10141235

by 2 Agus

Submission date: 17-Mar-2023 11:21AM (UTC+0700)
Submission ID: 2039105709
File name: jeas_1014_1235.pdf (508.45K)
Word count: 3837
Character count: 20645

VOL. 9, NO. 10, OCTOBER 2014 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ANALYSIS AND IMPLEMENTATION OF OPERATIONAL SECURITY MANAGEMENT ON COMPUTER CENTER AT THE UNIVERSITY X

Ibnu Gunawan, Agustinus Noertjahyana and Hartanto Rusli
Department of Informatics Engineering, Faculty of Industrial Technology, Petra Christian University, Surabaya, Indonesia
E-Mail: 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 was 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, 2013).

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.

This paper will show how to asses an Operational Security Management on Computer Center At the University X by applying risk management with CISSP knowledge to the operational security management on computer center at the university x.

RISK MANAGEMENT

Risk management is a combination of the three processes (Stoneburner, 2013), namely: Risk Assessment, Risk Mitigation and evaluation.

a) Risk Assessment

The steps to perform risk analysis is as follows (Stoneburner, 2013):

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

b) Risk Mitigation

Good strategy to perform risk mitigation can be seen in Figure-1 (Stoneburner, 2013).

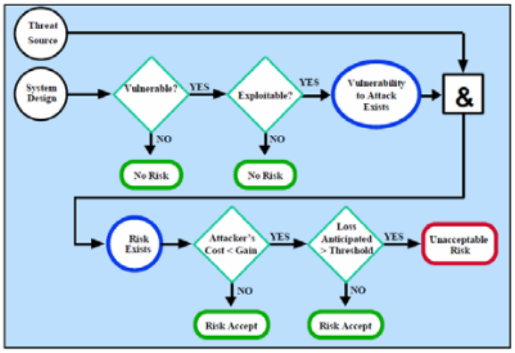

Figure-1. Risk mitigtion strategy (Stoneburner, 2013).

c) 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 Figure-2
- 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 are as follows:

1. Domain 1: Information Security Governance and Risk Management
2. Domain 2: Access control
3. Domain 3: Cryptography
4. Domain 4: Physical (Environmental) Security
5. Domain 5: Security Architecture and Design
6. Domain 6: Bussiness Continuity and Disaster Recovery Plan
7. Domain 7: Telecommunications and Network Security
8. Domain 8: Application Development Security
9. Domain 9: Operations Security
10. Domain 10: Legal, Regulations, Investigation, and Compliance

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.

The most difficult thing to do is mapping CISSP standard to risk management standard in order to create a questionnaire for capturing the truly characteristic of existing policy on university computer center x (Miller, 2012)

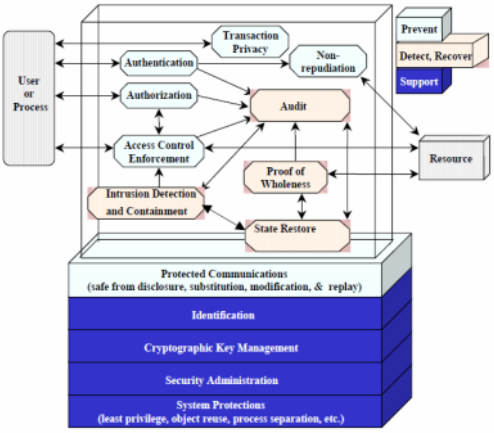

Figure-2. Technical control (Stoneburner, 2013).

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:

a. 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

b. 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.

c. 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

d. Telecommunications and Network Security

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

a. Yes b. not

e. Cryptography

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

a. Yes b. not

f. 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

g. 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

h. 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

i. 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:

(a) 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

(b) 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

(c) 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

(d) 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

(e) Cryptography

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

a. Yes b. Not c. Do not know

(f) 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

(g) Legal, Regulations, Investigations, and Compliance

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

a. Yes b. Not c. Do not know

(h) 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 Figure-3.

SYSTEM DESIGN

We will describe from system analysis to system design:

i. 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.

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

Figure-3. Example risk analysis questioner result.

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 loggings, 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 (Dubois 2013).

ii. 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 (Gomaa, 2011).

a. admin system design

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

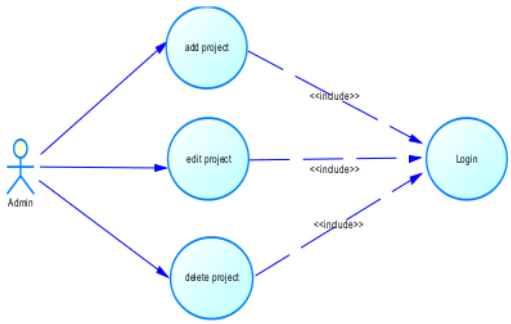

Figure-4. Use case diagram on page project admin.

A system design using Use Case Diagram and Activity Diagram is used to model the behaviors of users at once describe a work flow system and the system components. For more detail example, please see Figure-4.

After we compose an use case diagram, next we move to the activity diagram. For a single example, please see Figure-5.

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.

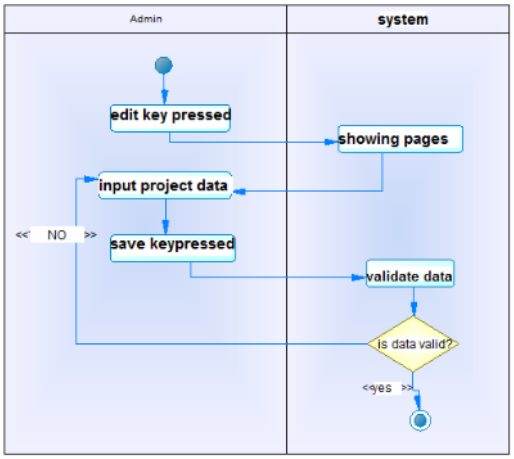

Figure-5. Activity diagram admin edit project.

And then we can build an entity relationship diagram like showed on Figure-6 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 Figure-7.

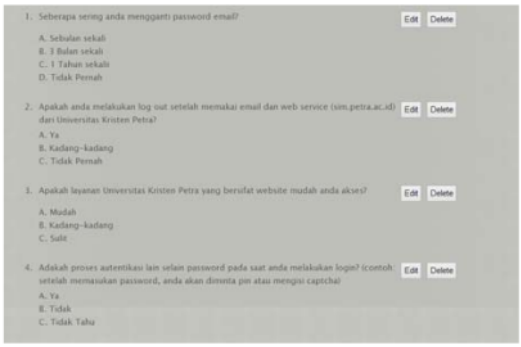

Figure-7. UI design.

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 fresher and more colorful. for example source code we can see on Figure-8.

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:

a) Perform login as we can see on Figure-9
b) Creating a project as we can see on Figure-10
c) Creating a questionnaire as we can see on Figure-11
d) Publishing the questionnaire as we can see on Figure-12
e) Seeing the results of the percentage of responses to questionnaires as we can see on Figure-13.

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 Figures 14, 15, and 16.

VOL. 9, NO. 10, OCTOBER 2014 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

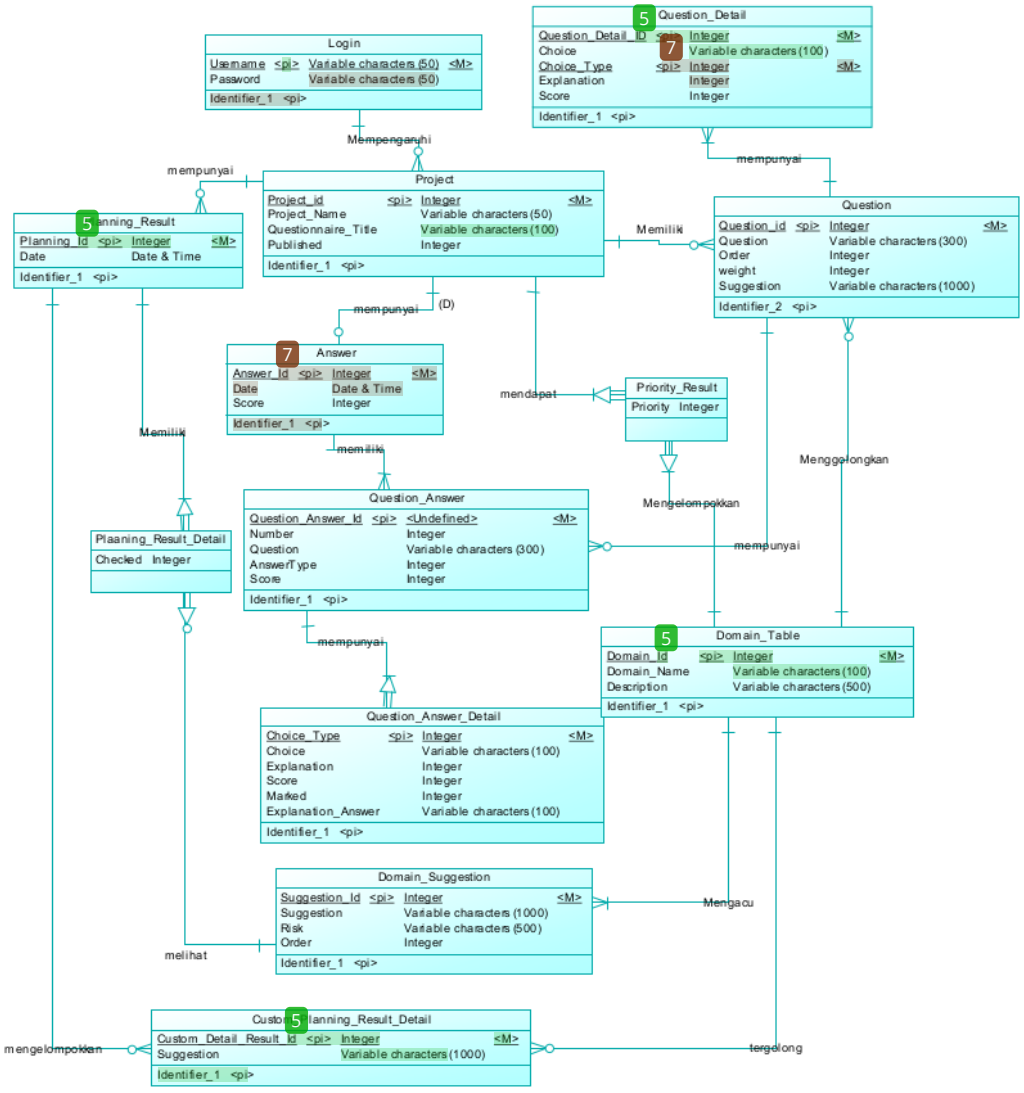

Figure-6. E-R diagram.

```
openAddDialog = function(){
$("#nama").val("");
$("#judul_kuesioner").val("");
$("#adddata").dialog("open");
mode = 'add'; editId = 0;}
```

Figure-8. Example source code.

Figure-9. Perform login.

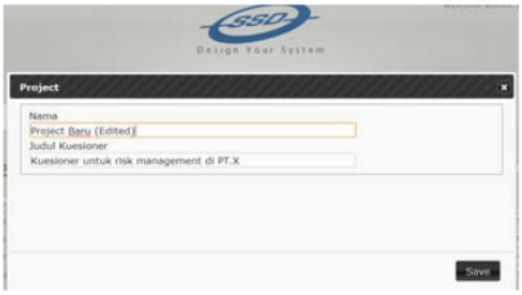

Figure-10. Creating a project.

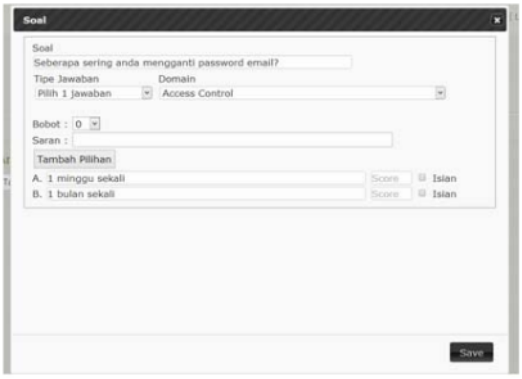

Figure-11. Creating a questionnaire.

Figure-12. Publishing questionnaire.

Figure-13. Percentage result.

Figure-14. planning result on admin pages.

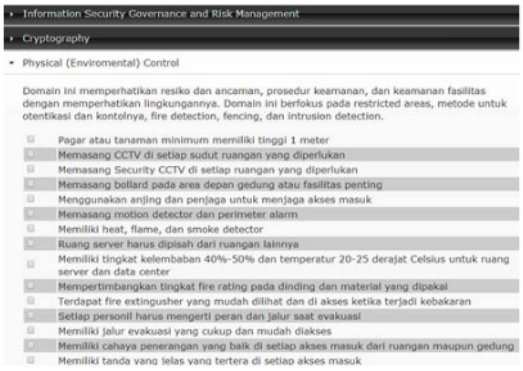

Figure-15. CISSP list standard.

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.

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.

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.

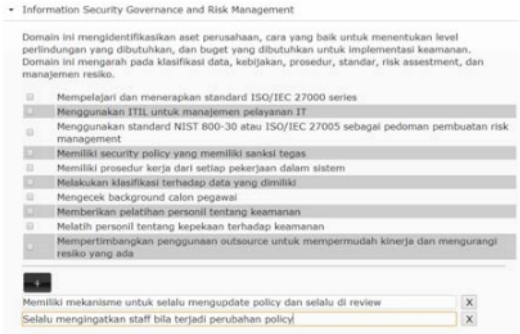

Figure-16. Adding domain suggestion.

Figure-17. Operational testing.

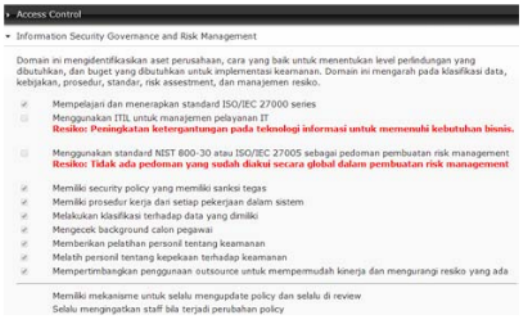

Figure-18. adding operational list detail.

Figure-19. Downloadable report.

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

Figure-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.

CONCLUSIONS

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. 2013. Building and Implementing a Successful Information Security Policy. Internet Software Marketing. Windows Security.com

Dubois Paul. 2013. MySQL (Developer Library) 5 ed. Addison-Wesley.

Gomaa Hassan. 2011. Software Modeling and Design: UML, Use Cases, Patterns, and Software Architectures. Cambridge University Press.

Miller C Lawrence. 2012. CISSP for dummies. For Dummies.

Stoneburner Gary., Alice Goguen and Alexis Feringa. 2013. Risk Management Guide for Information Technology System. NIST Special Publication 800-30 rev1.

10141235

ORIGINALITY REPORT

8%	7%	2%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ijert.org Internet Source	2%
2	123dok.com Internet Source	2%
3	Tipton, . "Contents", (ISC)2 Press, 2006. Publication	1%
4	Jorge Merchan-Lima, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez-Fonseca, Dorys Quiroz. "Information security management frameworks and strategies in higher education institutions: a systematic review", Annals of Telecommunications, 2020 Publication	1%
5	eprints.fri.uni-lj.si Internet Source	1%
6	ijcsia.uacee.org Internet Source	1%
7	repository.dinamika.ac.id Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		