SWISS GERMAN UNIVERSITY

MASTER OF INFORMATION TECHNOLOGY

THE ANNUAL CONFERENCE ON MANAGEMENT AND INFORMATION TECHNOLOGY

ACMIT 2020

IoT AND DATA CHALLENGES IN DIGITAL TRANSFORMATION

TANGERANG, 18 NOVEMBER 2020

Volume 7

Preface

First, on behalf of the committee, I would like to thank God since it is only with His grace that the proceedings of the Annual Conference on Management and Information Technology (ACMIT) 2020 can be published.

This proceeding is the publication of the papers which were presented in the ACMIT 2020. ACMIT 2020 conference was held by Master of Information Technology (MIT) at Swiss German University (SGU) on Saturday, 21st November 2020, with the theme "IoT and Data Challenges in Digital Transformation". This theme is considered since in the current digital era, IoT applications and data are becoming more and more important. Digital transformation should then take into account the challenges in these areas. This is especially relevant for MIT SGU who has the vision to become the training place of future digital transformation architects.

The theme was mainly reflected in the plenary sessions with the following speakers:

1. Adhiguna Mahendra (MIT SGU lecturer and Chief AI Research and Product Innovation at Nodeflux), who gave a presentation about "State-of-the-Art Deep Learning and Edge Computing, with Use Case in Video Analytics"
2. Pungky Sulistyo (Country Product Manager, Hewlett Packard Enterprise), who gave a presentation about "Edge Computing Business Model"
3. Tito Luthfan Ramadhan and Mochammad Dimas Editiya (Garuda Maintenance Facility), who gave a presentation about "Challenges and Opportunities MRO Industry through IoT, Big Data, and Machine Learning"

Together with the conference, some workshops were also conducted with themes in line with the topic of the conference. The workshops are:

1. Vortex: Open-Source Deep Learning Computer Vision Framework for Agnostic Edge Computing Deployment (in collaboration with Nodeflux)
2. Evolution of Programming and Its Applications Towards Computer Networking (in collaboration with Aruba)

I would like to sincerely thank all the speakers, the partners, and committee members of the ACMIT conference. Without their help, this conference can not be run.

At the end, I hope that the published papers in this proceeding can be beneficial for the readers.

Tangerang, 21st November 2020

Dr. Eka Budiarto, S.T., M.Sc.

Chairman of ACMIT 2020 Committee

Table of Contents

ACMIT 2020 Committee

Steering Committee

- Rector : Rector, Dr. rer. nat. FilianaSantoso
- Vice Rector of Academic Affairs : Dr. Irvan S. Kartawiria, S.T., M.Sc.
- Dean of Faculty of Engineering and IT : Dr. Maulahikmah Galinium, S.Kom., M.Sc

Organizing Committee

Chairman : Dr. Eka Budiarto, S.T., M.Sc
Secretary : St. Ayu Diana Lestari,S.Pd.
Treasurer : Lestari Nur Wijayanti, S,St (Finance)

Communication & P.R : Irzan Fahmi, S.Kom – Visual Design & Photographer
Ayu Angela Agusta, M.Si
Wisnu Agung Trilaksono A.Md.

Procurement : Latifah Bachrum

Registration : Florentina Vanessa Prisilla, B.Bus.
Artauly Blessing C. Pakpahan, S. Kep

Technical Program

Paper Reviewer : Dr. Eka Budiarto, S.T., M.Sc
Dr. Charles Lim, M.Sc.,
Dr. Maulahikmah Galinium, S.Kom., M.Sc.
Dr. Ir. Heru P. Ipung, M.Eng.
Dr. Ir. Moh A. Amin Soetomo, M.Sc
Dr. Ir. Lukas, MAI
Dr. Adhiguna Mahendra, Skom, Msc.
Burman Noviansyah, S.T. MSISPM
Kalpin E. Silaen, M.Kom

Moderator : Dr. Ir. Heru P. Ipung, M.Eng.

Proceeding : Dr. Charles Lim, B.Sc., M.Sc
Dr. Eka Budiarto, S.T., M.Sc.

Event Rundown

Saturday, 21st November 2020

Time	Topic & Speaker
08:00 – 08:30	: Registration
08:30 – 08:40	: Prayers and singing the National Anthem of Republic of Indonesia
08:40 – 09.50	: Opening speech from Vice Rector I of Swiss German University
09.50 – 09.00	: Welcoming speech by Head of MIT, Dr. Eka Budiarto, S.T., M.Sc as Chairman of the Committee
09.05 – 09.05	: Award ceremony to Ir. Nuki Agya Utama, M.Sc., Ph.D., lecturer of MIT SGU for his contribution to MIT SGU
Keynote Speech	
09:05 – 09:50	: **Speech I:** **Dr. Adhiguna Mahendra** Chief AI Research and Product Innovation at Nodeflux Topic: State-of-the-Art Deep Learning and Edge Computing, with Use Case in Video Analytics.
09:50 – 10:35	: **Speech II:** **Pungky Sulistyo** Country Product Manager, Hewlett Packard Enterprise Topic: Edge Computing Business Model
10:35 – 11:20	: **Speech III:** **Tito Luthfan Ramadhan and Mochammad Dimas Editiya** Garuda Maintenance Facility Topic: Challenges and Opportunities MRO Industry through IoT, Big Data, and Machine Learning
11:20 – 12:00	: Question and Answers
12:00 – 13:00	: Lunch Break
13:00 – 17:00	: Parallel Sessions + Workshops

Parallel Session Schedules
ACMIT 2020 – Saturday, 21st November 2020

Workshop Sessions

Time	Workshop 1	Workshop 2	Workshop 3	Parallel Sessiona
13:00 – 17:00	Vortex: Open Source Deep Learning Computer Vision Framework for Agnostic Edge Computing Deployment (Nodeflux) Requirement: Laptop with minimum min 8 GB RAM, i7 processing core	Evolution of Programming and Its Applications Towards Computer Networking (Aruba)	Malware Detection in Wi-Fi Network (Indonesian Honeynet Project-SGU-Aruba)	Presentation of papers submitted to ACMIT by the authors Session will be moderated

Parallel Sessions

No.	Time	Authors	Moderator
1	13:00 – 13:20	Eka Chatra	Dr. Ir. Heru Ipung, M.Eng.
2	13:20 – 13:40	Ivan	
3	13:40 – 14:00	Dhanny	
4	14:00 – 14:20	Marastika Wicaksono Aji Bawono	
5	14:20 – 14:40	Yudha Fernando	
6	14:40 – 15:00	Jhoni Marcos	
7	15:00 – 15:20	Maulid Ibnu Adhi Purwoko	

Implementation of Meltdown Attack Simulation for Cybersecurity Awareness Material

Eka Chattra[1], Obrina Candra Briliyant[2]

[1,2]Politeknik Siber dan Sandi Negara, Bogor, Indonesia

Article Information

Received:
Accepted:
Published:
DOI: 10.33555/ejaict.v…

Corresponding Author:

Eka Chattra and
Obrina Candra Briliyant
Email:
eka.chattra@poltekssn.ac.id
obrina@poltekssn.ac.id

ISSN 2355-1771

ABSTRACT

One of the rising risk in cybersecurity is an attack on cyber physical system. Today's computer systems has evolve through the development of processor technology, namely by the use of optimization techniques such as out-of-order execution. Using this technique, processors can improve computing system performance without sacrificing manufacture processes. However, the use of these optimization techniques has vulnerabilities, especially on Intel processors. The vulnerability is in the form of data exfiltration in the cache memory that can be exploit by an attack. Meltdown is an exploit attack that takes advantage of such vulnerabilities in modern Intel processors. This vulnerability can be used to extract data that is processed on that specific computer device using said processors, such as passwords, messages, or other credentials. In this paper, we use qualitative research which aims to describe a simulation approach with experience meltdown attack in a safe environment with applied a known meltdown attack scheme and source code to simulate the attack on an Intel Core i7 platform running Linux OS. Then we modified the source code to prove the concept that the Meltdown attack can extract data on devices using Intel processors without consent from the authorized user.

Keywords: *Cybersecurity, Cache Memory, Meltdown Attack, Processor, Out-of-Order execution*

1. Introduction

Cyber security awareness is very important to maintain confidentiality, integrity, and ensure service availability in the context of organization's digital services. Security is guarded in the form of personal data such as documents, messages, texts and even passwords used to access a service. One of the most effective way to provoke cyber security awareness is to experience the risks, the vulnerabilities and the exploits first-hand. In 2017, vulnerabilities were found in computer processors, especially Intel processors, which could be exploited using an attack called Meltdown[1]. Any Intel processor released since 1995, except for Intel Itanium and Intel Atom before 2013, could potentially be affected by this attack[2]. Meltdown was able to allow an attack to read memory addresses in the kernel that should not have been accessible to the user[3][4]. Meltdown can even be used on devices with admin access rights to get data from the virtual machine (VM) guest account[5]. The meltdown attack is capable of exploiting the out-of-order execution that occurs in modern processors[1]. Out-of-order execution is an optimization feature that maximizes the utilization of all units of the central processing unit (CPU) core, so it can run instructions in parallel and can help improve processor performance[6].

Considering the impact of this exploitation, *Kohli* [7]conducted research in 2018 by simulating a Meltdown attack using an environment that was run on a virtual machine, with

reference to the stages of the Meltdown attack carried out by *Lipp et al*. This is intended as educational material, learning media and courseware as cybersecurity awareness material for students or researchers to know and experience the vulnerabilities exploited by the Meltdown attack. Courseware is a tools that can be used for learning purposes and act as a physical means of conveying subject matter[8]. In this context, this study implements a simulation stage of the Meltdown attack based on the scheme proposed by *Lipp et al* with reference to the Meltdown simulation conducted by *Kohli*. The simulation goals is to displays the output of secret data containing 8 characters placed in the processor's cache, as a prove of the concept of Meltdown attack.

1.1 Meltdown Attack

Meltdown is a cyberattack by means of exploiting a processor vulnerability that allows an attacker to bypass the isolation boundary between the application and the operating system (OS) so that data or information retrieval can occur when an application is running. The name was derived from the fact that the attack was able to "melt" the insulation protection which the processor hardware should be able to provide. Meltdown affects almost all Intel's processors produced since 1995, except for Intel Atom before 2013. Meltdown can exploit and infect all types of computer devices, including smartphone devices and cloud services [1]. Logically, a Meltdown attack occurs when it is about to read data from memory. Meltdown designed to exploit the out-of-order execution that today's modern generation processors applied. During the out-of-order execution, the processes carried out in memory are stored through registers and cache. If the out-of-order is not executed, the instruction is discarded from memory and registers, but the content of the memory are not lost in the cache. Meltdown takes advantage of this condition by using a side channel to check the availability of locations in the memory in the cache [9]. The Meltdown attack consists of 3 main stages as follows: (1) the content of the memory location chosen by the attacker are loaded into the register so that they can be accessed by the attacker, (2) a transient instruction on the CPU access the cache-line, based on the confidentiality of the content in the register, (3) the attack uses the weakness of the side channel on the processor (flush and reload) to determine the cache paths that are accessed and the data stored in the memory register[2].

1.2 Out-of-Order Execution

Each CPU core has several execution units, each of which is capable of carrying out different types of operations. In managing to keep the unit stable while working, the CPU can see various instructions that will be carried out afterwards and start executing on each CPU core while waiting for the next instruction. The out-of-order execution is a modern technology for a processor to be able to work optimally from the execution units available in the CPU [10]. In an out-of-order execution, instructions are fetched in the order according to the compiler generated. Processors that have an out-of-order execution function do not have to wait for previous instructions to complete to execute the next instruction, it can perform parallel executions.

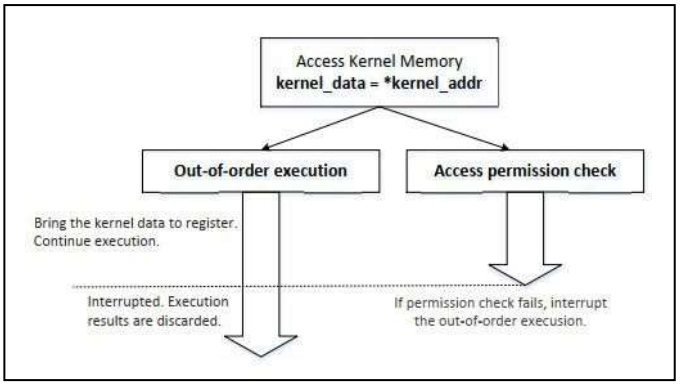

Figure 1. Out-of-Order Process on Modern Processors

As figure 1 depicted, in the out-of-order execution, the instructions will be executed in the order of data availability provided. As for doing so, after the processor takes program instructions from memory, then the instructions are sent to the instruction queue. When waiting for the queue, the instruction is allowed to leave the queue to carry out the next activity. Every time there is a call, the instruction will leave the queue to be executed. After that, instructions are sent to the unit accordingly. If all instructions command were to return to the registration result, then the result of the instruction are written to the register file.

1.3 Operating System

The operating system (OS) responds to a given process by managing the processes and system resources required by the user and the processes as mandated in the program. As the general platform of software, the OS performs basic tasks such as controlling and allocating, prioritizing process requests, controlling input and output devices, facilitating network systems and managing file systems. Most OS have applications that provide an interface to the resources managed by the OS. The OS functions as a hardware input/output management system as well as an interface in the use of software services. Linux is an OS that is free and open source. This makes Linux a very flexible and customizable OS. Most Linux distributions are designed for general use on desktop computers and network servers, but there are also distributions that are specific to different purposes and environments.

1.4 Simulation as a Learning Media

The simulation approach requires knowledge of the operation of the desired processes and output in a controlled environment. This information must be captured by the simulation model to represent the behaviour of the planned processes. But the level of detail included in the simulation will depend on the goal of the simulation [11]. For the purpose of cyber security awareness through meltdown attack simulation, the detailed unrelated processor works are not needed. So does the detailed information about how the program e.g. the source code are introduced to the victim's system. By reducing irrelevant or dynamic variables, the simulation can be constructed at a higher level to raised awareness caused by cyberattacks especially computer hardware exploits. After the framework of the simulation has been created, various computer configurations then may be created and much experiments can be perform according to several attack scenarios. And because the simulation's variable are controlled and safe in the virtual machine, they can be repeated and modified as needed so that all ground truth information can be identified and analysed.

2. Methods

The research method used in this research is qualitative research methods. This method is used to identify and understand the meaning behind the visible data used or proposed in previous research. The attack simulation design is based on the attack scheme conducted by *Lipp et al*. However, the stages in simulating a Meltdown attack are adjusted according to the research needs, which are carried out into several steps. These steps can be seen in Figure 2. These steps will also be the main reference for the design of the courseware.

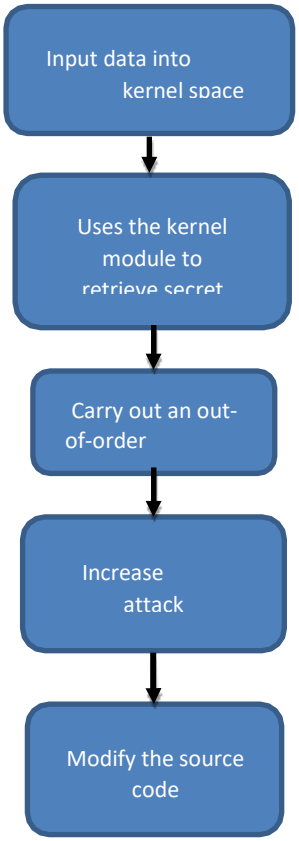

Figure 2. Meltdown Attack Simulation Scheme Planning

After understanding the visible data in the form of scheme and or concept of the research, then we used experiment method to gain a feasible approach of how to paint a picture of the danger of meltdown attack. The experimentation involved modifying source code so that the simulation can tests attack on user spaces. The modification also added some iteration so that the address reading can be conducted up to 1000 time. This loop procedure can improve the attack capabilities as such so that the attack's output can extract all available characters in the cache address. Quick comparison of research conducted with the references used is presented in Table 1.

Table 1. Research Comparison regarding Meltdown Attack

Comparison Variable	Previous Research	This Research
Virtual OS	Ubuntu 16.04	Ubuntu 18.04
Virtual Machine	Vbox 5.2	Vbox 6.0
Testing	Do not test attack on user space Does not test read address loops	Test attack on user space Test the loop reading address from 0-1000
Output	One character	All available characters

3. Result and Discussion

This chapter contains an explanation of what was done in the designed scheme along with the results obtained during the implementation process based on the experiments carried out.

3.1 Preparing the Attack Simulation

The first step for simulating an attack is carried out based on the need for the implementation stage. The attack simulation process requires a virtual laboratory environment. In this research, the environment will be run using Oracle Virtualbox 6.0, which uses the Ubuntu 16.04 operating system with an Intel core i7 processor. In order to simulate a Meltdown attack, the thing to consider is to ensure that the data was stored in kernel space (virtually). The data stored in this research is a string consists of 8 characters and stored as hardcode. These characters can later be seen or printed through a series of attack simulations.

```
static char secret[8] = {'P','A','S','S','W','O','R','D'};
static struct proc_dir_entry
*secret_entry; static char*
secret_buffer;
```

In some conditions, to increase the attack power, it is optional to use assembler code in the source code. Because Meltdown attack has a significant effect on a large number of repetitions that are carried out to find out the value entered into the cache. In this study, we tried 1000 times of iterative process. To simulate the output of the attack, modification of the original source code[7] were conducted to be able to print the secret characters that are retrieved from the cache.

```
// Prints all characters at the secret
value unsigned long kernel_data_addr
=0xfed0000; int k = 0;
for (k = 0; k < 8; k++) {
    Meltdown_attack(kernel_data_addr)
    ;
kernel_data_addr += 1;
}
```

Note that the unsigned line long kernel_data_addr = 0xfed0000 statement refer to the secret data address in the kernel module.

3.2 Implementation of Attack Simulation

After preparing the simulation environment, the next stage is implementing the attack simulation steps.

3.2.1 Input Data into Kernel Space

In the attack simulation concept, confidential data is stored in the kernel space indicating that the stored data can be read by a vulnerability caused by Meltdown. To be able to store confidential data, the kernel module was used as a library in the kernel. After compiling, the source code only needs to be run with the command "./(filename)" just like running common source code on Linux OS. There are several conditions for running a Meltdown attack simulation carried out on the kernel module[7]:

a. To simulate an attack, the address of the target confidential data is required. The target address will be obtained when inserting the kernel module into kernel memory. To perform these steps, run the command make to compile the kernel module. When finished compiling, you will see the addition of files in the form of kernel modules. It can be seen in Figure 3 before compiling the kernel source code, and Figure 4 after compiling the kernel source code

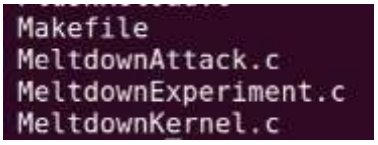

Figure 3. Before compiled

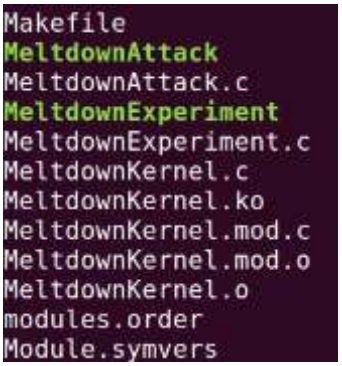

Figure 4. After compiled

b. After compilation, insert the kernel module into kernel memory with the command sudo insmod MeltdownKernel.ko so that the address of the secret data can be stored in the kernel. When the process is successful, it can continue to find the address of the secret data stored in the kernel message buffer using dmesg command.

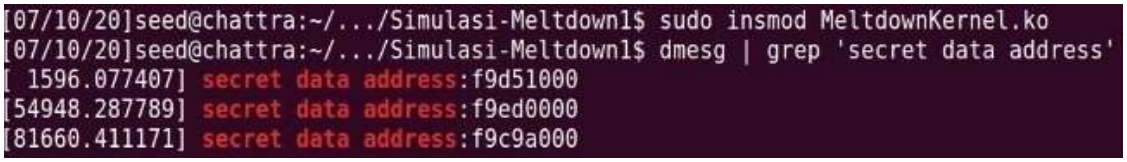

Figure 5. Process of obtaining Secret Address

Seen in Figure 5, the dmesg | command grep 'secret data address' can also be done so that search results can be found quickly and you can immediately see the address of secret data used in the kernel environment. In the figure there are 3 addresses of confidential data because the process carried out in this study is repeated. The address used is the most recent secret data address with a value of f9c9a000.

c. Stored confidential data must be in the processor's cache so that the attack simulation can run smoothly.

3.2.2 Utilized the Out-of-Order Execution

Once a confidential data address has been obtained, the address is entered in the source code

```
if (sigsetjmp(jbuf, 1) ==
0) {
Meltdown(0xf9c9a000);}
```

The source code is executed by utilizing an out-of-order execution where the stored data is entered into cache memory via a source code snippet as shown below.

```
int fd = open("/proc/secret_data",
 O_RDONLY); if (fd < 0) {
  perror("open"
  ); return -
  1;}
int ret = pread(fd, NULL, 0,
0); if (ret < 0) {
       perror("pread"
       ); break;}
```

3.2.3 Optimizing Attack

To be able to print secret characters stored in the kernel, it is necessary to increase the power of the attack by using a looping reading process of the kernel memory so that the value of the stored characters can be found and printed out. In this research, testing was carried out with the number of iterations of the same array as many as 256 at different loops. The test is described in Table 2 to see the results of the increase in attack power.

Table 2. Testing on Repetition Reading Secret Addresses

The number of repetitions of the read address	The number of loop 8 bits arrays	Result
0	256	Printed value 0
10	256	All values are printed
100	256	All values are printed
500	256	All values are printed
1000	256	All values are printed

3.2.4 Attack Simulation with Source Code Modifications

The Meltdown attack simulation can be run at this stage, but we decide to experiments and try to modified the source code so that the printed results can proved that the Meltdown attack simulation can retrieve all the data (all the characters) in the kernel memory. Note that the unsigned long line kernel_data_addr = 0xf9c9a000; address corresponds to the address on each device after inserting the kernel module into the kernel.

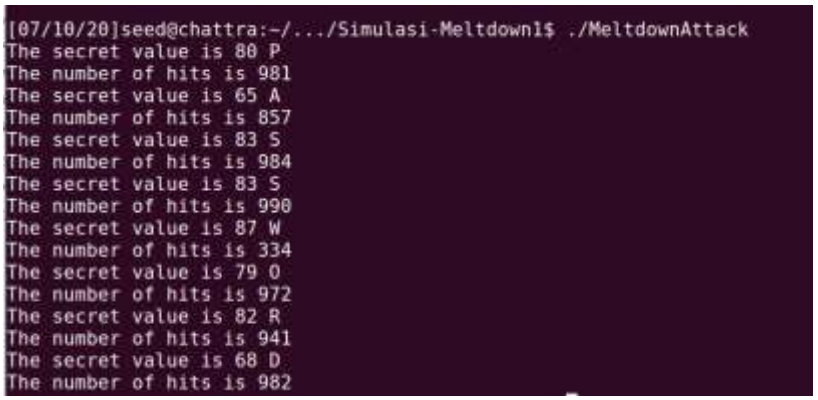

Figure 6. Modification of Meltdown Attack Simulation

Based on Figure 6, it can be seen that the Meltdown attack simulation can be carried out according to *Kohli (2018)* to print out a character of the secret data in the kernel. Also, by modifying the source code we can prove that the Meltdown attack can retrieve then print out all available characters of the secret data in the kernel.

4. Conclusion

Based on the attack simulation stages carried out, it can be concluded that a courseware for simulating a Meltdown attack consists of 4 steps that can be done by the learners. Those steps are: (1) input secret data into kernel space, (2) utilized the out-of-order execution, (3) optimizing attack, and (4) attack simulation with/without source code modification. However, previous to conducting such steps, the simulation environment must be setup and communicated between the instructor and the learners so that the context of the attack can be

understood. The attack simulation process requires a virtual laboratory environment with the correct hardware installed (e.g. Intel processors). Also, the virtual laboratory environment must ensure that the secret data was stored in kernel space. Simulated Meltdown attack provide by the steps can proves that the Meltdown attack can exploit the out-of-order execution built-in on the Intel Core i7 processor by issuing secret data values stored in the kernel memory. Further research can be explored regarding the notion of experimenting with the possibilities of other modification in the source code to found unknown capabilities of the attack, and thus helps identified other vulnerabilities in the target system. In terms of raising cybersecurity awareness, we encourage researchers to study the best way to explain about cyberattacks, cyber risks and threats in an effective way to learners and common audiences.

5. References

[1] M. Lipp *et al.*, "Meltdown : Reading Kernel Memory from User Space," 2017.
[2] M. K. Follow, "Meltdown and Spectre, explained," 2018.
[3] A. Prout *et al.*, "Measuring the Impact of Spectre and Meltdown," *2018 IEEE High Perform. Extrem. Comput. Conf. HPEC 2018*, pp. 1–5, 2018, doi: 10.1109/HPEC.2018.8547554.
[4] P. Company, "White Paper How the Meltdown and Spectre bugs work and what you can do to prevent a performance plummet THE I / O PROFILING Meltdown and Spectre : The facts," 2018.
[5] J. Sianipar, M. Sukmana, and C. Meinel, "Moving sensitive data against live memory dumping, spectre and meltdown attacks," *26th Int. Conf. Syst. Eng. ICSEng 2018 - Proc.*, pp. 1–8, 2019, doi: 10.1109/ICSENG.2018.8638178.
[6] Y. Kao and J. Huang, "High-Performance NAND Flash Controller Exploiting Parallel Out-of-Order Command Execution," pp. 160–163, 2010.
[7] K. Kohli, "Meltdown Attack Lab," no. February, pp. 1–15, 2018.
[8] Rusman, *Belajar dan Pembelajaran Berbasis Komputer Mengembangkan Profesionalisme Guru Abad 21*. Bandung: Alfabeta, 2012.
[9] H. Grover and D. Agrawal, "Design and architecture of Intel ' s core i7 processor," vol. 2, no. X, 2014.
[10] B. A. Ahmad, "Real time Detection of Spectre and Meltdown Attacks Using Machine Learning," no. April, 2020, [Online]. Available: http://arxiv.org/abs/2006.01442.
[11] M. E. Kuhl, J. Kistner, K. Costantini, and M. Sudit, "Cyber attack modeling and simulation for network security analysis," *Proc. - Winter Simul. Conf.*, pp. 1180–1188, 2007, doi: 10.1109/WSC.2007.4419720.

Medical Gases Cylinder Risk Evaluation To Prevent Risk

Ivan[1]

[1]Student of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received:
Accepted:
Published:
DOI:

Corresponding Author:

Ivan Ivan
Email:
leonhardivan@gmail.com

ISSN 2355-1771

ABSTRACT

Medical gases for medical treatment, are used to give gas therapy to the patient. They are widely used in hospitals, clinics, dental clinics, homes, and other healthcare facilities. They are essential and request zero faults. Because of the impact of medical gases fault, may could someone injury or even death. The incidents of using medical gases are still founding in several countries, including Indonesia. This research paper was conducted to give a perspective of risk evaluation, so medical gases cylinder management could get attention. Normally the incidents in using medical gases are caused by human error and fraud. Human error in using medical gases could make somebody death, and fraud could make financially lost which could affect operational cost. The explanation will be shown on the risk heat map and also the risk scorecard. This is facilitating to make it easier to take a decision for the priority of risk that should be mitigated or manage.

Keywords: *medical, gases, risk, management, hospital, engineer, instalasi, gas, medis.*

1. Introduction

The hospital is required zero faults in their operations. Therefore they need a good standard operational procedure and good risk management to prevent accidents. Safety of using medical gases cylinder should be triaged, considering medical gases as one of the main facilities at the hospital, so medical gases should have reliability when in use. Because a fault of using medical gases could make a serious injury or death. The safety of using medical gases must fulfill four safety principles: identity, adequacy, continuity of supply, and quality of supply.[1] Because of that safety principles, the hospital should train the human resources related to managing, distributing and maintaining the medical gases. A standard operating procedure based on ISO 31000: 2018 should be review and implementing it into the organization. This is to prevent the incident. [2] Sometimes when exchanging medical gases cylinders, the labeling and verifying which give the information for the contents is lack attention. The wrong medical gases cylinder contents supply could cause death incident. Since the fastest and accurate model to confirm the medical gases cylinder content is by reading the label, so it is an important notice to read it carefully. Although the medical gases cylinder has a different type of connector for each variety of gases. [3] To prevent dispensed the wrong gas to the patient, the important thing is to do cross-connection test. This test should be done by the contractor who is an expert on the medical gas pipeline system or authorized person. Cross-connection test is needed when we install the new pipeline system and also when change or modified existing system This is to meet the general safety of using medical gases, which is quality of supply.[1] The incident of using medical gases and also the risk causes with impact could give a picture of what frequently happens on using of medical gases. Like in table 1.

Table 1. Data of risk causes, risk impact and risk element.

No.	Citation	Risk causes	Risk Impact	Risk Element	Category
1.	Bankstown-Lidcombe Hospital in June and July 2016: dispensing incorrect gas to two neonates through a neonatal resuscitaire in Operating Theatre 8. [4]	The incorrect installation of the pipes and subsequent flawed testing and commissioning process, which should have detected the installation error.	2 Babies death because of inhale nitrous oxide instead of oxygen, it's prevented effective resuscitations	- Human Error - Standard Operating Procedure not applied	Human Error
2.	2 people died in Bengkulu hospital when inhale wrong medical gases supply, they inhale CO2 instead of N2O [5]	Wrong gas supply.	2 peoples death because of inhale Carbon Dioxide instead of Nitrous Oxide, during the surgery	- Human Error - No control of using medical gases	Human Error
3.	A hospital wanted to modify its existing gas supply for an expansion project. The modification was to move existing piping due to civil works (by another contractor) and to add connections to supply gases to 8 delivery rooms and an operating theatre. After several cancellations, work was scheduled by the hospital for a Friday. A Gas Company's engineering representative and contractor were to attend site to move the gas piping at the same time as other tradesmen working on other impacted services. At the last minute, the hospital changed the schedule to Saturday. The engineering representative could not be on site on Saturday but the contractor based on his qualification was instructed to complete the work without supervision. Work was completed on the Saturday. When performing pre-startup checks in the	The modification was to move existing piping due to civil works (by another contractor) and to add connections to supply gases to 8 delivery rooms and an operating theatre, without engineering representative.	When performing pre-startup checks in the operating theatres on Monday, the anaesthetist's stations started to alarm indicating low oxygen level in supplied gas.	- Human Error - Standard Operating Procedure not applied	Human Error

	operating theatres on Monday, the anaesthetist's stations started to alarm indicating low oxygen level in supplied gas. No patients were involved. [6]				
4.		Authorised person at hospital return full cylinder to supplier	Financial lost	- Fraud - No control of using medical gases	Fraud
5.	A simple mistake in the labelling and identification of medical gas lines resulted in a cross-connection of the oxygen and air, causing perioperative hypoxemia following the administration of a mixture poor in oxygen. [7]	Wrong medical gases pipeline system labeling.	2 people hypoxemia.	- Human Error - No periodic testing or verification.	Human Error
6.	3 Copper tube reporting lost in hospital, but no body knows when the pipeline was gone [8]	3 copper tube was disappear	Financial lost	- Fraud - Human error - No assets control	Fraud
7.	Run out of oxygen gases while doing surgery. [9]	Run out of medical gases	Patient hardly to breathe	- Human error - Standard Operating Procedure not applied	Human Error
8.	RESEARCH NOVELTY	- Cross connection - Wrong medical gases supply - Fraud - Run out of medical gases	Risk impact could be cause somebody injury, or even death, financial lost and bad reputation.	- Fraud - Human error - Standard Operating procedure not applied - No periodic testing and inspection	- Risk profile - Risk Analysis - Risk Assessment - Operation risk

This research paper's novelty is conducted to explain the fraud and human error has an impact on hospital reputation and financial (Table 1). Normally the risk happens in the organization or internal of the hospital. The medium level risk of fraud and high-level risk of human error is to determine the decision to minimized the gap between the high-level management and the operation. The following gap is :

1. Fraud because there is no surveillance of using medical gases.

2. Human error because of no training.
3. Standard Operating procedure not applied because of no knowlegde about medical gases risk impact. (No safety training)
4. No periodic testing and inspection.

2. Methods

A case study could be used to define incidents, testing theory, and make a new theory. [10] The case study methodology is based on qualitative analysis and focuses on observation of a social phenomenon, individual, organization, group, or institution. This method could see deep and analyze the incident and their causes factor. This method also could determine the process of some incidents. The investigation of the risk factor and risk element could make a good risk analysis. [11] The research method will be observation and collecting data, several accidents report will be analyzed.

Risk Evaluation (Figure 1), when risk scenarios are analyzing, two elements should be assessed, probability, and the risk impact. [12] Scorecard and heat map is used in the risk assessment process, by the risk assessment the organization will be aware of the risk causes and risk impact. The outcome will be risk mitigation of using medical gases at the hospital.[13]

Figure 1. Key risk indicators and risk reporting [12]

This research paper was conducted using Strategic Uncertainty Assessment Scorecard for Exposure, based on incidents that happen. It will be a focus on the Business/Operational and financial category of that table, to determine risk assessment. Risk analysis will be achieved with a risk heat map and calculation. [14] Visual scorecard to give us a perspective about risk probability and Risk Impact, and the result as a heatmap is made focus on a risk that should be prioritized. After prioritizing a risk, the solution will be risk management, at this step the risk will be mitigated.

Table 2. Strategic Uncertainty Assessment Scorecard for Exposure [13]

Categories of Strategic Uncertainity	Exposure					Likelihood				
	Low				High	Low				High
Business/Operational	1	2	3	4	5	1	2	3	4	5
Financial	1	2	3	4	5	1	2	3	4	5
Market Conditions	1	2	3	4	5	1	2	3	4	5
Technology	1	2	3	4	5	1	2	3	4	5
Business Relationships	1	2	3	4	5	1	2	3	4	5
Policy & Regulation	1	2	3	4	5	1	2	3	4	5

Risk analysis using a scorecard, change qualitative data to quantitative data. A scorecard is needed to assess the risk and could give input for planning activity and risk mitigation. Table 1 case study rated by using table 2 risk assessment scale 1 to 3, 1 is low or no effect for the process and 3 is for high and important and has an impact for the process. [13] This risk assessment guides the organization to scale the priority of the risk which should be immediately taking action, and also a decision for the risk control, mitigate, transfer, avoid or accept. Heat map results could be used to determine risk assessment (Table 2). Risk assessment could do by 5 X 5 heat map design. The vertical axis shows the probability of risk. The horizontal axis shows the risk impact. The risk result could be obtained by the formula below[15]

Risk = Risk Potential impact X Probability of risk

Table 2. Heat map of potential risk analysis.[15]

			RISK IMPACT				
			Negligible	Low	Medium	High	Extreme
			1	2	3	4	5
RISK PROBABILITY	Remote	1	1	2	3	4	5
	Unlikely	2	2	4	6	8	10
	Possible	3	3	6	9	12	15

	Likely	4	4	8	12	16	20
	Probable	5	5	10	15	20	25

The risk causes with the risk impact and risk probability could give a picture of what frequently happens on using of medical gases. This risk analysis could make a risk awareness and guidance to plan and organize risk. Risk analysis shows the risk causes normally because of human factors, no control of using medical gases, Standard operating procedure not applied, and fraud. This risk assessment with a scorecard and heat map could determine the risk which is important to be mitigated. Table 4 define Red color is a very high risk, orange color is for high risk and need to take an action immediately, a yellow color is for medium risk and need to find a solution to prevent the risk, green color is for low risk, Blue Colour is for no effect or acceptable. For example, if the risk does not cause death and not important it should be in a blue position.[14],[12]

Table 3. Risk Assessment.

VERY HIGH	Score 15-25, This is a very high impact with high probable to be happens, and should takes immediate action, how to mitigate or avoided the risk. Because it could be affected the business process and financial lost.
HIGH	Score 10-12, This is a high impact with likely to be happens, and should takes an action, how to mitigate the risk. Because it could be affected the business process and financial threats.
MEDIUM	Score 5-9, This is a medium impact with possible to be happens and should takes a plan to take an action with a reasonable time. Because it could be affected the business process and safety but not necessary.
LOW	Score 3-4, This is a low impact with chance of incident could be happens is unlikely. Because it almost no effect for the business process and financial.
VERY LOW	Score 1-2, This is a very low impact with chance of incident could be happens is remote. Because it is no effect for the business process, and financial, but it could be accept or tolerance.

Results and discussion

Table 4. Risk Probability Score

No.	Risk Category	Total number of favourable outcomes n(A)	Number of favourable outcome n(S)	Risk Probability n(A)/n(S)	Risk Probability in Percentage
1.	Human Error	6	6	1	100%
2.	Fraud	4	2	0,5	50%

Four types of medical gases normally using at a hospital is Oxygen, N2O, Air, and Vacuum, the total number of favorable outcomes is 6 because oxygen has a probability of changing with N2O, Air, and Vacuum, and N2O has a probability of changing with air and vacuum, the last one is air is possible to change with the vacuum. So there is 6 times the potential to cross-connection between

the gases caused by human error, there are also 6 possibilities. For the fraud, there are four types of medical gases, but the potential to do the fraud is 2 types of medical gases because normally compressed air and vacuum using an automatic machine, not a cylinder.

Table 5. Risk Probability Assessment.

PROBABLE	>90 % - 100%	5
LIKELY	>50% - 90%	4
POSSIBLE	>25% - 50%	3
UNLIKELY	>10 % - 25%	2
REMOTE	0% - 10%	1

Risk probability assessment is to define the risk probability score. 0% - 10% score is one or the event probability is remote. More than 10% to 25% score is 2 or the event probability is unlikely. More than 25% to 50% score is 3 or the event is possible. More than 50% to 90% score is 4 or the event is likely. More than 90% to 100% score is 5 or the event is probable.

Table 6. Risk Impact Score

No.	Risk Category	Risk Impact	Risk Impact Score
1.	Human Error	No Effect	1
		Wound	2
		Injury	3
		Permanent Disability	4
		Death	5
2.	Fraud	< Rp. 10.000.000 / year	1
		> Rp. 10.000.000 – Rp. 50.000.000 / year	2
		> Rp. 50.000.000 / tahun – Rp. 100.000.000 / year	3
		> Rp. 100.000.000 / tahun – Rp. 200.000.000 / year	4
		> Rp. 200.000.000 / year	5

The risk impact for human error has a score of 5 or very high level, if the impact is has possibility to make somebody death. The risk impact for the fraud category, if cause financial lost Rp. 100.000.000 and up per year it could be categorized at score 3 or medium level. For the human error category, if cross-connection or wrong gases supplied happens, it could be caused somebody death, and it could damage the hospital reputation.

Table 7. Risk assessment result

No.	Category	Risk Impact	Risk Probability
1.	Human Error (Business / Operational)	5	5
2.	Fraud (Financial)	2	3

Table 7 results would explain to the heat map, which is made easier to read. For example for the human error risk category, the risk impact is 5 or very high, because it could make somebody death, and the risk probability score is 1 or also probable. So the risk will be on a high level of risk. Herewith the explanation about how the impact and probability were scored. For the fraud, 200 beds of a hospital normally using around 800 cylinders per month for oxygen and 4 cylinders for N2O. So the financial loss per year is around Rp. 31.200.000 – Rp. 40.000.000 per year or even more. This sample and interview get from type C hospital.

3. Conclusion

We should decide on the risk priority, to focus on the important problem. After decided the risk priority scale, started to make a plan, running the program, analyzing, monitoring, and evaluating. After that risk assessment is needed to determine the next step to preventing the risk. So control, monitoring, and evaluation will be applied for the higher risk that could happen. Risk management is needed to make a security program. This is key to success protection. So this is should be a management function of some organization or procedure because the risk cannot omit, but it could be mitigated.[14] This research paper's novelty is found the fraud and human error have an impact on the hospital's reputation and financial shown by the level of risk. Fraud could affect the operational cost will be high, at the end could affect the price charge to the patient will be high also. To mitigate the risk of fraud and human error the author suggests using IT-based system control using the application.

4. References

[1] Great Britain and Department of Health, *Medical gases: health technical memorandum 02-01: medical gas pipeline systems.* London: Stationery Office, 2006.

[2] T. Y. Aldyth and S. D. Ede, "Evaluation of Risk Management Implementation in Medical Gas Installation Hospitals with ISO 31000: 2018 Approach," Aug. 08, 2019. https://doi.org/10.26911/theicph.2019.04.03 (accessed Oct. 03, 2020).

[3] J. R. Hart, "Medical Gas and Vacuum Systems Installation Handbook," 2015. https://b-ok.asia/ireader/2885311 (accessed Oct. 04, 2020).

[4] Chief Health Officer, "Bankstown - Lidcombe Hospital Medical Gases Incident : Final Report," p. 24, Aug. 2016, doi: https://www.health.nsw.gov.au/Hospitals/Documents/bankstown-lidcombe-incident-final-report.pdf.

[5] "Dokter Dianggap Lalai, Dua Nyawa Melayang - News Liputan6.com." https://www.liputan6.com/news/read/28945/dokter-dianggap-lalai-dua-nyawa-melayang (accessed Nov. 08, 2020).

[6] "EIGA TP_40_14_Recent_Incidents_SAC138.pdf." Accessed: Oct. 03, 2020. [Online]. Available: http://www.bcga.co.uk/assets/EIGA%20TP_40_14_Recent_Incidents_SAC138.pdf.

[7] M. Dangoisse, M. Lalot, and J. Lechat, "Connection error in the delivery of medical gases to a surgical unit," *Acta anaesthesiologica Belgica*, vol. 61, pp. 33–7, Mar. 2010.

[8] "Pipa Instalasi Gas Medis RSUD TP Dilaporkan Hilang." https://anteroaceh.com/news/pipa-instalasi-gas-medis-rsud-tp-dilaporkan-hilang/index.html (accessed Nov. 08, 2020).

[9] K. C. Media, "Oksigen Habis Saat Operasi Pasien, Ini Penjelasan Dokter," *KOMPAS.com*. https://regional.kompas.com/read/2015/08/15/09512711/Oksigen.Habis.Saat.Operasi.Pasien.Ini.Penjelasan.Dokter (accessed Nov. 08, 2020).

[10] *Eisenhardt, Kathleen M. Building Theories From Case Study Research. Academy of Management. The Academy of Management Review; Oct 1989; 14, 4; ABI/INFORM Global. pg. 532.*

[11] "Kothari_-_Research_Methodology_Methods_and_Techniques_-_2004.pdf." Accessed: Oct. 22, 2020. [Online]. Available: https://dinus.ac.id/repository/docs/ajar/Kothari_-_Research_Methodology_Methods_and_Techniques_-_2004.pdf.

[12] *Risk it practitioner guide.* Place of publication not identified: Isaca, 2009.

[13] A. Gray, J. Detre, B. Briggeman, and M. Boehlje, "Scorecarding and Heat Mapping: Tools and Concepts for Assessing Strategic Uncertainty," *International Food and Agribusiness Management Review*, vol. 09, Feb. 2006.

[14] P. Bowen, J. Hash, and M. Wilson, "Information Security Handbook: A Guide for Managers," p. 178, Oktober 2020.

[15] "communicate-risks-using-heat-map.pdf." Accessed: Oct. 29, 2020. [Online]. Available: https://web.actuaries.ie/sites/default/files/erm-resources/communicate-risks-using-heat-map.pdf.

Risk Management In Protecting Banking Sensitive Information at XYZ Bank Using COBIT5 Framework

Maulid Ibnu Adhi Purwoko[1]

[1]Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received:
Accepted:
Published:
DOI: 10.33555/ejaict.v…

Corresponding Author:

FirstName LastName
Email: email address

ISSN 2355-1771

ABSTRACT

POJK No.18 / POJK.03 / 2016 concerning the Implementation of Risk Management for Commercial Banks is addressed to the management and board of directors of Banks to improve provisions regarding compromised customer information disclosure to the public, and breaches of customer information have led to the need for risk management practices in the use of Information Technology (IT). Risk Control Assessment (RCA) is based on the COBIT 5 framework to assess risks associated with the use of Information Technology Asset in XYZ Bank. By mapping the RCA and the provisions of POJK No.18 / POJK.03 / 2016, it can help management obtain information on the level of compliance of the Bank with provisions relating to Banking sensitive information.

Keywords: *POJK, Risk Control Assessment, Banking Sensitive Information.*

1. Introduction

Bank XYZ is among the 10 largest banks in Indonesia, with assets of more than 160 trillion rupiah. As a bank that is transforming into a digital bank, various types of digital services for various lines of business segments are presented with various kinds of technological innovations by building digital infrastructure as a support. The application of technology plays an important role in the collection and processing of data and / or information, its availability for the right person / user in the right format and at the right time which can support business decisions and strategic thinking. And with this initiative, XYZ Bank management realizes the risks involved in every innovation presented to its customers. And with this initiative, XYZ Bank management realizes the risks involved in every innovation presented to its customers.

Risk is considered as something that might go wrong in an establishing process and also a combination of the likelihood of an event and its effects. There are three categories of risks on the enterprise which is projects risks, product risks and business risks [1]. The need for an effective framework in managing these risks, especially in safeguarding sensitive bank information. Hence the organization must learn to stabilize the possible negative effects of risk against the possible gains of its related opportunity.

In Indonesia, the Financial Services Authority (OJK) has regulated matters relating to risk management related to the use of information technology at commercial banks in POJK No.18 / POJK.03 / 2016. Therefore, it becomes a guide for Banks in managing Information Technology in the aspects of risk management. Thus, Banking Industry needs a comprehensive framework covering all aspects of risk management due to various reasons such as the need to create appropriate internal controls, and prevent issues related to software errors and sensitive data exsposure [2]. Control Objectives for Information and Related Technology (COBIT), a comprehensive framework for IT governance and risk measurement in an organization. COBIT can provide standard practices that can assist organizations in implementing various processes and procedures in terms of risk management aspects[3].

COBIT 5 provides a comprehensive framework that can assist companies in achieving their goals for corporate IT governance and management. And it can be said to help companies in creating optimal value from IT applications. By maintaining a balance between realizing benefits and optimizing the level of risk and use of resources.

2. Research Method

The methods used in this research include:

- Observing by conduct in-depth discussions with professional experts involved in the Risk work unit as well as IT Security and Governance
- Literacy Method; namely searching for journals related to the COBIT framework, especially those related to the subject matter of Risk Management, IT Security and Governance.
- Conceptual method; In COBIT 5 Framework based on APO, BAI and DSS
- Providing questionnaires (Risk Control Assessment) to the Head of the Information Security Risk Management Division and the Head of the IT Security Policy Unit. Where in the process it will ask different concerns from one another.

In conducting the research, we work based on the IPO (Input-Process-Output) technique. This is expected to be in accordance with the purpose of using the COBIT framework in validating qualities from an audit point of view. In accordance to [4] that in producing audit quality it can be seen from 3 points of view, namely: an input perspective, a process perspective and a results / output perspective. Where in its implementation can produce an ethical aspect that is useful for quality formation. Among the ethical aspects according to [4] are: integrity, objectivity and independence.

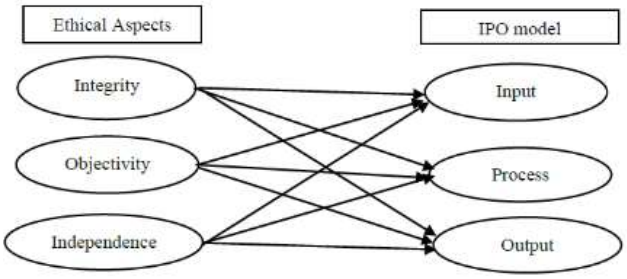

Figure 1. Ethical Aspect in IPO Model [4]

In the input process we ensure that by entering data according to other journal references so that it can be managed in the process of producing output in the form of a framework that can be used based on the COBIT framework, which is related to planning and organizing, development and implementation, and related to deliverable services.

The framework was created for the purpose of overcoming weaknesses in risk management and control that have been adopted by XYZ Bank, including:

• Maturity level, in how to assess and comply

• There is duplication of existing controls, thus making XYZ Bank lacking a single control repository.

• The need for clarity of processes and solutions for risk assessment

In the decision to use COBIT has been set by the team at XYZ Bank where a team is formed of governance experts in determining a basic risk management framework. The defined processes and templates to be used

are appointed by a team consisting of the IT security and risk management unit. There are 3 areas that underlie this, including:

• What form the conceptual framework will be used

• Identification of 'entity' standards for evaluating risks and controls

• Identification of how the process is in carrying out a Risk control assessment (RCA).

3. The Framework

The framework is defined by linking risks affecting technology and best control practices according to industry standards as defined in COBIT. Three goals have been set, among others :

1. Acting as a tool to facilitate risk assessment and effective control in technology.
2. Acting as a reporting framework to demonstrate how technology has met the requirements of reporting regulations, including the requirements contained in OJK regulations.
3. Acting as a means that can encourage assurance to management.

Following are the steps in implementing a framework using COBIT according to the expected outcome based on the risk rating [5], including :

• Risk identification level I (Severe) is defined based on information that has a financial or non-financial impact such as technology, business operations, people, law, regulatory, financial reports, financial crime and reputation.

• Risk identification level II (Major) is the main risk that is divided into 2 levels in terms of the impact that will be generated and its impact on business operations. At level II (Major) as related to the risks associated with IT technology as a supporting unit:

- Lack of IT support, especially in relation to the design and testing environment.

- IT systems that are not available as a support in a work unit

- Lack of awareness of the security of IT use

• On the identification of controlled objectivity; Where every risk that falls into the level II category can be identified with the use of COBIT. Table 1 shows the mapping of these risks in level II categories with controls identified for each risk of using technology[6] [7].

Table 1. Mapping Level Risk

Risk Control Assessment		
Adequate Design of IT System	**Availability of IT system**	**IT Security**
APO1 Define Information Architecture strategy	BAI2 Acquire application requirement software	APO1 Define Information Architecture strategy
APO3 Technology direction	BAI3 Acquire Technology solution	APO2 Define IT organization and relationship
APO8 Manage Quality Relationship	BAI5 Manage IT resources	APO9 Assess and Manage IT Risk
APO10 Manage Project Suppliers	DSS1 Devine and manage service level	BAI2 Acquire application requirement software
BAI1 Manage Programme for automated Solution	DSS3 Manage performance	DSS5 Ensure system Security
BAI2 Acquire application requirement software	DSS4 Ensure continuity service	DSS11 Manage Data
BAI3 Acquire Technology solution	DSS8 Manage Incident data	DSS12 Manage Phisical Environment
BAI6 Manage Changes	DSS3 Manage problem	
BAI7 Install and accredit solution changes	DSS11 Manage Data	
	DSS12 Manage Phisical Environment	
	DSS13 Manage Operation	

4. Identifying the Entities

In the design of IT systems, key entities related to model management are needed, where the model must be assessable and also to control risk. Logically this can be related to objectives related to reporting mechanisms and how to control support services on a technology platform [8].

In IT design, it can be defined in a model related to:

- **Person entity**: Where in this section there is certainty of duties and how it is correlated with social aspects (compliance, rules, work methods, culture, norms, personality, etc.) With the existence of an entity person is expected to be able to carry out risk assessment and control of the complete use of technology.
- **Process entity**: In providing support, control and governance in the IT environment, a process that can represent this is required.
- **Technology entity**: dealing with components in IT, such as: applications, servers, networks and firewalls.
- **Governance entity**: Relates to compliance with applicable and determined regulations, both from internal and regulatory agencies. And on this matter, it is recommended to know the control information and risks that may occur. Also important in meeting the target status for the development or change of a project before going live.

In determining IT services is one of the methods of this bank to fulfill the objectivity of the function of IT services. Identification of support services in a service scope consisting of the top types of services in a catalog that can be used as a reference. Service forms can be represented in the form of a support service map. The map consists of an explanation of the technology components in support of a quality form of end-to-end service. Each process entity and technology entity will differ greatly in linking to multiple support services. From this statement, it is expected that the results will be in accordance with the key management model of the key entities, so it can be said that a lot of flexibility can also be used as an expansion of IT services. In addition, it must also be adjusted to the needs of the organization today, tomorrow and in the future. Among these entities are interrelated and possibly useful in conducting risk assessments by means of developing and providing end-to-end service risk profiles in relation to overall management of the entity's management.

5. Implement and define the RCA Process

Figure 2 shows the process according to an overview that describes the risk assessment process in five steps [9]. Where the main task at each step should be identified. Process assistance in scope, schedule and how to carry out a risk assessment can be explained in detail.

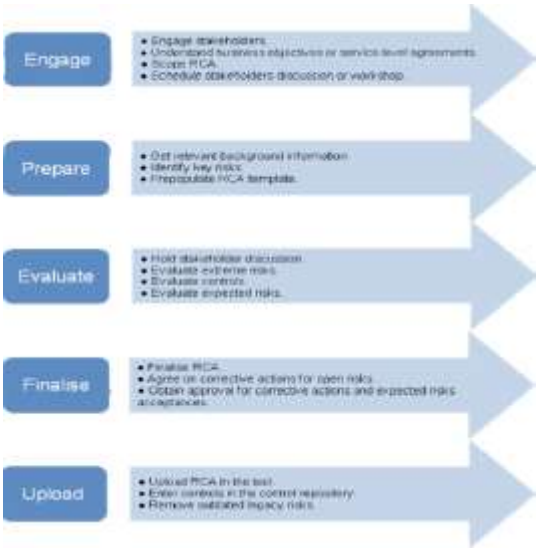

Figure 2. Risk and Control Assessment Process Step

The purpose of developing the RCA process is how to make certainty in the analysis and consistency of risk control involving a team. Excel templates can be used as a support tool to determine whether the available controls are feasible and can assist in determining risk. Templates are used by all entities defining all information assets. Templates are specified in capturing the following information:

- OJK control requirements and best practices
- Defining risk according to the level of potential risk
- Application according to the control process of COBIT
- Ownership of control
- Conduct an assessment of the available controls whether they are effective or not
- What actions will be taken to exercise control effectively
- The final stage of how the details of the action can be accommodated with data on the owner of the action and the target date for the action

In the template, complete information is carried out by the risk owner himself so that it can be reviewed and assessed by the integrated risk team. Then in the process of reporting open risks, it is entered into a risk management tool to record the closing actions taken. Consists of Tags :

- Entity owner: Risk Control Assessment (RCA) owner
- Risk owner: Who is responsible for the risk
- Owner of control: The owner who is responsible for maintaining the effectiveness of the control
- Owner of action: Which is determined due to ineffective controls

6. Result and Discussion

Based on the results of the observation and questionnaire on XYZ Bank. It can be concluded based on RCA step as follows :

- Adequate design of IT System.

APO1, related to the information architecture strategy, XYZ Bank is available and has implemented the Information Technology Strategic Plan (RSTI).

APO3, the direction of use and development of technology has also been well managed.

APO8, the quality management of the relationship between IT as a supporting unit and Line of Business (LOB) as a partner is quite good in providing technology application solutions. Although there are several GAPs, sometimes business initiatives for reasons of speed and accuracy often bypass IT and work directly with third parties.

APO10, collaboration with suppliers is inevitable, and potential risk factors are sometimes a second thing, so the business team often deviates from existing standards.
BAI1, the use of automated solutions has been widely implemented and has become a consideration for business units to be able to enhance systems / applications, especially those related to customer transactions.
BAI2, deals with build-in and in-house IT applications, where there is no ASR (Application Security Requirement) as a reference for security standards in IT applications.
BAI3, the latest technology solutions have been implemented and taken into consideration by management
BAI6, according to BAI3 which also has a correlation, it can also be explained that every change must be recorded properly. And the CCB (Change control board) mechanism which is held weekly with a permanent IT team.
BAI7, deals with the implementation of all change solutions related to technology use initiatives.

- Availability of IT System.

BAI2, It can be explained that every application at XYZ Bank must meet the minimum security requirements in accordance with IT Security standards.
BAI3, Obtaining Technology Solutions in accordance with the objectives and benefits of the Bank's business initiatives by always innovating in order to meet customer expectations by opening feedback channels for each service.
BAI5, Manage IT resources in a professional manner by consistently conducting continuous training, with centralized training facilities in Bogor by bringing in professional trainers from within and outside the country.
DSS1, Develop and manage service levels centrally by a Service Quality work unit.
DSS3, Manage performance by continuously updating information technology as a support.
DSS4, Ensuring service continuity by always innovating on digital products.
DSS8, Manage incident data well, because CSIRT rules are available as a standard reference for incident management.
DSS9, Managing problems has not been centrally still decentralized according to business units.
DSS11, Manages data fairly well, with tools namely DMS (Data Management System).
DSS12, Manage the physical environment fairly well and apply various kinds of the latest technologies such as Face Recognition Access.
DSS13, Managing operations towards office transformation to Digital Bank by implementing agile development.

- IT Security.

APO1, Information Architecture Strategy cannot be defined structured.
APO2, IT organizations are still not mature enough in terms of the types of work that are still overlapping.
APO9, Lack of risk management for IT, because the mainset of the IT team is only a support, not a bank-wide enabler.
BAI2, Rules for the use of software as security prerequisites have been set in IT security standards.
DSS5, System Security Standard is quite comprehensively regulated in the IT Security Standard provisions.
DSS11, In managing data related to security events, it is good because it has implemented SIEM.
DSS12, Physical Environment Management in terms of data security is good enough with the availability of capable data security mechanisms.

Regarding the training stages, there are generally many terms, using the RACI chart we can define each term into a task and function of each part such as the entity owner, risk owner, control owner and owner of the action. RACI itself is responsible, actionable, consulted and informed (see example in Figure 3[10]). Responsibilities can also be mapped into job descriptions with various performance evaluation criteria for each function or it could be the job level. And this arrangement will have an impact on employees.

RISK / Entity	CEO	COO	Integrated Risk	Facility Mgmt	IT Sec & Gov	Human Capital
Activity/Deliverables						
Manage Logical Security	I	I	C	C	R	C
Manage Physical Security	I	C	C	A	C	-
Reporting Security Incindent	I	A	I	I	R	I

Figure 3. RACI Chart example

Figure 3 can illustrate, where the facility management department is responsible for the continuous availability of physical security, while the chief operating officer (COO) is responsible for the incident reporting mechanism along with how to respond and the follow-up process. Meanwhile, every staff, both employees and vendors, in acting and working outside the office, it is in the attention of the HC team that they can be consulted regarding the logical security of the company's assets, namely the employees themselves and also be informed for the reporting.

The main challenge according to duties and responsibilities as in the example of the RACI matrix above is in explaining each process to stakeholders who have different backgrounds and understandings. This must be managed properly in order to be able to understand the risks where a training program is needed at various levels[11]. By involving more :

- In making adjustments to the training material delivered by the risk experts. Speaking of entity owners, there is a simple description of a process provided through a compulsory computer-based continuous training. As for risk and control owners, training details which include a sample and test, can then be delivered through classrooms in different locations or through web-based training sessions.
- By adjusting the training provided by risk experts to the audience. For entity owners, a simple process overview is provided through compulsory computer-based training. For risk and control owners, training is detailed and includes samples and tests, and delivered via classrooms at different locations or via web-based training sessions.
- Offering, as part of the mandatory training program, this awareness training session can be expected to explain the process by providing links and contacts to local risk experts within the organization with further guidance.
- By holding workshops it is hoped that we can disseminate relevant information to stakeholders, by starting the risk assessment process. Training resources were used to facilitate control self-assessment (CSA) at different locations.
- In the modification of the description, related to the role and how the performance evaluation process and real-time to be able to include specific tasks in risk and control.

7. Result and Discussion

The reporting process uses a simple spreadsheet which functions to maintain risk and control the repository for each entity. Within each entity, tools such as the Excel spreadsheet used to track risk can be used by members of the risk team, helping to determine actions to take and other matters. In the use of database repositories, generally serves to maintain risk over control within the organization[12]. Therefore, tools were developed to collect information about all entities. which will assist in :

- Centralized risk repository and information control

- In the process the RCA can help track all actions that have been determined and that have been approved
- Every service risk is Traceable
- Every closure action can be tracked
- Report to senior executives on risks based on requirements and levels of risk
- The basis for reporting on regulatory requirements is contained in a common risk and control database

8. Conclusion

In the development and implementation stage it took nearly two years. While the central team is responsible for developing the process, risk resources are work unit based, so it plays an important role in the implementation, training process, etc. Because the implementation is in different locations, it requires the involvement of several work functions in the team. Changes will make some work units resistant, with the feedback mechanism that the team uses to help in the process of aligning and correcting each change. This can help in increasing the maturity of the process. Other tangible benefits of this initiative :

- This exercise is very helpful for banks in managing risk and the control process according to best practice standards as well as from the regulator (OJK) and other regulatory processes. The spreadsheets in the RCA provide separate filters for implementation of compliance levels.
- Repository processes really help maintain consistency. This is done by creating a separate sub-unit within the risk team to ensure a quality check for each RCA prior to inclusion in the repository.
- The training package is generally seen as an important and valuable delivery by the risk team and is based on the needs of the participants. For example, a 15-minute training package for all entity owners was developed and implemented using an e-learning portal, while a detailed process training package was developed specifically for risk and control owners.

9. References

[1] R. Lock, T. Storer, I. Sommerville, and G. Baxter, "Responsibility modelling for risk analysis," *Reliability, Risk, and Safety*, no. September 2009, 2009.

[2] B. D. W. Hubbard, "Risk Management: A Very Short Introduction to Where We've Been and Where (We Think) We Are," *The Failure of Risk Management*, pp. 21–35, 2015.

[3] H. Haviluddin and A. Patricia, "Exploring COBIT Framework for Information Technology Governance (ITG) at Mulawarman University, Samarinda, East Kalimantan, Indonesia: A Descriptive Study," *Enhancing Sustainability, Competitiveness & Innovation*, no. 01, 2012.

[4] A. Agus and N. Aziza, "The effects of ethical factors in financial statement examination: Ethical framework of the input process output (IPO) model in auditing system basis," *International Journal of Financial Research*, vol. 11, no. 2, pp. 136–145, 2020.

[5] W. J. Fletcher, "The application of qualitative risk assessment methodology to prioritize issues for fisheries management," *ICES Journal of Marine Science*, vol. 62, no. 8, pp. 1576–1587, 2005.

[6] J. Barve, "COBIT Case Study: IT Risk Management in a Bank." [Online]. Available: https://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-IT-Risk-Management-in-a-Bank.aspx.

[7] M. Wolden, R. Valverde, and M. Talla, "The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system," *IFAC-PapersOnLine*, vol. 28, no. 3, pp. 1846–1852, 2015.

[8] R. D. S. De Haes, W. Van Grembergen, "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities," *COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities*, p. 25, 2013.

[9] B. W. Main, "Risk Assessment : A review of the fundamental principles," *Risk Management*, vol. 24, no. 4, pp. 1–7, 2008.

[10] S. Zhang and H. Le Fever, "An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-

BSC Model," *Journal of Economics, Business and Management*, vol. 1, no. 4, pp. 391–395, 2013.

[11] V. M. Sunder, "Lean six sigma project management - A stakeholder management perspective," *TQM Journal*, vol. 28, no. 1, pp. 132–150, 2016.

[12] U. Noor and A. Ghazanfar, "A survey revealing path towards service life cycle management in COBIT 5," *2016 11th International Conference on Digital Information Management, ICDIM 2016*, pp. 68–73, 2016.

Analysis correlation of the Implementation Framework COBIT 5, ITIL V3 and ISO 27001 for ISO 10002 Customer satisfaction

Marastika Wicaksono aji bawono [1], Mohammad Amin Soetomo[2], Thata Apriatin[3],

[1]Master of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received: 28 November 2020
Accepted: 28 November 2020
Published: 6 December 2020
DOI:

Corresponding Author:

Marastika Wicaksono Aji Bawono , Mohammad Amin Soetomo,and Thata Apriatin

Email:
marastika.bawono@student.sgu.ac.id
mohammad.soetomo@sgu.ac.id
thata.apriatin @student.sgu.ac.id

ISSN

ABSTRACT

Abstract — This study aims to determine and provide information about the corellation of COBIT 5, ITILV3 ,and ISO 27001 for customer satisfaction. This study uses a causal associative method with a quantitative approach. The population of this research is all customers of company Quota Broadband Internet. The sampling technique in this research is probability sampling technique through simple random sampling. The research sample was 135 customers. The results showed that there was an corellation of COBIT 5 (6.Customer-oriented service culture), ITIL V3 (Service Operation 4.2 Incident management), and ISO 27001 (A.16 Information security incident management) for 10002 (3.4 customer satisfaction).. The biggest influence is COBIT 5 on ISO 27001 with a T statistic of 6,960 and a P value of 0,000.

Keywords — COBIT 5, ITILV3, ISO 27001, ISO 10002, Customer Satisfaction

1. Introduction

This study explores the analysis of the link between the introduction of a variety of frameworks to increase customer satisfaction in the business. Within this business, the COBIT 5 framework is used as a governance framework that focuses on the scope of 6. Customer-oriented service culture and RACI work position framework based on job descriptions and has introduced the ITIL V3 framework that focuses on service operation 4.2 Incident management using the engine management service application service desk.managed problem with customer service center for internet service complaints handling.[7] to reduce corporate cyber crimes using the ISO 27001 information system security, which focuses on the scope of A. 16 Information security incident management for information security.[9] Both frameworks seek to enhance 3.4 customer satisfaction in compliance with ISO 10002 framework requirements. The purpose of this research is therefore to examine the combination of parameter tools from different frameworks that have been applied in order to obtain best practice parameters and tools that can increase customer satisfaction .[16] The use of information technology poses a major risk to information systems and in particular, to critical resources due to its own nature[1]

Information security must also be carefully maintained and controlled. Information security is the protection of information from various threats to ensure continuity of operations, minimize business risks and maximize investment returns and business opportunities [2].

By using an international standard framework to guarantee 100% security protection, a set of benchmarks or guidelines is required to help maintain a sufficient level of protection for the corellational use of resources.

Customer satisfaction is one of the main outcomes measured. Customer satisfaction is the result of the goods and services of the business are equal to or greater than the requirements of the customer[3]. The degree of customer satisfaction can be calculated on the basis of five key factors to be regarded by a company, namely a) the product, customers are satisfied if the goods are reliable and durable. (b) Quality of service, customers are satisfied if the services provided are provided as planned, especially in the service sector.(c) Empathy emotionally, pride of consumers is preserved because of brand name and swift response is fulfilled when concerns and problems are identified. (d) Price, goods of the same quality but of a comparatively lower price would offer greater value to customers.[23] (e) Fees, customers do not have to pay installation or repair costs if there is an internet service disruption because it is included in the terms of the contract.

2. Literature Review

COBIT 5 offers a mechanism to ensure that the information technology used by businesses is in line with business needs. In addition, COBIT 5 is managed appropriately ensuring responsible managed appropriately use of information technology resources and ensuring information technology risks , so that information technology can support business properly and be able to maximize benefits provided. [5]. ITIL V3 is a compilation of best practices for handling IT services. ITIL V3 helps businesses to realize the value of their IT services to internal and external stakeholders. The ITIL safety management approach describes the establishment of formal protection in a management organization[7]. A variety of good practices, such as ITIL V3 and ISO/IEC 27001, can be used as a basis for developing a sound information security process[8].

The ISO/IEC 27001 standard specifies the requirements for the proper design and implementation of the Information security management system (ISMS) within the organization to ensure that appropriate and proportionate controls are chosen to protect the information assets and to provide trust to interested parties[9].The integration of best-practice security practices such as ISO/IEC 27001 into best-practice service management processes such as ITIL V3 helps organizations to mitigate overall costs in order to maintain an acceptable level of security, manage risk effectively and reduce overall risk[10].The ISO/IEC 27001 standard ISO/IEC 27001 is based on the Code of Practice released by the United Kingdom Department of Trade and Industry in 1989, which slowly became BS7799. ISO/IEC 27001 is a set of standards that can be used by organizations to create, deploy and maintain the Information Security Management System (ISMS)[2]. Based on a number of journals and the above definition, the novelty of research conducted by ITIL V3 researchers, Quota Broadband Internet, and customer satisfaction. The author has the initiative to analyze the basic concepts for the application of COBIT 5, ITIL V3 and ISO 27001 on 10002 customer satisfaction.

Al Faruq et al. said, IT organizations have adopted standards, i.e. ISO 2000 (Service management), ISO 9001 (Quality management system) and ISO 27001 (Quality management system) for information security have gained additional benefits such as customer satisfaction and confidence .[16]

In addition, Sahibudin et.al confirms that the combination of ITIL V3, Cobit and ISO/IEC 27002 is of benefit to the organization's objectives.[16] ITIL V3 will define procedures, plans and processes, COBIT 5 for metrics, benchmarks and audits, and ISO/IEC 27002 for resolving safety concerns relevant to risk reduction. [9]. In carrying out our research mapping COBIT 5 scope 6. Customer-oriented service culture applicable to ISO/IEC 27001: 2013 scope A.16 Information security incident management distance analysis ITIL V3 scope (Service operation 4.2 incident management) to figure 1.ITIL V3 .[4]

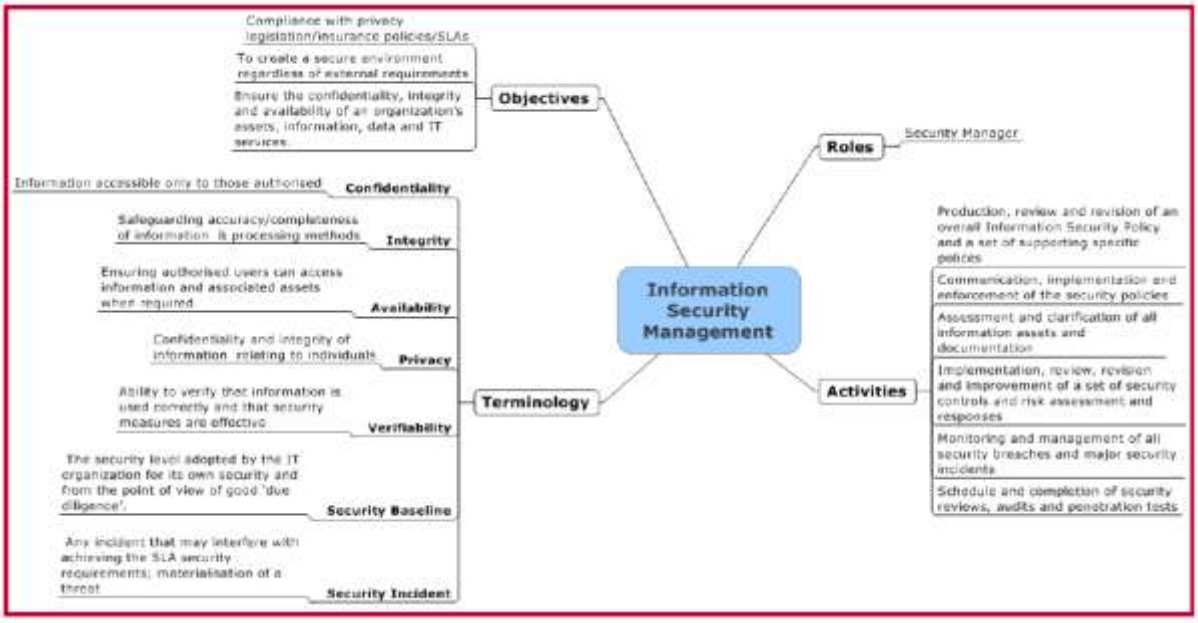

Figure 1. ITIL V3 Information security management

In carrying out our research mapping, we focus on the integration of the COBIT 5 link-up space structure (6. Customer-oriented service culture) as information technology governance in the management of RACI organizational structures and the introduction of the ITIL V3 framework-corellation domain-based activities for IT service management [6].

In the handling of internet disruptions within the framework of Service Operation 4.2 Incident management which has an impact on the achievement of international standards in ISO 27001 companies within the scope of A.16 Incident management to improve 3.4 Customer satisfaction with the implementation of ISO 10002. There are elements of innovation or results of this study in this study that differentiate the following methods from previous research:

Table 1. The difference between this study and other papers

No	Paper Tittle	Methods	Contribution novelty	Weaknesses
1	Marastika wicaksono aji bawono,Mohammad Amin Soetomo, Thata Apriatin, "Analysis The corellation of the Implementation of Cobit 5, ITILV3 and ISO 27001 for ISO 10002 Customer satisfaction"	(Structual equal modeling) SEM PLS 3.2.4 Professional. Quantitative Research Path analysis	determine the existence of a causal corellation due to implementing various best practice frameworks in the company	This data processing application SEM PLS will only get maximum results if we use a small data size, but it is not very suitable for research with large samples. Requires interviews with 5 in-depth respondents using random sampling to increase data accuracy that the results of the validity of the quantitative research method have answered all hypotheses

2	B. Al Faruq, H. R. Herlianto, S. H. Simbolon, D. N. Utama, and A. Wibowo, "Integration of ITIL V3, ISO 20000 & iso 27001:2013forit services and security management system," Int. J. Adv. Trends Comput. Sci. Eng., vol. 9, no. 3, pp. 3514–3531, 2020, doi: 10.30534/ijatcse/2020/157932020	**PDCA** (Plan,do,check,act) Qualitative Research	Companies adopt some framework intention to meet the international standards and certification will get more benefits such as improved standards	Research results depend on the ability and experience of the researcher. Possible changes in the behavior of the object of study Non-standard research procedures.r.

3. Method

For a quantitative approach, the study uses the causal associative method. Test was conducted on customers of the Company Quota Broadband Internet This location was chosen on the basis that the issue presented in the study included the company Quota Broadband Internet Period. This research was conducted between July and December 2020. Both customers of the Quota Broadband Internet Service were part of the population of this report. The sampling method used in this analysis is the technique of random sampling by simple random sampling. The research sample consisted of 135 external customers. The data collection technique shall be in the form of a questionnaire given to the customers of the Quota Broadband Internet Company. The questionnaire was based on a variety of observations and synthesized hypotheses, the questionnaire was based on a range of observations and synthesized hypotheses, conceptual principles, operational descriptions and a network of testing instruments. Study data analysis using SEM PLS version 3.2.4 Technical application tools.

4. Results and Discussion

Outer Models The results of research using SEM PLS version 3.2.4 Professional are shown in Figure 2 and 3 below:

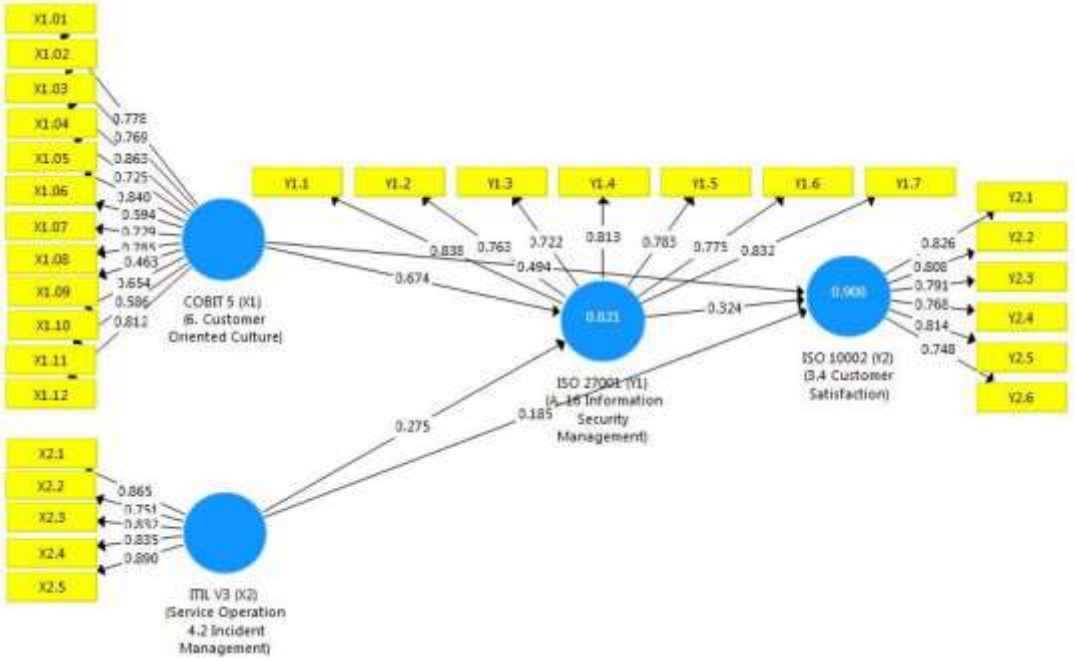

Figure 2. Initial outer models

In the initial outer model, classification is used to exclude data anomalies outside the structural and below the uniform figure that are not appropriate for testing in the study Outer loadings value shows the relationship between the indicator and its architecture [12].

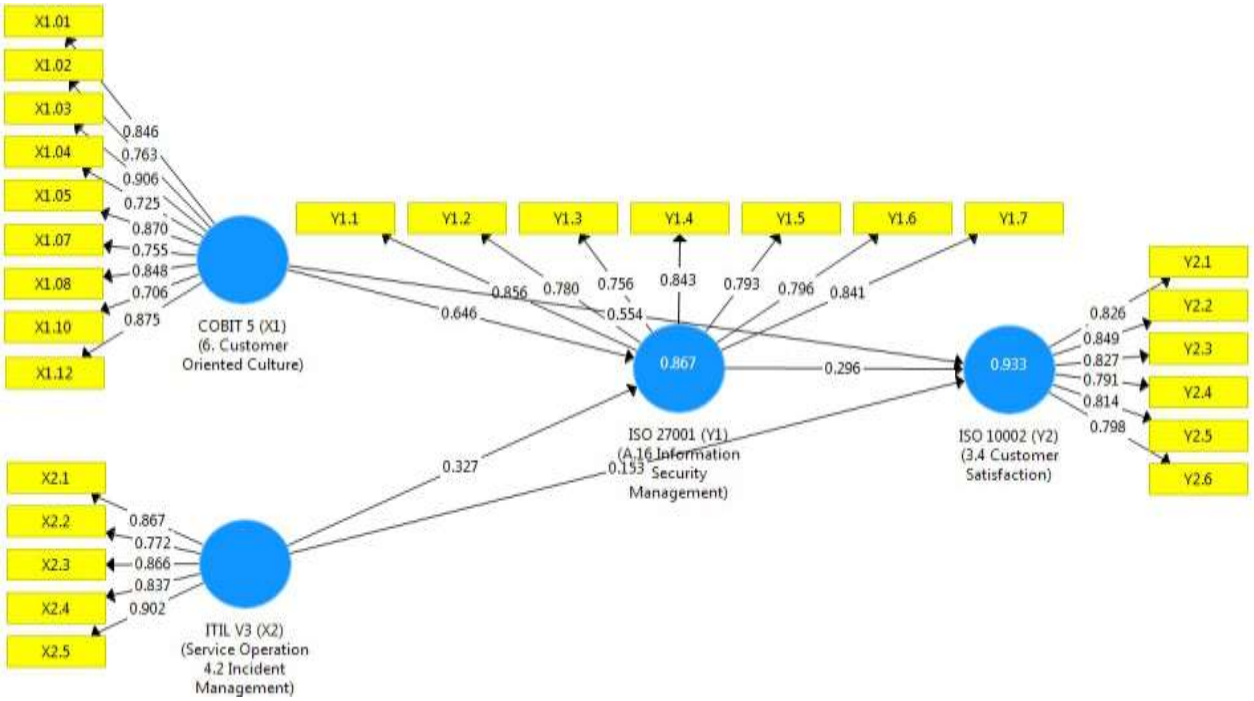

Figure 3. Final outer models

The low external load value indicator implies that the indicator does not function on the measurement model.[5] For each independent and dependent variable, the effects of the following initial external model are shown in the statement instrument:

Table 2. Framework statement instrument

Statement instrument **COBIT 5 (X1)**	**Statement instrument** **ITIL V3 (X2)**	**Statement instrument** **ISO 27001 (Y1)**	**Statement instrument** **ISO 10002 (Y2)**
Scope 6.Customer-oriented service culture	**Scope Service operation 4.2 incident management**	**Scope A.16 Information security incident management**	**Scope 3.4 Customer satisfaction**
X1.01.The Company is already aligning IT and business strategy	X2.1.The Company ensures that standard methods and procedures are used for efficient and fast response, analysis,documentation, and sustainability management and incident reporting	Y1.1.The Company control over responsibilities and management procedures must be established to ensure prompt, corellationive and regular information responses security incident.	Y2.1.Customers have a perception about the extent to which customer expectations have been met in the internet service received

X1.02.The Company conducts IT service delivery in line with the business requirements	X2.2.The Company increases visibility and communication incident to business and IT support staff	Y1.2. The Company control of the will Information security incidents should be reported through the appropriate channel management as quickly as possible.	Y2.2 Customer satisfaction has been fulfilled according to customer expectations contained in the performance report contract of the service leveel guarantee and service leve agreement
X1.03.Customers Realize the benefits of IT support investment portfolio and services	X2.3 The Company have a business perception of IT through use from a professional approach to finishing quickly and communicate incidents as they occur	Y1.3. The Company controls employees who use organizational information systems and services must record and report each observe or suspect information security weaknesses in the system or service.	Y2.3 The customer knows if there is maintenance of internet which can cause down time that has been calculated in the MTTR (Mean time to repair) for service interruptions
X1.04.The Company knows the importance of using the application, adequate information and technology solutions	X2.4 The Company synchronize incident management activities and priority with business	Y1.4.The Company control over Information security events have to be assessed and it must bedecide whether they will be classified as an information security incident.	Y2.4 The company and the customer carry out the provisions of the SLA (Service level agreement) and SLG (Service level guarantee) requirements which are expected to be 95% according to what has been agreed with the customer in order to meet a high level of customer satisfaction.
X1.05.The Company has IT agility solutions in the face of business competition	X2.5 The Company Maintain user satisfaction with the quality of IT services.	Y1.5 The company controls Information security incidents should be responded to accordingly with a documented procedure.	Y2.5 The company provides complaints via the care center for customers so that they can send complaints about interruption of internet services so that the handling of complaints is carried out openly and responsively
X1.06.The Company optimizes the empowerment of human resources for business support processes by integrating applications and technology into business processes		Y1.6 The company controls the knowledge and information data obtained to analyze and resolve information security incidents should be used to reduce the likelihood or impactuture incidents.	Y2.6 The company improves the competence of employees in each work unit in resolving complaints consistently, systematically, and responsive way
X1.07.The Company submits the RJPP program (the company's long-term plan) benefits, on time, within budget, and in meetings requirements and quality standards		Y1.7 The company establishes and implements procedures for identification,gathering, obtaining and preserving information,that can be evidence.	

X1.08.The Company has human resources who are competent and motivated IT personnel to support business processes			
X1.9 The company maintains an effective internal control system			
X1.10.Business partners control the information chain between them?			
X1.11.The Company provides Knowledge, expertise and initiativefor Employees to business innovation			
X1.12.The Company has an internal policy on IT services			

Table 3 Outer Loadings

Indicator	**Latent Variable**			
	COBIT 5 (X1) **6.Customer-oriented service culture**	**ITIL V3 (X2)** **Service operation** **4.2 incident management**	**ISO 27001 (Y1)** **A.16 Information security incident management**	**ISO 10002 (Y2)** **3.4 Customer satisfaction**
X1.01	0.846			
X1.02	0.763			
X1.03	0.906			
X1.04	0.725			
X1.05	0.87			
X1.07	0.755			
X1.08	0.848			
X1.10	0.706			
X1.12	0.875			
X2.1		0.867		
X2.2		0.772		

X2.3		0.866		
X2.4		0.837		
X2.5		0.902		
Y1.1			0.856	
Y1.2			0.780	
Y1.3			0.756	
Y1.4			0.843	
Y1.5			0.793	
Y1.6			0.796	
Y1.7			0.841	
Y2.1				0.826
Y2.2				0.849
Y2.3				0.827
Y2.4				0.791
Y2.5				0.814
Y2.6				0.798

The analysis uses a standard external load weight of 0.7. The findings indicate that all external load values are >0.7 for each predictor.[15] In most sources, a factor weight of 0.70 or more is believed to have been fairly well validated to describe latent constructions. Higher external load indicators have a higher contribution to describe latent construction. On the other hand, indicators with low external loads have a poor contribution to defining their latent (valid) construction. The AVE value must be higher (>0.5). [7]

Table 4 Average variance extracted (AVE)

Latent Variable	***Average Variance Extracted*** **(AVE)**
COBIT 5 (X1) (6. Customer-oriented service culture)	0.662
ITIL V3 (X2) (Service operation 4.2 Incident management)	0.722
ISO 27001 (Y1) (A.16 Information security incident management)	0.656
ISO 10002 (Y2) (3.4 customer satisfaction)	0.668

Based on the above table, it is shown that the value of AVE COBIT 5 (X1) (6.Customer-oriented service culture value is 0.662. AVE ITIL V3 (X2) (Service operation 4.2 incident management) is 0.722. AVE ISO 27001 (Y1) A.16 incident management value of 0.656. ISO 10002 (Y2) AVE price (3.4 Customer satisfaction is 0.668). This is the result of the Convergence Test Validity Study of the Average Variance Extract (AVE) value > 0.5. [22]

Discriminant validity refers to the degree of variance between the non-calculated characteristics of the measurement system and the theoretical principles of the variable. Discriminant Validity of the reflexive measurement model can be determined on the basis of the Fornell Larcker criterion value and the cross-loading value of the manifest variable for each latent variable. The criterion for the value of the Fornell Larcker criterion must be greater than the AVE value of each latent variable, the criterion for the Fornell Larcker criterion must be greater than the AVE value of each latent variable, which means that the degree of mismatch between attributes which should not be calculated by the measuring instrument is small, so that the discriminant value is included in the criterion.

Table 5 Fornell larcker criterion

Latent Variable	**COBIT 5 (X1) 6.Customer-oriented service culture**	**ISO 27001 (Y1) A.16 Information security incident management**	**ITIL V3 (X2) Service operation 4.2 incident management**	**ISO 10002 (Y2) 3.4 Customer satisfaction**
COBIT 5 (X1) 6.Customer-oriented service culture	0.814			
ISO 27001 (Y1) A.16 Information security incident management	0.911	0.810		
ITIL V3 (X2) Service Operation 4.2 Incident management	0.811	0.851	0.850	
ISO 10002 (Y2) 3.4 customer satisfaction	0.949	0.932	0.855	0.818

The table above shows that the value of the latent variable association between COBIT 5 (X1) (6.Customer-oriented service culture) is 0.814 higher than the AVE value of 0.662. ITIL V3 (X2) (Service operation 4.2 incident management) of 0.850 is higher than the AVE of 0.722. The value of 0.81 ISO 27001 (Y1) is greater than the value of 0.656 AVE. ISO 10002 (Y2) 3.4 The customer satisfaction value of 0.818 is higher than the AVE value of 0668 (ISO 10002 3.4). The above table shows that the value of the latent variable relation between Cobit 5 (X1) (6.Customer-oriented service culture) is 0.814 higher than the AVE value of 0.662. ITIL V3 (X2) (Service operation 4.2 incident management) is 0.850 higher than the AVE of 0.722.The value of 0.81 ISO 27001 (Y1) is greater than the value of 0.656 AVE. (Y2) 0.818 is greater than the value of 0.668 ISO 10002 (Y2) (3.4 customer satisfaction). Criteria for the importance of cross-loading, that is, if the value

of the correlation between the latent variable and one of its indicators (manifest variable) is greater than the value of the correlation with other latent variables, then the latent variable may be said to predict the indicator better than other latent variables [15].

Table 6 Cross Loadings

Indikator	Latent Variable			
	COBIT 5 (X1) **6.Customer-oriented service culture**	**ITIL V3 (X2)** **Service operation 4.2 oncident management**	**ISO 27001 (Y1)** **A.16 Information security incident management**	**ISO 10002 (Y2)** **3.4 Customer satisfaction**
X1.01	0.846	0.620	0.728	0.794
X1.02	0.763	0.647	0.696	0.671
X1.03	0.906	0.639	0.777	0.843
X1.04	0.725	0.710	0.703	0.669
X1.05	0.870	0.553	0.721	0.808
X1.07	0.755	0.685	0.737	0.745
X1.08	0.848	0.577	0.756	0.796
X1.10	0.706	0.923	0.756	0.758
X1.12	0.875	0.598	0.784	0.831
X2.1	0.642	0.867	0.641	0.691
X2.2	0.680	0.772	0.742	0.729
X2.3	0.722	0.866	0.737	0.738
X2.4	0.712	0.837	0.702	0.748
X2.5	0.681	0.902	0.779	0.718
Y1.1	0.682	0.743	0.856	0.714
Y1.2	0.715	0.731	0.780	0.740
Y1.3	0.818	0.576	0.756	0.786
Y1.4	0.664	0.755	0.843	0.681
Y1.5	0.719	0.721	0.793	0.759
Y1.6	0.831	0.589	0.796	0.846
Y1.7	0.708	0.719	0.841	0.730
Y2.1	0.726	0.740	0.776	0.826
Y2.2	0.802	0.680	0.748	0.849
Y2.3	0.802	0.591	0.799	0.827
Y2.4	0.749	0.862	0.753	0.791
Y2.5	0.759	0.745	0.770	0.814

Y2.6	0.813	0.574	0.723	0.798

Based on the above table, it can be seen that the COBIT 5 (X1) (6. Customer-oriented service culture) of the predictor is greater than the value of other latent variables. Latent values of ITIL V3 (X2) (Service operation 4.2 incident management), ISO 27001 (Y1) (A.16 Information security incident management) for ISO 10002 (Y2) (3.4 Customer satisfaction).
The reliability test consists of the composite reliability test and the Cronbach alpha test used to test the reliability value of the variable indicators. A variable can be declared to be met if it has a composite reliability and an alpha value of >0.7 Cronbach [8].

Table 7. Composite Reliability and Cronboach's Alfa

Latent Variable	***Composite Reliability***	***Cronbach's Alpha***
COBIT 5 (X1) 6. Customer-oriented service culture	0.946	0.935
ITIL V3 Service operation (X2) 4.2 Incident management	0.928	0.903
ISO 27001 (Y1) A.16 Information security incident management	0.930	0.912
ISO 10002 (Y2) 3.4 customer satisfaction	0.924	0.901

Based on the above table, it is shown that the composite reliability and the Cronbach alpha value of all study variables are >0.7.[5] These results indicate that each variable met the composite reliability and the Cronbach alpha, so that it can be concluded that all variables have a high degree of reliability.
Internal model evaluation is a structural model assessment consisting of the path coefficient, the R-square T-statistic (bootstropping), predictive significance, and model fit.[23] The path coefficient assessment is used to denote the intensity of the association or effect of the independent variable on the dependent variable.

Table 8. Path Coefficient

Latent Variable	***Path Coefficients***
COBIT 5 (X1) (Customer-oriented service culture) to ISO 10002 (Y2) (3.4 customer satisfaction)	0.554
ITIL V3 (X2) (Service Operation 4.2 Incident management) to ISO 10002 (Y2) (3.4 customer satisfaction)	0.153
ISO 27001 (Y1) (A.16 Information security incident management) to ISO 10002 (Y2) (3.4 customer satisfaction)	0.296
COBIT 5 (X1) (6.Customer-Oriented service cultutre) to ISO 27001 (Y1) (A.16 Information security incident management)	0.646
ITIL V3 (X1) (Service Operation 4.2 Incident management) to ISO 27001 (Y1) (A.16 Information security incident management)	0.327

Based on the above table, it is shown that the greatest coefficient of direction for the correlation of COBIT 5 (X1) (6. Customer-oriented service culture) on ISO 27001 (Y1) (A.16 information security incident management) is 0.646.
The second big correlation is COBIT 5 (X1) (6. Customer-oriented service culture) for ISO 10002 (Y2) (3.4 Customer satisfaction) of 0.554. The third big effect is ITIL V3 (X2) (Service operation 4.2 incident management) on ISO 27001 (Y1) (A.16 Information security incident management) of 0.327. The fourth largest association is ISO 27001 (Y1) A.16 Information security incident management for ISO 10002 (Y2) (3.4 Customer satisfaction) of 0.296.The fifth highest effect is ITIL V3 (X2) (Service operation 4.2 incident management) for ISO 10002 (Y2) 3.4 customer satisfaction) of 0.153.
Based on the interpretation of these correlations, it is shown that all variables in this model have a positive path coefficient. This shows that if the value of the path coefficient is greater on one independent variable on the dependent variable, the stronger the correlation on the dependent variable will be between the independent variables.
Coefficient determination (R-Square) is used to measure how much endogenous variables are affected by other variables. The R-Square result of 0.67 and above indicates that the endogenous latent variables in the structural model indicate the effect of the exogenous variables (which influence) on the endogenous variables (which are affected) in the good community. In the meantime if the result is 0.33-0.67, it is in the medium-sized group and if the result is 0.19-0.33, it is in the weak category[1].
On the basis of the data processing carried out using SEM PLS 3.2.4 Professional[12], the R Square value is obtained as follows:

Table 9. R-Square

Latent Variable	R Square	R Square Adjusted
ISO 27001 (Y1) (A.16 Information security incident management)	0.867	0.865
ISO 10002 (Y2) (3.4 customer satisfaction)	0.933	0.931

The R-Square value of the ISO 10002 3.4 Customer satisfaction (Y2) variable of 0.867 is included in the Positive category The acquisition of this value explains that the percentage of ISO 27001 (Y1) (A.16 Information security incident management) can be explained by COBIT 5 (X1) (6.Customer-oriented service culture) and ITIL V3 (X2) (Service operation 4.2 incident management) of 86.7%.The remaining 13.3 per cent is influenced by variables other than COBIT 5 (6.Customer-oriented service culture) (X1) and ITIL V3 (Service operation 4.2 incident management) (X2).
The square value of the 0.933 vector (Y2) is included in the right group. The acquisition of this ISO 10002 3.4 customer satisfaction indicates that the percentage of Customer satisfaction (Y2) can be defined by COBIT 5 (6. Customer-oriented service culture) (X1), ITIL V3 (Service operation 4.2 incident management) (X2) and ISO 27001 (A.16 Information security incident management) (Y1) by 93.3 %.
The remaining 6.7% were affected by variables outside COBIT 5 (X1) (6. Customer-oriented service culture ITIL V3 (X2) (Service operation 4.2 incident management) and ISO 10002 (Y2) (3.4 Customer satisfaction). Hypothesis tests by looking at the value of T-Statistics and P-Values The study hypothesis may be described as agreed if the value of P-Values is <0.05[12].

Table 10. T-Statistics and P-Values

Latent Variable	*T-Statistic*	*P-Values*
COBIT 5 (X1) (6.Customer-Oriented service culture) To ISO 10002 (Y2) (3.4 customer satisfaction)	5.091	0.000
ITIL V3 (X2)(Service Operation 4.2 Incident management) to ISO 10002 (Y2) (3.4 customer satisfaction)	2.648	0.008
ISO 27001 (Y1) to ISO 10002 (Y2) (3.4 customer satisfaction)	2.733	0.006
COBIT 5 (X1) (6.Customer-Oriented service value) to ISO 10002 (Y2) (3.4 customer satisfaction)	6.960	0.000
ITIL V3 (X2) (Service Operation 4.2 Incident management) to ISO 10002 (Y2) (3.4 customer satisfaction)	3.260	0.001

Based on the above table, it is shown that the correlation of COBIT 5 (X1) (6.Customer-oriented service culture) to ISO 10002 (Y2) (3.4 customer satisfaction) with a T-Statistic value of 5.091> T-Table value of 1.969 (ш=0.05) and a P-Value of 0.000=0.05.
There is therefore a strong and important link between COBIT 5 (X1) (6.Customer-oriented service culture) and ISO 10002 (Y2) (3.4 Customer satisfaction).
This means that the better COBIT 5 is applied, the better the customer's satisfaction. Corellation of ITIL V3 (X2) (Service Operation 4.2 Event Management) to ISO 10002 (Y2) 3.4 Customer satisfaction with a T-Statistic value of 2.648> T-Table value of 1.969 (5-007=0.05) and a P-Value value of 0.008=0.05. There is also a strong and important link between ITIL V3 (X2) (Service Operation 4.2 Incident Management) and ISO 10002 (Y1) (3.4 Customer Satisfaction). This means that the better ITIL V3 (X2) (Service operation 4.2 Incident management) is applied, the better Customer satisfaction is achieved.
Corellation of ISO 27001 (Y1) (A.16 Information Security Incident Management) to ISO 10002 (Y2) (3.4 Customer Satisfaction) with a T-Statistic value of 2.733> T-Table value of 1.969 (ш=0.05) and a P-value of 0.006 <ш=0.05.There is a positve and significant corellation of ISO 27001 and customer satisfaction. That means that the better ISO 27001, the better ISO 10002 (Y2) (3.4 customer satisfaction). corellation of COBIT 5 (X1) (6.Customer-oriented service culture) to ISO 27001 (Y1) (A.16 Information security incident management) with T-Statistic value of 6,960> T-Table value of 1,969 (ш=0,05) and P-Value of 0.000<ш=0,05.
There is a positve and significant corellation of of COBIT 5 (X1) (6.Customer-oriented service value) for ISO 27001 (Y2) (A.16 Information security incident management) This means that the better COBIT 5 (6.Customer-oriented service value) is applied, the better ISO 27001 (Y2) (A.16 Information security incident management is applied. The correlation of ITIL V3 (X2) (Service operation 4.2 incident management) on ISO 27001 (Y1) (A.16 Information security incident management) with a T-Statistic value of 3.260> a T-Table value of 1.969 (ш=0.05) and a P-value of 0.001 <ш=0.05.
There is a positive and significant corellation of ITIL V3 (X2) (Service operation 4.2 incident management) and ISO 27001 (Y1) (A.16 Information security incident management). This means

that the better ITIL V3 (X2) (Service opeartion 4.2 incident management) is applied, the better ISO 27001 is applied. The five hypotheses suggested in this analysis are therefore accepted. This is because each of the corellations shown has a T-Statistic value > a T-Table value of 1,969 (ш=0,05) and a P-Table value of <0,05. So that it can be claimed that exogenous variables on endogenous variables have a positive and meaningful correlation.
The largest effect is COBIT 5 (X2) (6.Customer-oriented service value) on ISO 27001 (Y1) (A.16 Information security incident management) with a T statistic of 6.960 and a P value of 0.000.
The structural model of the T-Statistic results is shown in Figure 3 below:

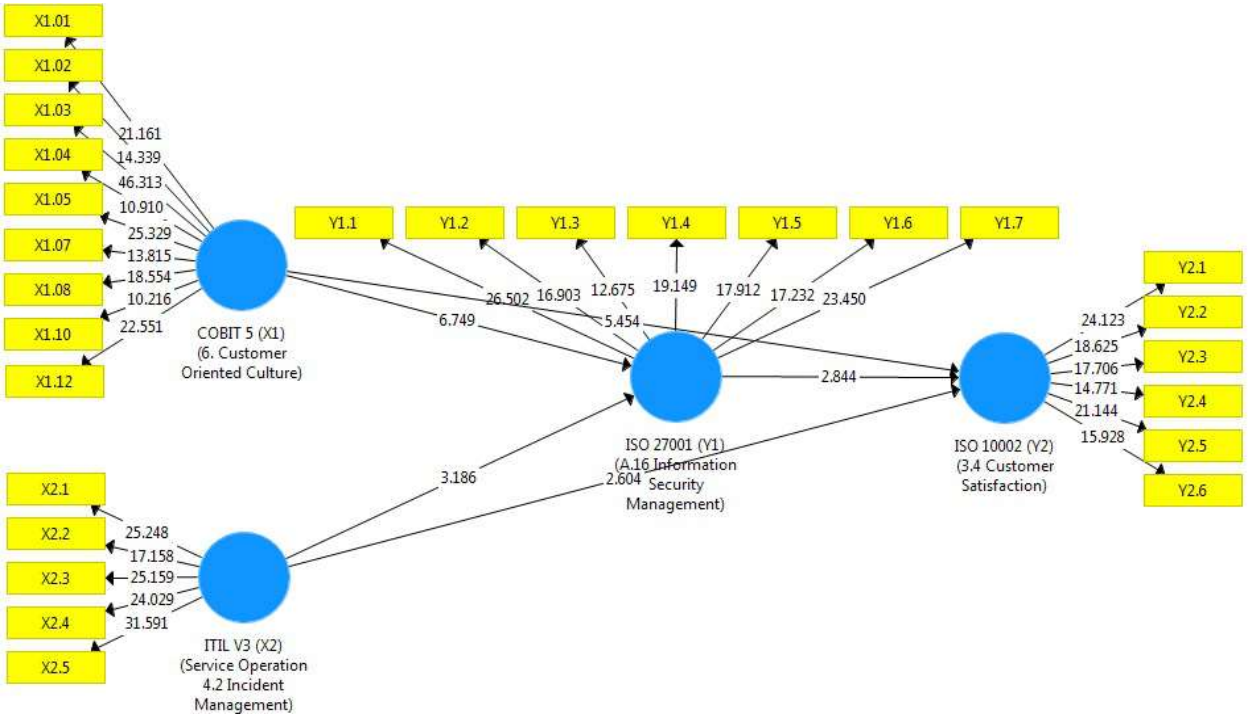

Figure 4. *T-Statistic*

The PLS model was evaluated by looking at the statistical significance (Q-square) of the constructive model.[10] The objective of the Q-square is to measure how well the observed value is generated by the model and also by estimating its parameters [19]. Measurement parameters are sure, if the results of the measurement suggest that the Q-square value is more than 0 (zero), then the model must be said to have the required predictive value. In the meantime, if the Q-square value is less than 0 (zero) it means that the model lacks predictive relevance. The Q-square equation results are as follows:

Table 11. T-Statistics and P-Values

Latent Variable	**Q Square**
ISO 27001 (Y1) (A.16 Information security incident management)	0.526
ISO 10002 (Y2) (3.4 customer satisfaction)	0.578

The table above shows that the Q-square value of ISO 27001 (Y1) is 0.526. The Q-square value of ISO 10002 (Y2) (3.4 customer satisfaction) is 0.578. The results of the calculation show that the Q-square value is more than 0 (zero), so the model deserves to be said to have a good observation value or the model

deserves to be said to have a relevant predictive value. The Model Goodness Test (Model Fit) uses the Standard Fit Index (NFI) which is a measure of the suitability of the model on a baseline or zero basis. The null model is typically a model that indicates that the variables used in the projected model are not intercorellations .[16]

Table 12. Model Fit

Model Fit	**Nomed Fix Index (NFI)**
Saturated Model	0.418

5. Conclusion

Based on the results of the above measurements, the value of the Nomed Fix Index (NFI) on the Saturated Model is 0.418.[9] The study model analyzed was 41.8%in the fit or good category .[21] The results of the research findings suggest that there is a positive and significant correlation the application of COBIT 5 (X1) (6.Customer-oriented service culture), ITIL V3 (X2) (Service operation 4.2 incident management) and ISO 27001 (Y1) (A.16 Information security incident management) to ISO 10002 (Y2) (3.4 Customer satisfaction) [18] .This is consistent with the research results which show that ITIL and ISO/IEC 27001 systems can be used together as a basis for the development of a sound information security process. Both ITIL and ISO 27001 describe safety requirements for all aspects of infrastructure risk management services [13]. The system promotes management views that encourage and define services offered, manage user roles, manage tickets and generate management reports[9].

The value of government information technology (ITG) should use the latest method of ITIL V3 (Service operation 4.2 incident management) COBIT5 (X1) (6. Customer-oriented service culture) with ISO/IEC 27002 for effective use of ITG in the Moroccan Parliament.[17] ITIL V3, COBIT 5 with ISO/IEC 27002 as a set of organizations with legislative obligations, government control, public policy assessment, parliamentary diplomacy and the strengthening of parliamentary relations with constitutional institutions, good governance, advanced regional conferences, civil society and citizens[15]. Researchers would like to thank the leadership and the staff and customers of Quota Broadband Internet Company who have given permission to provide moral assistance in carrying out this report .[20]

6. References

[1] A. Jaschob and L. Tsintsifa, “IT-Grundschutz: Two-Tier risk assessment for a higher efficiency in IT security management. ISSE 2006- Secur Electro Bus Process”, Inform. Secur. Solut. Eur. Conf. Rome, Italy. pp: 95-101, 2006.

[2] A. Rezakhani, A. Hajebi, and N. Mohammadi, “Standardization of all information security management systems”, International Journal of Computer Applications,(8), pp.4-8. 2011.

[3] B. Al Faruq, H. R. Herlianto, S. H. Simbolon, D. N. Utama, and A. Wibowo, “Integration of ITIL V3, ISO 20000 & iso 27001:2013forit services and security management system,” Int. J. Adv. Trends Comput. Sci. Eng., vol. 9, no. 3, pp. 3514–3531, 2020, doi: 10.30534/ijatcse/2020/157932020.

[4] B. M. Practice, ITIL Service Operation. 2011.

[5] B. Niehaves and K. Ortbach, “The inner and the outer model in explanatory design theory: The case of designing electronic feedback systems,” Eur. J. Inf. Syst., vol. 25, no. 4, pp. 303–316, 2016, doi: 10.1057/ejis.2016.3.

[6] “BS ISO 10002 : 2018 BSI Standards Publication Quality management — Customer satisfaction — Guidelines for complaints handling in organizations,” 2018.

[7] D. Dragan and D. Topolšek, “Introduction to Structural Equation Modeling : Review , Methodology and Practical Applications,” no. June, 2014.

[8] E. R. Larrocha, J. M. Minguet, G. Díaz, M. Castro and A.Vara, “Filling the gap of Information Security Management inside ITIL: proposals for postgraduate students”, IEEE EDUCON Edu. Engg. pp: 907-912, 2010.

[9] F. Al-Hawari and H. Barham, “A machine learning based help desk system for IT service management, Journal of King Saud University – Computer and Information Sciences, pp. 1-17, 2019.

[10] Fornell and D. F. Larcker, “Evaluating structural equation models with unobservable variables and measurement error,” Journal of marketing research, pp. 39-50, 1981.

[11] G. W. Cheung and R. B. Rensvold, “Structural Equation Modeling : A Evaluating Goodness-of- Fit Indexes for Testing Measurement Invariance,” no. July 2012, pp. 37–41, 2009.

[12] I. Ghozali, Structural Equation Modeling - Alternative Method with Partial Least Squares (PLS). Semarang: Universitas Diponegoro, p. 39, 2014.

[13] ISACA, "cobit 2019 5: A business framework for the governance and management of enterprise IT", Isaca, 2012.

[14] J. F. Hair, M. Sarstedt, C. M. Ringle, and J. A. Mena, "An assessment of the use of partial least squares structural equation modeling in marketing research," pp. 414–433, 2012, doi: 10.1007/s11747-011-0261-6.

[15] J. Henseler and W. W. Chin, "Structural Equation Modeling : A A Comparison of Approaches for the Analysis of Interaction Effects Between Latent Variables Using Partial Least Squares Path Modeling," no. August 2013, pp. 37–41, doi: 10.1080/10705510903439003.

[16] K. V. Warre, "Security controls in service management. SANS Institute reading room", 2010. from http://www.sans.org/search/results.

[17] M. Motii, and A. Semma, "Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament", IJCSI International Journal of Computer Science Issues, Volume 14, Issue 3, pp. 49-58, May 2017.

[18] K.L. Thomson, and R.V. Solms , "Information Security governance: COBIT or ISO 17799 or both?", J. Comput. Secur. 24, pp. 99-104, February 2005.

[19] Riadi, E., 2018. Statistik SEM structural equation modeling dengan Lisrel. Yogyakarta: CV Andi Offset.

[20] R. Sheikhpour, and N. Modiri, "A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management", Indian journal of science and technology, 5(2), pp.2170-2176, 2012.

[21] S. Sahibudin, M. Sharifi, and M. Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations," Proc. - 2nd Asia Int. Conf. Model. Simulation, AMS 2008, pp. 749–753, 2008, doi: 10.1109/AMS.2008.145.

[22] T. Pereira, and H. Santos, "A security audit framework to manage Information system security. In International Conference on Global Security, Safety, and Sustainability," Springer, Berlin, Heidelberg, pp. 9-18, September 2010.

[23] S. Yamin dan H. Kurniawan, The New Generation Processes Research Data with Partial Least Square Path Modeling. Jakarta: Salemba Empat, p. 54, 2011.

[24] W. Boehmer, "Appraisal of the corellationiveness and efficiency of an Information Security Management System based on ISO 27001". Proc. Second Int. Conf. Emerging Security Information, Sys. & Technolos. Yogyakarta: Ekonisia, 2005.gies. pp: 224-231, 2008.

[25] V. Grover, M. J. Cheon, and J. T. C. Teng, "of Service Quality and The Effect of on the Outsourcing Partnership Functions Information Systems," vol. 12, no. 4, pp. 89–116, 2015.

[26] V. Rangan, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements," vol. 2013, 2013.

Identification of Positive Clandestine Intelligence Threats In Cyber Terrorism For National Security

Yudha Fernando[1], Mohammad Amin Soetomo[2]

[1]Sekolah Tinggi Intelijen Negara, Bogor, Indonesia, [2]Swiss German University, Tangerang 15143, Indonesia

Article Information

Received:

Accepted:

Published:

DOI: 10.33555/ejaict.v…

Corresponding Author:

Mohammad Soetomo

Email: mohammad.soetomo@sgu.ac.id

ISSN 2355-1771

ABSTRACT

This study is motivated by the vigilance towards the development of cyberspace technology that is so fast that it causes dependence on it in almost all fields. This condition poses a potential threat to our national resilience in various fields, especially in the national security sector. Researchers try to identify the threat of Positive Clandestin Intelligence (PCI) in the form of cyber terrorism on national security, so that it can bring stakeholders to a better level of knowledge. Theories and concepts used are related to threats, national security, positive clandestine intelligence, terrorism and cyber terrorism (CT). This study is a qualitative method and the type of research is descriptive qualitative. Interview and literature review are used in primary and secondary data collection. Data is evaluated and analyzed with an interactive analysis model. Researchers also validate by measuring the degree of accuracy between the data that occurs in the object of research with data that can be reported by researchers. This study succeeded in identifying the types of PCI CT targets, forms of PCI CT attacks, psychological motivations of PCI CT perpetrators and the position of PCI CT threats in the taxonomy of Rogers M.K.'s cybercrime behavior.

Keywords: *Cyber Terrorism, Nasional Ressiliance, Terrorism, Positive Clandestine Intelligence, PCI*

1. Introduction

Discussions on national security threats that are created in cyber space is something that cannot be avoided for parties dealing with issues of national security. This study tries to provide a picture in the form of identification related to the threat of cyber terrorism from the perspective of national security intelligence. The results of this study are expected to provide vigilance related to cyber terrorism as a PCI for stakeholders in the field of national security, particularly intelligence related to national security. In Article 1 paragraph 1, Law no.17/2011, mentioned that intelligence is knowledge, organization, and activities related to policy formulation, national strategies, and decisions based on the analysis of the information and facts gathered through working methods for the detection and early warning in the context of prevention, deterrence, and response to any threats to national security.[6]

In the era of industrial revolution 4.0 today, a threat to national security has found new forms, including threats of positive manifold PCI. Conceptually, PCI has various forms, one of which is terror, the activity by the opposing agent with the negative intentions. The method has been successfully dialectic of terror with their external environment in order to create fear.[3] Dynamic development of technology and globalization cannot avoid and become supporting factors for the existence of this terror threat; the terror threat in question is the threat of terror in cyberspace or cyber terrorism.[1]

Below what PCI, terorism definition, threats according to Indonesian law, roles of intelligence in national security, and how cyber techniques formed and developed for terrorism acts are reviewed.

1.1. PCI

Intelligence in a country is defined in three appearances, namely appearance as an organization, appearance as an activity, and appearance as knowledge.[12] Intelligence as an activity means a closed activity, either in the form of clandestine activities or covert action; these activities include activities that are routine in nature and intelligence operations that are temporary and time-limited.[9][11] The output of intelligence activities is called PCI, which can take the form of espionage, propaganda, social conflict or terror [12].

1.2. Terrorism

Whittaker, citing several definitions of terrorism, including Walter Reich who stated that terrorism is a strategy of violence designed to promote desired outcomes by instilling fear in the public at large. Terrorism is the use or threat of using violence, which aims to achieve political change.[2]

1.3. Threat

Law no.17/2011 of National Intelligence states that a threat is any effort, job, activity and action, both from within the country and abroad, which are assessed and/or proven to endanger the safety of the nation, security, sovereignty, territorial integrity of the Unitary State of the Republic of Indonesia, and national interests in various aspects whether ideological, political, economic, socio-cultural, or defense and security.[6] A threat is a thing, a situation, an event, an action that can endanger, complicate, disturb, cause pain, harm, etc.[3]

Basically, threats have goals and interests, namely as follows:

1) State: the threat interests are the sovereignty and independence of the state and territorial integrity.
2) Nation: the threat interest is national unity and the noble values of the nation.
3) Government: the interests of the threat are government policies and actions and government legitimacy.
4) Society: the interest of the threat is the life of the community and the interests of the community groups.
5) Individual: the threat is the security of one's soul and family and assets.[13]

1.4. National Security

As part of the national security system, intelligence acts as an early warning system and a strategic system to prevent strategic incidents that threaten national security.[12] National security is generally defined as a basic need to protect and safeguard the national interests of a nation which states by using political, economic and military power to face various threats both from outside and from within the country; national security can also be interpreted as a condition that is national in nature and describes the freedom of the state, society, and citizens from all forms of threats and/or actions, whether influenced by external or internal factors; and national security is defined as a basic need to protect and safeguard the national interest of a nation by using political, military and economic power to face threats both from within and outside the country.[10] This view supports the argument that national security in a democratic country generally includes state security, public security and human security.

1.5. Cyber Terrorism

Cyber craft can be defined as any type of intelligence activity that uses telematics technology as the media; the forms of cyber craft range from propaganda in the form of defamation through social media, hoax, hate speech to 'high tech' such as cyber terrorism by using dos attach, malware and ransomware.[4][8]

The definition of cyber terrorism can be defined as the use of computer network techniques to make the main infrastructure of a computer network malfunctioning, with the aim of intimidating or coercing the government and community groups.[2] Meanwhile, the main infrastructure for computer networks is

systems and assets which, if destroyed, will have an impact on infrastructure security, economic security and the security of the public health system; this includes the energy industry, food, transportation, banking, communications, government and cyberspace itself.[2][4] The perpetrators of cyber terrorism can be state actors (SA) and nonstate actors (NSA).[8] It depends on the motivation of the intelligence organization user who uses PCI cyber terrorism as an intelligence activity in cyberspace.

This study attempts to identify the shape, type and psychological motivations of terrorists, so that it can be input for the country's national security system in finding a solution.

2. Methods

This is a qualitative study. The study used a qualitative approach. The qualitative approach chose, because this study aims to identify the threat of PCI cyber terrorism to national security through social phenomena, that occur from the subject's point of view, where the researcher is the key instrument.

This qualitative research process involves important efforts, such as asking questions and procedures, gathering specific data from informants, inductively analyzing data ranging from specific themes to general themes, and interpreting the meaning of the data.[5] The qualitative approach was considered by researchers as appropriate to identify the threat of PCI cyber terrorism to national security as a social phenomenon that tends to be described in descriptions in the form of words rather than numbers.

The research method used is a qualitative description method by studying the forms of PCI cyber terrorism threats to national security. Qualitative descriptive research seeks to describe, record, analyze and interpret the forms of PCI cyber terrorism threat to national security. In other words, this study aims to obtain information about the existing situation. This descriptive research uses a case study model, where the researcher tries to identify the form of PCI cyber terrorism threat to national security. The final report for this study has a flexible structure or framework. Anyone involved in this form of research must apply an inductive research perspective, focus on individual meanings, and translate the complexity of a problem [14].

2.1. Data Validation

This study uses triangulation techniques in the data validation stage. Triangulation technique is checking data by matching it with something outside the data for comparison; triangulation techniques are carried out through interviews, direct observation and indirect observation [5][14].

2.2. Data Collecting Method

The main data sources obtained by researchers in this study are words, actions and additional data such as other documents. This study uses data collection techniques to obtain primary and additional data sources.[14] The types of data obtained in this data collection consist of primary data and secondary data. Primary data were obtained through in-depth interviews with informants (practitioners, academics and researchers); meanwhile, secondary data obtained from observation and study of documents related to the research objectives [5].

2.3. Data Evaluation

Evaluating information is an integral step in the analysis process, and in general, evaluation is carried out when the information is obtained. Data is evaluated according to the level of confidence in the data source as well as the accuracy of the actual information.[14] When evaluating information, analysts ask questions such as:

1) What is the level of trust in information sources?
2) Has the source of information supported by the previous information?
3) How accurate is this information?
4) How is that information status at this point?

The evaluation process is needed, because deception is something that is commonly encountered in the intelligence world. To create levels or levels of information, analysts can use information accuracy codes and information reliability codes.[9]

3. Result & Discussion

This study succeeded in collecting primary data and secondary data to be used as material for further analysis.[5][14] The primary data that the researchers succeeded in obtaining came from in-depth interviews with intelligence researchers, academics and intelligence practitioners. In order to increase the quality of the analysis results, researchers also collected secondary data using observation techniques and document study. The primary and secondary data are then evaluated according to the level of confidence and accuracy of the actual information. The evaluated data is then reduced by summarizing, selecting main points, focusing on important things related to the identification of the threat of PCI in the form of cyber terrorism against national security.

Primary data obtained from interviews with intelligence practitioners (resource person A) explained that intelligence activities in the form of PCI cyber terrorism have indeed occurred in Indonesia. This can be seen from the wannaCry virus incident which attacked a number of hospitals in 2017. The attack is classified as cyber terrorism using the Ransomware method. In addition to these examples, the resource person also added several examples of cyber terrorism attacks such as cyber terrorism attacks on the General Election Commission (KPU) servers in 2004 and 2005. The form of cyber terrorism attacks in 2004 took the form of defacing the display of the national tabulation page of the KPU's voting results. Meanwhile, the form of cyber terrorism attack in 2005 was in the form of KPU takedown server, so that the internet network at the KPU national tabulation center could not function. According to the informant, the objectives of cyber terrorism (CT) attacks are divided into three types of attacks, namely data confidentiality, data integrity and finally data availability.

The next primary data, researchers obtained from the results of in-depth interviews with terrorism lecturers at the State Intelligence College (STIN), DR. Supriyadi, SE., M.Si. In the in-depth interview, he explained that the form, form of cyber terrorism attack can be in the form of a virus outbreak, which is a virus attack that enters our computers; Spam mail/mailbomb is an attack that usually occurs in someone's email sent by irresponsible people; Dos Attack is an attack that can paralyze a person's computer system if they are sent a dos attack; Unauthorized Access is an infiltration of our computers without our knowledge and without our permission.

Primary data for the three researchers obtained from interviews with the Executive Director of the Center of Intelligence and Strategic Studies, DR (Candidate) Ngasiman Djoyonegoro. According to him, the phenomenon of cyber terrorism is in accordance with one of the books he wrote, namely Intelligence in the Digital Age. Terrorism attacks are no longer conventional, but will use cyber media. This is related to the increasing difficulty of the terrorist movement in carrying out conventional threats.

In addition to the primary data, the researchers also succeeded in obtaining secondary data with engineering studies documents. Researchers obtained data in the form of the Taxonomic Continuum of cybercriminals ranging from new people (novice) and amateurs in the form of ordinary delinquency to major acts of terrorism. This taxonomy researcher got from the book The Psyche of Cybercriminals: A Psycho-Social Perspective by Roger M.K.[15] The explanation of the taxonomy of cybercrime can be explained as follows:

1) Script Kiddies (SK), are individuals with limited technical abilities, without really understanding what the impact of their behavior is.
2) Cyber-punks (CP), namely groups that "expand" the punk mentality into cyberspace. This group has no respect and no care for authority, symbols and social norms.
3) Hacktivist (H), which is a term used for individuals or groups who perform deviant behavior, but with semantic camouflage to disguise their actions.

4) Thieves (T) are criminal in general. His main motivations are financial gain and greed.
5) Virus Writers (VW), starting from adolescence and developing into a category of ex-writers in line with their cognitive and chronological development and maturity. There is a sensation of mental challenges and academic practice (learning) in the viral creation process.
6) Professional (P) is the most elite category group in cyber criminals, who have competitive intelligence and gray activity. These P individuals can engage in high-profile scams to corporate espionage.
7) Cyber-terrorists (CT) can be part of the military or paramilitary of a country and are positioned as soldiers or vice versa as liberation fighters in cyberspace warfare. Their goal is the same as in traditional military, which is to win battles or wars. CT carries out two functions, namely attacking the enemy's defense system and society and protecting its own system from similar attacks from the opposing side.

Furthermore, researchers also obtained data related to the motivation of cybercriminals [15], namely:

1) Social Learning Theory. The social learning process works in the context of social structures, interactions and situations. Criminal behavior is a function of the variables of the social learning process, especially reinforcement. The main mechanisms in social learning include differential reinforcement and imitation. Definitions in one's social environment are achieved by imitation and observational learning. Reinforcement can be in the form of tangible and intangible rewards in the form of the activity itself, money, or social rewards including increased status in social interactions. Over time, imitation is no longer important because it is the reinforcement or consequences that determine the next behavior.
2) Moral Disengagement-moral justification. Cyber criminals are generally described as modern Robin Hoods, who carry a valuable function in society.
3) Anonymity and Social Control Theory. Research on online behavior has found that people behave differently in cyberspace than in the real world. Individuals tend to be more aggressive, less tolerant, more indiscriminate, and their opinions tend to be more polarized to extreme points on the continuum. In simple terms we can understand that online behavior reflects the actual individual self in conditions without self-control and without social norms or pressure.

From the secondary data from literature study, it can be seen that cyber terrorism is the most dangerous level in the cybercrime taxonomy. This can be seen from the perpetrators, methods and targets that can be categorized as threats to the national security of a nation. Meanwhile, in terms of psychological motivation, cyber terrorism is motivated by the Moral Disengagement - moral justification and Anonymity and Social Control Theory variables. This can be seen from the behavior of terrorists who are generally described as modern Robin Hoods, who carry a valuable function in society so as to produce an act of moral justification. Radical thinkers tend to be more aggressive, less tolerant, more indiscriminate. Their actions and opinions tend to be more polarized to extremes on the continuum. In simple terms Rogers [15] argues that online behavior reflects the actual individual self in conditions without self-control and without social norms or pressure.

3.1. Data Evaluation

Prunckun, 2014 [16] the evaluation process firstly assesses the source's reliability and, secondly, the information's accuracy. In theory, this process is performed on each piece of information collected. However, in agencies collecting large volumes of data, this may be an automated process where a generic rating is assigned if the data are merely stored, but if used in an intelligence research project, it is reevaluated on an individual basis. Each piece of data is assigned an alphanumeric rating indicating the degree of confidence the analyst has in that piece of information. This system is universally known as the *admiralty ratings.*

After the primary and secondary data have been collected, the next step is the researcher evaluates the accuracy and confidence level of the data source. The results of this evaluation can be seen in table 1 below.

Table 1. Data Accuracy & Trustworthiness

No.	Type of Data	Sources	Trust	Accuracy
1	*Books*	*Library*	*A*	*1*
2	*Interview*	*Practitioner*	*B*	*2*
		Researchers	*B*	*2*
		Academics	*A*	*2*

3.2. Data Visualization

After data cleansing from data collection method the researchers present several tables such as the goal table of cyber terrorism, the form of cyber terrorism attacks, the position of cyber terrorism attacks in the taxology of cybercrime and the psychological motivation of cyber terrorism perpetrators. Here is how it looks.

1) PCI threats in the form of CT to national security have three types of targets, namely:
   - Confidentiality: Disclosure of confidential target data belongs to the government that may cause fear; this is similar to typical terrorist activities. An example is seen in the case of Snowden and several groups of democracy activists in western countries who disclose confidential government and company data to the public due to differences in political attitudes.
   - Integrity: Manipulate the integrity of an application/network system, so that it did not work normally. For example, an unauthorized data changed incident during the KPU's tabulation process by cyber terrorists in 2004 and 2005.
   - Availability: Terminate authorized users' access to the computer network, so that the application was unavailable. This happened in 2017 in several hospitals in Indonesia that were affected by the wannaCry virus. The indication of inaccessible networks at related hospitals was devastated.

Figure 1. Types of Cyber Terrorism Target

2) From the research findings based on threats of PCI Cyber Terrorism to national security: the forms of attacks used are shown at Figure 2. Forms of Cyber Terorrism Attacks.

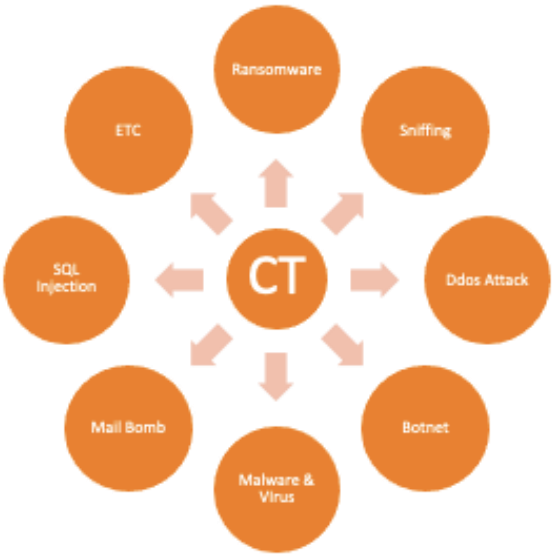

Figure 2. Forms of Cyber Terrorism Attacks

3) Moreover, the study has found types of cybercrime perpetrators' motivation, CT actors fall into the Moral Disengagement/moral justification and Anonymity & Social Control Theory groups. Motivation can arise from one of these types or a combination of the two. See figure 3 venn diagram upon the results of CT perpetrators' motivation in carrying out acts of terrors.

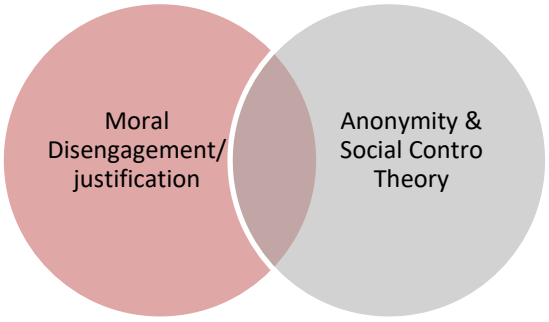

Figure 3. Motivation of CT Actors

4) This study also succeeded in finding the threat level of CT in the Taxonomy Continuum of cybercrime behavior, which ranges from new people (novice) to major acts of terrorism. Here is how it looks taken from the book The Psyche of Cybercriminals: A Psycho-Social Perspective by Roger M.K [15].

In the taxonomy of Rogers' cybercrime behavior[15], it appears that the position of CT is on the far right. This shows that the level of cyber terrorism threat is the highest compared to other forms of cybercrime. This is because the impact generated by the threat of cyber terrorism is very large and can disrupt national resilience in the security sector.

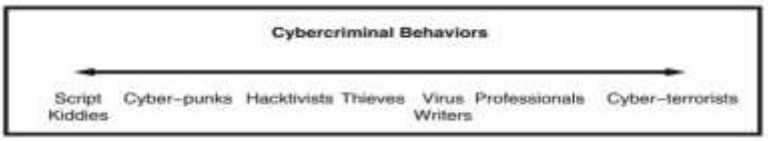

Figure 4. Cyber Crime Rogers' Taxonomy of Behavior [15]

4. Conclusion

PCI has undergone a dialectical process along with the changing environment in which PCI is used. Terrorism, as a form of PCI, also experiences this dialectical process. Terror is no longer just a form of bomb

and bullets, but has metamorphosed into bits and bytes. Perpetrators of terror acts no longer need to come out of their hiding places, because they can carry out acts of terror with only a computer. The threat of PCI in the form of CT against national security needs special attention for stakeholders in the field of national security, so that national resilience does not become disrupted.

In this study, researchers have succeeded in producing knowledge to identify the threat of PCI cyber terrorism against national security. The knowledge that the researchers generated is in the form of PCI CT target types, forms of PCI CT attacks, psychological motivation of perpetrators of PCI CT action and PCI CT threat position in Rogers M.K's taxonomy of cybercrime behavior[15].

5. References

[1] Benjamin, Cole. "*Conflict, Terrorism and the Media in Asia*". Routledge. 2006.
[2] Whittaker, David J. "*Terrorist and Terrorism in the Contemporary World*". Routledge. 2004.
[3] Barry Buzan, People. *States and Fear: an Agenda for International Security Studies in the Post-Cold War.* (Boulder: Lynne Rienner Publisher, 1991).
[4] Mutimer, David. *Beyond Strategy: Critical Thinking and the New Security Studies, In Contemporary Security and Strategy*. Craig A Snyder (ed). (London: Macmillan Press Ltd, 1999).
[5] Sugiyono. *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Alfabeta. Bandung. 2009.
[6] Law No.17/2011 of National Inteliigence states.
[7] Brian, Jenkins. *International Terrorism: A New Kind of Warfare*. Santa Monica: CA: Rand Corporation. 1974.
[8] Sederberg, Peter C. *Terrorist uths: Illusions, Rhetoric, and Reality Change*. Harpercollins College Div, 1993.
[9] Irawan Sukarno. *"Ilmu Intelijen".* Puslitbang BIN & STIN. STIN PRESS. 2014.
[10] Wahyono S.K. "*Pengertian dan Lingkup Keamanan Nasional*". Program Pasca Sarjana UI, Kajian Stratejik Ketahanan Nasional. 2003.
[11] Saronto, Yohanes Wahyu. "*Intelijen Teori, Aplikasi dan Modernisasi*". PT Ekalaya Saputra. 2004
[12] Widjajanto, Andi. Wardhani, Artanti, "*Hubungan Intelijen-Negara*". Jakarta. 2010.
[13] Darmono, Bambang. "*Keamanan Nasional: Sebuah Konsep dan Sistem Keamanan bagi Bangsa Indonesia*". Sekretariat Dewan Ketahanan Nasional. 2010.
[14] Suharsaputra, Uhar. DR, M.pd. *Metode Penelitian.* PT. Refika Aditama. Bandung. 2014.
[15] Rogers. M.K. 2010. *The Psyche of Cybercriminals: A Psycho-Social Perspective* in Ghosh. S. & Turrini. E. (Ed). Cybercrimes: A Multidisciplinary Analysis. New York: Springer.
[16] Prunckun, H., "Scientific Methods of Inquiry for Intelligence Analysis (Security and Professional Intelligence Education Series)", 2nd. ed., Rowman & Littlefield, 2015

The Impact of Knowledge Management on Service Quality of News Researcher in XYZ Television

Jhoni Marcos[1], Mulya Riawan Mashudi[2]

[1]Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received:
Accepted:
Published:
DOI: 10.33555/ejaict.v…

Corresponding Author:

Jhoni Marcos
Email:
jhoni_marcos@yahoo.com

ISSN 2355-1771

ABSTRACT

The main objective of this research is to find out whether there is an impact of the implementation of knowledge management (KM) on the service quality of the news researcher (NR) work unit in the news divisions at XYZ Television. The positive influence of KM is expected to improve the service quality provided to news producers as users. So that it also has a positive or increasing impact on the quality of the news produced. This type of research is applied research, with experimental research methods. According to the level of exploration, this study uses a comparative method by comparing the results before and after the implementation of KM. According to the type of data, this study uses qualitative data. For this reason, a survey was conducted using a questionnaire before and after the implementation of KM to 28 news producers as respondents. These respondents were the total population of users who are received NR services. The rating scale used is a Likert scale. The statistical test used for this study used paired sample t-test using IBM SPSS 25, which tests the hypothesis whether there is a significant impact of KM implementation. This study has proven that the application of KM can improve the service quality of NR. This increase is indicated by the significance value of the service before and after the implementation of KM. So that this research is expected to contribute to the improvement of service quality in each work unit of news researchers in television media in Indonesia, especially in the news division.

Keywords: *Knowledge Management, Service Quality, News Researcher*

1. Introduction

XYZ Television is general entertainment channel. Where all types of programs are provided, there are entertainment, information, sports and news. Not like a news channel whose overall program composition is filled with news content only. In XYZ Television, News is one of the programs that contributes about 30% of the total daily broadcast. But News is an important part of a television media company, since it can be a bargaining position in society and government. In news, speed of reporting is a must, where news must be fast, actual and complete, packed with a grace period that is narrow enough to immediately be presented to viewers.

In XYZ news division, a News Researcher (NR) greatly contributes to a series of news program production. The NR unit provides additional important information and knowledge to the news producer (user) who will create a news script. The material from NR unit is the basis for information or reinforces the news information that will be presented. The service quality of NR will affect the output given to the user.

The author works at this company as the Head of the News Facilities and Operation Department in charge of the News Researcher (NR) work unit. So, the author is responsible for improving the service quality in this work unit. Discussions through FGDs and working meetings are often held to discuss the SQ of this NR. The author tries to identify the problems. Using root-cause analysis approach, some of the problems identified can be described in the Fishbone Diagram in figure 1.1.

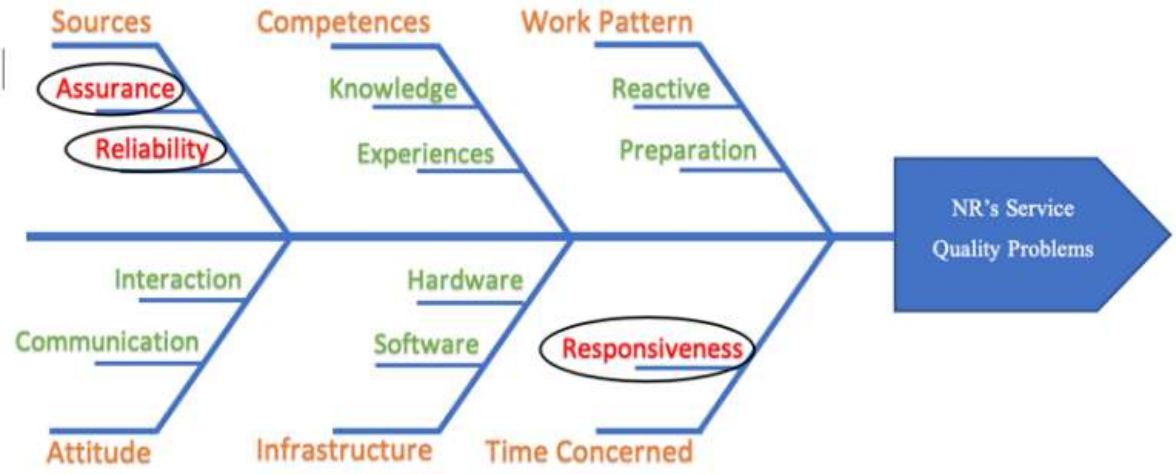

Figure 1. Root-Cause Analysis by Fishbone Diagram of NR's Service Quality Problems

Figure 1 [1] shows that there are three main problems circled in the figure. These three main problems are considered to be improved immediately in order to improve the SQ of NR, which is guaranteed data availability, accuracy of data/ information and validity sources, and speed of data delivery. These three main problems also often appear in evaluation meetings in the News Division. Based on the consideration of time that is also limited, this research is only focused on the three main problems mentioned. These problems are classified as problems with Service Quality (SQ).

Broadly the dimensions of service quality accepted are tangibility, empathy, reliability, responsiveness, and assurance [2]. Based on the identification of root-cause analysis problems as depicted in the fishbone diagram in figure 1.1, the three main problems to be investigated are, where the guarantee of data availability can be classified in the assurance dimension, accuracy of data/ information and validity sources can be classified in the reliability dimension, and the speed of data delivery included in responsiveness dimension category.

The currently working patterns of the NR unit in this XYZ Television is reactive rather than anticipatory. With this currently work pattern, it takes more time to deliver data or information to News Producers (user), and frequently also problems with the availability and accuracy of data or information caused by limited deadlines. Users always request data or information to the NR unit mostly only an hour before the on-air. While one news researcher with another has different experiences, maturity and knowledge. Certainly, one another will provide a different level of service.

Knowledge Management (KM) is a business concept that has developed rapidly, especially since the 2000s. In general KM is a process that coordinates the use of information, knowledge and experience. Knowledge is the result of information that has been processed. Where there are values, insights, experiences, and contextual information that will help someone in evaluating and combining new experiences, so as to create a new knowledge [3]. Knowledge would be very useful for stakeholders who are able to access, through a collaborative environment. It would be useful for decisions making, fast learning, data analysis, and others.

For this reason, the author thinks that KM can be applied to solve three main problems in SQ in this NR unit. For this reason, this study was conducted to prove the author's hypothesis. Author in this paper will focus to make research about the three main problems that occurred in NR unit. As mentioned before, the Service Quality (SQ) discussed is limited to the speed of delivery time (responsiveness), data availability (assurance) and the accuracy (reliability) of the data/ information that provided to the user. This paper discusses empirically whether and how KM can be used to improve SQ.

2. Theoretical Background

This section defines and discusses the nature of service quality and knowledge management in general based on existing theories. Then explained more about the lifecycle of knowledge management and the dimensions that exist in service quality.

2.1. Service Quality

One measure to determine whether a company/ organization has a good service quality is whether or not the target set by the company/ organization has been achieved. The achievement of company/ organizational goals is strongly supported by the quality of existing human resources. If the quality of its human resources is good, it is expected that the quality of the company/ organization will be good too. However, to get good service quality it is necessary to manage quality effectively.

The dimensions of service quality (SERVQUAL) that are widely accepted are tangibility, empathy, reliability, responsiveness, and assurance [2]. Such measurements are known as service quality (SERVQUAL) models. In the SERVQUAL model, service quality is defined as "global judgment or attitude regarding the superiority of a service" [4], while the definition of service quality which is often referred to as service quality [5] is how far the difference is between reality and customer expectations for the service they receive or receive. Hope is the desire of customers from the services that may be provided by the company.

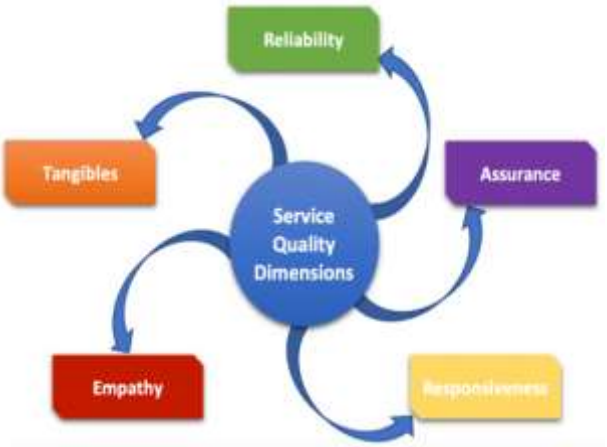

Figure 2.1.

Figure 2. Service Quality Dimensions [6]

The SERVQUAL model has a service quality dimension based on a multi-item scale, which is then designed to measure customer expectations and perceptions, as well as the gaps that exist between the two in the service quality dimension. Initially, Parasuraman et al. (1985) identified 10 main dimensions, with 22 variables related to services, then all dimensions and variables were analyzed using factor analysis. The results of the analysis found that apparently several criteria could be used to assess service quality. This criterion includes ten potential dimensions that complement each other. The ten dimensions are physical evidence, credibility, reliability, responsiveness, competence, communication, security, courtesy, understanding, and access. Then in subsequent studies, Parasuraman et al in 1988 perfected the dimensions and then reprocessed them so that they were finally simplified into 5 dimensions, namely:

1. Direct evidence (tangibles); include equipment, physical facilities, communication facilities, and employees.
2. Reliability (reliability); that is, the ability to provide the promised service with accuracy, integrity and satisfaction.
3. Responsiveness (responsiveness); that is, the desire of service providers to help customers and provide services responsively and quickly.
4. Guarantee (assurance); including ability, service availability, knowledge, courtesy, and staff trust, free from risks and danger.
5. Empathy (empathy); including good communication, easy relationships, personal attention, and understanding customer needs.

The service quality dimension for NR, which is the main concern in evaluation discussions, is reliability, assurance and responsiveness. Because these three dimensions are highly expected to increase in the services provided by NR to their users. So, service quality dimensions in this research will be focused and limited to three dimensions, namely reliability, assurance and responsiveness. The other dimensions, namely empathy and tangible, do not match the service character of NR. These two dimensions are more appropriate in relation to other services, such as service by receptionists in hotels.

In the context of management and service quality evaluation, the formulation of the problem and the determination of management decisions to be taken or determined is the answer to the question; What is at issue? Where is the service quality in question? When do we fix this service quality problem? Why do we need to fix? Who should do it? How to implement and manage the service quality?

2.2. Knowledge Management

KM refers to identifying and utilizing collective knowledge in an organization to help competing organizations [7]. Typically, KM consists of a knowledge process that is supported by infrastructure, so that management capabilities and activities can support and enhance the knowledge process. Knowledge

management has been increasingly seen as one of the most important practices for organizations to improve its efficiency, effectiveness and long-term competitive advantage [8].

The purpose of knowledge management is not to manage all knowledge but only the most important knowledge needed by the organization. KM is needed to ensure that people will have the knowledge they need, where they need it, and when they need it. That is, the right knowledge, in the right place, at the right time [9]. KM is not about creating a new department, but how to make a small change to the workings of an organization. In general, KM aims to create a knowledge environment that requires changes in organizational values and culture, by changing work behavior and patterns, and giving workers easy access to each other to relevant information resources [9].

Effective knowledge management plays an important role in the emergence of a knowledge-based economy [10]. This effectiveness has been described as one important element for organizations to ensure sustainable strategic competitive advantage. Knowledge management is expected to be a key driver of organizational quality and an important tool for organizational survival, competitiveness and profitability. Therefore, to create, manage, share and use knowledge effectively is very important for the organization.

The main goal of Knowledge Management are as follows:

- To improve the quality of management decision making in an organization, by ensuring that throughout its life cycle reliable and safe data / information can always be available.
- Capture, develop, share and use organizational knowledge.
- To be able to increase efficiency by reducing the need for rediscovering knowledge.

Such knowledge processes such as knowledge creation, sharing, acquisition, transfer and application [11]. The literature on KM includes several categories of KM practices and activities. It can be divided into knowledge creation, incorporation and dissemination. Similar to this view, this paper proposes that the KM lifecycle can be divided into four main types [12]:

1. Knowledge Acquisition,
2. Knowledge Codification,
3. Knowledge Storage,
4. Knowledge Sharing.

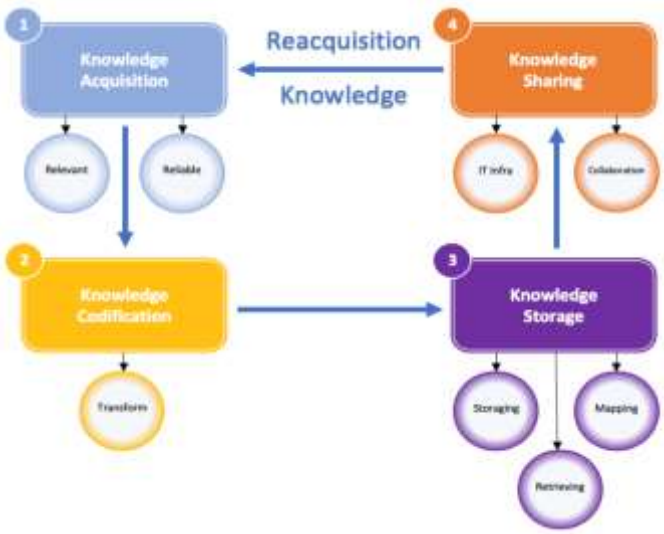

Figure 3. Knowledge Management Lifecycle Diagram [13]

Although these types, to some extent, are interrelated and overlapping, they can be distinguished individually because of their different focus. Each of the four KM processes is briefly explained below.

2.2.1 Knowledge Acquisition

Knowledge acquisition stands for organizational practice aimed at gathering information from extra-organizational sources [14]. External networks and collaborative arrangements are important sources of knowledge for all types of organizations. Users form a very important group from which knowledge must be obtained if the organization is to succeed. For example, user feedback systems, data mining, business intelligence and collaboration with partners and research institutions are characteristics of very advanced knowledge acquisition practices.

2.2.2 Knowledge Codification

Codification and storage are very important for reactivating and integrating knowledge. The codification of knowledge itself consists of a series of activities needed to compile tacit knowledge into explicit form, to store documented knowledge and to provide the latest documented knowledge to others in the organization [15]. This is based on the availability of technology systems, platforms and tools, as well as the right information and communication. Then related employee skills and motivation are used to make employee knowledge explicit and to compile and store it, so that it can later be used in systems and documents.

2.2.3 Knowledge Storage

Knowledge storage refers to activities related to managing knowledge resources. It is very important that this knowledge must be stored properly. Ideally, this needs to be equipped with information technology tools and platforms that will facilitate codification so that it is effective in storing explicit knowledge in databases, making it easier to find and transfer this knowledge.

2.2.4 Knowledge Sharing

Sharing knowledge is the key to managing knowledge, whether it is tacit or not. For those with tacit knowledge, organizations must encourage face-to-face communication and the creation of shared learning experiences, and build a culture of knowledge sharing [16]. Knowledge sharing activities include informal communication, brainstorming sessions, guidance and coaching. In this paper, the context of sharing is also through facilities, namely through a centralized database. So, everyone works in a collaborative way. To be able to share together all the knowledge gained and possessed.

2.3. Hypothesis

The hypothesis for this research has been defined as follows:

Ho: There is no difference in the mean value of service quality (assurance, reliability and responsiveness) before and after Knowledge Management is applied.

Ha: There are differences in the mean value of service quality (assurance, reliability and responsiveness) before and after Knowledge Management is applied.

3. Research Methods

In this section, the implementation of the proposed model and the evaluation of the model will be discussed. This research is using applied research with experimental that compare two situation and measure it based on quantitative research.

The impact of KM on service quality was then empirically tested by analyzing a survey of 28 respondents, collected from the all of news producers in XYZ Television as users. 28 respondents are not a sampling, but the total population of users who get services from NR.

This survey was given to all these users before the KM implementation and after the KM implementation. So that later we can see the difference in the pre-post scores.

Data collection technique in this research used a questionnaire with a Likert scale. Responses to the items in the questionnaire will be separated in four alternative answers, namely 1 (Strongly Disagree), 2 (Disagree), 3 (Neutral), 4 (Agree), and 5 (Strongly Agree). Service quality questionnaires were used before and after implemented of knowledge management to all users.

Figure 4. The pre-post survey was conducted to 28 respondents

The basic concept of a paired sample t-test is as follows:

- Paired sample t-tests are used for whether there are differences in the average of two paired samples.
- The two samples in question are the same sample but have two data.
- Paired sample t-test is a part of parametric statistics, therefore as per the rules in parametric statistics, research data must be normally distributed.

Service quality is one of the most widely researched topics in the organizational behavior literature and has been actively studied. Prerequisites for high quality service have been widely studied. However, KM issues have not been included among the many service quality factors to be examined. In general, it seems that the KM literature rarely discusses the impact KM can have on "soft" performance issues, such as service quality. KM processes constitute such contextual features of the work environment, which can enrich the job and increase service quality. The KM process in an organization can help workers in a knowledge intensive environment so as to build mutual understanding to get value from knowledge. More specifically, knowledge acquisition increases service quality because it involves access to new knowledge collections that can improve efficiency in carrying out one's duties. Codification of knowledge also helps people find the data or information they need faster and more effectively in carrying out their tasks.
Sharing knowledge can meet the social needs of individuals involved in it. They will bind to each other, and become more confident. Knowledge retention increases employee recognition and appreciation, because it is based on the recognition of the value of individual expert knowledge. In short, the authors suggest that employees will be more satisfied with their work insofar as they experience the KM process in their work environment. The approach of solution to solve the problems is depicted in Figure 3.1. This figure illustrates how the relationship of independent variables can have an impact on the dependent variable with the accompanying dimensions.

Figure 5. Solution approach to improving SQ of NR

4. Results and Discussions

The results of research obtained through the stages of the method previously described. Where here also further explained the need for support in conducting research.

4.1. Implementation of Knowledge Management

The implementation of a new work pattern with the KM concept began in the middle of May 2019. Prior to implementation, the author first conducted socialization both internally and externally to the department. In the internal department, the author conducts socialization and knowledge sharing about KM to NR. In the external department, the writer does it to the news producer as the user. The work patterns adopted in adopting KM are illustrated as in the figure 4.1.

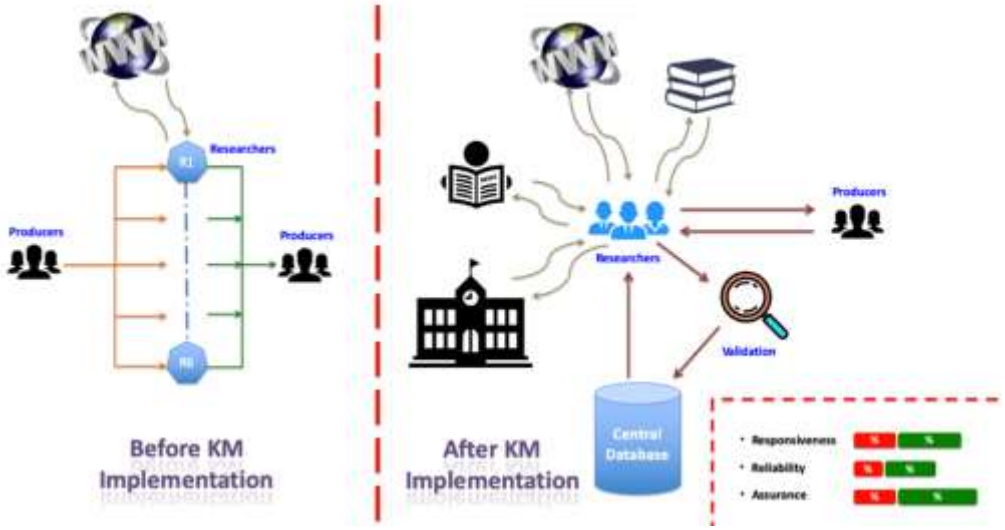

Figure 6. Expectation of KM implementation workflow

Figure 4.1 illustrates two different work patterns, between before and after the implementation of KM. In the left side of picture, it can be explained that just before KM was applied, the pattern of action was reactive. NR works only when there is a request for data / information needed by the user. Where data requests are usually approximately one hour before the news is broadcast. So that NR has only a little time to fulfill several requests at the same time almost simultaneously from several news producers. NR can only search for data / information requested from one source, namely the internet. Then with all its limitations, NR provides its services as much as possible.

In contrast to the right side of picture, work pattern when KM has been applied. Where NR will work more anticipatory, not only when there is a request from the user, but has begun to search for data / information that might later be needed from the user before being asked. Sources can be from the internet, books, papers, from institutions that work with XYZ Television, such as BPS (Statistics Indonesia), ANRI (National Archives of the Republic of Indonesia, and other authorized institutions.

4.2. The Operationalization of The KM Variable

Operationalization for the independent variable KM by applying the cycle that is in the KM concept, which starts with Knowledge Acquisition, then Knowledge Codification, then Knowledge Storage and finally Knowledge Sharing.

- Knowledge acquisition; in the application in NR, we collect data/ information from various sources that can be trusted and accounted for. These sources include books, journals, papers, seminars, related institutions, resource persons, and the internet.
- Knowledge codification; in the application in NR, data/ information in the form of verbal or audio video is codified first. So that data/ information changes in written form that can be stored in a database.
- Knowledge storage; in the application in NR, data/ information that has been collected, is stored in a structured table in a centralized database.

- Knowledge sharing; after data/ information is stored in a database, it can be accessed together or collaborated by news researchers. So, when the user needs the data/ information later, all that remains is to be pulled from the database and processed into a new knowledge before it is given to news producers as its users.

4.3. The Operationalization of The SQ Variable

Operationalization for the dependent variable SQ is by testing the three dimensions previously discussed, namely the dimensions of Reliability, Assurance and Responsiveness.

- Dimensions of reliability; contains problems that must be solved in it, namely the need for data accuracy, valid or accountable sources, consistency, and complete.
- Dimensions of assurance; contains problems that must be solved in it, namely guarantees of good cooperation between users and service providers, guarantees of knowledge of service providers and guarantees of meeting the needs of users of the services provided.
- Dimensions of responsiveness; contains problems that must be solved in it, namely the readiness in providing services with responsiveness at all times, and can provide responses to the needs of the service quickly.

4.4. Statistical Testing

After obtaining the complete questionnaire data from 28 respondents, the authors conducted a statistical test of the data using the IBM SPSS 25 application. The results are as follows in the table 4.1. This test compares the significance value between before and after the implementation of KM to SQ.

Table 1. Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Before	24.96	28	4.342	.821
	After	39.32	28	4.769	.901

From the table 4.1 it can be analyzed that this research uses a sample of n1=28 and n2=28 respondent. The mean value for X = 24.96 and mean value for Y = 39.32. standard deviation (Sx) = 4.342, and standard deviation (Sy) = 4.769. From these results it can be seen that the average value of service quality after applying knowledge management is higher than before, which means that there was an improvement in SQ after KM was implemented.

Table 2. Paired Samples t-Test

		Pair 1 Before - After
Paired Differences	Mean	-14.357
	Std. Deviation	3.423
	Std. Error Mean	.647
	Lower	-15.685

	95% Confidence Interval of the Difference Upper	-13.030
t		-22.192
df		27
Sig. (2-tailed)		.000

Tests using a two-tailed test with a significance level a = 5%. The level of significance in this case means the risk of making a wrong decision to reject the correct hypothesis is as much as 5%.

From the paired sample test table, the results are obtained:

- t value was obtained from the paired sample test table = -22.192
- t table value of a = 5%/2 = 2.5% (two-tailed test) with degrees of freedom (df) n-1 is 28 – 1 = 27. With 2-sided testing (significance = 0.025) the results obtained for t table amounted to 2,052.
- Test Criteria:
    - Ho is accepted if $-t_{table} \leq t_{count} \leq t_{table}$
    - Ho is rejected if $-t_{count} < -t_{table}$ or $t_{count} > t_{table}$
    - Based on probability:
        - Ho is accepted if $P_{value} > 0.05$
        - Ho is rejected if $P_{value} < 0.05$
- The results of the comparison of t_{table} and t_{count} are:
    - Value of $-t_{count} < -t_{table}$ (-22.192 < -2.052) and P_{value} (0.000 < 0.05) then Ho is rejected.
    - This matter means there are differences in the average value of service quality (assurance, reliability and responsiveness) before and after Knowledge Management is applied.
    - Value of t_{count} negative shows that the average value of service quality before applying knowledge management is lower than afterwards.

Based on the statistical explanation above it can be seen that the application of KM can improve the quality of service in NR. This is reinforced by the theory that KM aims to create a knowledge environment that requires changes in organizational values and culture, by changing work behavior and patterns, and giving workers easy access to each other to relevant information resources [9]. Service issues related to assurance, reliability and responsiveness that can still be corrected through the application of KM.

As for the KM implementation, there are significant changes in each dimension with the highest order, namely the responsiveness dimension, then the assurance dimension and finally the reliability dimension.

4.5. The Results of Gap Analysis

After the application of KM in SQ, the results can be seen based on the gap analysis previously discussed in chapter 3. Here we can see the different situations from before and after KM was applied.

Current situation:

- Guaranteed availability of data / information needed.
- More choices of data / information sources to meet the requested needs.
- Has data / information source validity.
- Response time given by NR is much faster in conveying data / information provided to users.
- A lot of time is spent searching for data / information needed before the request arrives.

Ideal situation:

- Changes in workflow from reactive to anticipatory can be realized.
- Guaranteed availability of data from several valid and integrated sources of choice, by presenting it more quickly and responsively.

Based on the survey conducted using a questionnaire, it can be concluded that the pre-survey and post-survey are as follows:

- In the pre-survey, the highest score that can be generated from each dimension can only reach a value of 4. The dimension that has the highest total score of 4 is assurance 38.1%.
- In the post-survey, the highest score that can be generated from each dimension can reach a value of 5. Dimensions which have the highest total score of 5 are responsiveness of 58.9%.
- The largest score difference is in the dimension of responsiveness, where it has a difference value of 55.3%. The second rank is occupied by the reliability dimension of 25%, and the last rank is occupied by the assurance dimension of 16.7%.
- So, it can be concluded that with the application of KM, the most significantly increased dimension of service quality is responsiveness. This indicates, the response given by NR is much faster than before KM was implemented.

Table 3. Highest Score Average of Each Dimension Survey Results

Dimension	Highest Score Average Pre-Survey	Highest Score Average Post-Survey	Difference of Highest Score Average
Reliability	14.3%	39.3%	25%
Assurance	38.1%	54.8%	16.7%
Responsiveness	3.6%	58.9%	55.3%

5. Conclusion and Recommendation

5.1. Conclusion

Based on data analysis using the IBM SPSS 25 application, the results show that there is positive impact in SQ after KM is applied to NR work units on XYZ Television. The average value before is smaller than after KM was applied, which means that there was an improvement in SQ after KM was implemented. This explains that by applying KM, it can increase the SQ of NR. Of the three dimensions in SQ the most affected are the responsiveness dimension. Where this dimension is the most significant increase in value. The second rank is occupied by the reliability dimension, and the third rank is occupied by the assurance dimension.

This is reinforced by the results of observations and discussions (FGD) that the speed of data presentation that was previously longer, when after the application of KM becomes faster and more responsive when users need services.

The SQ in question is in the form of reliability, assurance and responsiveness. The application of KM is carried out for seven months through the cycle of knowledge acquisition, knowledge codification, knowledge storage and knowledge sharing.

5.2. Recommendation

The author advises XYZ Television to continue to implement KM, because KM can indeed maintain service quality and, thereby, grow high quality service by changing workflows from reactive to anticipatory patterns. So, KM will anticipate and fill the knowledge gap between one researcher and another. KM needs to provide an average standard of quality for all news researchers in terms of expected service quality. KM approach with data centralization is expected that everyone in this unit can access data and information together. So that the time of providing data will be faster and more accurate and will certainly ensure its availability.

The same thing the authors recommend to similar companies like XYZ Television which has a news division in it. By implementing the same thing on XYZ Television, it is expected to also be able to give the same results in accordance with the evidence given by this research.

6. References

[1] J. Marcos, "THE IMPACT OF KNOWLEDGE MANAGEMENT ON SERVICE QUALITY OF NEWS RESEARCHER IN XYZ TELEVISION," Swiss German University, Tangerang, 2020.

[2] A. Meesala and J. Paul, "Service quality, consumer satisfaction and loyalty in hospitals: Thinking for the future," *Journal of Retailing and Consumer Services*, vol. 40, pp. 261–269, Jan. 2018, doi: 10.1016/j.jretconser.2016.10.011.

[3] R. Abdullah, M. H. Selamat, U. P. Malaysia, S. Sahibudin, A. Alias, and U. T. Malaysia, "A framework for knowledge management system implementation in collaborative environment for higher learning institution," *Journal of Knowledge Management Practice. Retrieved from http://www.tlainc.com/articl83.htm Abell, A., & Oxbrow, N*, 2005.

[4] A. Parasuraman, V. A. Zeithaml, and L. L. Berry, "A Conceptual Model of Service Quality and Its Implications for Future Research," *Journal of Marketing*, vol. 49, pp. 41–50, Sep. 1985.

[5] A. Parasuraman, V. A. Zeithaml, and L. L. Berry, "SERVQUAL: A Multiple-Item Scale for Measuring Consumer Perceptions of Service Quality," *Journal of Retailing*, vol. 64, pp. 12–40, 1988.

[6] R. Kant, D. Jaiswal, and S. Mishra, "The Investigation of Service Quality Dimensions, Customer Satisfaction and Corporate Image in Indian Public Sector Banks: An Application of Structural Equation Model(SEM)," *Vision*, vol. 21, no. 1, pp. 76–85, Mar. 2017, doi: 10.1177/0972262916681256.

[7] A. Kianto, M. Vanhala, and P. Heilmann, "The impact of knowledge management on job satisfaction," *J of Knowledge Management*, vol. 20, no. 4, pp. 621–636, Jul. 2016, doi: 10.1108/JKM-10-2015-0398.

[8] S. Sukumaran, S. S. Amalathas, C. G. K. Simon, S. S. Mustapha, I. A. T. Hashem, and A. F. Zulkifli, "A Case Study on Knowledge Management Implementation in the Banking Sector – Issues and Challenges," in *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)*, Subang Jaya, Malaysia, Oct. 2018, pp. 1–6, doi: 10.1109/ICACCAF.2018.8776746.

[9] D. R. O. Shannak, "Knowledge Management Strategy Building," *European Scientific Journal*, vol. 8, p. 27, 2012.

[10] F. O. Omotayo, "Knowledge Management as an important tool in Organisational Management: A Review of Literature," p. 24, 2015.

[11] H. Lee and B. Choi, "Knowledge Management Enablers, Processes, and Organizational Performance: An Integrative View and Empirical Examination," *Journal of Management Information Systems*, vol. 20, no. 1, pp. 179–228, Jul. 2003, doi: 10.1080/07421222.2003.11045756.

[12] U. M. S.D, C. Sivasubramanian, and T. N. S. Dath, "A comprehensive analysis of knowledge management in Indian manufacturing companies," *Jnl of Manu Tech Mnagmnt*, vol. 28, no. 4, p. JMTM-08-2016-0107, May 2017, doi: 10.1108/JMTM-08-2016-0107.

[13] M. Sa, "A NEW LIFE CYCLE MODEL FOR PROCESSING OF KNOWLEDGE MANAGEMENT," p. 10, 2006.

[14] W. M. Cohen and D. A. Levinthal, "Absorptive Capacity: A New Perspective on Learning and Innovation," *Administrative Science Quarterly*, vol. 31, pp. 128–152, 1990.

[15] R. Filius, J. A. de Jong, and E. C. Roelofs, "Knowledge management in the HRD office: a comparison of three cases," *Journal of Workplace Learning*, vol. 12, no. 7, pp. 286–295, Nov. 2000, doi: 10.1108/13665620010353360.

[16] I. Nonaka, "The Knowledge-Creating Company," in *The Economic Impact of Knowledge*, Elsevier, 1998, pp. 175–187.

7. Acknowledgement

Firstly, the author wishes to give thanks to Allah Subhanahuwata'ala who guards me in this research, because without Allah Subhanahuwata'ala, I couldn't complete this thesis.

Secondly, thanks to my family for the support. And the last but not least, thanks to Swiss German Univeristy and all the lecturers, especially to Dr. Ir. Moh. A. Amin Soetomo, M.Sc., Dr. Mulya Riawan Mashudi,S.T., MEM., Dr. Charles Lim, M.Sc, and MIT Study Program Head Dr. Eka Budiarto, S.T., M.Sc., who helpful in guiding me from beginning.

This paper is a conversion from my thesis which I did to complete my master's studies. Hopefully this research is useful for others, because I really feel the benefits, both for the company where I work and I personally.

Free Open-Source High – Availability Solution for Java Web Application Using Tomcat And MySQL

Dhanny[1], Sandi Badiwibowo Atim[2]

[1,2] PT. Danwin Cipta Niaga, Jakarta Selatan 12430, Indonesia

Article Information

Received:
Accepted:
Published:
DOI: 10.33555/ejaict.v…

Corresponding Author:

Dhanny
Email: dhanny@gmail.com

ISSN 2355-1771

ABSTRACT

With the growth of the internet, the number of web applications is also growing. Many web applications are becoming more important to the stakeholders that they cannot afford downtime which can cause loss of revenue, loss of productivity, etc. In the past, only big organizations with deep pocket could afford implement high-availability for their web application, but nowadays there are free open-source software programs that support high-availability feature available to everyone. This research studied the feasibility of implementing high-availability for Java web application system without using commercial software. This research compared the capability of proprietary and free open-source high-availability solution for Java web application based on a simple high-availability design, where a test Java web application was deployed into the environment based on proprietary and free open-source solutions, and tested how well each solution perform when problem occurs. The result showed that the free open-source high-availability solution worked, but not as well as proprietary one. However, the proprietary high-availability solution for database did not perform well, and neither did the open-source one. This research concludes that the free open-source high-availability solution works and thus made high-availability become much more affordable, especially for individual or small organizations with budget constraints.

Keywords: *High Availability, Java, Web Application, Architecture*

1. Introduction

Along with the growth of the internet, the number of web applications has also been growing rapidly. The web applications can vary in size, complexity, number of users, working hour, etc.

These web applications serve different purposes to their users. There are web applications for commercial as well as non-commercial purposes. The businesses of all size already understand the power of the internet, and leverage the internet to grow their businesses. In fact, many businesses built their business foundation on web applications. For these organizations, it is very important to ensure their web applications continuously operate without any or minimum disruption. There are also web applications built for non-commercial purposes and community websites providing online services for its member and many others. The availability of these web applications is also as important as the commercial ones.

It can be seen that in most situations if not all, it is very desirable that these web applications can always operate without any disruption, or in other words, implement high-availability.

1.1. Technology

The early version of the web started as static web pages which visitor can access to view their content [1]. When a visitor accessed the website, the server serves the page based on the static information in the file system, such as documents and images [2]. However, these static websites quickly evolve into dynamic websites.

Web application is defined as an application that is accessed via the Web browser over a network such as the Internet or an intranet [3]. In this document, we also refer to web application as website that is powered by server-side program scripts to provide dynamic behaviour. Thus, in general this document does not refer to website with static contents as web application.

1.2. Stateless and Stateful Web

Nowadays, when visitor visits a website, typically he would expect the website to remember his credentials, preference, locations, etc., even if it is only temporary. However, the core HTTP protocol used by the Internet communication is stateless. Stateless means that all information about a request must be stored in the request itself [4]. To achieve a useful user interaction, it would be necessary to be able to keep information longer than the duration of a single request-response cycle. Java has the concept of session which represents a series of request-response exchanges between a user and a web application.

1.3. Multi-tier Web Application

With proper sizing, one can always setup a complete web application server on a single computer. In many scenarios, this approach is acceptable.

According to Java Enterprise Edition blueprint, the functionality of an application can be separated into isolated functional areas called tiers [5]. The following are the description of the tiers:

1. The client tier consists of application clients that access the server. It is usually located on a different machine from the server.
2. The web tier consists of components that handle interaction between clients and the business tier.
3. The business tier consists of components that provide business logic for an application.
4. The enterprise information systems (EIS) tier consists of database servers, enterprise resource planning systems, and other legacy data sources, like mainframes.

1.4. High Availability Definition

A simple way of understanding high-availability is to think that a system must be always functioning at all time. However, this definition does not provide sufficient detail for proper management of the system. The simplistic definition above is also a very idealistic one. In practice, high-availability always comes with a cost. Thus, the benefits of having high-availability system must justify its cost. Some formal definitions related to high-availability: Availability is the ability of an IT service or other configuration item to perform its agreed function when required [6].

Downtime is the time when an IT service or other configuration item is not available during its agreed service time [6].

Availability is calculated or measured as the percentage of time that a system operates during its intended duty cycle [7]. In the context of high-availability, the availability metric is often specified by the number of 9 (nines).

1.5. High Availability Design

There are several design techniques relevant to achieving high-availability: Load balancing, Mirroring, Clustering. “Server load balancing deals with distributing the load across multiple servers to scale beyond

the capacity of one server and to tolerate a server failure" [8]. With respect to web application, a load balancer is usually placed between the clients and several web servers.

1.6. Cause of Downtime

A study stated that planned downtime accounted for 80% of all downtime, while less than 20% was unplanned downtime [9]. The causes of planned downtime include activities such as backup, recovery, hardware upgrade, software upgrade, system administration, production test, and other activities that plan ahead a system downtime.

1.7. Proprietary Solution for High-availability

A survey by New Relic shows that for Java users, the most commonly deployed proprietary application servers are WebSphere and Oracle [10]. For proprietary database, Oracle Database was the top market share leader, followed by Microsoft SQL Server [11].

1.8. Free Open-source Software

"Free software" means software that respects users' freedom and community. Roughly, the users have the freedom to run, copy, distribute, study, change and improve the software. With these freedoms, the users (both individually and collectively) control the program and what it does for them" [12].

Open-source software comply with the criteria: free redistribution, inclusion of source code and compiled source code, allowing derivative works, maintaining integrity of the author's source code, and so on [13].

Commercial high-availability solutions have been around for long time. However, nowadays there are also free open-source high-availability solutions. Being free, it usually means they are free to acquire, but many times professional services and trained resources are required to implement and maintain such solutions.

According to JRebel technology report [14], Tomcat appeared to be the most commonly deployed free open-source application server, and WebLogic is the second most popular one.

The popular free open-source database are MySQL, PostgreSQL, Firebird, and many others. A survey by Jelastic showed that MySQL was still hold the highest market share among free open-source database servers [15].

2. Research Design and Experiment

The methodology used to achieve the intended objectives were by doing literature study, conceptual high-availability design, developing a simple test Java web application, design and implementation using proprietary and free open-source solution.

2.1. Setup

This research proposed the high-availability design that is relatively simple to setup based on the nature of Java-based web application. The experiment was setup and conducted in a single virtual machine instance, in which multiple instances of the web application server and database server were configured; and excluded the virtual machine failure scenario, as this would mean every configured web application server and database server instances within it would not be available. The virtual machine instance was installed Windows 2008 R2 operating system.

2.2. Java-based Online Shop

The web application was a simplified online shop, where user can browse the product catalogue and place their orders. Therefore, the functionality of the web made application was made simple, but yet still sufficient to represent the user experience in the aspect of unavailability.

2.3. Behavior in Non-High-Availability Deployment

In a deployment without high-availability design, the sample web application was deployed with Java Web /Application Server and Database Server. The sample web application was compiled and packaged into a WAR file. The database was setup with relevant tables and prepopulated data. The web application uses JDBC to connect to the database for the read and write operation.

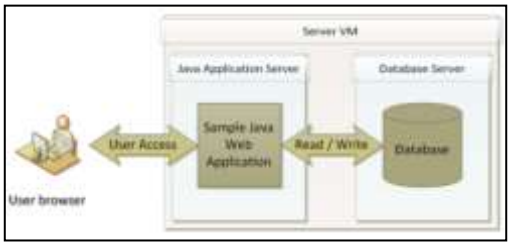

Figure 1. Single Server Deployment

In the event of failure at the Java application server, the user will not be able to access the web application at all, and thus will be getting error on the internet browser. In the event of failure at the database server, the user will still be able to access the web application partially. Certain parts of the web application that involve access to the database would encounter error.

2.4. Automated Web Application Test

Apache JMeter Version 2.7 r1342410 was used to simulate the user accessing the website. A JMeter test plan was created to simulate user performing the following steps using web browser. The test plan was configured such that it simulates if a user encountered an error, he stops. Therefore, the number of submitted orders in the database indicated how many users encountered error.

2.5. High-Availability Deployment

In order to achieve high-availability of the web application, the following conceptual design was proposed.

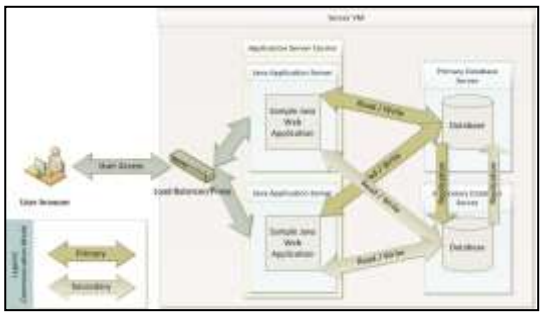

Figure 2. Proposed High-Availability Deployment

Two database servers were setup, with one as the master and the other as the slave. The master was the main one that was used for normal read-write operation, whereas the slave was the standby backup. Under the normal the web application in each instance application server instance accesses the primary database. In the event of failure of the secondary database server, it could be fixed without impacting the usage of the web application.

2.6. Application Server down Scenario

JMeter test plan was executed to simulate 10 users accessing the web application and each user repeated the action 5 times. In a non-error scenario, there were 50 orders submitted, each with 3 order lines. Once the JMeter test plan started, the application server log files or console was monitored. The one showing activity was shutdown 20 seconds later to simulate server crash. The WebLogic app server was shut down by issuing a force shutdown command from its admin console, whereas the Tomcat app server was shut down by executing the shutdown script. This scenario was repeated 5 times, the results were captured, and each time, the database records was reset to initial state and the servers were restarted.

2.7. Database Server down Scenario

The failover from primary database to secondary database was initiated manually using Oracle's command-line utility program. This simulated the unavailability of the primary server. The manual failover was done 15 seconds after the JMeter test plan started.

The preliminary test of the proprietary solution showed that the failover process required more than 1 minute to complete. Therefore, the JMeter was executed to simulate 10 users accessing the web application, and each user repeated the action 25 times. In a non-error scenario, there were 250 orders submitted, each with 3 order lines.

Based on the configuration free open-source solution, mysql_proxy was expected to perform the important role of routing the connection from the application to the primary database server, and route to secondary server if the primary is not available.

3. Results and Discussion

3.1. Session Replication and Failover

WebLogic Application Server.

The user always accesses the web application via the proxy at port 8080 of the Web Server. This proxy server routes the user requests to the appropriate server, which is either ManagedServer1 at port 7051 or ManagedServer2 at port 7052. In this research, it was configured to use "round-robin-affinity" algorithm. Using the example illustrated in Figure 8, if ManagedServer1 is down, User 1 will not be able to access it anymore, and the proxy will actually detect that ManagedServer1 is no longer available. Since there is a replica of User 1's session in ManagedServer2, User 1 can continue to use the web application without any disruption. And the User 1 session in ManagedServer2 becomes the primary session. This process is known as "session failover".

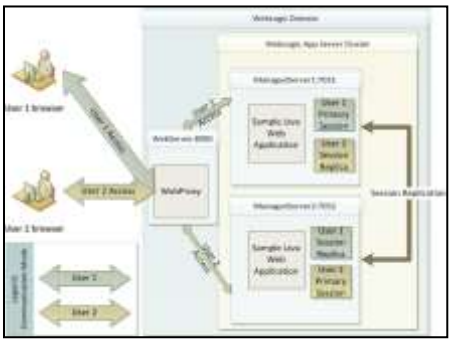

Figure 3. WebLogic Session Replication

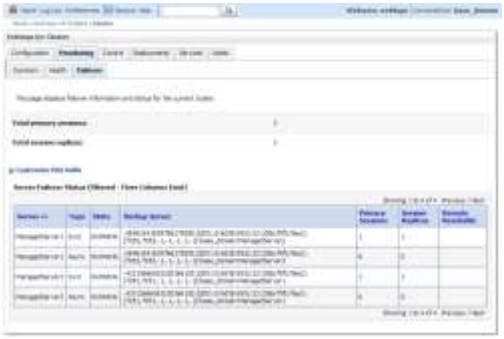

Figure 4. WebLogic Failover Monitoring

The WebLogic Admin console can be accessed to monitor the status of the sessions in the cluster as shown in Figure .

Tomcat Application Server.

In this research, the mod_jk was configured to load-balance with sticky-session. The user always accesses the web application via the mod_jk proxy, which routes the user requests to either Tomcat1 or Tomcat2 server appropriately. Essentially, this worked in the same manner as the round-robin-affinity algorithm of the WebLogic cluster.

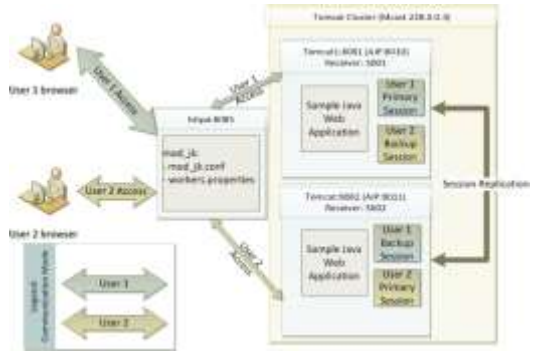

Figure 5. Tomcat Session Replication

Figure 6. Tomcat1 and Tomcat2 Manager Console

However, Tomcat did not have centralized Admin console. It only had Admin console on each instance of the server. Figure and Figure 6 shows the session monitoring page available in the console of each Tomcat instances.

The results showed that the application servers in both the proprietary and free open-source solutions did work properly providing high-availability in term of session failover. Setting up WebLogic was relatively easier as it could be done from the web-based Admin console. Although setting up the Tomcat cluster and Apache Web Server with mod_jk module was rather manual and technical, it could be done by following the guides provided in their websites as well as other related articles in the internet. Thus, one can consider using such free open-source solution as an alternative to proprietary solution at the application server layer.

3.2. Database Replication and Failover

Oracle Database Server

The Oracle database instances were configured for Data Guard. The first database instance called “Prod” was configured as the Data Guard primary Database. Then a Data Guard Physical Standby database, called “Stdby1” was created in a rather manual way. The configuration and control files for the secondary database were created using command line based on the primary database, and the database files were manually duplicated from primary to secondary. Then the secondary database configuration files were altered to become suit the appropriate configuration as secondary database. Lastly, Oracle listener was configured for the secondary database.

According to Oracle documentation, the optional Active Data Guard feature introduced in Oracle Database 11g enables the Physical Backup database to function in read-only mode. Prior to this version, the Physical Backup can only be in “mounted” state, in which query cannot be executed against it. In order to facilitate database failover process, Data Guard Broker was configured for the two instances using DGMGRL. The Data Guard Broker had to be activated in both instances by executing “alter system set dg_broker_start=true” while connected to each instance using SQLPLUS. Then the data guard configuration was creating a configuration using DGMGRL to register the Prod instance as the Primary database, and the Stdby1 instance as the Physical standby database. Manual failover was manually initiated by connecting DGMGRL to the Stdby1 instance and executing “failover to stdby1”.

MySQL Database Server

Two MySQL instances were configured in Master-Slave replication scheme. Two database instances, called Mysql1 and Mysql2 were configured to listen at port 3307 and 3308 respectively. The Mysql1 instance was configured to perform binary logging of selected database. The Mysql2 instance was configured to become

the slave for Mysql1 instance. The replication was also verified when the sample application schema created only in the Mysql1 instance also appeared in the Mysql2 instance.

MySQL did not actually have failover mechanism. But with Master-Slave configuration as this, if the Master server fails, the application can immediately switch to access the Slave database, and resume its operation. The results showed that the database servers in both proprietary and free open-source solutions did have the replication mechanisms that work properly.

Server-Agnostic Java Web Application

In this research, the sample web application was implemented without using any vendor specific feature in the program code. However, there were some difference as described below:

1. When connecting to Oracle database, the web application used the data source at the WebLogic server layer which had been configured to use Oracle JDBC driver. When connecting to MySQL database, the web application used the MySQL Connector/J driver packaged within the web application WAR file. Because the sample web application used the Spring framework, only the data source definition in the Spring configuration file needed to be changed when the database changed.
2. For WebLogic deployment, the web application WAR file included weblogic.xml file that contains WebLogic specific directive.

3.3. Application Server down Scenario Results

Table 1. Application Server down Scenario Results

	Proprietary Solution			**Free Open-source Solution**		
Iteration	**F**	**PF**	**T (s)**	**F**	**PF**	**T (s)**
1	6	0	93.38	3	0	59.46
2	5	1	66.47	2	0	61.41
3	0	0	86.07	8	0	59.58
4	0	0	81.41	8	0	55.73
5	1	0	83.29	0	0	63.21
Average	**2.4**	**0.2**	**82.12**	**14.6**	**0**	**59.88**

F = Failure, where order did not get submitted at all.

PF = Partial failure, where order was submitted, but there were missing order lines.

T = Time required to complete one test iteration.

The results showed that the proprietary solution had an average of 2.4 failures, compared to 14.6 failures of the free open-source solution. However, the time taken by the proprietary solution to complete the test was 1.37 times longer than the free open-source one.

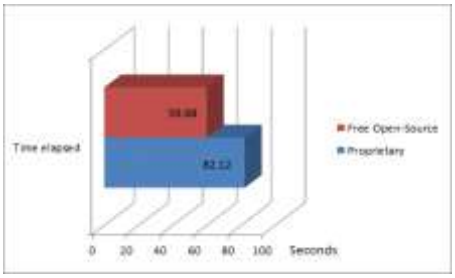

Figure 7. Average Time Elapsed in Seconds

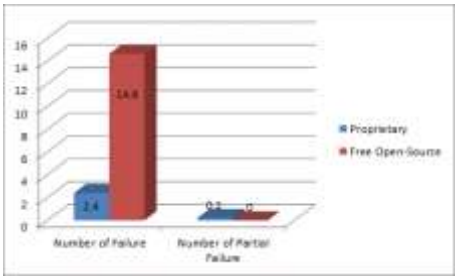

Figure 8. Average Number of Failures When One Application Server Was Down

Based on the result obtained, the availability measure can be estimated.

Table 2. Availability Estimation

	Proprietary Solution	Free Open-source Solution
Average Elapsed Time (s)	82.12	59.88
Average Time Per User (s)	1.6424	1.1976
Estimated Downtime (s)	3.94176	17.48496
Estimated Uptime (s)	78.17824	42.39504
Availability (%)	**95.20**	**70.80**

The results indicated that the free open-source solution performed better in term of speed; but did not perform as well as the proprietary solution in term of high-availability.

As observed in the experiment, in both solutions shutting down one of the application servers did not completely disrupt the users. Thus, one could purposely shutdown one server for maintenance or application upgrade without causing major disruption to user.

3.4. Database Server down Scenario Result

For the proprietary solution, the failover was performed 5 times and the result was shown below.

Table 2. Proprietary Database Server down Scenario Results

Iteration	**Failover Time (s)**	**Failures**
1	48.54	218
2	55.61	244
3	54.43	241
4	55.42	240
5	57.34	245
Average	54.27	237.6

The Oracle primary database on average required 54.27 seconds to complete. Compared to the application server down scenario, the downtime was much longer failure happened to the database server. As the result showed, the number of failures was very high. This was because, during failover, the web application encountered error, and no order could be submitted. Similar test scenario was not performed for the free-open source solution. Because if the primary server was shutdown, no further order can be submitted until

the application was changed to point to the secondary database manually. However, it was also important to note that the secondary MySQL server was always up.

In terms high-availability feature by database replication, both the Oracle and MySQL databases did work as expected. The MySQL Master-Server replication scheme showed better availability as both instances were always up (hot standby), MySQL database definitely can be an alternative to proprietary solution such as Oracle Database. With some application logic or load-balancer or proxy that could control which database instances the application should access, one could potentially orchestrate the start-up and shutdown of the MySQL instances to allow maintenance or schema upgrade with minimal downtime.

This research observed that it was not possible to orchestrate such database start-up and shutdown of the Oracle database instances to allow maintenance or schema upgrade with minimal downtime; because at the same time, only one database instances can be open for read and write operation.

3.5. Cost Comparison

The free open-source solution proposed in this research was completely free to use, including for commercial purposes. Optionally, some of these free open-source solutions had third party consultants if the in-house personnel require extra support. The proprietary solution proposed in this research had price tags in many places. The Oracle products such as WebLogic Application Server and Oracle Database were licensed either per user or per processor [16].

Both proprietary and free open-source solution require hardware and operating system. In terms of monetary cost, it is obvious that the proprietary solution cost much more than the free open-source solution.

4. Conclusion and Future Works

4.1. Conclusion

This research attempted to compare proprietary and free-open source high-availability solution for Java web application using Tomcat and MySQL from capability point of view, and drew the following conclusion:

1. For application server, Tomcat server and Apache Web Server with mod_jk – as part of free open-source solution, can provide high-availability by session replication and failover in cluster like WebLogic – as part of proprietary solution. But it may not perform as well as WebLogic in this aspect.
2. In terms of complexity, both types of solution are equally complex. Some free open-source solutions are also supported professionally and commercially.
3. For the database server, this research concluded that both proprietary and free open-source databases such Oracle and MySQL respectively can provide high availability by data replication.
4. In general, when using free open-source software such as Tomcat and MySQL regardless of the purpose, there are risk involved as they usually do not have guaranteed support. This risk increases as the complexity increases in the high-availability solution.
5. It is very apparent that using Tomcat and MySQL as free open-source high availability solution cost less than proprietary ones in terms of software cost.
6. The availability of the free open-source high availability solution for Java based solution using Tomcat and MySQL has made it much more affordable. However, one should be aware of the risks when using free open-source solution and decide if it is acceptable.

4.2. Future Works

Due to the limited time and resource, this research focused its attention to the application server and database server components of a web application. Some other aspects of the high-availability solutions for Java web application could be further researched. The following are some recommendations for future research:

1. Redundancy for other components of the system, such as the load-balancer and proxy should be studied as well.

2. In addition to standard HTTP traffic, future research should consider high-availability solution for Java web application involving HTTPS traffic.
3. Use separate servers for the system components as well as the test client. This research contained all the software in one virtual machine. Installing the components in separate servers brings the experiment closer to actual production environment, even if the servers are virtual machines.

5. References

[1] "The birth of the Web | CERN." https://home.cern/science/computing/birth-web (accessed Oct. 01, 2020).

[2] D. Helic, "Server-side Technologies CGI, PHP, Java Servlets, JSP," 2004. http://coronet.iicm.edu/lectures/mmis/material/slides_serverside_main.pdf (accessed Nov. 30, 2015).

[3] "Strategic Guide on Web Designing | Learn How to Design Your Own Website." http://wspgweb.com/web-application-development.php (accessed Oct. 03, 2020).

[4] B. Goetz, "Java theory and practice: Are all stateful Web applications broken?," 2008. https://www.ibm.com/developerworks/library/j-jtp09238/index.html (accessed Oct. 05, 2020).

[5] E. Armstrong *et al.*, "Distributed Multitiered Applications," 2005. https://docs.oracle.com/javaee/1.4/tutorial/doc/Overview2.html (accessed Oct. 05, 2020).

[6] Joe Hertvik, "Service Availability: Calculations and Metrics, Five 9s, and Best Practices – BMC Blogs," 2020. https://www.bmc.com/blogs/service-availability-calculation-metrics/ (accessed Oct. 05, 2020).

[7] W. J. Bender and A. Joshi, "High Availability Technical Primer Availability , High Availability , and Fault Tolerance : What do these terms mean ?," pp. 1–13, 2004.

[8] C. Kopparapu, *Load Balancing Servers , Firewalls , and Caches Chandra Kopparapu*. 2002.

[9] P. Soila and N. Priya, "Causes of Failure in Web Applications (CMU-PDL-05-109)," *Parallel Data Lab.*, 2005, [Online]. Available: http://repository.cmu.edu/pdl/48.

[10] Newrelicblog, "The Death of WebSphere and WebLogic App Servers? New Infographic shows the Rise of OSS Java - New Relic Blog," 2012. https://blog.newrelic.com/product-news/infographic-oss-java-wins-in-the-cloud-era/ (accessed Sep. 15, 2020).

[11] SolidIT, "DB-Engines Ranking - popularity ranking of database management systems," 2020. https://db-engines.com/en/ranking (accessed Nov. 01, 2020).

[12] I. Free Software Foundation, "What is free software? - GNU Project - Free Software Foundation," 2019. http://www.gnu.org/philosophy/free-sw.html.

[13] Opensource.org, "The Open Source Definition (Annotated) | Open Source Initiative Version 1.9," 2007. https://opensource.org/osd-annotated (accessed Oct. 20, 2020).

[14] JRebel, "2020 Java Technology Report | Rebel," 2020. https://www.jrebel.com/blog/2020-java-technology-report (accessed Sep. 15, 2020).

[15] M. Sprava, "Open source database market share within Jelastic: February 2012 | Jelastic," 2012. https://jelastic.com/blog/open-source-database-market-share-within-jelastic-february-2012/ (accessed Oct. 20, 2020).

[16] Oracle, "Oracle Technology Global Price List Software Investment Guide," pp. 1–13, 2012, [Online]. Available: http://www.oracle.com/us/corporate/pricing/technology-price-list-070617.pdf.

9 772355 020149

SWISS GERMAN UNIVERSITY
The Prominence Tower
Jl. Jalur Sutera Barat No. 15,
Alam Sutera, Tangerang
15143 Indonesia
E-mail: *marketing@sgu.ac.id*