Analysis And Implementation Of Operational Security Management On Computer Center At The University X

Ibnu Gunawan, Agustinus Noertjahyana, Hartanto Rusli
Department of Informatics Engineering, Faculty of Industrial Technology, Petra Christian University, Surabaya, Indonesia 60236
ibnu@petra.ac.id

Abstract - **This paper presents how to asses an Operational Security Management on Computer Center At the University X. In carrying out operations using information technology-based computer network, it is an organization needs to consider factors in information systems security. The Security of communication networks is absolutely necessary to be able to provide continuous service to its users. Most of the staff were involved in the making of this security policy, often feel confused in starting to work, due to not having enough experience or feeling that it will not require a policy because there was no incident related to a security policy. To resolve these problems, we need a tool to help the staff in making the security system design that is structured with implementation modules sourced from security policy and risk management module so that it can be monitored if an error occurs. In last section, this paper show how to testing by using the engine to perform the questionnaire calculations, making planning and operations. Occurs similarity between the results of risk management high risk states with a CISSP standard studied on a case study.**

Keywords : CISSP, Security, Planning and Operational.

INTRODUCTION

In carrying out operations based on information technology, especially with the use of a computer network infrastructure, organizations not only need to make a good information system, but also need to consider the safety factor as one of the supporting information systems are reliable. Secure communications network is absolutely necessary to keep the organization in order to always be able to provide continuous service to its members. The need for this security system needs to be clearly defined and may ultimately be implemented in practice to be able to support operations in an organization's information systems. By applying the appropriate procedures for each activity, it is expected to be able to judge the right to security needs in accordance with what is required by the organization (Danchev, 2003).

To be able to build a security policy that provides a good foundation in the future, then the first step that must be developed is to create a security policy that can reduce the risk of misuse of the resources available in the organization.

Most of the staff were involved in the making of this security policy, often feel confused in the start of manufacture, because did not have enough experience or feeling not require a security policy because there was no incident related to a security policy.

University X grew even bigger this time and pick the various kinds of information systems to run their operations. With the increasing number of systems that exist in every activity, then this needs to be considered related to the security system.

Because of the problems it is an important need today is to help the staff to give depth to the design of a security system that is structured with modules sourced implementation of module security and risk management policies that can be monitored in case of violation.

SECURITY SYSTEM DESIGN

Many organizations underestimate the value of an IT asset owned, usually this is because IT is an indirect cost. In fact, if only there was an attack on the server, it will be able to lead the organization can not carry out their activities properly. The attack on the website may lead to an organization can not provide information services to the users / the customer's. Thus, the organization will lose both material and immaterial. By doing the design of an effective security system, it can help the organization to protect its assets (Noel, 2007). Overview of the relationship between the attack and the item can be seen in Figure 1.
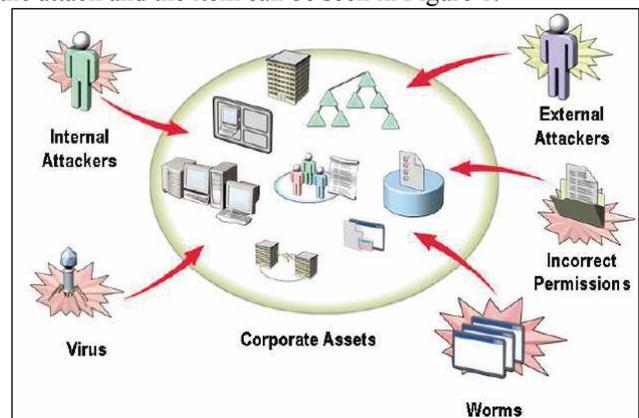

Fig 1. Asset and attacker

SECURITY POLICY

Security policy is a plan, which explains about what constitutes an important asset of the organization, and how to protect it (Danchev, 2003). The purpose of a security policy is to provide an explanation to the users of the system over which the assets are permitted to be used and which ones should not be used, and to then be entered into the part of the organization's security system.

Documents should be clear and easy source for any user to be able to understand and comprehend and define the resources that are potential targets of all sorts of attacks.

RISK MANAGEMENT

Risk management is a combination of the three processes (Stoneburner, 2002), namely: Risk Assessment, Risk Mitigation and evaluation.

1. Risk Assessment

The steps to perform risk analysis is as follows (Stoneburner, 2002):

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

2. Risk Mitigation

Good strategy to perform risk mitigation can be seen in Figure 2 (Stoneburner,2002).
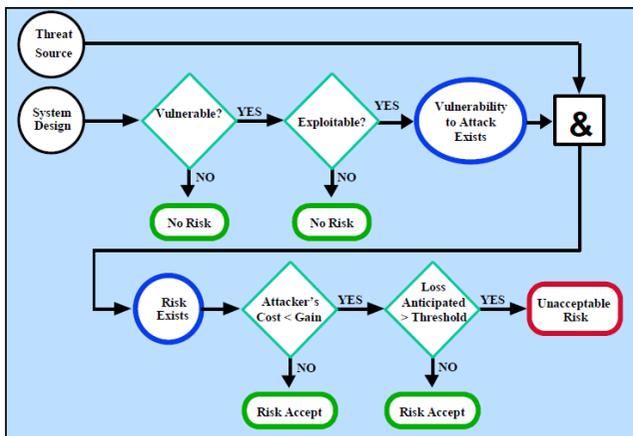

Fig 2 Risk Mitition Strategy (Stoneburner, 2002)

3. Risk Evaluation and Control

For the implementation of controls to prevent possible risks, organizations need to think about both the process control technically, management and operations, or do a combination of more than one control that aims to further streamline the process control of IT systems in the organization.

- Technical Control
  Technical controls can be grouped into 4 main categories like fig 3
- Management Security Control
- Operations Security Control

CISSP

CISSP (Certified Information System Security Professional) is a certification in the field of information security. (Conrad,2010) In accordance with current global progress, the need for security and development in the field of technology continues to evolve. Safety first is a hot issue in the technology alone, but now has become part of our lives everyday. Security noticed by any organization, government agencies, companies, and even military units.CISSP itself divides the definition of security in 10 areas called with 10

domains. 10 domains are considered to include all the parts of a computer, network, business, and security information. 10 domains in the CISSP is as follows:
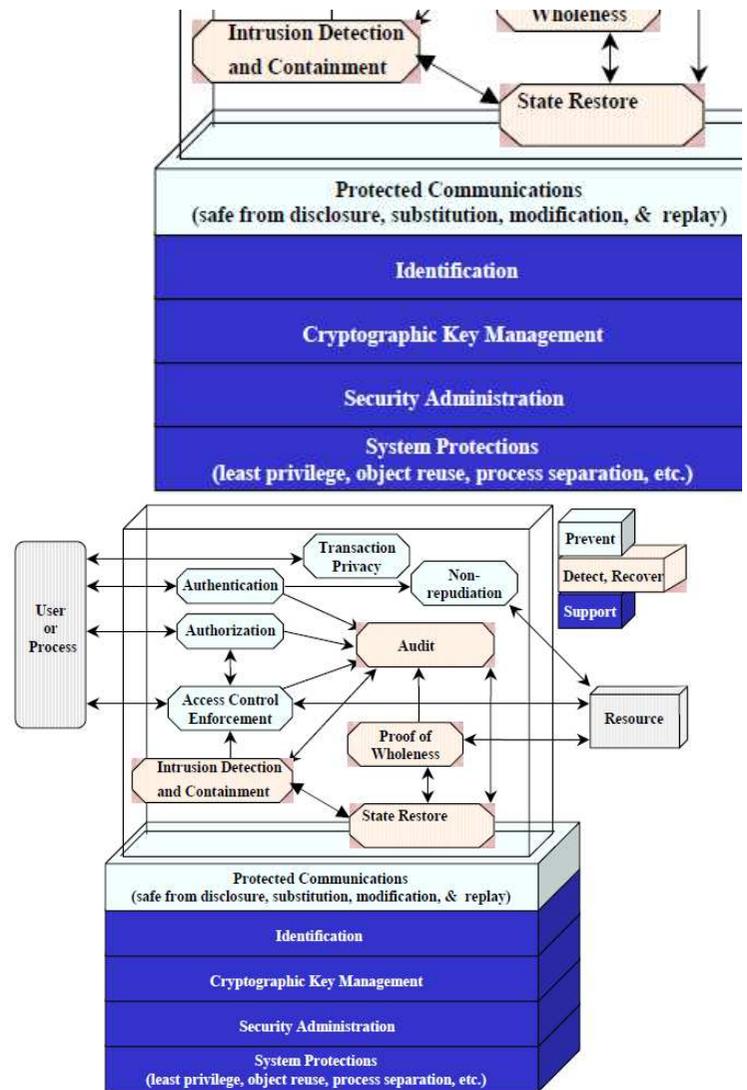

Fig 3: Technical control (Stoneburner, 2002)

REQUIREMENT ANALYSIS

University X is currently growing more rapidly with a mission of " IT - based campus" which means to use information technology more prevalent not only among faculty, staff , and staff but also the students who are in it . For example , for a staffing system that uses a special application , the system input value for each lecturer can enter grades online , academic system that provides registration services online student study plans , as well as other support systems . With these examples can be seen more and more systems started there and where any employee or student to use the same code for each system , so in this case required a security policy .

Given the problems it is necessary to do an analysis of the risk to the risk that information technology can impact the operations of University X. Through risk analysis , especially the university computer center which was subjected to more easily we can know the risks of what could happen , measure how big the risk is , and how its impact , and get the results of risk calculations Which is of particular concern to the risk that is not a priority special .

Of the subject has been mentioned that the central computer can handle all the problems that exist and also take the

policy from the calculation of risk that has been done . Thus the security system central computer can be safe and well monitored .

RISK ANALYSIS

Here is an example of questioner resulted of mapping

questioner CISSP standards and risk management that we do to some of the existing policy on university computer center x divided by user and system owner :

User Questioner sample:

1. Access Control

Questioner: 1. How often do you change your email password?

a. Once a month b. 3 months c. once a year
d. never

2. Security Architecture and Design

Questioner: 11. According to you, what qualities (specs) provided computer by computer center?

a. Is sufficient b. Mediocre c. less worthy

3. Physical and Environmental Security

Questioner: 15. How do you think about the environment control such as the placement of electrical wiring, placement of personnel, and fire safety?

a. Less well b. Pretty good c. very good

4. Telecommunications and Network Security

Questioner: 20. Did you know the IP address version 6?

a. Yes b. not

5. Cryptography

Questioner: 30. Was your password consists of a combination of small capital letters, containing numbers, and other requirements?

a. Yes b. not

6. Business Continuity and Disaster Recovery Planning

Questioner: 32. The event of a power failure during the learning process, if there is such a power generator to power the lights back on?

a. Yes b. not

7. Legal, Regulations, Investigations, and Compliance

Questioner: 35. Did you ever take advantage of the software license provided by the Computer Center as a CD-Key of Windows and other applications?

a. Yes b. not

8. Software Development Security

Questioner: 39. How does the quality of the software provided by the Computer Center? (if often error)

a. Excellent b. Fine, rare error c. Poor, often an error

9. Operations Security

Questioner: 41. How often do you see drivers (hard drive, flash) after accessing your computer infected with viruses at University X?

a. Often b. Rarely c. never

Owner Questioner sample:

1. Access Control

Questioner: 6. How many times authentication error tolerance limits owned by the user?

a. 3 times b. 5 times c. 10 times d. no restrictions

2. Security Architecture and Design

Questioner: 11. Is there a certain standard of maintenance of the computers used in the Computer Center Petra?

a. There, ... b. Not c. Do not Know

3. Physical and Environmental Security

Questioner: 16. How often the air conditioner (AC) to the central computer room or server room in the service?

a. 1 month b. 3 months c. 1 year d. never

4. Telecommunications and Network Security

Questioner: 29. Was there ever a network connection at the University experience down?

a. Ever, ... times b. Never c. Do not Know

5. Cryptography

Questioner: 37. Is there a standard encryption method to be applied to the document storage?

a. Yes b. Not c. Do not know

6. Business Continuity and Disaster Recovery Planning

Questioner: 39. Are there certain parts that perform the steps Bussiness Impact Analysis (BIA) in the event of an accident?

a. Yes b. Not c. Do not know

7. Legal, Regulations, Investigations, and Compliance

Questioner: 52. Was used software are protected from SQL Injection?

a. Yes b. Not c. Do not Know

8. Software Development Security

Questioner: 62. Was meeting minutes in a paper shredder if it is not used?

a. Yes b. Not c. Do not Know

And the some of the result can be seen on fig 4 below.

No.	Soal	Percentage Score	Likelihood
1	How often do you change your email password		
	A month	0	0
	3 month	2	0
	A year	21	2
	never	77	8
2	Do you log out after use email and the web service (sim.xxx.ac.id) University?		
	Yes	70	8
	Sometimes	18	2
	never	12	0
3	Is University X service that is easy you access the website?		
	easy	55	5
	sometimes	41	5
	hard	4	0
4	Is there any process other than password authentication when you login? (example: after entering the password, you will be asked to fill out a captcha or pin)		
	Yes	9	0
	no	73	8

Fig 4 example risk analysis questioner result

SYSTEM DESIGN

We will describe from system analysis to system design:

1. system analysis

For the purpose of obtaining information necessary for the design of security systems , need to be made questionnaire addressed to the user or population . Making questionnaires starting the login process , if entered as a guest it can only work on the questionnaire . If entered as admin then can create a project in which there is a menu -making questionnaire .

Project data will be stored into the database and the admin can continue on making the questionnaire . After that , the admin can create problems questionnaire and each

question will be saved in the database after stored , will directly Replaces zoom with Javascript using Ajax . Having had enough to make the necessary questionnaire questions , the admin can publish that question to be accessed and filled out by the user . Then after the user has filled out a questionnaire with a sufficient amount , then the application will make the process of scoring and the score will be recorded in the database .

The results of the scoring will be continued on the risk analysis process to find the priority , then the priority will be known by the admin and can continue on the planning process . In the planning process , the system will mendapatkankan priority data are consistent with the risk management process and entered into the database . Once the domain sorted by priority which is more important .

From the results that the user can view the guidelines to do to design a security system based on standard CISSP and will proceed to the operational process . At the operational processes , the admin can review the selected design in the planning process in accordance with the planning months on submit . In operation page can print the report .

To provide a login feature, create project, view the questionnaire, the questionnaire publish, view answers to questionnaires, planning, and operational then built a system which consists of four components, namely, PHP, Web Services, Javascript, and database servers. In PHP component, there is the user interface for logging, manufacture of a new project, view project, questionnaire development, view the questionnaire, and publish the questionnaire.

To perform these features, the web service is needed in order to display the project data and questionnaire data. The data obtained from the database server component.

That is a MySQL database that is stored on the server. Access to the database is done by the web service components then the data is displayed every time the user accesses the page questionnaire project or appearance. To be able to perform the create, view, update, and delete the database required admin privileges.

2. system design

In general, the application is made is divided into two parts, namely the design of the system admin and Guest. In the design of the admin and guest system will be described by using use case and activity diagrams.

a. admin system design

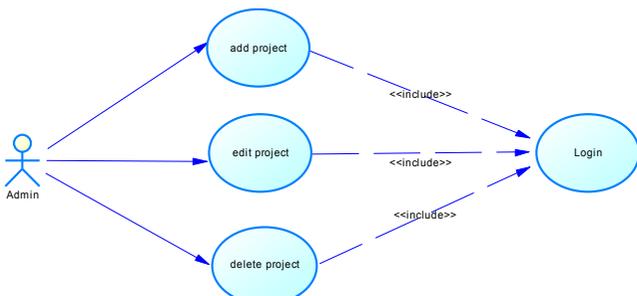In the admin system design is necessary to design a system design to fit the needs.

Fig 5 Use Case Diagram on Page Project Admin

A system design using Use Case Diagram and Activity Diagram is used to model the behavior of users at

once describe a work flow system and the system components. For more detail example, please see fig 5.

After we compose an use case diagram, next we move to the activity diagram. For a single example, please see fig 6.
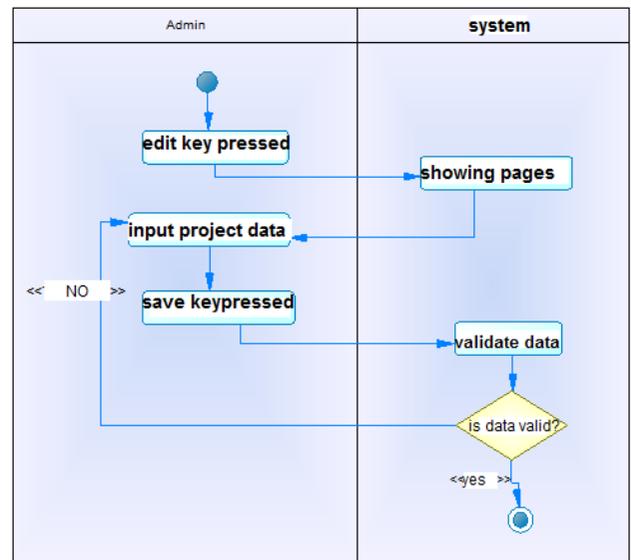
Fig 6. Activity diagram admin edit project

And then we can build an entity relationship diagram like showed on fig 7 on the next page. After we build our database then we can move on to design our application user interface. We showed one of them on fig 8.
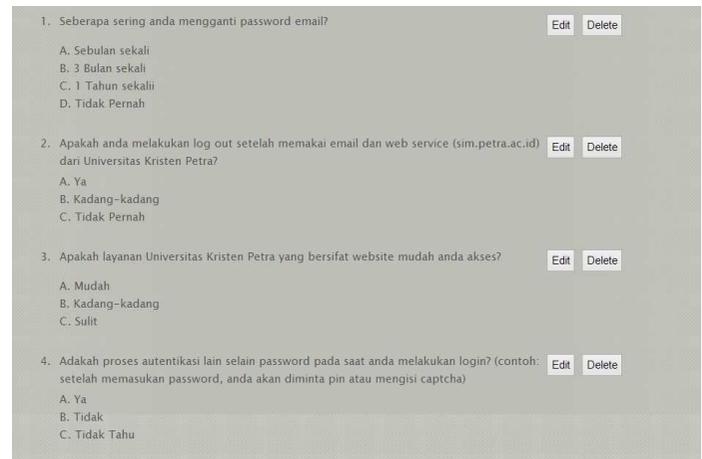
Fig 8 UI Design

SYSTEM IMPLEMENTATION

This section will explain the implementation of the interface and implementation of an application system that has been created. In order for the program to run properly, you should perform the installation on the computer prior to use. Software necessary for the program to run properly is to use notepad + + and XAMPP localhost server. In making this application requires a connection using localhost as quickly as do the development and testing of applications.

The process of making a software application in the project will use the PHP language with the help of Javascript and Ajax to make the user interface more attractive. For database management, using PhpMyAdmin.

Login

Username	<pi>	Variable characters (50)	<M>
Password		Variable characters (50)	

Identifier_1 <pi>

Question_Detail

Question_Detail_ID	<pi>	Integer	<M>
Choice		Variable characters (100)	
Choice_Type	<pi>	Integer	<M>
Explanation		Integer	
Score		Integer	

Identifier_1 <pi>

Mempengaruhi

mempunyai

Project

Project_id	<pi>	Integer	<M>
Project_Name		Variable characters (50)
Questionnaire_Title		Variable characters (100)
Published		Integer

Identifier_1 <pi>

mempunyai

Memiliki

Question

Question_id	<pi>	Integer	<M>
Question		Variable characters (300)	
Order		Integer	
weight		Integer	
Suggestion		Variable characters (1000)	

Identifier_2 <pi>

Planning_Result

Planning_Id	<pi>	Integer	<M>
Date		Date & Time	

Identifier_1 <pi>

mempunyai (D)

Answer

Answer_Id	<pi>	Integer	<M>
Date		Date & Time	
Score		Integer	

Identifier_1 <pi>

Priority_Result

Priority	Integer

mendapat

Menggolongkan

Mengelompokkan

Memiliki

memiliki

Plaaning_Result_Detail

Checked	Integer

Question_Answer

Question_Answer_Id	<pi>	<Undefined>	<M>
Number		Integer	
Question		Variable characters (300)	
AnswerType		Integer	
Score		Integer	

Identifier_1 <pi>

mempunyai

Domain_Table

Domain_Id	<pi>	Integer	<M>
Domain_Name		Variable characters (100)	
Description		Variable characters (500)	

Identifier_1 <pi>

mempunyai

Question_Answer_Detail

Choice_Type	<pi>	Integer	<M>
Choice		Variable characters (100)	
Explanation		Integer	
Score		Integer	
Marked		Integer	
Explanation_Answer		Variable characters (100)	

Identifier_1 <pi>

Domain_Suggestion

Suggestion_Id	<pi>	Integer	<M>
Suggestion		Variable characters (1000)	
Risk		Variable characters (500)	
Order		Integer	

Identifier_1 <pi>

Mengacu

melihat

Custom_Planning_Result_Detail

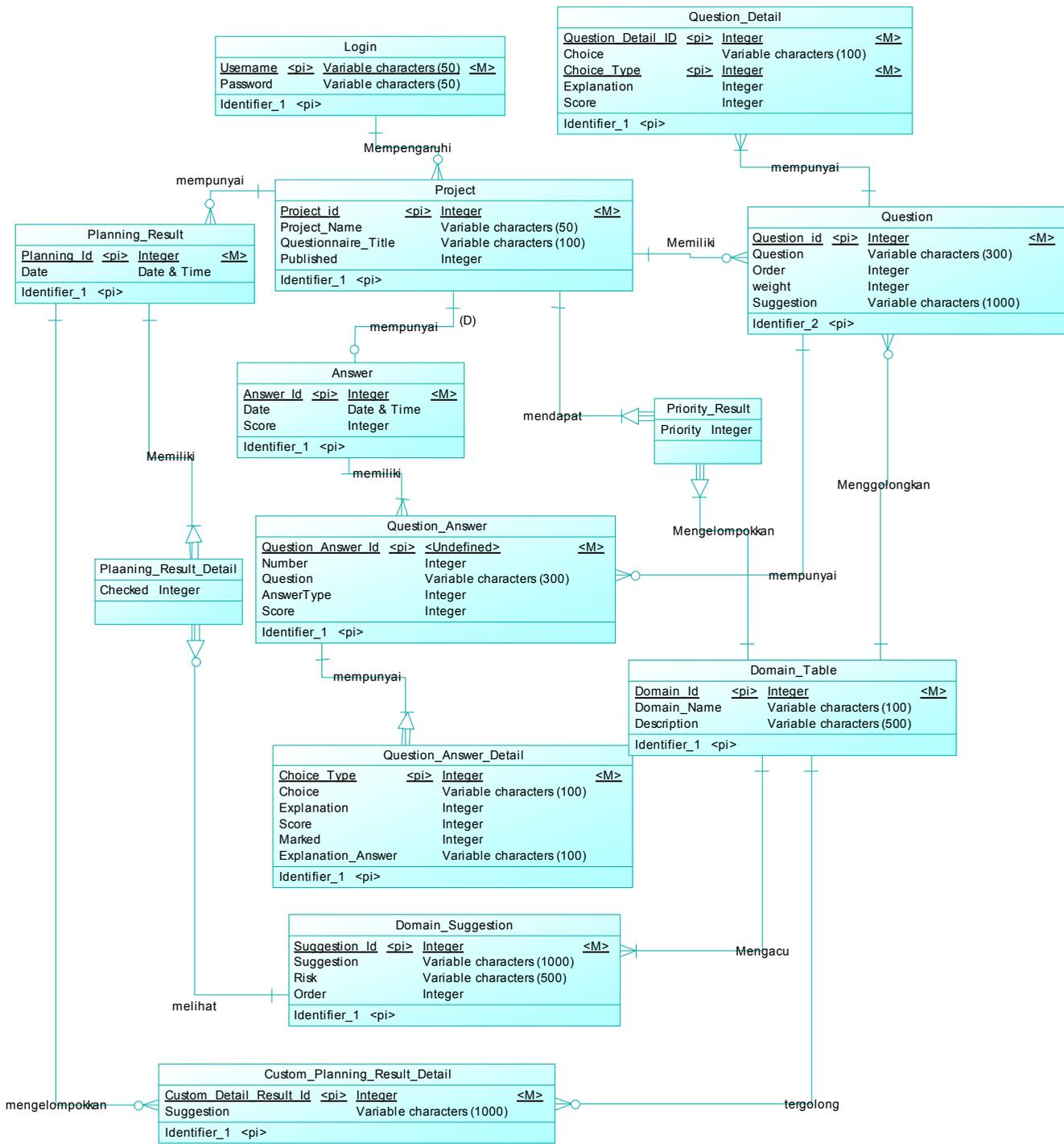|			
Custom_Detail_Result_Id	<pi>	Integer	<M>
Suggestion		Variable characters (1000)	

Identifier_1 <pi>

tergolong

mengelompokkan

Fig 7 E-R diagram

We use standard library has been used by many programmers in the world to make a good web application and accompanied by supporting the use of other libraries. Some libraries used in the application of this thesis include:
• Ajax, which is used to make the user interface more attractive to look at.
• Jquery-ui, which is used to make the look more fresh and more colorful. for example source code we can see on fig 8

```
openAddDialog = function(){

    $( "#nama" ).val( "" );

    $( "#judul_kuesioner" ).val( ""
);

    $( "#adddata" ).dialog( "open"
);

    mode = 'add';

    editId = 0;

}
```

Fig 8. Example source code

SYSTEM TESTING
        This section will describe the results of the testing of the software to evaluate the results of the calculation of the questionnaire to preparing operational reports. As for the types of tests performed, among others:
• Tests on the calculation of the questionnaire.
• Tests on the planning results.
• Testing of operational reports.
• Tests on the results of standardized management CISSP.

TESTS ON THE CALCULATION OF THE QUESTIONNAIRE
In the software will do the calculations testing the questionnaire as an administrator and the steps needed to achieve calculation of the questionnaire.
To achieve the calculation of the questionnaire, the user needs to do:
1. Perform login as we can see on fig 9
2. Creating a project as we can see on fig 10
3. Creating a questionnaire as we can see on fig 11
4. Publishing the questionnaire as we can see on fig 12
5. Seeing the results of the percentage of responses to questionnaires as we can see on fig 13
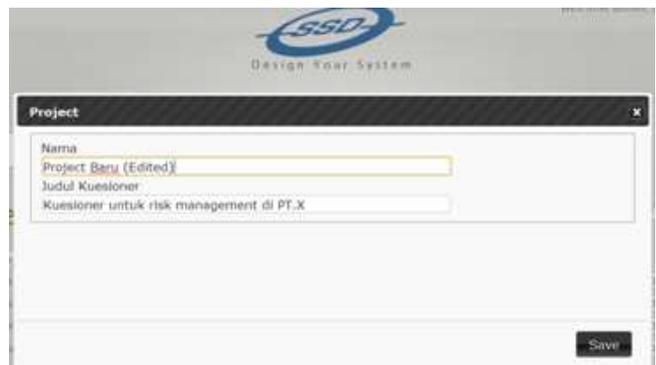

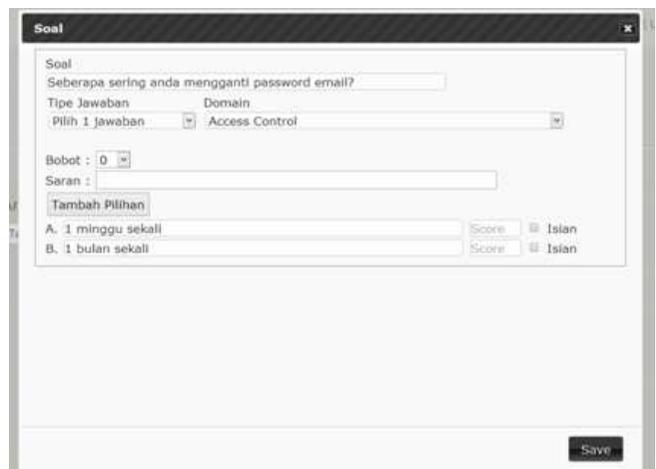Fig 9. Perform Login

Fig 10. Creating a project

Fig 11. Creating a questionaire

Fig 12. Publishing questionnaire

Fig 13. Percentage result

TESTS ON THE PLANNING RESULTS

Tests conducted on the parameter selection of standard CISSP per domain, the addition of a custom planning, and manufacturing planning. Testing begins from planning to go to the admin page. Planning page aims to provide a security administrator is not standard raw CISSP Security Administrator to assist in the making of a good security system. This planning page gets the input data is a result of risk management priorities and made the accordion and classification based on per domain CISSP. For the result we can see on figure 14, 15, and 16.

Fig 14 planning result on admin pages

Fig 15 CISSP List Standard

TESTING OF OPERATIONAL REPORTS

Tests conducted on election planning parameters, the addition of a custom planning, planning and record keeping.

The test starts with the opening page of the menu operations through operations on the home page. Upon entry into the operational page, the user can select a link in the form of month and year format in accordance with the planning in the submit. The goal is for a review of the standard CISSP selected on the planning process. We can see the result start on figure 17, figure 18, to figure 19.

fig 16. Adding domain suggestion
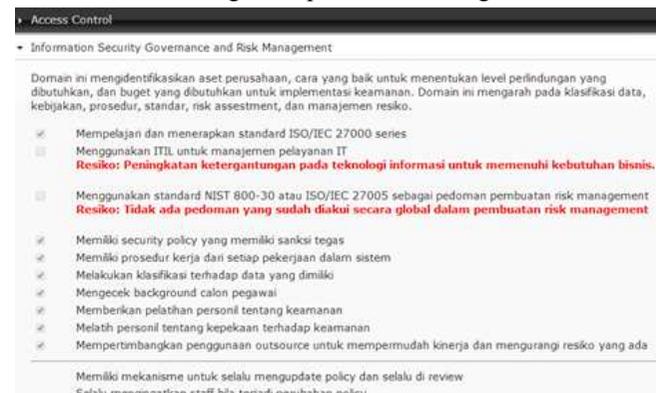

Fig 17. Operational testing

Fig 18 adding operational list detail

TESTS ON THE RESULTS OF STANDARDIZED MANAGEMENT CISSP

In the software will be tested in the operational process proceeds by month and year of planning was made. Tests carried out on standard-making parameters CISSP, CISSP standard modification, and deletion of the CISSP standard.

Fig 19.downloadable report

The first step taken by the user is to login as the auditor as can be seen in fig 20

Fig 20 Log in as an auditor

After auditors login, then the user will go to the main menu as an auditor as we can see in figure 21

Figure 21 auditor menu

After entering as an auditor, the user can choose to view the menu and edit standard CISSP domains of the CISSP. CISSP Domain menu, the user can see the description of the 10 domains of the CISSP. CISSP Domain menu at all access login as admin and guest. We can see it on figure 22.

Once users see what CISSP 10 Domains and description, users can perform on Standards CISSP management by selecting the Edit menu CISSP Standards. As we can see on figure 23.

Figure 22. CISSP 10 domain menu

Figure 23. CISSP Standard Edit menu

CONCLUSION

Based on a system that has been developed and the results of the testing that has been done, we can conclude some of the following:

- we have been made a editable questionaire engine for Security Administrator so that it can be changed by the user or in a custom suit your needs.
- It takes a long time to make access to the database. The cause of this can be assumed from XAMPP localhost program that is not compatible with Windows 8, or due to use mysqli as the database programming language that led to slower access speeds as seen many case studies that use a MySQL database programming language gain access speed is much faster.
- There are similarities between the results of risk management stating risk in a high risk category to the CISSP standard on the operational part. The things that need to be considered by the Computer Center, is giving the password on the storage media (flash, portable hard drive), imposes limits on the user authentication fault tolerance, disaster evacuation drills Giving, Restrict access so that employees can not do indiscriminate access outside offices, and users rarely or never change the password periodically

REFERENCES

Conrad, Eric. (2011). "Eleventh Hour CISSP Study Guide". Syngress, 2010.

Danchev, Dancho. (2003). "Building and Implementing a Successful Information Security Policy". Internet Software Marketing. Windows Security.com

Noel, Michael. (2007). "Microsoft ISA Server 2006 Unleashed". Sams Publishing, 2007.

Stoneburner, Gary., Alice Goguen, and Alexis Feringa. (2002). *Risk Management Guide for Information Technology System.* NIST Special Publication 800-30.