ABSTRACT

Computer center can be defined as an area that provides several computer services to employees. In information technology audit and control, it is important to present computer center controls that help to create a secure environment. This is because computer center plays an important role to the company and contribute much of information and data storage to the company. So, it is important to protect and ensure the computer center is secure. This study will focus on the development of prototype for computer center. It can be used as a guide for very small enterprise IT company in Malaysia to design the computer center in their company by following the concepts in information technology audit and controls.

Keywords: Computer center, information technology audit and control, data center.

1. INTRODUCTION

We are required to develop one computer center model that follows the computer center controls. Some considerations that we must take are physical location, construction, access, air conditioning, fire suppression and power supply. We need to highlight various things such as their strengths and several related problems.

This computer centric model can give people some idea on how to arrange and locate their computer services center. Computer center is important to be planned because this is the place usually all types of data is located and stored. Computer center need to be secured to ensure that each of hardware, software, and data is safe and protected from any malicious intent or any disaster that might occur anytime [1].

This paper will discuss about the development of the computer center model for very small enterprise. The model has been design based on the some of the control’s objective in information technology audit and control concepts.

Part 2 of the paper will discuss what are the main objectives of computer center control. Part 3 will provide a description of the project. Part 4 of the paper will discuss about the controls applies in the development of computer center model. Part 5 mention about the strength of the model and Part 6 deals with the summary of the paper. Part 8 shows the computer center model that has been developed.

2. OBJECTIVES OF COMPUTER CENTER CONTROL

Based on Hall, J.A and T. Singleton (2005), the objectives of applying computer center control are:

**Integrity of the information** - Controls are designed with the objective of ensuring the integrity, confidentiality, and availability of information. Data, the principal component of an information system, are processed, sorted, categorized, summarized, and manipulated to provide information for the decision-making process. Management relies on the integrity of a system’s data and programs in making critical decisions. Controls that allow management to make decisions based on bona fide information processed in a controlled environment are critical. In order to ensure the integrity of information, the auditor should
evaluate controls over data, transactions, and programs.

**Security** - Security of computer systems is an important concern in most organizations and includes protection of hardware, software, and data from unauthorized access and use. Controls should be in place to safeguard information system assets against loss or destruction and to promptly identify when such loss or destruction has occurred. Controls should limit access to data and programs to individuals authorized to operate or maintain specific systems. Appropriate controls should also be in place to limit access to computer hardware. In order to ensure the security of computer systems, the auditor should evaluate data, physical, and program security controls.

- **Data Security and Confidentiality**
  Access to data, an important asset, should be limited to those individuals who are authorized to process and maintain data or who are responsible for specific data and records.

- **Physical Security**
  Access to the data center and related assets should be limited to those individuals such as management and operations staff requiring access to perform their job functions. Access to the computer room should be monitored and controlled using card access systems or thumbprint. Physical safeguards should also include fire prevention, insurance, preventative maintenance, and inventory control over data files such as magnetic tape, disk, CD-ROM and others.

- **Program Security**
  Access to program files and libraries should be restricted to authorized personnel through the use of security software. Program updates should be monitored and controlled using library management software. Appropriate segregation of duties should be established to ensure that the programming function does not have unrestricted access to production programs.

**Compliance** - Failure to comply with the various internal and external procedures and regulations could adversely affect the organization. Viewed from a public standpoint, compliance or non-compliance has an impact on how the organization is perceived to run its business. Controls are necessary to ensure compliance with the following:

- **Laws and regulations** at the international, federal, state, and local level, as well as any specific industry-related regulations and tariffs.
- **Auditing standards**, regarding the conduct of audits, as established internally, as well as by The Institute of Internal Auditors (IIA), the Canadian Institute of Chartered Accountants (CICA), the American Institute of Certified Public Accountants (AICPA), other authoritative bodies, and any other locally prescribed practices.
- **Policies and procedures** developed internally for each of the organization’s functional areas.

### 3. PROJECT DESCRIPTION

This computer center model is designed for very small enterprise IT companies. The IT company can be divided into three sizes, namely (1) Very Small Enterprise: VSEs, having the number of person 1-25 persons; (2) Small Enterprises having the personnel from 26 to 100 persons and (3) Medium/Large Enterprise having upward of 100 employees [2].

For security purposes, we provide security systems which use close circuit television (CCTV) and thumbprint device. CCTV is TV system that does not broadcast TV signals to public but transmits them over to limited monitor. CCTV is applied for to the security and surveillance which the purpose is to monitor the flow in and out at the main area. In this model, the CCTV is providing at the second main entrance, server room and at the documentation and file storage room.

For the thumbprint, it also provides at the second main entrance, server room and at the documentation and file storage room. The purpose of this thumbprint device is for access control. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. The objective is to monitor and control who are authorized to enter in the office or the room.

To monitor the door position a magnetic door switch is used. Request-to-exit devices can be a pushbutton or a motion detector. When the button is pushed or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door.

Beside that, for the safety we put the fire alarm system at the electricity room and at the documentation and file storage room. The purpose is to detect if any incidents happen. The system will
sound an alarm if it detect there is any smoke or if the temperature at the electricity room high.

This model is design where all the main room such as server room, documentation and file storage room and electricity room are placed at the back corner. The idea is to avoid the main room from the work and public area which all the staff or people entrance. This computer center control model also has three exit entrances which can be used if any incidents happen. One of the exit doors we put nearby to the main room.

To consolidate more security feature at the model of computer center control, we put the several fire extinguisher at the placed which suitable for the security. The purpose is to facilitate if any incident happen.

4. CONTROLS FOR COMPUTER CENTER MODEL

**Physical Location** - The physical location of the computer center directly affects the risk of disaster and unavailability. The computer center should be away from human-made and natural hazards. Our computer center’s system is located at the third floor of a multi-storied office building.

**Construction** - Site location and the construction of a building and the data center have an impact on the risks to systems. The computer center should be a protected area within the building. All the utility and communication lines should be underground.

Communications in computer center is based on networks running the IP protocol suite. Computer center contains a set of routers and switches that transport traffic between the servers and to the outside world. The connection of this network is based on bus network topology where connected via a shared communications line.

**Access** - Access to the computer center should be limited to the operators and other employees who work there. Physical access control is essentially a perimeter control, should be employed to limit access to the center. There are 2 devices involved in accessing to our computer center which are biometric thumbprint device and closed circuit television (CCTV).

The biometric fingerprint devices are located at 3 places where they are at the second entrance after through receptionist room, the server room entrance and the storage room. This biometric device allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual.

Then, there are 3 places that the CCTV were located which in the receptionist room, server room and file and documentation storage room. CCTV is used to monitor areas to detect incidents and record events for use as evidence and to inform investigations.

**Air Conditioning** - Air conditioning is used to keep the room cool. It may also be used for humidity control. The primary goal of computer center air conditioning systems is to keep the server components at the board level within the manufacturer's specified temperature or humidity range. This is crucial since electronic equipment in a confined space generates much excess heat, and tends to malfunction if not adequately cooled.

**Fire Suppression** - Every computer center needs to have fire prevention and fire extinguishing systems in order to prevent and avoid from any loss. There are 2 fire alarm systems that are located in electrical room and storage room. This fire alarm system should be connected to permanently staffed fire fighting stations. There is also fire extinguishing system that dispenses the appropriate type of suppressant for the location. Manual fire extinguishers also are placed at every section in the computer center.

**Power supply** - In our computer center, we use Uninterruptible Power Supply (UPS) system which provides electrical power to the computer center in case of commercial power failure. It acts as a battery backup which maintains a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available. This UPS system will also protects against unexpected surges in power that might damage the data processing equipment in the system.

5. STRENGTHS

The computer center model that we have designed has made the security as the main aspect to be considered while design because we notice that as a computer center it is very important to have a secure environment especially from disaster that might occur in the future. In our design we have design the computer center to have three emergency exits so that if anything occurs, there are several ways for the worker inside the center to safe themselves and things inside the center. Apart of that, the strength of our design relies on the other security aspect to safeguards the center itself. We design the center to give the person in charge at the reception side to control the entrance so that none of people can get easily access to the portion inside the
computer center. As for security purposes also, we equip the center with thumb print technology so that only authorized person have access to certain parts inside the center, for example the server room which is the very important place to be safeguards.

6. CONCLUSION

This paper explored operation control related to the structure of the control of computer center operation. The purpose of the control of computer operation is to create a secure environment. For our model, we look some of the control that contributes directly to the security of the computer center environment such as physical control, construction, access, fire suppression and power supply. All of these controls are important to avoid from disaster that can disrupt or destroy the organization’s computer center. There are three types of disaster that always happened in organization computer center which are natural disaster, human-made disaster and system failure.

For our model, we decided to place computer center at the third floor because to avoid from any disasters happen such as natural disaster like flood. In our computer center we provided two meeting room, pantry, toilet, reception, two manager room, server room, electricity room, employees’ area and utilities room. A systematically arrangement of each rooms and others part in the computer center can make an employees easy to move anywhere and do it their works.

7. REFERENCES
