robots.txt, robotstxt.org/robotstxt.html)
4.2.4	*Enumerate Applications on Webserver (OTG-INFO-004)*	Calculate the amount of web applications that running on the target web server and knowing the open ports of the target website.	Fail (Nmap, Whois)
4.2.5	*Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005)*	Discovering the developer comments on the website target and find leaked information and metadata to have better system knowledge.	Fail (Wget, Inspect Element Chrome, HTML file)
4.2.6	*Identify Application Entry Points (OTG-INFO-006)*	Discovering how requests and responses were formed from target website based on the information given within GET and POST requests.	Success (reqbin.com, ZAP)
4.2.7	*Map Execution Paths Through Application (OTG-INFO-007)*	Create the system mapping of the target website and understanding the main workflow.	Fail (Maltego)
4.2.8	*Fingerprint Web Application Framework (OTG-INFO-008)*	Discovering the type of used framework from the target website that will give better understanding and proper option of the security testing methodology.	Fail (WhatWeb, Wappalyzer)
4.2.9	*Fingerprint Web Application ((OTG-INFO-009)*	Discovering the version of the building component of the target website to determine weaknesses and exploitation methods that are suitable when system penetration occurs.	Fail (WhatWeb, Wappalyzer)
4.2.10	*Map Application Architecture (OTG-INFO-010)*	Discovering and knowing the overall system architecture and workflow of the target website.	Fail (Maltego)

C. Testing Analysis of OWASP Testing Guide Version 4 Framework

The results of penetration testing using OWASP Testing Guide Version 4 Framework on Testing for Information Gathering module in Table 1. shows the target website successfully passed in phase (OTG-INFO-001), (OTG-INFO-002), (OTG-INFO-003), (OTG-INFO-006) and failed in phase (OTG-INFO-004), (OTG-INFO-005), (OTG- INFO-007), (OTG-INFO-008), (OTG-INFO-009), (OTG- INFO- 0010). Explanation of failure on every failed phase on the tested website is when the examiners can find detailed information within the purpose of the 10 phases from the Testing for Information Gathering module. Phases that do not passed will expose the vulnerabilities and weaknesses of the target website because in the penetration testing scenario, examiners are pretended to be as same role as the attacker that need to find information for going further to the website system. The following table shown below is a table of testing results on the target website.

The purpose of reviewing these modules is to describe and breakdown the effect to the website system when it fail to passed the testing processes. From the 10 kinds of testing process that tested from the Testing for Information Gathering module, 6 out of 10 testing were not passed and will gave vulnerabilities and security holes on the target website. The passing percentage of information gathering scope is 40%, that later will be calculated further on risk management processes.

D. Risk Management Assessment Analysis Based on OWASP Testing Results

Based on the vulnerabilities and weaknesses of the website obtained from the penetration testing using OWASP Testing Guide framework, there is a few risks that must considered on. Risks will be listed according to the penetration testing results with the module Testing for Information Gathering, where this module focused on how to maintain and secure the specific, sensitive, and deployment information of the targeted website. Risk assessment process started with risk identification, risk analysis, and ended with risk evaluation process.

Table 2. Analysis Table of The Testing Results

Number	Module	Effect
4.2.4	*Enumerate Applications on Webserver (OTG-INFO-004)*	Attacker can discover amount of website that hosted on the server of website target, that can lead to the further knowledge of estimation average hosted website architecture. Knowing the open ports can also lead for choosing the effective attack that can go through directly to the specific ports function.
4.2.5	*Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005)*	Attacker can discover the source of building component or template that used for developing the target website. By knowing that information, the attacker will know the developing source and search for weaknesses related to the leaked information.
4.2.7	*Map Execution Paths Through Application (OTG-INFO-007)*	Attacker can discover the entire mapping flow of website developing component used along with their specific functions.
4.2.8	*Fingerprint Web Application Framework (OTG-INFO-008)*	Attacker can discover the type of developing framework that used to build the target website that have purpose to learn weaknesses and attacks that well-matched for system penetration usage to the target website.
4.2.9	*Fingerprint Web Application (OTG-INFO-009)*	Attacker can discover the version of the website builder component to investigate through about the weaknesses and types of attacks for system penetration usage to the target website.
4.2.10	*Map Application Architecture (OTG-INFO-010)*	Attacker can discover the main and entire system architecture of the target website and take out the important information to be investigated further for carrying out the attacks on the target website.

Risk Identification

The risk identification process started by grouping the risks based on IT resource in the specified organization. Identification processes will generate a several risks that may happen on every IT resource the organization have. On this risk identification context, the scope of process will take on the vulnerabilities obtained from testing results of penetration testing using OWASP Testing Guide Version 4, Testing for Information Gathering Module. The following table shown below is risk identification table.

Table 3. Risk Identification Table

Risk Assessment Scope: Information Leakage of Website (Based on OWASP Testing Guide: Testing for Information Gathering module testing results)			
Risk Code	Risk Threats/Identification/Source	Risk Description	Risk Impact
R1	Enumerating web applications and web server	Calculating the amount of web applications that running on the target web server and knowing the open ports of the target website.	Attacker can discover amount of website that hosted on the server of website target, that can lead to the further knowledge of estimation average hosted website architecture. Knowing the open ports can also lead for choosing the effective attack that can go through directly to the specific ports function.
R2	Reviewing website developer comments and metadata	Discovering the developer comments on the website target and find leaked information and metadata to have better system knowledge.	Attacker can discover the source of building component or template that used for developing the target website. By knowing that information, the attacker will know the developing source and search for weaknesses related to the leaked information.
R3	Website system and workflow mapping	Creating the system mapping of the target website and understanding the main workflow.	Attacker can discover the entire mapping flow of website developing component used along with their specific functions.
R4	Reviewing website developing framework	Discovering the type of used framework from the target website that will give better understanding and proper option of the security testing methodology.	Attacker can discover the type of developing framework that used to build the target website that have purpose to learn weaknesses and attacks that well-matched for system penetration usage to the target website.
R5	Reviewing website version	Discovering the version of the building component of the target website to determine weaknesses and exploitation methods that are suitable when system penetration occurs.	Attacker can discover the version of the website builder component to investigate through about the weaknesses and types of attacks for system penetration usage to the target website.
R6	Website main architecture and overall connected system mapping	Discovering and knowing the overall system architecture and workflow of the target website.	Attacker can discover the main and entire system architecture of the target website and take out the important information to be investigated further for carrying out the attacks on the target website.

Risk Analysis

The risk analysis process is started by analyzing risks calculation that already listed on risk identification process. During the risk analysis process, it begins with the determination of the likelihood and impact levels. The likelihood and impact rating will become input for the likelihood and impact matrix table. The likelihood and impact rating with matrix table are explained on Table 4. and Table 5., while the likelihood and impact score of the risks is shown in Table 6.

Table 4. Likelihood and Impact Table

Likelihood Table		Impact Table	
Rating	Criteria	Rating	Criteria
1	Rare	1	Insignificant
2	Unlikely	2	Minor
3	Possible	3	Moderate
4	Likely	4	Major
5	Almost Certain	5	Catastrophic

1 2 3 4 5

Table 5. Matrix Table of Risks Likelihood and Impact

5	Medium	Medium	High	High	High
4	Low	Medium	Medium	High	High
3	Low	Medium	Medium	Medium	High
2	Low	Low	Medium	Medium	Medium
1	Low	Low	Low	Medium	Medium
	1	2	3	4	5

Based on the risk identification phase, the list of risks that has been identified according to penetration testing results will be given the likelihood dan impact level score. The score of likelihood and impact level were given based on internal and external condition within the organization system, also the framework ISO 31000 have a important role on this level scoring. The following table shown below is a table of the likelihood and impact level of the risks.

Table 6. Risk Analysis Table

Risk Code	Risk Description	Likelihood Level	Impact Level
R1	Calculating the amount of web applications that running on the target web server and knowing the open ports of the target website.	Possible (3)	Major (4)
R2	Discovering the developer comments on the website target and find leaked information and metadata to have better system knowledge.	Rare (1)	Insignificant (1)
R3	Creating the system mapping of the target website and understanding the main workflow.	Possible (3)	Minor (2)
R4	Discovering the type of used framework from the target website that will give better understanding and proper option of the security testing methodology.	Possible (3)	Moderate (3)
R5	Discovering the version of the building component of the target website to determine weaknesses and exploitation methods that are suitable when system penetration occurs.	Unlikely (2)	Minor (2)
R6	Discovering and knowing the overall system architecture and workflow of the target website.	Possible (3)	Moderate (3)

Table 7. Risks Likelihood/Impact Mapping Table

	5	🟨	🟨	🟥	🟥	🟥
	4	🟩	🟨	🟨 R1	🟥	🟥
	3	🟩	🟨	🟨 R4, R6	🟨	🟥
Impact	2	🟩	🟩 R5	🟨 R3	🟨	🟨
	1	🟩 R2	🟩	🟩	🟨	🟨
		1	2	3	4	5
				Likelihood		

Table 8. Risk Evaluation Table

Risk Code	Risk Description	Likelihood Level	Impact Level	Risk Level
R1	Calculating the amount of web applications that running on the target web server and knowing the open ports of the target website.	Possible (3)	Major (4)	Medium
R2	Discovering the developer comments on the website target and find leaked information and metadata to have better system knowledge.	Rare (1)	Insignificant (1)	Low
R3	Creating the system mapping of the target website and understanding the main workflow.	Possible (3)	Minor (2)	Medium
R4	Discovering the type of used framework from the target website that will give better understanding and proper option of the security testing methodology.	Possible (3)	Moderate (3)	Medium
R5	Discovering the version of the building component of the target website to determine weaknesses and exploitation methods that are suitable when system penetration occurs.	Unlikely (2)	Minor (2)	Low
R6	Discovering and knowing the overall system architecture and workflow of the target website.	Possible (3)	Moderate (3)	Medium

Risk Evaluation

The risk evaluation process is calculated by multiplying the likelihood and impact of each risk. The risks is evaluated by researcher by following the likelihood/impact matrix table. The result is as illustrated in Table 6. Based on the likelihood/impact matrix table, only 4 risks on specified scope should be evaluated and prioritized, as this group of risks have a medium score on the calculation likelihood/impact. The prioritized risk basically has a medium and high score from mapping process, thus this score likely will gave a significant impact and loss to the company’s IT system if not handled and fixed well. The risks mapping of likelihood/impact matrix and risk evaluation level are explained on Table 7. and Table 8.

As the risk evaluation processes going on, the final step is making the recommended actions to do for handling the consequences if the risk happens on the company’s system and treatment to the risk aftermath. This final step is the main goal of this research, with the IT risk management processes that goes on from the penetration testing phase until the risk management process. Hopefully the calculation of the risks that obtained from information gathering scope, based on OWASP Testing Guide version 4 framework within Testing for Information Gathering module will help to maintain and improving the service capability of the company’s system and management to the customer and also to keep the way up for company’s main goal and achievement. The table shown below is the IT risk management table with the recommended action and treatment of the risk that has been identified and analyzed to have medium score of risk within the two process before.

Table 9. IT Risk Management Treatment & Recommended Actions

Risk Code	Risk Threats/Identification/Source	Risk Description	Risk Treatment
R1	Enumerating web applications and web server	Calculating the amount of web applications that running on the target web server and knowing the open ports of the target website.	Implementing Intrusion Detection System (IDS) and Honeypot system which have functions to detect the incoming unauthorized activity and prevent attacks. Using Activating the Port Scanner Detection function on router can be a good recommendation for avoiding further system penetration by attacker.
R3	Website system and workflow mapping	Creating the system mapping of the target website and understanding the main workflow.	Implementing Intrusion Detection System (IDS) and Honeypot system which have functions to detect the incoming unauthorized activity and prevent attacks. Usage of encryption and reducing the exposed sensitive information can also be done.
R4	Reviewing website developing framework	Discovering the type of used framework from the target website that will give better understanding and proper option of the security testing methodology.	Learning and implementing how to secure the used website framework, that have different method and procedure for every framework (in this case: CodeIgniter) to prevent the penetration and control by attacker. On the detailed advanced security, administrator can use the advanced query to protect the website from many forms of dangerous attack, like XSS Scripting & SQL Injection, that will be explained later on other phase of OWASP Testing Guide.
R6	Website main architecture and overall connected system mapping	Discovering and knowing the overall system architecture and workflow of the target website.	Website administrators can build and deploy the security system as strong as possible to secure the sensitive information from entire web architecture when attacker start the scanning or information gathering progress. Proxy servers, IDS, encryption, and security module on each part of website system can be used as a solution to secure website architecture information.

All the result and analysis of system vulnerabilities, weaknesses, and recommended actions from technical testing that already done by penetration testing method with OWASP Testing Guide Version 4 framework will produced to risk management guidelines. The risk management guidelines based on all technical vulnerabilities risks that harms the website system. Risk assessment process that consists of 3 main phases (identification, analysis, evaluation) carried out by using ISO 31000 framework and the results of penetration testing process, that used as the main structure of the risk assessment.

V. Conclusions

Penetration testing and risk management assessment has been completed and going well. The notable point that noted here is every website that used to be a center of sharing and managing information has many vulnerabilities that cannot be seen from the outside or user viewpoint. If these vulnerabilities left ignored without security improvement, it will produce risks and losses that could impact the organization data and users who entrust the website to store their personal information. Website security testing is the right thing to do for overcome the security holes and gaps on the related websites, and one of the methods of website security testing is the penetration testing method. Pretending to be an attacker who wants to obtain information illegally or disrupt the structure of the website by attacking the back end is the main characteristic of penetration testing method. It will gain a website vulnerabilities and weaknesses that has not been seen by users when they use the functionality normally. The penetration testing framework that used in this study is the OWASP Testing Guide Version 4. Based on researches that has been done before, this framework is the most relevant and appropriate for penetration testing processes. Vulnerabilities and weaknesses that founded have been compiled and analyzed to found out the ways for overcome the technical problem caused by. Eventually, risks can harm the system anytime if these vulnerabilities showed up on the website. Therefore, a risk management action is necessarily needed for the organization to protect the company from significant risks that can stun the company's goals & achievements. Another objective is for taking the proactive actions to reduce risks that can cause losses based on the vulnerabilities and weaknesses of the website that have been technically tested by using penetration testing methods. Risk management assessment is carried out based on ISO 31000:2018 standard, with the identification, analysis and evaluation stages. The risk level graph shows that 4 out of 6 risks have medium level and the 2 other risks have low level of likelihood/impact score. The results obtained from the making of risk management guidelines are expected to help the organization management in order to protect the company from any significant risks that can stunt the organization main goal. Risk management is also expected to be a guidelines and recommendation to improve the quality of company services and to maintain quality assurance that is useful for the organization and also the customer.

References

[1] Benes, L. (2013). OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. *Journal of Strategic Security*, *6*(3Suppl), 22–37. https://doi.org/10.5038/1944-0472.6.3s.3

[2] Crane, L., Gantz, G., Isaacs, S., Jose, D., & Sharp, R. (2013). *Introduction to Risk Management: Understanding Agricultural Risk*. 39. Retrieved from http://www.extensionrme.org/pubs/IntroductionToRiskManagement.pdf

[3] Dahl, O. (2005). *Using coloured petri nets in penetration testing*. 89. Retrieved from http://brage.bibsys.no/xmlui/handle/11250/143799

[4] de Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The ISO 31000 standard in supply chain risk management. *Journal of Cleaner Production*, *151*(March), 616–633. https://doi.org/10.1016/j.jclepro.2017.03.054

[5] Dirgahayu, T., Prayudi, Y., & Fajaryanto, A. (2015). Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server. *Jurnal Ilmiah NERO*, *1*(3), 190–197. Retrieved from http://nero.trunojoyo.ac.id/index.php/nero/article/download/29/27

[6] Edam, H. A. Ü., Ctga, O., Edam, H. A. Ü., Ctga, O., & Üniversitesi, K. H. (2018). *Digital Open Source Intelligence and International Security : A Primer Digital Open Source Intelligence and International Security : A Primer*. (July).

[7] Fitri, S. D., Setyowati, D. L., & Duma, K. (2019). *Implementasi Manajemen Risiko Berdasarkan ISO 31000 : 2009 pada Program Perawatan Mesin di Area Workshop PT . X*. *6*(1), 16–24.

[8] Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. *Creative Information Technology Journal*, *4*(4), 264. https://doi.org/10.24076/citec.2017v4i4.119

[9] Hasan, A., & Meva, D. (2018). Web Application Safety by Penetration Testing. *4TH International Conference on Cyber Security (ICCS)*, (January), 159–163.

[10] Hassan, N. A., Hijazi, R., Hassan, N. A., & Hijazi, R. (2018). The Evolution of Open Source Intelligence. *Open Source Intelligence Methods and Tools*, (1), 1–20. https://doi.org/10.1007/978-1-4842-3213-2_1

[11] Hoepman, J.-H. (2014). *Privacy Design Strategies*. *9*, 446–459. https://doi.org/10.1007/978-3-642-55415-5_38

[12] Husein, G. M., & Imbar, R. V. (2015). *Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT . Jabar Telematika (JATEL)*. *1*, 75–87.

[13] Hussain, M. Z., Hasan, M. Z., Taimoor, M., Chughtai, A., Taimoor, M., & Chughtai, A. (2017). Penetration Testing In System Administration. *International Journal of Scientific & Technology Research*, *6*(6), 275–278.

[14] Jenter, D., Rock, M., & Morgenstern, P. H. (2014). *Scientific Approach on OSINT Training Program Development based on a Skill-Management-System for European Law Enforcement Agencies*.

[15] Kawakita, M., & Shima, S. (2018). Detection, auto

analysis of cyber threats using open source intelligence. *NEC Technical Journal*, *12*(2), 80–84.

[16] Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management*, *14*(4), 272–300. https://doi.org/10.1057/rm.2012.9

[17] Lubis, A., & Tarigan, A. (2017). Security Assessment of Web ApplicationThrough Penetration System Techniques. *Jend. Gatot Subroto Km*, *4*(100), 296–303. Retrieved from www.pancabudi.ac.id

[18] Petersen, R. L. (2017). *Enhancing identification and reporting of potentially harmful public data on Danish organizations by Summary (English)*.

[19] Pratama, E., & Wiradarma, A. (2019). *Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study : X Company)*. (July), 8–12. https://doi.org/10.5815/ijcnis.2019.07.02

[20] Review, A., Mariani, A., & Oldra, S. B. (2015). *FRAMEWORK IMPLEMENTATION FOR OWASP*. (1).

[21] Sedek, K. A., Osman, N., Osman, M. N., & Jusoff, H. K. (2009). Developing a Secure Web Application Using OWASP Guidelines. *Computer and Information Science*, *2*(4), 137–143. https://doi.org/10.5539/cis.v2n4p137

[22] Sena, A. De. (2019). *ISO Standards Applicability and a Case Study About ISO 31000 in a Portuguese Municipality*. *4*(4), 102–111. https://doi.org/10.11648/j.ajtab.20180404.11

[23] Shanley, A., & Johnstone, et al. (2015). Selection of penetration testing methodologies: A comparison and evaluation. *AISMC - Australian Information Security Management Conference*, *2015*, 65–72. https://doi.org/10.4225/75/57b69c4ed938d

[24] Stiawan, D., Idris, M. Y., Abdullah, A. H., Aljaber, F., & Budiarto, R. (2017). Cyber-attack penetration test and vulnerability analysis. *International Journal of Online Engineering*, *13*(1), 125–132. https://doi.org/10.3991/ijoe.v13i01.6407

[25] Sukapto, P., Desena, J. D. H., Ariningsih, P. K., & Susanto, S. (2018). Integration of risk engineering by ISO 31000 and safety engineering: A case study in a production floor of sport footwear industry in Indonesia. *International Journal of Simulation: Systems, Science and Technology*, *19*(4), 22.1-22.12. https://doi.org/10.5013/IJSSST.a.19.04.22

[26] System, A., & Marx, M. (2014). *The Extension and Customisation of the Maltego Data-Mining Environment into*.

[27] Yeboah-Ofori, A. (2018). Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics*, *7*(1), 87–98. https://doi.org/10.17781/p002378

[28] Young, J., Campbell, K., Fanti, A., Alicea, A., & Weiss, M. (2018). The Development of an Open Source Intelligence Gathering Exercise for Teaching Information Security. *Thirteenth Midwest Association for Information Systems Conference*, (May 2018).

Authors' Profiles

Anak Agung Bagus Arya Wiradarma is the 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, network programming, and network security application.

Gusti Made Arya Sasmita, Male, is a lecturer at Department of Information Technology, Faculty of Engineering, Udayana University Bali, Indonesia. He got his bachelor's degree in Electrical Engineering, Udayana University, Bali in 1997 and master's degree in Informatics Engineering, Gadjah Mada University in 2003. His research interests are Audit and Network Security.

How to cite this paper: Anak Agung Bagus Arya Wiradarma, Gusti Made Arya Sasmita, "IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company)", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.12, pp.17-29, 2019. DOI: 10.5815/ijcnis.2019.12.03