IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT (Case Study: Election Commission of X City)

Agenda

- Item 1
  - Details
- Item 2
  - Details
- Item 3
  - Details
- Item 4
  - Details
- Item 5
  - Details
- Item 6
  - Details

Open Source Talk

This medium talk based on how the open source project connects with IT security aspects. Some open sources project that taking part on this paper are OWASP and OSINT, and it will show how the combination of open source project can create a better security performance on the context of IT risk management concept of the related organization / case studies.

enjoy :)

Behind the Scene…

high mobility & Information disclosure

illegal action of information manipulation

website security & protection importance

testing standardization and availability

risks concern

risk handling recommended actions

Research Objective & Limitation

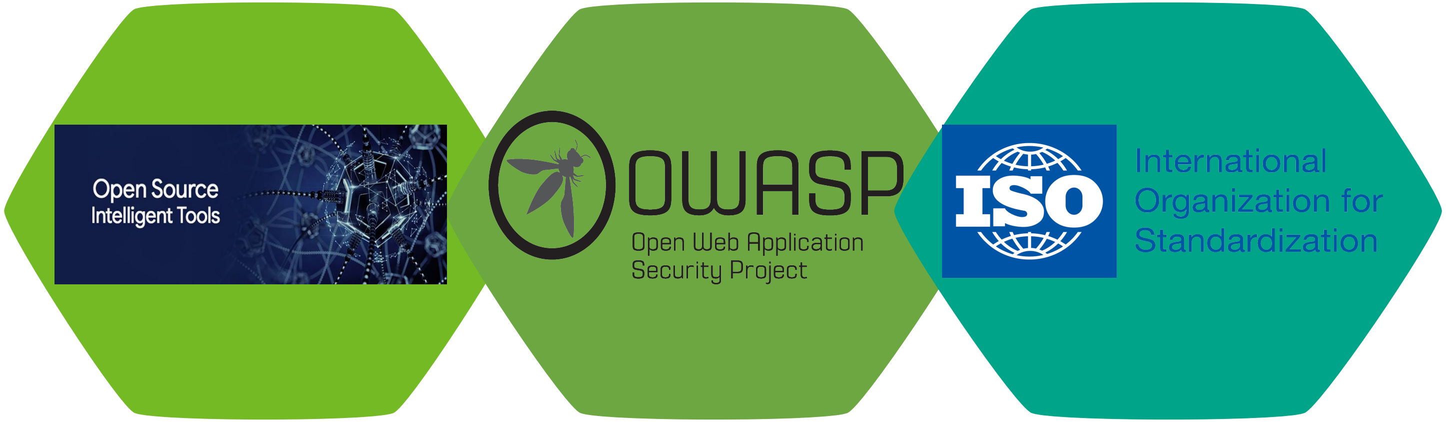
- Identify the security level and system vulnerabilities on the official website of the Election Commission of X City.
- Identify the testing results and analysis on the official website of the Election Commission of X City using the OWASP Framework.
- Giving recommended actions to improve security and protection on the official website of the Election Commission of X City.

- The research only focuses on the security testing of the official website of the Election Commission of X City through penetration testing method using the OWASP Testing Guide version 4 and tools with the concept of Open Source Intelligence with risk management guidelines based on ISO 31000 Framework.
- The research results only up to the evaluation report and recommended actions that were offered, so the decision of upgrading or changing the website system depended on the related organization

The Primary Parts

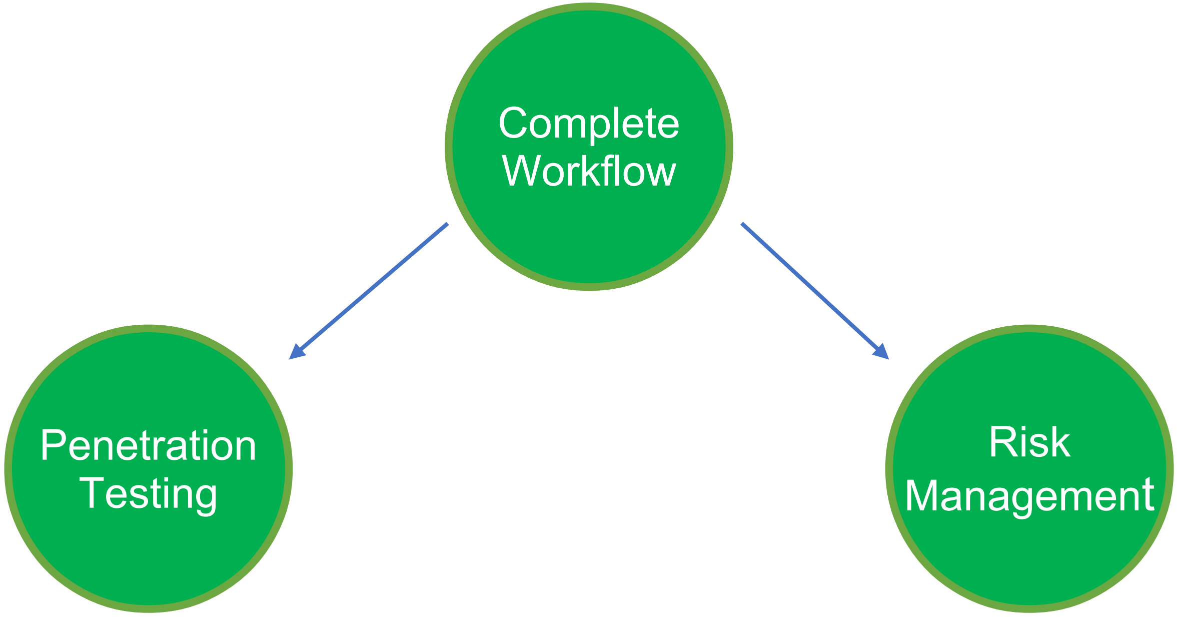
OSINT // OWASP // ISO 31000

OSINT (*Open Source Intelligence*) is part of an intelligence discipline that based by public data sources analysis for the information acquisition and certain intelligence needs. **//** OWASP is a non-profit organization that focused on improving software security. **//** ISO 31000 is one of the guidelines issued by ISO (International Standard Organization) for the treatment of risk management activities.



Research Methodology

The research workflow is illustrated by 3 main flowcharts which show the research primary points ...



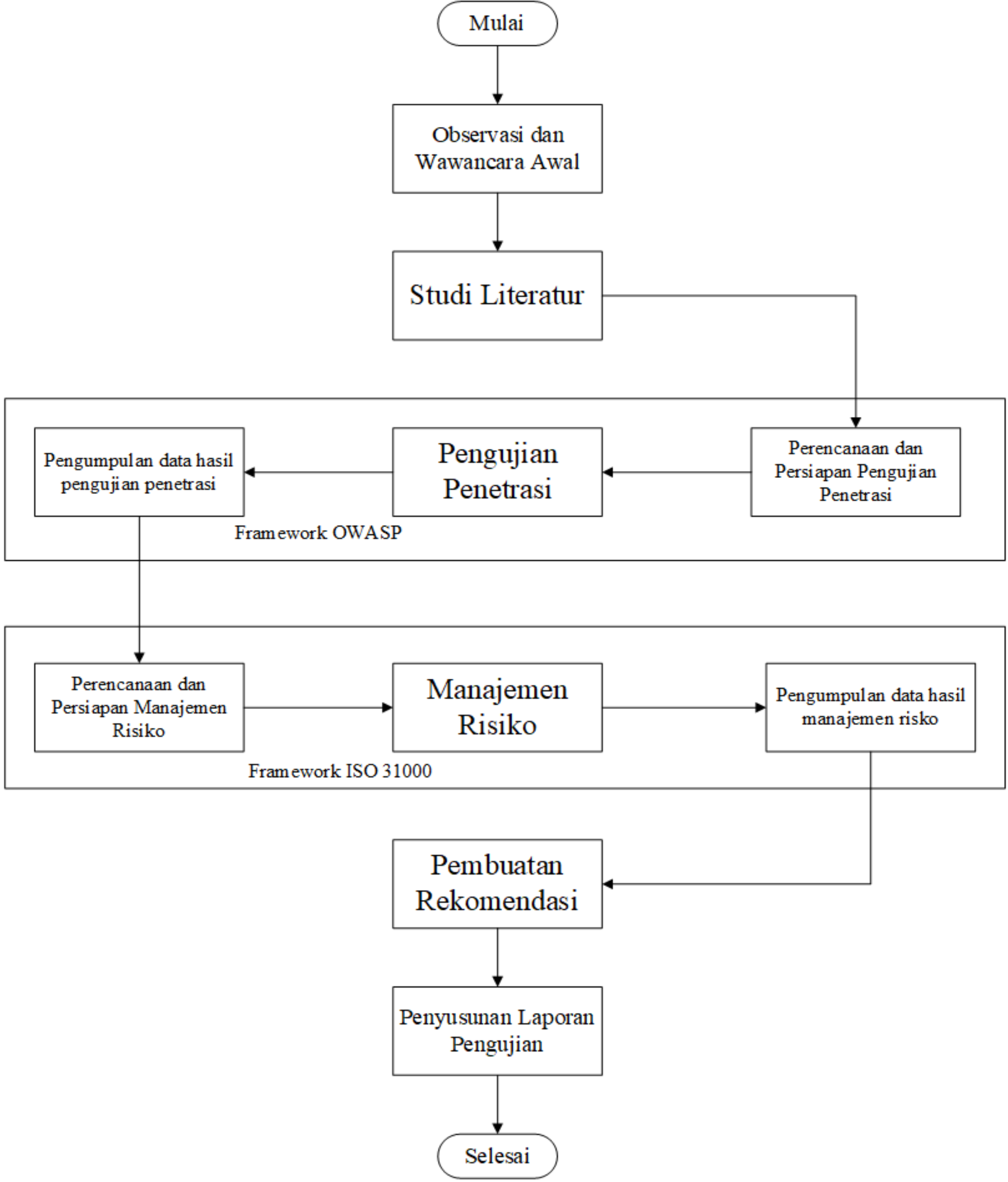
Main Flowchart

Preliminary Observation & Literature Study

Penetration Testing

Risk Management

Recommended Actions & Testing Reports

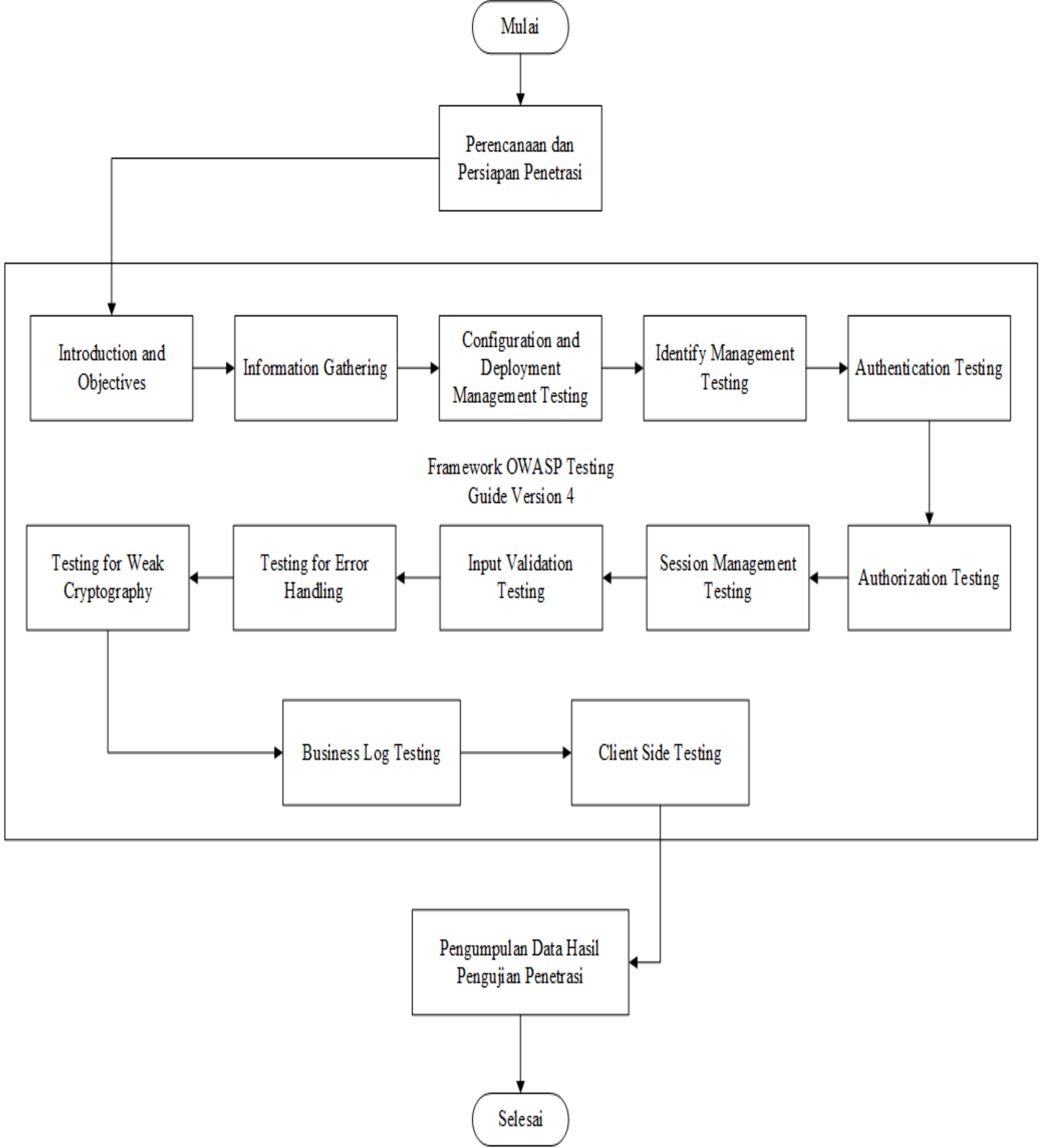

Mulai
Observasi dan Wawancara Awal
Studi Literatur
Perencanaan dan Persiapan Pengujian Penetrasi
Pengujian Penetrasi
Pengumpulan data hasil pengujian penetrasi
Framework OWASP
Perencanaan dan Persiapan Manajemen Risiko
Manajemen Risiko
Pengumpulan data hasil manajemen risko
Framework ISO 31000
Pembuatan Rekomendasi
Penyusunan Laporan Pengujian
Selesai

Penetration Testing Flowchart

OWASP Testing Guide Version 4

OSINT based testing

11 modules, 90 total submodules

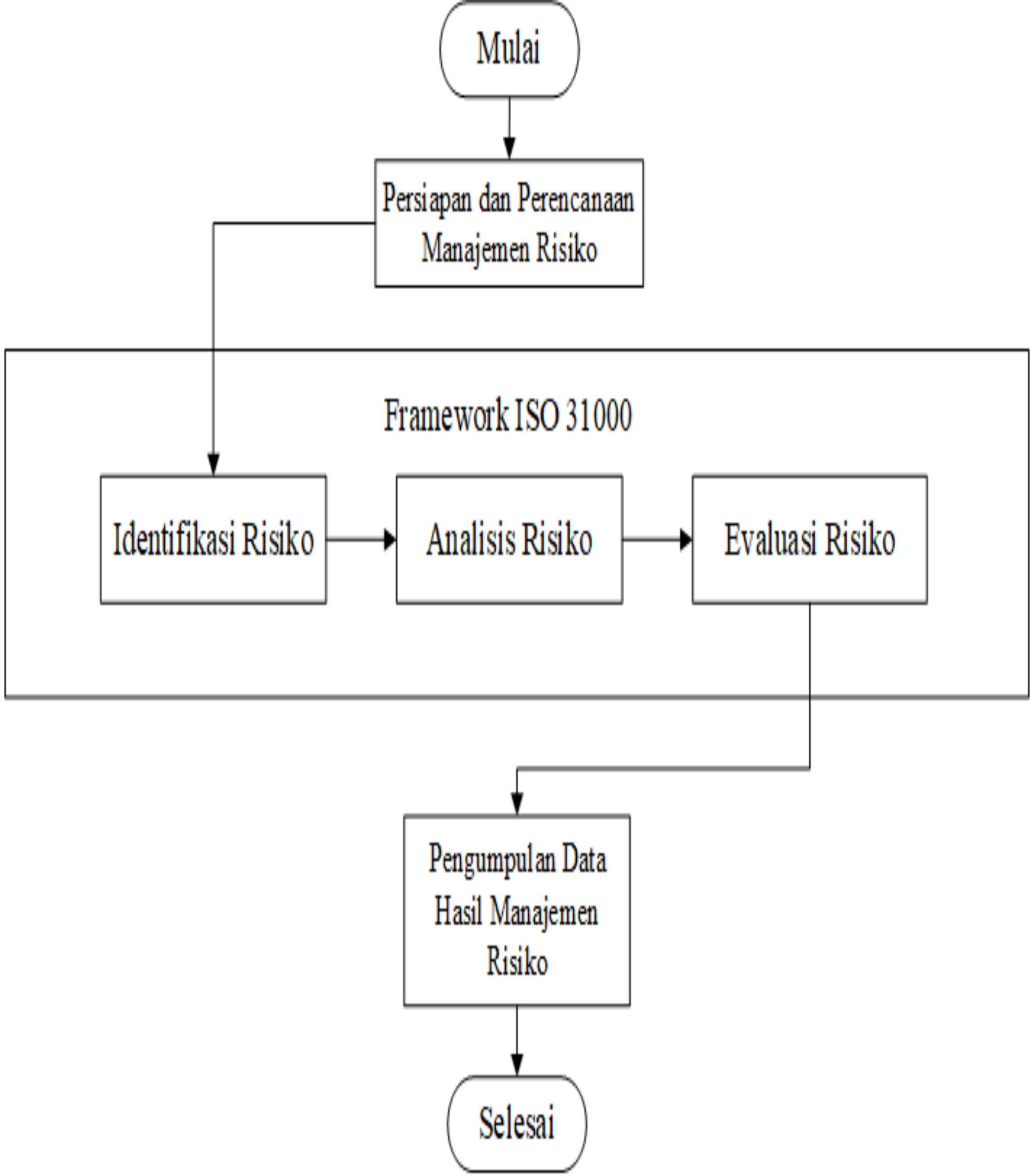

Mulai
Perencanaan dan Persiapan Penetrasi
Introduction and Objectives
Information Gathering
Configuration and Deployment Management Testing
Identify Management Testing
Authentication Testing
Framework OWASP Testing Guide Version 4
Authorization Testing
Session Management Testing
Input Validation Testing
Testing for Error Handling
Testing for Weak Cryptography
Business Log Testing
Client Side Testing
Pengumpulan Data Hasil Pengujian Penetrasi
Selesai

Risk Management Flowchart

ISO 31000

Risk assessment

Risk identification, analysis, evaluation


Mulai
Persiapan dan Perencanaan Manajemen Risiko
Framework ISO 31000
Identifikasi Risiko
Analisis Risiko
Evaluasi Risiko
Pengumpulan Data Hasil Manajemen Risiko
Selesai

OWASP Open Web Application Security Project | Testing Guide 4.0

✅SUCCESS ❌FAIL ⚠️POSTPONED

Penetration Testing Results
OWASP Testing Guide Version 4

OWASP Testing Guide V4 Testing Modules

- Testing for Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for Weak Cryptography
- Business Logic Testing
- Client Side Testing

Penetration Testing Results
OWASP Testing Guide Version 4

Modules	Submodules	Submodules Test Results
Testing for Information Gathering	**10**	4 Success, 6 Failed
Configuration and Deployment Management Testing	**9**	5 Success, 2 Failed, 2 Passed
Identity Management Testing	**5**	5 Postponed
Authentication Testing	**10**	2 Failed, 8 Postponed
Authorization Testing	**4**	3 Failed, 1 Postponed
Session Management Testing	**8**	3 Success, 5 Postponed
Input Validation Testing	**17**	3 Success, 9 Failed, 5 Postponed
Testing for Error Handling	**2**	1 Success, 1 Failed
Testing for Weak Cryptography	**4**	3 Success, 1 Postponed
Business Logic Testing	**9**	2 Success, 6 Failed, 1 Postponed
Client Side Testing	**12**	4 Success, 3 Failed, 5 Postponed

Details:

11 main modules with 90 total submodules testing

25 succeed submodules, 32 failed submodules, dan 33 submodules postponed

International
Organization for
Standardization

Risk Management Results
ISO 31000

Risk Assessment; Identification >> Analysis >> Evaluation

Risk Identification

Risk Code	Risk Identification
R1	Reviewing website developer comments and metadata
R2	Finding website system and workflow mapping
R3	Reviewing website developing framework
R4	Reviewing website version
R5	Finding website main architecture and overall connected system mapping
R6	Finding security verification of file extension types
R7	Reviewing irrelevant files on the website.
R8	Testing the web server authentication mechanism.
R9	Testing the bypass action of the website authentication mechanism.
R10	Testing the parameters validation used in the website directory.
R11	Testing the bypass action of the website authorization mechanism.
R12	Reviewing website developer comments and metadata

Risk identification processes will generate a list of risks that may happen on every IT resource that the case studies organization have. On this risk identification context, the scope of process will take on the vulnerabilities obtained from testing results of penetration testing using all of modules on OWASP Testing Guide Version 4 framework, amounting to 11 modules and OSINT-based tools assistance.

Risk Identification

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*

The risk analysis process will analyze the risk calculations based on the risk identification process. This process continues with determining the level of likelihood and impact of the risk listed. The level of likelihood and risk impact will be a main source for assessing the level of each risk.

An assessment of the risk impact and likelihood level is given based on internal and external conditions of the organization's system and the sources related regarding the likelihood and impact of each existing risk

Matrix Table of Risk Level Assessment

Impact					
5	🟨	🟨	🟥 R19	🟥 R22	🟥 R14, R17
4	🟩 R12, R13	🟨 R11, R18	🟨 R1, R10, R20, R28, R29	🟥 R9, R16	🟥
3	🟩 R30, R32	🟨 R15	🟨 R4, R6, R8	🟨	🟥
2	🟩 R31	🟩 R5, R27	🟨 R3, R7, R21, R24	🟨 R7	🟨
1	🟩	🟩 R2, R25, R26	🟩 R23	🟨	🟨
	1	2	3	4	5

Probability

Detail:

Green: Low

Yellow: Medium

Red: High

Risk Evaluation

Risk Code	Risk Identification	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.	Medium
R2	Discovering the developer comments on the website target and find leaked information and metadata to have better system knowledge.	Low
R3	Creating the system mapping of the target website and understanding the main workflow.	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.	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.	Low
R6	Discovering and knowing the overall system architecture and workflow of the target website.	Medium
R7	Discovering the vulnerabilities and security holes in the way the target website works to validate the types of file extensions that can enter the system.	Medium
R8	Finding files that are outdated, invalid, and no longer relevant to the current conditions of target website to look for information leaks in the context of deeper exploitation of the system.	Medium
R9	Discovering the vulnerabilities and security holes in the authentication mechanism used in the application configuration and management of computing resources on the target web server.	High
R10	Discovering the vulnerabilities and security holes in website authentication mechanisms when receiving bypass actions from users.	Medium
R11	Discovering the vulnerabilities and security holes in the validation system of parameters used by the website.	Medium
R12	Discovering the vulnerabilities and security holes on the user authorization page that displayed on the website.	Low

The risk evaluation process is carried out by starting the calculation of the impact and likelihood matrix table values to determine level of each risk.

Based on the ISO 31000 standardization, the risks that must be prioritized by examiners are at medium and high levels. The matrix table that contains a mapping and assessment of the impact and likelihood values shows 21 out of 32 risks that are at medium and high levels.

…The Explanation Continues…

The matrix table that explains a mapping and assessment of the impact and probability rating, shows 21 risks out of 32 risks that are at medium and high levels and those risks have a significant effect and can cause major loss on the organization system if not handled properly.

After the risk evaluation process is completed, it has been found that detailed explanation are 11 risks with a low level, 15 risks with a medium level, and 6 risks with a high level. The final step is to create and plan the recommended actions for later can be applied when the risks that have been identified, analyzed, and evaluated happen in related organizations.

These actions are needed to overcome the outcome and consequences that will happen on the organization if the risk occurs, and the proper handling of the condition’s aftermath.

IT Risk Management
Recommended Actions

The last stage of this research is making recommended actions and treatments to handle the outcome and consequences of risks to the organization. All of the recommended actions for overcome the risks is expected to help maintain and enhance the capabilities of IT system, services, and information management from the organization to customers and also to keep the organization stable in achieving the goals. The treatment of every each of the risk that are already identified, analyzed, and evaluated are explained on next table …

Risk Code	Risk Treatment
R1	Implementing an Intrusion Detection System (IDS) and a Honeypot system that has the function to detect unauthorized login activity and prevent further attacks. Enabling the Port Scanner Detection function on a router can be a good recommendation to avoid advanced system penetration by attackers.
R3	Implementing an Intrusion Detection System (IDS) and a Honeypot system that has the function to detect unauthorized login activity and prevent attacks. The use of encryption and reducing sensitive information that opened to the public can also be done.
R4	Learn and apply how to secure a website framework that used on the website, which has different methods and procedures for each framework to prevent penetration attacks and control switchover by attacker. More detailed recommendations for advanced security action is administrators can use advanced queries or scripts to protect websites from various forms of malicious attacks, such as XSS Scripting & SQL Injection.
R6	Website administrators can develop a website security mechanism as strong as possible to secure sensitive information from the entire web architecture when an attacker starts a scanning actions to gather information. Proxy Server, IDS, encryption, and security modules on every part of the website system can be used as a solution to secure website architecture information.
R7	Implementing security and protection of files types or extensions that uploaded to website by knowing and learning the programming language used to build related websites, because each programming language has different ways and mechanisms in compiling the scripts used to make the system file extension validation
R8	Administrators of the website are expected to do a files reviewing that stored and displayed to the public on websites with outdated conditions and are no longer relevant based on the current situations to prevent the manipulated information by the attacker to be used as objects of further attacks. If there are such files, the administrator can immediately delete them from the website.
R9	Implementing the security mechanism for application that has responsibility to configure the computing resources installed on a web server (in this case: Cpanel & WHM), the application of security can be done by: • Use strong passwords • Uses firewall, anti-virus and anti-rootkit protection • Update the application regularly • Using brute-force protection • Checking hosted websites, etc.
R10	Validating authentication security mechanisms that can be attacked by bypassing actions by properly checking the permissions of each role on the website and tightening system access policies to prevent falsification of identities that shouldn’t valid.
R11	Applying security and protection mechanisms against web tampering attacks by: • Do not put parameters into the form of query string (URL) • Using one session token to reference an object that is stored in the server side cache (HTML Form Field) • Using cryptography on the HTTP Header sent from the server side (HTTP Header) • Perform configuration on the server side to prevent parameter changes made by the attacker

…and so on until #risk29

CONCLUSION

The making of risk treatment with recommended actions of every risks on the organization is the main goal of this research. All the result and analysis of system vulnerabilities, weaknesses, and recommended actions from penetration testing security testing based in OWASP Testing Guide Version 4 framework and with applied OSINT concept, will help to maintain and improving the service capability of the company's and also to keeping up the company's main goal.

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.

2020

Finish

Thank You