Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RISK MANAGEMENT IN INFORMATION TECHNOLOGY USING FACILITATED RISK ANALYSIS PROCESS (FRAP) (CASE STUDY: ACADEMIC INFORMATION SYSTEMS OF SATYA WACANA CHRISTIAN UNIVERSITY)

[1] JAKSON PETRUS MANU BALE, [2]EKO SEDIYONO, [3]MARWATA

[1] Student In Information System Department, SATYA WACANA CHRISTIAN UNIVERSITY
[2] Prof. In Information System Department, SATYA WACANA CHRISTIAN UNIVERSITY
[3] Lecturer In Faculty of Economics and Business, SATYA WACANA CHRISTIAN UNIVERSITY
E-mail: [1]jakson.petrus@yahoo.co.id, [2] ekosed1@yahoo.com, [3]marwata@staff.uksw.edu

ABSTRACT

This paper describes a risk management on information technology to support the sustainability of academic information system at the university. The purpose of this study was to identify and quantify risks of application of information technology in academic information system at the university level, with cases in SWCU (SIA-SAT), prioritizing information technology risks are found, and determining how the risks can be controlled or reduced. The methodology used was a qualitative method, the data collected through library research and field study: interviews, observation and analysis method Facilitated Risk Analysis Process (FRAP). The result achieved was the discovery of risks, namely the risk that mainly service availability, security and integrity of data, as well as the service policy. Handling the risk then carried through the stages of FRAP, the form control list for each risk, determining suitable control through cross reference sheet, and recommendations for action that can be performed in an action plan.

Keywords: *FRAP, Information System, Risk Management, Academic*

1. INTRODUCTION

The rapid development of information technology and its convenience has been widely used to support various activities and processes in many areas including academic environment. Nowadays, the application of technology in the form of an integrated information system is expected to simplify and accelerate working process.

Academic information systems have a variety of important roles in the course of the academic processes in university environment that has used information technology to support the academic process. One example of its use is in the Academic Information System of Satya Wacana, or better known as SIA-SAT.

SIA-SAT is an integrated system with various kinds of services to support the academic activities within the Satya Wacana Christian University. SIA-SAT is available for faculty and students, i.e. student custody services, teaching schedule, assesment, re-registration, course registration, course requests, study card checking, results of study, lecture and conference schedule, transcripts, billing information, thesis registration, library lending information, as well as integrated with other services such as health care and students finance.

Information assets owned by the university needs to be protected. They can be hardware, software, systems, data, and brainware (user). How that is done is with preventive protection, by analyzing the risk of damage to the system.

Issues that will be examined are as follows:

1. How to identify, analyze and measure the identified risks, and determine risk management priorities using the stages of the Facilitated Risk Analysis Process (FRAP) at SIA-SAT Satya Wacana Christian University (SWCU).
2. How to make protection controls to overcome or mitigate these risks.

The results of this study are expected to provide a variety of advantages, as follows:

1. Identification and prioritization of risks in the application of Information Technology SIA-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SAT using Facilitated Risk Analysis Process (FRAP).

2. Helping Satya Wacana Christian University to manage or cope with risks that may occur in the implementation of SIA-SAT.
3. Provide recommendations that can be used as reference material in the development of academic information systems in a university environment.

2. LITERATURE REVIEW

2.1. Related Topics

Sections and subsections should be numbered and titled as 1.0, 2.0, etc. and 1.1, 1.2, 2.1, 2.2, 2.2.1, etc. Capital letters should be used for the section titles. For subsections, the first letter of each word should be in capital letter and followed by small letters. One line space should be given above the sub section while no space should be given below the heading and text

Related research on FRAP performed on one private company in Indonesia, PT. INTRA ASIA INSURANCE. The purpose of the study was to measure and manage risks in enterprise information technology by using FRAP, including the documentation and security systems [1].

The other study is a measurement of risk information technology at PT. Verena Oto Finance Tbk. The results are risk analysis, risk measurement results, and recommendations. It was concluded that the highest risk possibilities that can impede business processes is the occurrence of an error in the program, misinformation and interference with the infrastructure. It is thus very important for the company to improve the risk management of information technology [2].

University uses technology to support academic activities should know the consequences of the use of IT in information systems as well as possible and continue to evaluate and manage risks that arise because of the risk that eventually will be an impact also on the sustainability of the academic process.

The use of IT in SWCU especially on SIA-SAT has not kept pace with IT risk management. It is seen from the absence of a clear IT governance. Based on direct interviews on BTSI (Board of Technology and Information Systems) and research about IT governance on the SIA-SAT by using COBIT [3], it is noted that the use of IT in the SIA-SAT SWCU reached the level of "repeatable", it means the processes that occur are already known and carried out continuously, but there is no clear rule regarding IT risk management.

Based on above studies, this research will be conducted to discuss the risk management of academic information system using FRAP method, by taking the case of SIA-SAT SWCU.

2.2. Risks

The term risk has many definitions. Risk is closely related to uncertainty, which occurs due to lack or unavailability of enough information about what's going to happen [4]. Something uncertain (uncertain) can be beneficial or detrimental. According to Wideman [5], uncertainty that is likely to benefit known as opportunity, while the uncertainty likely to result in losses referred to the risk.

In the perspective of information technology, risk is the potential threats that exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization [6].

Based on these definitions, it can be concluded that the risk is always associated with the possibility of something unexpected adverse or unwanted. So, for a loss, although the loss was very small, then we are dealing with risk [7].

2.3. Risk Management

Risk management is a field of science which deals with how an organization implements various sizes in mapping out the existing problems by putting the various approaches in a comprehensive and systematic management [8].

Risk management is an attempt to determine, analyze, and control the risks in every activity of the organization or company in order to obtain the effectiveness and higher efficiency.

By applying risk management, some of the benefits to be gained are [8]:

1. Having a basis for making decisions.
2. Able to provide direction for the company in view of the effects that may arise both short and long term.
3. Encourage managers in making decisions to always avoid risks and losses, especially in terms of financial losses.
4. Allows companies obtain minimum losses.
5. Risk management concept that is designed in detail to build towards a sustainable company.

According to Hughes [9], the risk of information technology is divided into six main classes:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. Security: the risk that the information be changed or used by unauthorized persons. For example, computer crime, internal breaches, and cyber terrorism.
2. Availability: the risk that the data can not be accessed, for example, after a system failure, human error (human error), configuration changes, and others.
3. Recoverability: the risk that important information can not be recovered within a reasonable time after the events related to the security or availability, such as software and or hardware failure, external threats, and others.
4. Performance: the risk that the information was not available when needed, for example caused by a distributed architecture, the server can not handle the demand when it reaches the peak load, or topographically diverse.
5. Scalability: the risk that the growth of the business, the bottleneck configuration, and architectural forms makes it impossible to handle new applications and major business cost effectively.
6. Fidelity: the risk that management or user information violated the requirements of regulatory authorities. It is intended to include violation of the rules, a written company guide, and internal policies.

2.4. Information System

Information security must contain three essential elements [10], namely:

1. Confidentiality: aspects that ensure the confidentiality of data or information, ensuring that the information can only be accessed by authorized people and ensure the confidentiality of data sent, received and stored.
2. Integrity: aspect that ensures that data is not altered without consent authorities, the accuracy and integrity of information must remain intact.
3. Availability: aspect that ensures that data will be available when needed, ensuring that users are entitled to use the information and related devices when needed.

These are three aspects that are vulnerable to security risks, either through physical threats, through the network infrastructure, user negligence, lack of human resource competencies, and through access to hardware or software is invalid. It is therefore necessary measures to recognize, anticipate, and minimize the risks that may occur.

3. FACILITATED RISK ANALYSIS PROCESS (FRAP)

Facilitated Risk Analysis Process (FRAP) according to Peltier [1] is an approach to the process of determining the risk and impact, priority setting process, and the process of determining security controls. FRAP allows an organization to use its own resources to carry out a risk assessment as much as could be done by other approaches [11]. FRAP is basically in accordance with the standard pattern for qualitative risk assessment. FRAP method to identify stakeholders and put the information assets under their ownership [12]. In terms of time, FRAP takes a short amount of time that a couple of days instead of weeks or months, cost effective, as well as utilize the capabilities of experts in it.

Risk measurement process by using FRAP divided into several sessions [13]:

3.1. Pre-FRAP Meeting

This stage is the most important sessions in the process of analyzing risk. This session involves IT managers, project leaders and facilitators. There are three important components produced in this process:

- Scope Statement: restrictions on the things that will be reviewed.

- Visual Models: An overview of the analysis process or foil diagram that describes the process that will be reviewed.

- Establish the FRAP team: Team FRAP usually consists of several members representing their respective fields.

3.2. The FRAP Session

FRAP session may be extended up to 3 days but in general this process take as long as 4 hours and involve about 7 (seven) to 15 (fifteen) members and no more than 50 (fifty) and at least four (4) people. In this method there are three processes:

- Identified Risk: do the process of identifying the risks that are likely to threaten the system information.

- Risk prioritized: making a priority of the risks to be faced, from high to low with the use of the table associated with the impact on businesses and vulnerability.

- Controls Identified: based on the risks to be faced, making control of protection that can be done to deal with or mitigate these risks.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.3. Post FRAP Session

This process is the last session of the FRAP. Post FRAP Meeting divided into two processes:

- Cross Reference Sheet: a working paper which is based on a table of risks and controls to identify control tables that match the identified risks.

- Action Plan: a working paper that is made to determine the appropriate type of risk mitigation in accordance with the state of the system, but it is also determined by whom and when the reduction will be carried out.

In this process, a cross reference sheet takes a long time compared to other processes. Cross reference sheets are used to determine the control that matches the risk.

Results of FRAP is a comprehensive document that identifies threats, prioritize threats, and identify controls that can help overcome these risks [14].

4. RESEARCH METHOD

Fieldwork was conducted over a period of approximately three (3) days in SWCU by conducting structured interviews and direct observation. Interview questions derived in accordance with the standards defined by the FRAP method Peltier published in softcopy.

This research was conducted using qualitative descriptive methods. Qualitative research is research procedures which produce descriptive data (not a number), the form of speech or writing and observable behavior. Reasons for using qualitative methods is that with this method, researchers can figure out how to view the subject of research and also circumstances that can not be represented by statistical figures. The data obtained were analyzed immediately, followed by another data search and analysis, and so on until deemed achieve adequate results.

Through qualitative methods, researchers can know the subject of the environment and see them develop a definition and give an opinion on the aspects studied. It also can be done learning about the experiences or risks that may have never known before. In this qualitative method allows researchers to investigate the actual concepts encountered in daily activities.

The FRAP process has provided the steps in risk management: Pre FRAP Meeting, The Session FRAP and FRAP Post Meeting. FRAP provides control lists in assessing the risk of information systems to be studied, and has covered various aspects of security. In doing the interviews, not all participants will be asked questions regarding any existing control list, but only on the areas of responsibility of each. Moreover conducted structured interviews also necessary that represent control list and verify the answers are given.

Data used in this study are primary and secondary data. Primary data is the primary data obtained from interviews and observations also accompanied by a responsible party in their respective fields, in this interview conducted at the parent BTSI as research and policy implementers, and advanced data search into relevant units, such as network division, software development, and database management.

Secondary data is data that supports research, obtained through a search using an intermediary media, to find evidence, through observation, notes and or related research either published or unpublished.

FRAP stages to be performed consists of three (3) stages:

1. FRAP Pre Session
2. The FRAP Session
3. FRAP Post Session

In the stages of pre FRAP session, conducted four major stages of research, including the scope statement, visual models, determination of FRAP members, and scheduling.

Scope statements are the stages that contain any matters which would be reviewed. The researcher acts as a facilitator who will explain the stages of FRAP to the BTSI. In this stage, discussions with management BTSI to limit the scope of research to be done, needs BTSI, and what is allowed to be tested, the extent to which researchers may conduct research on BTSI and adapted to the scope of FRAP.

Visual model is a visual form that shows the steps being taken in FRAP. With visual models, lines of inquiry can be followed by a clear, other than that it is easier to trace.

Determination of FRAP members performed as the final stage of pre FRAP meetings, through discussions later determined FRAP members involved in the research, based on their respective roles as key individuals. Scheduling is done to adjust the time agreed by each unit as well as key individuals.

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The next stage is FRAP session, consisting of three stages: risk-identified, prioritized risk, and control identified.

Risk-identified is the stage in which researchers conducted interviews to the BTSI and direct observation of the risk and vulnerability. The results of identification is then inserted into a table, which contains a list of any risks found.

After determining the risk, then the risk priorities are determined using the priority matrix, which is made up of vulnerability and impact. Both of these indicators will then be incorporated in a priority matrix to determine risk priorities. Next is to determine controls to minimize and overcome these risks. Control adjusted by FRAP control list and put into the control identified.

The final stage is the post FRAP, in which the data processing has been obtained. This stage produces three main outputs: a cross reference sheet, action plan, and the final report. As described that cross-reference sheet is the result of a control list and control-identified; action plan is the result of processing-identified risks with control lists provide a clear picture of how each risk will be treated, complete with a working plan.

5. RESEARCH RESULTS

5.1. Pre FRAP Meeting

5.1.1. Scope Statement

Scope statement is the phase that contains the things that will be reviewed. Researcher as facilitator will explain to the BTSI FRAP. In this stage BTSI discussed with management regarding the scope of the study limitations, the needs of BTSI, what is allowed to be tested, the extent to which researchers may conduct research on BTSI and adjusted to the coverage in the FRAP.

The discussion is limited to a few parts associated with SIA-SAT: part Information Systems (IS), Information Technology (IT), and BTSI. Section SI-SAT include AIS system consisting of software and databases. In the research that includes IT network infrastructure and servers. Also be carried out interviews and observation matters relating to the policies and regulations relating to the SIA-SAT.

5.1.2. FRAP Participants

FRAP members involved in the study are determined based on their respective roles as key individuals. Scheduling is done to adjust the time agreed by each unit as well as key individuals.

The FRAP members are formed as follows:

1. The Head. Information Systems.
2. Coordinator. Software Development.
3. Coordinator. Database Administrator.
4. Division of Information Technology.
5. Division of Computer Network and Internet.

After the determination of the members of FRAP, then followed by FRAP Session that lasted for approximately one hour per unit interviewed.

5.1.3. Visual Model

Visual model is a visual form to show the FRAP process. Here is a visual model that has been done and has been adapted to the SIA-SAT.

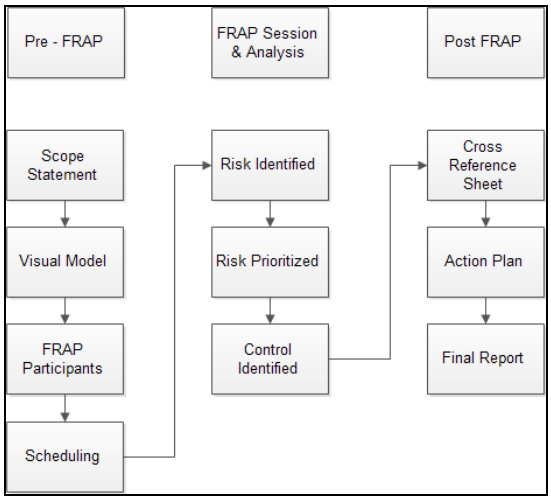

Figure 1 Visual Model

Visual models are used during the session FRAP to determine when a process starts and ends. The advantages of the use of visual models in FRAP is to show the flow of processes that occur in sequence and beneficial learning process by applying the concept of neuro-linguistc learning programming, namely mechanical advantage (write elements studied) and visual (see diagram to understand the process) [1].

5.2. The FRAP Session

FRAP Session conducted for approximately forty minutes to an hour per unit and key individuals. This session contains interviews and direct observation. Based on interviews and observations then obtained a list of identified risks.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.2.1. FRAP Session Deliverables

Based on interviews and observations were conducted on each unit BTSI obtained the following findings.

The absence of an ongoing plan to maintain the availability of data for the SIA-SAT. This is due to not having a data processing center (data center). In addition, the results of a routine backup process is still stored locally. If the local backup data can not be used due to several causes such as fire, damage, theft, natural disasters, and so on, the system may lose some or all of the data. This is due to the location of the backup just to be in the campus alone, and do not have a Disaster Recovery Center (DRC) that is separated from the campus environment, such as cloud [2].

Blueprint of the current network is not available, so the only network infrastructure reference is based on the old topology. Existing network topology only refers to the old topology ever made in 2008 in the form of hardcopy that framed on manager's room, and have not been able to describe changes that occur on the network for 6 years (2008-2014). There are weaknesses in terms of documentation, where there is no standard reference that can be used in maintaining the network infrastructure. Documentation is also required for network planning and network governance in the future, as part of the IT infrastructure itself.

It is worth to consider upgrading the hardware, especially servers. Based on interviews, the server used is still burdened with the number of users in over 600 people, resulting in slow access, and about 2000 people on the user, the server will experience peak loads, where the activity in the AIS-SAT takes a very long process, and usually takes about 2 hours to complete all the processes. SIA-SAT takes the greatest memory of all existing processes. This always happens whenever the process of SIA-SAT with the number of users. The server can process the data, however, compromising user comfort. Slow access could harm the user, such as students wait longer or lose a class because of slow access to classes that had already taken first taken by another student. To anticipate this, SIA-SAT is scheduled differently for each faculty, but slow access.

Switch using old models that do not support Spanning Tree Protocol (STP), and VLAN Trunking Protocol (VTP). In complex multi network switches, STP must be enabled and set manually. STP allows a network LAN switches and bridges connected to each other in redundant with a mechanism that could prevent bridging loops. Bridging the data packet loop is swirling in the network to locate the address and could cause traffic congestion on the network (broadcast storm).

Hardware infrastructure does not guarantee high availability. There are no servers that can serve as redundant servers to ensure availability of access when handling requests from the user abundant. There is no peer servers for redundancy and load balancing. Server Load Balancing (SLB) functions as a process and technology that distributes traffic on multiple servers using available networking tools.

Audit and assessment of the overall network has never been done. Assessment of the network ever undertaken, but only as a bonus from the initial network construction. Ever Task Force was formed to assess the existing network, but can not account for the task force by providing a clear report on network usage and technical data needed to assess the network.

In terms of finance, IT department said that the investments made in infrastructure, especially IT hardware is still small. To perform device procurement, IT departments must apply first to the BTSI. The cost of purchasing the server is still obtained from government assistance. It is certainly the budget need to be considered by the management as well as the university.

Software development relies entirely on two key individuals: one for software developers and one for the database administrator. These two key individuals who handle software SIA-SAT, there is no other team. There has been no official documentation made regarding the development of the SIA-SAT. The plus side is the work so far can be handled well and quickly because it only involves two people, but it is also opening it up to a loss of knowledge due to the lack of sharing knowledge about the development of the SIA-SAT. This will decide the transfer of knowledge to subsequent developers and academic activities could be interrupted at any time if the key individual is unable to perform their duties, such as illness, accident, resign, or other causes.

There is no application testing mechanism. According to the interview, mentioned that ideally there should be a separate machine for making, testing, after which the software can be used. But for SIA-SAT, a test environment is only done by the programmer, after it is applied directly to the user, for example, there is a system of rules that changed calculation values, to simulate changes in accordance with the manual counting if it is used

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

directly. There has been no testing mechanism, for example, system acceptance testing, the stage where software testing by real users to ensure that the software is able to handle the tasks that are required in real-world scenarios in accordance with the required specifications.

Based on the interview, Quality of Service (QoS) has not been made clear. This is because the intended QoS depends on the bandwidth per segment and priority scheduling. If done correctly then the QoS bandwidth usage can be reduced, which in turn can reduce the cost of purchasing a monthly bandwidth. If QoS is not properly managed, purchased unused bandwidth optimally resulting in waste costs due to not getting the maximum benefit as funds are spent each month.

Physical security of network devices is still lacking, because any time the room was left unlocked and unguarded (a case in Building E), allowing free access to the network, making it vulnerable to theft, vandalism, and other illegal activities that endanger the state of network devices. The condition of the wiring in the room also needs to be trimmed in order to avoid short-circuiting that can damage the device.

The storage location of the application, database, and backup used to be in the campus environment (Building E). This raises the risk of data loss caused by an extreme case, for example, natural disasters, fire, theft device, and so on, then there is a risk of losing part or all of the data. There are no other locations are used to store the backups, which raised the risk of losing data in the backup.

Adherence to the rules relating to the SIA-SAT, for example, grade submission timeline, the process of SIA-SAT, and perform activities according to standard operational procedure (SOP). Based on interviews with the ISO standardization never applied, less favored administrative process, which is more commonly used process is the manual way, and there is no clear rule that requires it.

5.2.2. Identified Risks

In addition to determining the list of risk, vulnerabilities identification and impacts if those risks occur. Vulnerability and the impact then crossed into the priority matrix to determine the priority of each risk. The results are shown in Table 1.

Table 1: Identified Risks

No.	Type	Description	Vulnerability	Impact	Priority
1	INT	Damage to the device resulting in data loss.	L	H	C
2		Computer virus infection resulting in lost or corrupted data.	L	H	C
3		System failures that resulted in unaccessed system.	L	H	C
4	AV	Power outages.	M	H	B
5		The data presented are not saved because the system is overwhelmed handling *requests* from multiple *users.*	M	H	B
6		Short-circuiting that causes damage to the device.	L	H	C
7		Slow access over the network because of increased *delay* and *latency* that slows down access and the possibility *of data loss*occurs due to the absence of a clear implementation of QoS in the network.	M	M	B
8		Overwhelmed *servers* handling *requests* because *the server* hardware specifications are still low.	H	M	B
9		Applications that do not meet the needs of *the user* updated appropriately.	M	M	B
10		The system does not function properly because the key individuals can not carry out tasks.	M	H	B
11		Lose some or all of the data in the event of a natural disaster or other extraordinary events that happened within the university as*Data Recovery Center* (DRC) is also in the university environment.	L	H	C
12		The lack of documentation because the system relies heavily on key individuals involved so it will disconnect / inhibit the transfer of knowledge to the next developer.	M	H	B
13	SEC	Theft device.	M	H	B
14		Unauthorized access to *the server* room and network devices.	M	M	B

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

15		Illegal access to the network.	M	M	B
16	FID	The system runs ineffective / inefficient because not / has never been a formal audit of the overall system performance.	M	M	B
17		Operational runs as is / does not follow *the standard operation procedure* (SOP)	M	L	C
18		Unexpected costs arising from damage to the network device / application.	L	M	C

Table 1 contains the identification and prioritization of risk. There are four types of risks that have been collected: Integrity (INT), availability (AV), security (SEC), and fidelity (FID). How to get the priority is to do the analysis based on vulnerability and impact priority matrix, with the scale of high (H), medium (M), and low (L).

Table 2: Priority Matrix

Vulnerability	Impact		
	High	*Medium*	*Low*
High	**A** -	**B** 8	**C** -
Medium	**B** 4, 5, 10, 12, 13	**B** 7, 9, 14, 15, 16	**C** 17
Low	**C** 1, 2, 3, 6, 11	**C** 18	-

Description: *High Priority* (Red), *Medium Priority* (Orange); *Low Priority* (Yellow), *Non-Corrective* (Green).

A = corrective action must be implemented
B = advised to corrective action
C = require monitoring

From Table 1 and Table 2, it can be seen the identification and prioritization of risk, there are at least 18 (eighteen) the risks identified.

INT is the integrity risk, ie the risk associated with the consistency of data and that the data should not be changed without the permission of the authorities. AV is a risk of the type of risk associated with the availability, which is related to the availability of data and systems, where the data should be available when needed / accessed. Risks that threaten the availability of the data included in this type.

Furthermore, there is a risk with the SEC or type of security, which in this study was aimed at physical access security of the system and network system, and the last is the risk of type FID or fidelity, ie the risk associated with the implementation of the SIA-SAT based on operational policies that have been made. Risks associated with the rule, for example, the Standard Operational Procedure (SOP), financing, efficiency and management systems are included in this type.

In Table 2, it can be seen how to make decisions regarding the priorities of a risk. On the table there is a column that shows the risks and vulnerabilities of a line that shows the scale of the impact of risk. By putting the risk in accordance with the vulnerability and the impact it will get priority risks.

Risks with high susceptibility (H) is a risk that has a high chance of occurrence or happening frequently. Risks to the medium susceptibility (M) is a risk that has a chance of events that are, for example, slow network access when worn a lot of users, less than optimal use of bandwidth, and so on. Risks with low vulnerability (L) is a risk that has a low chance of occurrence, eg device damage due to fire, natural disasters and so on.

The level of impact shows how the impact of a risk to the academic process. High level indicates that the risk has an impact that can disrupt the academic process and need special attention, the level of the medium showed that the impact caused an effect but still can be solved, and the impact of low shows the impact caused not have a huge effect.

The spread of risk priorities shown in Table 1, there are at least 18 risks were identified, and of these 18 risks, as seen in the distribution of risk priorities in Table 2, there are 11 medium priority risks, and 7 low priority risks. Priority results denoted by the alphabet A, B, and C. A signaling alphabet corrective actions to be implemented, the risk with the alphabet B is advised to corrective action, and risks with alphabet C has a low priority but still require monitoring.

5.2.3. Control List

To address the risks that have been shown in-identified risks, the next step is to create a control for controlling those risks. Control list is based on the existing control class FRAP. The classes defined in control list are adjusted for risk that is on identified risks, and serve as controls for each risk. The results of the control list shown in Table 3.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Control List

No..	*Class*	Information
1.	*Backup*	Implement *backup* of the data and store data in more than one place and media only.
2.	*Recovery Plan*	Developing, documenting, testing, and ensuring data recovery procedures are functioning properly.
3.	*Access Control*	Prevent unauthorized access to information include the ability to detect, report threats on information security, and limit access to personnel authorities.
4.		Implementation of encryption *(data, end-to-end)* to prevent unauthorized access and to the security of transmitted information.
5.		Implement access control mechanisms to prevent unauthorized access. These mechanisms include the ability to detect, *logging*, and reporting the illegal access attempt.
6.		*Operation control:* a mechanism to protect the database from unauthorized access and modification of the outside of the system can be determined and implemented.
7.	*Acceptance Testing*	Develop testing procedures to be followed during development or during the application and modification of the existing application that includes user participation.
8.	*Anti-virus*	Installing anti-virus software on each computer unit and ensure that anti-virus is always updated automatically.
9.	*Policy*	Develop policies and procedures to restrict access rights or to give special privileges to certain parties.
10.	*Training*	Including *user* training and documentating adequate instruction on how to use the system properly.
11.		Documentation that covers the entire system development and maintenance.
12.		To evaluate the performance and capabilities of employees in developing and managing the system.
13.	*Management Support*	Provide operational guidance to staff in implementing the system parts and technology used in the company and ensures the exchange of data using an application that is used to run properly and safely.
14.		Ensuring support from management on the sustainability of the system, for example in terms of cost / budget and other regulations that affect the course of the system.
15.	*Corrective Strategies*	Develop a corrective strategy system, eg. software development strategies, architecture network devices, and databases.
16.	*Physical Security*	Implement mechanisms to restrict physical access to network devices.
17.	*Maintenance*	Provides support for the availability of hardware, such as UPS.
18.		Perform maintenance and agreement of the supplier to facilitate ongoing operational status of the purchased hardware.
19.	*Audit / Monitor*	Implement monitoring mechanisms, report, and audit of the overall system as activities that need to be done periodically.
20.	*Service Level Agreement*	Defines the responsibilities, defines the agreed level of expectations (eg, QoS), high availability, determines the quality of the target and the minimum acceptable requirements.
21.	*Proprietary*	Control of property rights.

Based on Table 3, there were 21 controls. Class control is made in order to cover all the risks that have been identified. How to determine the control class is the class to compare with each FRAP control the risks identified and the search for connection. Class-identified controls related to the risk to be incorporated into the control list. Description of each class control was made into a general statement that can control all the risks included in the class of risk.

5.3. Post FRAP Session

5.3.1. Cross Reference Sheet

Identified risks and control list are combined into cross reference sheet for risk mapping and grade control. Cross reference sheet is made with a view to determining the appropriate controls for each risk. Thus, risk management becomes more clear and focused, because the cross reference sheet has mapped control classes, descriptions of risk, types of risk, and risk priorities into one interrelated unity. The result can be seen in Table 4.

Table 4: Cross Reference Sheet

No.	Controlling Class	Description	Risk #	Type	Priority
1.	*Backup*	Damage to the device resulting in data loss.	1	INT	C
		Computer virus infection resulting in lost or corrupted data.	2		
		System failures that resulted in unaccessed system.	3		
		Short-circuiting that causes damage to the device.	6	AV	
		Lose some or all of the data in the event of a natural disaster or other	11		

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

		extraordinary events that happened within the university as *Data Recovery Center* (DRC) is also in the university environment.			
		Power outages.	4	A V	B
2.	*Training*	The system does not function properly because the key individuals can not carry out tasks.	10		
		The lack of documentation because the system relies heavily on key individuals involved so it will disconnect / inhibit the transfer of knowledge to the next developer.	12		
3.	*Access Control*	Theft device.	13	SE C	B
		Unauthorized access to *the server* room and network devices.	14		
		Illegal access to the network.	15		
5.	*Acceptance Testing*	The data presented are not saved because the system is overwhelmed handling *requests* from multiple *users.*	5	A V	
		Updated applications do not appropriately meet the needs of *the user*.	9		
6.	*Corrective Strategies*	Slow access over the network becauseof increased *delay* and *latency* that slows down access and the possibility *of data loss* occurs due to the absence of a clear implementation of QoS in the network.	7		
		Overwhelmed servers handling requests because the *server* specification is low.	8 9		
7.	*Audit / Monitor*	The system runs ineffective / inefficient because not / has never been a formal audit of the overall system performance.	16	FI D	B
		Operating system runs potluck / as is/ do not follow *the standard operation procedure* (SOP)	17		C
8.	*Manage-ment Support*	Unexpected costs arising from damage to the network device / application.	18		C

The cross reference sheet consists of 8 class controls. Related information can be placed on-identified risks associated with the information from the control list. This is important because they form the structure of the network of relationships that exist between different pieces of data in the two previous tables and tables form a more dense, making it easier reading for the next stage, which makes the work plan or action plan.

5.3.2. Action Plan

The final stage of the analysis using FRAP is making a work plan or action plan. After cross-reference sheet is formed, the action plan will be prepared to explain the actions that can be taken by the management and operation of how to control the risks that have been identified and prioritized. Similar to cross-reference sheet, an action plan was formed by combining the control list-identified risks by giving a clear picture of how each risk will be treated, complete with a working plan. The results of the action plan are shown in Table 5.

Table 5: Action Plan

No.Risk	Type	Description	Priority	Control	Action
#1	INT	Data loss due to damage to the device.	C	18, 19	Carry out maintenance and software *upgrades* on a regular basis or
#2		Damage / loss of data due to a virus.			Install and update*antivirus*
#3		Data loss due to system failure.		1, 2, 15	Perform backupss for databases and file systems.
#4	AV	Power outages.	B	17	Using UPS or backup generator.
#5		The data presented are not saved because the system is overwhelmed handling *requests* from multiple *users.*		15, 17, 20	Increasing network and *server* hardware specifications, hardware *upgrades,* network design and optimization and application servers, build a new *datacenter.*
#8		Overwhelmed *servers* handling *requests*because the*server* specs are still low.			
#6		Short-circuiting that causes damage to the device.	C	16, 19	Checking and repairing wiring and electrical system, make sure the device is in an ideal temperature, ensuring *Mini Circuit Breaker* (MCB) to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

					function properly.
# 7		Slow access over the network because of increased delay and latency that slows down access and the possibility of data loss occurs due to the absence of a clear implementation of QoS in the network.	B	15, 18, 20	Perform network optimization by applying QoS according to the applications running on the network.
# 9		Applications that do not meet the needs of *the user*updated appropriately.		7, 12	Involving *users* in the development of the system
# 10	AV	The system does not function properly because the key individuals can not carry out tasks.	B	10, 11, 12	Creating documentation that is clear and complete about the systems, incl. software, databases and hardware (network), provide sufficient *training* for staff and developers to come.
# 12		The lack of documentation because the system relies heavily on key individuals involved so it will disconnect / inhibit the transfer of knowledge to the next developer.		10, 11, 21	
# 11		Lose some or all of the data in the event of natural disasters that struck the university environment because the DRC is in the university environment as well.		1, 2, 20	Adding DRC in a separate location from the campus environment, for example by using *cloud*tech nology.
# 13	SEC	Theft device.		3, 4, 5, 6	Securing the room, routine monitoring and improved control, *upgrades firewall,*
# 14		Illegal access to the network.			
# 15		Unauthorized access to *the server* room and			
		network devices.			configuration, patch security holes in the operating system that runs the network.
# 16	FID	The system runs ineffective / inefficient because not / has never been a formal audit of the overall system performance.	C	15, 19	Conduct periodic audits so that the BTSI can determine the condition of the system and assist in making decisions.
# 17		Operating system runs potluck / do not follow *the standard operation procedure*(SOP)			Creating and ensuring operational system made in accordance with the SOP, and raise awareness among users of the importance of security and integrity of the system.
# 18		Unexpected costs arising from damage to the network device / application.		1, 2, 17, 18, 19	Shifting the risk of damage to hardware *vendors* or suppliers.

Action plan shown in Table 5, each of the risks listed together with the risk of type, description, priority risks, controls do, and work plans. In preparing the action plan, a risk can have some control in accordance with the type of risk. That is, in dealing with a risk can be applied to multiple controls simultaneously interrelated. The controls are still in general terms, and then described in the action plan.

From Table 5, it appears that every risk has been mapped to the corresponding control. In the column there are recommendations that can be taken to address the risk. An action can solve more than one risk, this happens because there is a correlation between each risk, so by doing an action plan to address some of the risks as well.

6. CONCLUSION

FRAP method can be applied in the university environment, the previous method is widely used by various companies to perform risk management. In the case of SIA-SAT, FRAP is used because there are few participants involved directly in the management and development of the system,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

involving local experts participants themselves, not costly and requires a relatively short time. FRAP process utilizing the knowledge possessed by the local expert, so that the analysis can be done relatively quickly. FRAP process can be completed for an average of one hour per session for a maximum of five days.

From the results of this study concluded several things. SWCU needs to do sustainable planning (contingency planning) in the development and maintenance of academic information system clear and focused and not only based on the current needs alone. Availability of services needs to be improved, for example by making the data center and Disaster Recovery Planning (DRP) by placing the DRC in a separate location from the campus.

Improved network performance needs to be done, for example by making better QoS settings and upgrading the hardware used because the specification of network devices that in use is still relatively low.

Security and maintenance of network devices, especially devices have not been adequate, necessary security access physical and logical devices, for example by increasing the physical security surveillance, routine monitoring, updating the firewall configuration, and patching security holes of used application.

Thorough audit needs to be done because there has not yet been made official audit of the SIA-SAT. The results of the audit can be used by BTSI to determine the condition of the system and the SIA-SAT related policies, such as operational policies and rules regarding the security of the system.

Development of SIA-SAT is still heavily dependent on key individuals, it is necessary to manufacture good documentation and training to delegate role of key individuals, so that the system can still run when key individuals are absent or unable to perform their duties.

This research can be further developed and carried out the deeper investigation and verification of the existing risks and requires mechanisms for monitoring the course of the proposed risk management.

7. ACKNOWLEDGEMENTS

Thank you to Mr. Partono BTSI with the permission of the research that has been given so I can retrieve the data needed to complete this study. Thanks also are given to all staff and SWCU BTSI that has helped researchers in providing the necessary data.

REFERENCES:

[1] Peltier, T., Information Security Risk Analysis, Auerbach/CRC Press Release, 2001, Washington D.C.

[2] Wood, T., Cecchet, E., Ramakrishnan, K.K, Shenoy, P., Merwe, J., Arun, V., Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges, University of Massachusetts Amherst & AT&T Labs, 2010, https://www.usenix.org/legacy/events/hotcloud10/tech/full_papers/Wood.pdf.

[3] Tileng, Kartika G., Analysis of IT Governance Implementation at UKSW (Case Study: SIA-SAT), Magister of IS, 2011, IT SWCU.

[4] Hansson, Sven O., Risk, The Stanford Encyclopedia of Philosophy, Spring 2014 Edition, Edward N. Zalta (ed.), forthcoming URL=http://plato.stanford.edu/archives/spr2014/entries/risk/.

[5] Wideman, R.M., Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities, 1992, Project Management Institute.

[6] ISO/IEC. 2008. Information technology: Security techniques-Information security risk management. ISO/IEC FIDIS 27005:2008

[7] Pramana, T., Business Risk Management, 2011, Sinar Ilmu Publishing. p14.

[8] Fahmi, Irham. 2010. Manajemen Risiko: Teori, Kasus, dan Solusi. Bandung: Alfabeta.

[9] Hughes, G., Five Steps to IT Risk Management Best Practices, 2006, Risk Management, 53 (7), 34-40.

[10] Supradono, B., Information Security Risk Management Using the OCTAVE Method., 2009, Media Elektrika. 2 (1): 4-8.

[11] Visintine, Vishal, Global Information Assurance Certification Paper : An Introduction to Information Risk Assessment, © SANS Institute 2003, As part of GIAC practical repository. GSEC Practical, Version 1.4b.

[12] Innerhover, Using an Enterprise Architecture for IT Risk Management, The Pennsylvania State University, 2006, http://citeseerx.ist.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

psu.edu/viewdoc/summary?doi=10.1.1.108.6754.

[13] Peltier, T., FRAP, Peltier Associates Ltd. 2002, http://www.peltierassociates.com/frap.htm.

[14] Vidalis, S., 2010, Calculating the Value of Information Assets in the Threat Assessment Process, Journal of Newport Business School, Department of Computing, Newport, http://dspace.newport.ac.uk/dspace/bitstream/10774/258/1/Vidalis,%20Stilianos%20Calculating%20the%20Value%20of%20Information%20Assets.pdf.