CHAPTER II :LITERATURE REVIEW

2.1 Introduction

This chapter concentrate on the literature review related to this study. The previous concepts and studies related with this study were discussed briefly. This chapter extensively discuss the concept of IT infrastructures and services which including the definition, the issues of IT security management in IT infrastructures and the rationale components of IT security maintenance framework implementation.

2.2 Initial Work on Information Infrastructures

Henderson & Kyng (1992), from the area of Participative Design, proposed the term "tailoring" to describe the very practical types of rework required to enable workplace information technology to operate inside a specific organizational context. They demonstrated how sophisticated organizational technologies had to be dismantled, broken down, modified, and reconfigured before they could be helpful to a company (Greenbaum, & Kyng, 2020). Henderson and Kyng (1992) claimed that this demonstrated how technical progress was carried out in the latter phases of implementation and usage, and suggested the term "continuous design in use" to describe it.

The significance of this idea which was not explored further in Computer-Supported Cooperative Work (CSCW) that it provided an early hint of how design might be extended out in space and time. After a few years, Karasti et al. (2010) revisited and tried to expand this concept. They said that the CSCW's focus on short-

term temporal elements of workplace technology was at the cost of a longer-term perspective, which they viewed as critical when engaging with any type of changes.

They tried to blur the lines between design, implementation, and usage, as well as subsequent phases like maintenance and redesign, based on Henderson and Kyng's work. They coined the term “continuing design”, which is described as a “development orientation in which the relationship between short and long term; traditionally seen as a tension which is addressed and accounted for from the perspective of infrastructure time by incorporating it as a foundational design consideration” (Henderson and Kyng, 1992). They claimed that this reorientation was essential since its operate on different timeframes than conventional IT projects.

Unlike conventional IT projects, which last three to five years and are referred to as "project time," seconds last decades and are referred to as "infrastructure time." Their study raises the issue of how CSCW type analysis could concentrate on extended temporal scales and other IIs-related peculiarities.

According to Edwards et al. (2007), problems in aligning entrenched disparities across local systems create pressures of competition or accommodation between systems, which may be alleviated by the development of 'gateways’, which enable numerous divergent systems to interact. Tensions and differences between local systems may eventually result in pressures that force periodic modifications and redevelopments to suit changing internal and external conditions (Ribes and Finholt 2009). As a result, infrastructure advancement need simultaneous efforts on many fronts. Infrastructure design, for example, must act as a connection forwards to future expected users/uses. Simultaneously, infrastructure deployment necessitates the construction of functional bridges between the e-general infrastructure's characteristics and the specific locations where they are used. In this regard, Ribes and Finholt (2009) emphasis that people

attempting to start, develop, and build infrastructures must combine the ‘demands of the present' with those envisioned as essential in the ‘future'; which they refer to as ‘The Long Now' (longue durée) after Wallerstein (1998). Their essay highlights how infrastructure expansion efforts are often unexpected and prone to failure. Today's sought-after future-proof systems, which aim to serve all purposes, even some not yet imagined in often end up as tomorrow's legacy systems.

2.3 Literature Review Knowledge Framework Overview

Literature review framework is about the topics that will be cover in this chapter in genaral overview. The study of literature begin with the core of this research knowledge which is about the Information Technology (IT). Then, within this topics, literature review had covered the topic of IT infrastructure and IT security.

In the topic of IT infrastructure, it consist of subtopics which is IT infrastructure requirement, IT infrastructure planning, IT infrastructure governance and IT infrastructure limitation. For the topic of IT security, it consist of subtopics which is IT security risk, IT security offensive protection, IT security offensive detection, IT security management and IT security maintenance.

Hacking, viruses, and other kinds of cybercrime have become a significant worldwide issue in recent years, with a rise in recorded instances of hacking, infections, and other forms of abuse. Although computer crime has existed since the dawn of computers, the difference today is the greater breadth accessible to would-be attackers, owing in large part to the Internet's ubiquity. The many advantages that the Internet and, by extension, the World Wide Web provide have led to broad popular acceptance. At the same time, its increasing use has exacerbated the difficulties that come with it, and there doesn't seem to be a day that goes by without a cybercrime event of some sort being recorded (Hadlington, L., & Chivers, S., 2020).

The following Figure 2.1 is about the summarization of topics cover for literature review in this chapter.

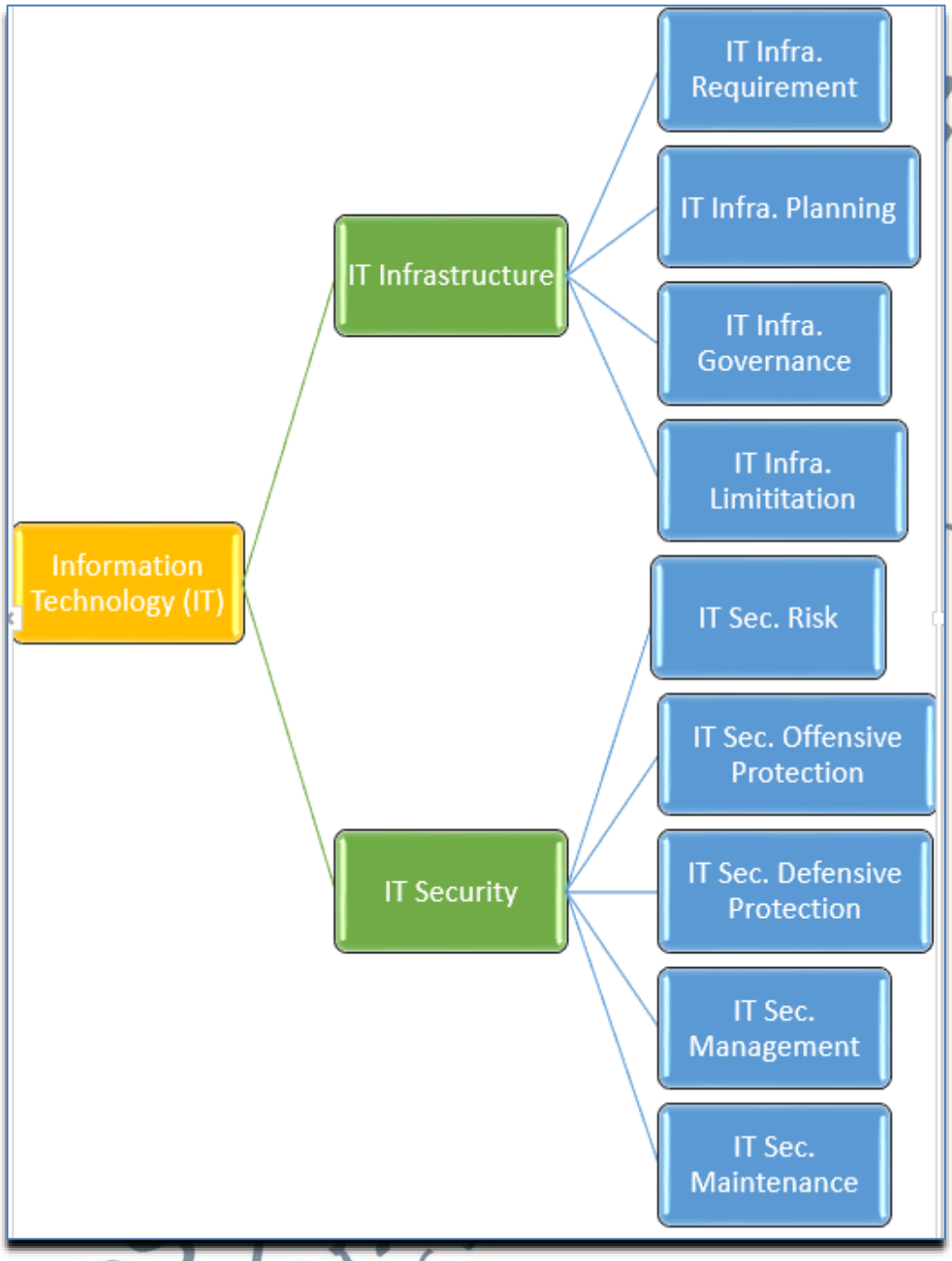

Figure 2.1: Topics Cover in Literature Review

2.4 Information Technology

The development of technology for information technology infrastructure which is very fast in producing a wide range of computer products cause some medium sized organizations are confused and ambiguous as to what should be done to the

infrastructure of information technology (Laudon, 2012). This resulted in tragedy 'white elephant' where infrastructure is purchased by the organization were not fully utilized or not used at all (Kulikova et al., 2012). This ambiguity is likely due to the lack of control or it does not give the impression and clear benefits to business activities and organizational management (Straub & Welke, 1998; Tu & Yuan, 2014).

When it comes to information infrastructures, the concentration is on four factors. Infrastructures are community-shared resources; the various components of an infrastructure are incorporated through standardized interfaces, open in the context that there is no hard limit between what is included with the infrastructure and what is not, and who can use or for what intended function; and they are diverse, consisting of various types of components whether on human aspect as well as technological.

A common resource amongst diverse groups of consumers develops as infrastructure. This is in contrast to artifacts like as Microsoft Word and Excel, which each user has their own private copy and may use freely. The gap between word processing software and the Internet's e-mail infrastructure exemplifies this disparity. Each user of a word processor has their own copy, and the usage of one user's system does not affect the use of others. The Internet's e-mail infrastructure, on the other hand, is a shared resource for all of its users. All e-mails are sent and received via the same network. Furthermore, how one user interacts with the infrastructure may have an impact on other users. If a single user transmits a large quantity of data, the network may get congested, causing difficulties for everyone else.

Individual actors often purchase various elements of an infrastructure on their own. Responsible must be compatible in order for the entire infrastructure to function. As a result, defined interfaces (protocols) between modules are essential for the construction of infrastructures. Infrastructures are open in the idea that there are no

restrictions on the number of users, computers, or other technological components that may be connected to them. Infrastructures are diverse socio-technical networks that include a wide range of networks including both technical and social players.

The worldwide TCP/IP network, for example, is made up of many sub-infrastructures: e-mail, news, and web infrastructures. These networks may be seen as distinct infrastructures in certain ways. However, many new infrastructures, such as those enabling electronic commerce, are constructed on top of and integrate these disparate Internet sub-infrastructures, resulting in heterogeneity. They are, nevertheless, diverse in that they include non-technological components. The Internet, for example, entails the efforts of a huge number of support workers. The Internet would not function without them (Hanseth, O., & Lundberg, N., 2001).

As a result, the information technology infrastructure requirements of campus sized businesses will be examined in order to address this issue. Plans are made to the infrastructure of information technology is not simply to facilitate commerce and organization but it must be in line with the mission and objectives of the organization (Stoneburner & Goguen, 2002; Turel etc al., 2017).

Such planning should be in terms of information technology needs of an organization. Next, it seeks to be implemented and operated well for the success of an organization, whether it is for profit or social service.

2.5 Information Technology Infrastructure

The necessity to construct a medium-sized information technology infrastructure necessitates a high cost of failure in order to ensure that the infrastructure operation's downtime is kept to a bare minimum. The complexity of information

technology is constantly evolving further complicate the process of implementation of information technology infrastructure in a medium-sized organization. However, it should be balanced with the vision, mission and objectives of an organization.

This requires careful planning for the short and long term period in implementing the medium-sized information technology infrastructure. This study only focuses on campus-sized organizations only. However, it can also be applied to small and large sized organizations as appropriate surroundings. Information technology strategic plan should be provided to achieve a balance between the comprehensive implementation of information technology infrastructure with business planning within the organization (Sarriegi and Santos, 2008; Turel etc al., 2017).

Implementation of information technology infrastructure in their organizations do not plan or soon to be avoided. This is because an organization will evolve over time. So, there will be little growth the size of the information technology infrastructure such as increasing the number of employees, increase the number of transactions in a given time, increase the number of computers and servers and so on.

If the implementation is made without planning, disruption to the business activities of an organization of moderate size will occur. Usually, this is rare in the new organization but these problems will arise when an organization has been operating for more than ten years, or even earlier than that. There is two types of IT infrastructure requirements which is physical requirements and logical requirements.

2.5.1 Physical Information Technology Infrastructure Requirements

Generally there are three main physical requirements in an IT infrastructure, including hardware, software and communication network as illustrated in Figure 2.2.

It also know as an IT assets. It should be known at an earlier stage of development infrastructure as these can explain what is necessary and not necessary for implementation an information technology within an organization (Bourgeois, 2014).

Physical needs for information technology hardware specifications include minimum, maximum or optimum for personal computers, laptops and computer servers used in an organization (Bourgeois, 2014; Nwankpa J. K. & Datta P., 2017). The use of information technology hardware are also involves specification for thin client or workstation computer as needed along with the physical specifications of the server subscribed as a IT service providers (Sveen and et al., 2007; Nwankpa J. K. & Datta P., 2017).

Specifications for a hardware necessary according to the application or software used in medium-sized organizations to avoid problems such as the frequency of failed time (down time), failure of physical components, computer server that is not functioning properly and others (Hovav & Arcy, 2012). In addition, the need to set the specifications of the physical requirements at either the minimum, optimum or maximum. It should be parallel with the use of computer software and information systems.

Along with the specification of the physical needs of the information technology, the impact and the costs need to be analyzed and drawn together (Tan et al., 201). Increased IT infrastructure demand, on the other hand, may only be possible for a dominating corporation or a successful cartel, whereas the other reason entails lower performance targets as well as additional expenses, such as higher inventory and increased organizational complexity (Child, 2018). In light of this literature we hypothesized that:

H1: IT assets significantly positive influences the IT infrastrucure for IT security maintenance.

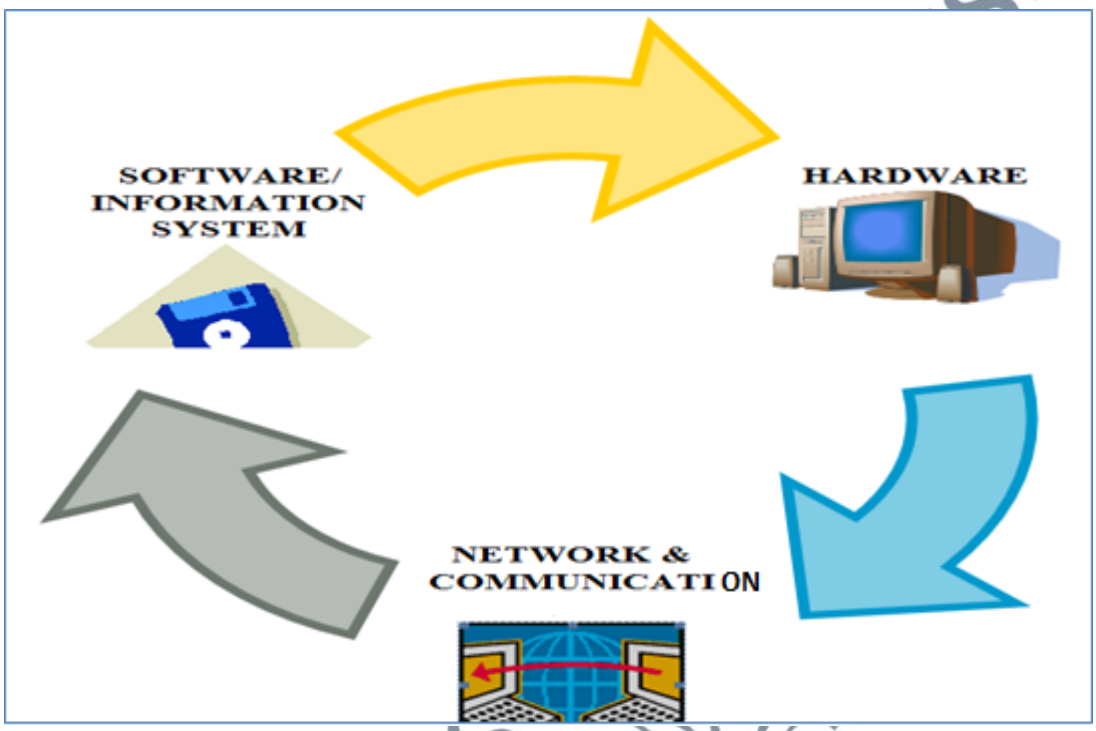

Figure 2.2: Physical of IT Requirements

Those for achieving the hadware elements is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H1a: Hardware significantly positive influences the IT assets of IT infrastrucure for IT security maintenance.

Requirements in terms of use of the software for a medium-sized organizations are highly critical. It requires sophisticated software such as Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) business information technology solutions for their medium-sized. Implementation of ERP and CRM software like this can manage data organization soundly and safer. This can reduce the problem of security and the failure of information technology functions such as data

compromising's problem, issue or Windows operating system is not functioning well and others.

In common-purpose computing portals like desktop computers, the machinery is made up of numerous parts, each of which has a significant number of national items (e.g., configuring registers) that govern its function. Furthermore, the parts communicate with one another through a variety of control communications. We must guarantee that an adversarial cannot influence or view any state components or control signals such that a security goal (e.g., confidentiality, integrity, availability, etc.) is breached or a protective device is circumvented in order for the hardware to operate securely.

Consider kernel-level crypto brain chemicals, which execute all computations in the kernel space (e.g., Microsoft Cryptography API: Next Generation, Linux Cryptographic API). The secret key is kept in files inside the kernel space by the kernel (running at Ring 0 privilege) and are shielded from user-level programmed (running at Ring 3 privilege) via a mixture of page technique and processors privilege mode segregation in these systems. Memory access requests from a direct memory access (DMA) peripheral device, on the other hand, are not limited to the page mechanisms authentication. (Potlapally, 2011).

For decades, hardware has been regarded as the primary protection for security-sensitive activities. This may be seen in the long-standing usage of hardware security modules (HSMs) for crypto processing, such as the tamper-evident/resistant IBM Crypto cards, and the more recent interest in protecting sensitive processes using trusted computing technologies like Intel SGX and ARM Trust Zone (Tudosa, et al., 2019)

Physical verification is a more manageable issue than software verification because machinery is more consistent. Nevertheless, many of the problems are distinct,

and others in firmware may be far worse. Pointers, for particular, are notoriously hard to cope about properly, and several ‘‘verifiable" languages, such as Gypsy, forbid pointer operations. Coordinates, on the other hand, are simply references that are used extensively in physical processes. As a result, enforcing address manipulating integrity is critical to the formal handling of hardware. Secure cryptographic hardware provides precisely this kind of control. A basic base and limits system can ensure that a project's memory access does not exceed its allowed limits. As a result, the physical processes offer fundamental structure that can be depended on by the validation of greater safeguards constructed on top of it (Young, 1991).

Those for achieving the hadware elements is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H1b: Software significantly positive influences the IT assets of IT infrastrucure for IT security maintenance.

Software requirements for information systems solutions for a business problem is obvious because it is based on transactions and business processes involved, such as the sale and purchase, registration, payment and so on. However, the requirements in terms of physical infrastructure to run the process and the business transaction or as a platform, usually is not obvious and less ready for mid-sized organizations. In reality, it's very important as a platform for software or system information to move quickly to complete the transaction, process and business problems.

By adopting common methods such as penetration and patch4 and inputs screening (seeking to prevent harmful input) and adding content in a proactive way, security architecture comes easily from a web security strategy. To put it another way,

access control is mainly concerned with identifying and correcting identified security vulnerabilities after they have been exposed in deployed systems.

Software authentication is the protection of identifying and eliminating flaws in software by planning, developing, and evaluating it for security. In this manner, computer security professionals try to create technology that can actively resist assault. Let consider an example: while monitoring HTTP traffic as it comes via port may help prevent SQL injection attacks, fixing the faulty code and avoiding the session token altogether is a better strategy (Morrison et al., 2018).

All across the project lifecycle, safety is a constant concern in Security Development Life Cycle (SDLC). Fault minimization is necessary for safe software design, but it is not sufficient (Hall et al., 2011).

Supplying key demographic for an application program's safety is a hard process because: (1) lack of efficient methods and parameters of software security risk; (2) security must be regarded from the oldest stages of design, but may not become apparent until the software is in use; and (3) the people who construct and then use the operating systems must be taken into account when estimating security risk. System security is aided by several aspects of the project life cycle. Pfleeger and Cunningham (2010) look at a variety of topics, including system definition, protocols testing, and the behavior of computer programmers, users, and hackers. Because of the number of dimensions, a diverse set of metrics is required to adequately describe security for evaluation and predictions.

Those for achieving the hadware elements is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

H1c: Information System significantly positive influences the IT assets of IT infrastrucure for IT security maintenance.

There are needs in terms of network communication where it involves hardware and software. It is more focused on the technology used for data communication in a computer environment. Software and hardware used should be capable of supporting communication network technology used by mid-sized organizations (Park et al., 2008). Examples of network technology is Ethernet.

Nonetheless, coping with such obligations in the fast-paced and increasingly controlled world wherein we operate continues to be a challenge. Every business that wants to thrive in today's connected society must have Information System (IS) protection and Risk Management (RM). Companies often adopt a management framework based on an Information System Security Risk Management (ISSRM) approach for a variety of reasons, including regulation, commercial growth possibilities, and even management enhancement (Mayer et al., 2019). However, handling with ISSRM effectively is becoming more challenging. In a nutshell, the following are the major concerns:

• The complexities of today's information systems, which are also ever increasing

• Managing an ever-increasing amount of risk-related laws (Mayer and Feltus, 2017).

Those for achieving the hadware elements is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H1d: Network and communication technology significantly positive influences the IT assets of IT infrastrucure for IT security maintenance.

Strictly speaking, all physical requirements of hardware and software, especially the operating system such as Windows should support and work well in this data communication network technology. Specification used for software, hardware and communication networks should be balanced and supportive of each other.

2.5.2 Logical Information Technology Requirements

Logical needs of information technology is something that is abstract, namely regarding the governance of information technology. Among them is the cost, staff and policy as illustrated in Figure 2.3. It is these elements that support and management is essential to ensure that information technology infrastructure facilities can be used at an optimal level. Thus, the use of information technology to work to improve profitability and reduce business operating costs.

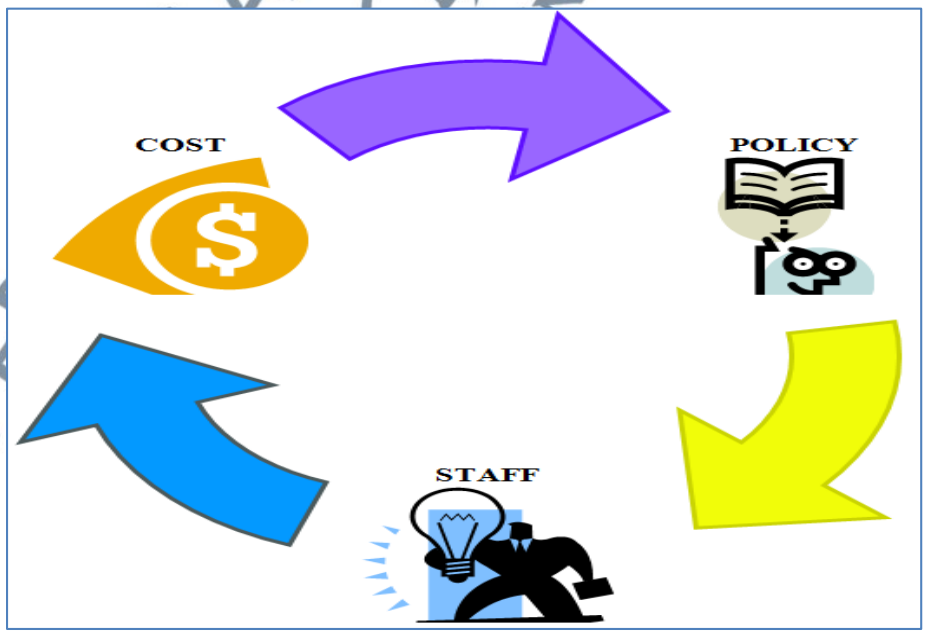

Figure 2.3: Logical of IT Requirements

Costs, staff and the policy as well as the physical needs of information technology which it is interdependent and support each other. With regard to cost, convenience technology available information should not only be used to solve the problem trivial in business but it should help improve the productivity and quality of an organization.

Cost is an issue that is very critical and sensitive because it is an expense for an organization. For a medium-sized organization, it is necessary to calculate the Return of Investment (ROI) that a comprehensive review of a purchase or implementation of the project for an information technology infrastructure.

With regard to the staff or employees in a department or unit of information technology, they usually spend a lot of time to solve the problem of information technology fiddling like virus problem, data entry errors, correction format document files, lost password, and so on. All of these important issues to be addressed in the organization, but some of these problems can be handled by employees involved. This can be done with the help of information technology to hold exercises and settlement procedures to all employees involved in the organization (Nwankpa and Datta, 2017).

It would be better for the organization medium-size this focus group employee information technology to improve organizational capabilities in business activities that can reduce costs and improve profitability, such as increasing service use of information technology by customers, resulting in an information system that helps business activities, the use of information technology for promotional purposes effective, efficient customer service and so on. The employment of workers for the organization also needs to have a good basic computer usage (Nwankpa and Datta, 2017).

Next in respect of policies developed by the organization, especially for the field of information technology, it should be smart, easy to understand and long term usage. It is important to ensure the continuity and travel information systems and information technology infrastructure in the organization running smoothly.

Employees who provide information technology support services for the computers of the server and the end users of information technology is having one of the best human resources to maintain the quality of service. These guidelines require the recruitment of information technology by the human resources for the organizations involved that meets international standards (Franceschini and Galetto, 2006; Haes et al., 2017).

Similarly happen to the maintenance policy for information technology infrastructure. The maintenance policy for information technology infrastructure must have a Service Level Agreement (SLA) which is a maintenance agreement that is constantly updated and applied without having to buy new equipment or expand the size of the central infrastructure of existing data storage (Vance and Siponen, 2012).

The key importance of information technology is applicable to meet the needs of customers ranging from internal and external organizations involved (Siponen, 2005; Haes et al., 2017). For example, if a customer organization wants to visit the website of the organization, but the site is always problematic and repeated problems occur. In this context, it can not meet the needs of customers well even gives a bad image to the organization.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

2.5.3 Information Technology Infrastructure Planning

The design of a medium-sized information technology infrastructure is vital to achieve the effectiveness of its use in the long term, governance and boost the productivity and quality of business in an organization. Whatever something to plan beside the IT infrastructure, planning is requires a thorough understanding of the fundamental things or not an inherent or otherwise (Khurana and Basney, 2009; Haes et al., 2017).

In designing the IT infrastructure, implementation of existing information technology in the organization needs to be clear as like a critical information systems used in the process of transactions, existing data transactions stored along with the growth forecast for a period of time such as five years, ten years and more, the number of users who use the information system along with the forecast increase in its use in the future, inventory information with respect to sources of information and the use of traffic in network communication such as e-mail with the expected increase in future (Arora and Hall, 2004; Héroux & Fortin, 2018).

The management structure of the components in information technology such as information technology resources, user information systems, business information systems or business data needs to be managed properly by the information technology infrastructure (Khurana & Hadley, 2010). All four of these components play an important role in achieving the aspirations of the organization in the field of business or any operations. The productivity of a business can be improved and the cost of business operations can also be reduced.

All of the components of the information technology infrastructure which needs to be implemented in the present and expanding development needs for the future. Planning and good governance in the information technology infrastructure provides a good impact on the data, information systems, users of information systems and resources of IT infrastucture.

The design of a medium-sized information technology infrastructure can be built to meet business demands, prolonged and implemented efficiently. Aspects of management, communication and security can be designed together, total, vulnerable and strong.

The productivity of employees, particularly in the field of information technology can be improved by creating systems that can run automated of computerized. The systems that can be automated and computerized will reduce errors which is often made by humans and will speed up the implementation time.

Policy regarding the usage and implementation of information technology infrastructure in medium-size can be created with a better and smart way, especially regarding the ethical usage of computer applications, usage of data and information technology which facilities available in the organization such as an e-mail, the Internet, information systems, computer applications and others (Melara et al., 2003; Héroux and Fortin, 2018). Training for the IT staff can be managed with more structured, easy to understand and good control by the organization.

2.5.4 Information Technology Infrastructure Governance

The problems that arise from the not well planning in IT infrastructure will result in not good governance of IT infrastructure. The components of IT infrastructure are

available in a separately but in certain situation, there are requirements for these components to combine or meet each other. This problems will triggered the unstable and complicated situation in information technology management.

Data is an invaluable asset to any organization as it plays an important role in implementing the processes and transactions of the business within an organization. If it is not administered properly, especially the data which obtained from information systems such as Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Financial Information System and others, flaws will occur in the entire of the information system for the organization (Blank and Gallagher, 2012).

This situation can be happen due to the not well designed provision of IT infrastructure platform. Those an example like the storage of the server does not have a good method of control and to secure the data in tandem within the increase quantity of data that must be stored (Straub, 1990; Héroux & Fortin, 2018).

This imbalance will become more complicated by the inherent security problems of on-line information system and the use of internet technology by employees in the organization. The internet will reveal cyberspace of organization into a cyber situation that is not known about who will access it especially some one from outside. Low level of IT security impelementation inside the organization to the cyber environment will facilitate the spread of the virus, hacking, spam and others (Siponen and Willison, 2009; Héroux & Fortin, 2018).

Lack of security aspects in IT infrastructure will allow the occurrence of the problems like high frequency of failure, loss of important data, issues of privacy, data theft and others. These problems need to be dealt with promptly by IT staff of the

organization. If not, the time for them to act in a more productive to help the business processes of an organization will decrease (Vulreport, 2015).

Another problem that arises is that it will cause digital communication problems mainly through communication technologies medium such as an e-mail due to the e-mail server fail to function or not function very well. In a medium-sized corporate organizations, e-mail is an important communication tool for many business tasks such as giving the orders, delivery reports, form requests, confirmations and other things. With that, likened the other situation such as an e-mail failure including the failure of other tools of communication such as video conferencing, telephone line or VoIP and others.

Non governance practices of the management in IT infrastructure will have a negative effect in the implementation of pro-active planning of IT infrastructure (Bashir and Kesan, 2011). Next, it will become a constraint in terms of execution time is limited and requires a long time of IT infrastructure operations. Also, the constraints of high cost implementation and maintenance cost is also will be higher.

2.5.5 Information Technology Infrastructure Limitation

Management practices without information technology infrastructure planning will result in issues that can be identified clearly as the use of poor quality products, unmanaged systems, security issues, safety issues and integration issues (Sunyaev and Tremmel, 2009; Birk and Wegener, 2011). As discussed previously, the balance between physical needs in IT infrastructure such as hardware, software and network communications will not take in place. This is among the factors causing imbalance in implementation of IT infrastructure.

Usage of the non quality software and hardware are happens because of unwell managed and implemented hastily. Software and hardware purchased from a supplier of information technology within different purchasing time can cause problems in the functionality between hardware and software (Buyya and Vecchiola, 2013). This is because the production of any IT infrastructure components was not the same between the manufacturers.

Within that, it will cause main problems in the integration of IT infrastructure's components. Similarly, production of different products can cause of integration and support issues will arise as the updating of information technology products are very quickly updated with new versions. Thus, the problem of integration between new information technology components or products to an old IT infrastructure will occur and derived the problems (Birk and Wegener, 2011).

Management of information systems and existing software in an organization which is done separately, such as configuration, interfaces and tools used is a way of not good governance in IT infrastructure (Bang and Lee, 2013). Those, it can cause problems to the IT staff training because too many differences IT products exist and should be known by every staff in the operation of IT infrastructure.

Another most important issue that arises from not well planning of IT infrastructure is a low level of security implementation. Unsecured IT infrastructure happened because of too many differences between one another within IT services and components. Then, the situation will complicate the process of security updates to the information system or software because of the the differences. Each IT services and

components requires a different updates and at the different times according to the information technology products manufacturers or suppliers (Rahman, 2014).

The integration between the components of the IT infrastructure is essential to facilitate the process of cooperation between the components. The integration can reduce the cost, the usage of high profiles human resources but increase security aspects of IT infrastructure. Then, integration aspects also facilitates the operation to be done in IT infrastructure (Rahman, 2014).

As a conclusion, the lack of planning for the implementation of the information technology infrastructure in moderate size can cause of variety problems. The entire of IT infrastructure should be flexible, easy to integrate with each other, can be expanded according to the organization's development, centralized security management and so on. Not well planning of IT infrastructure will create a situation that is very difficult to manage and not good governance.

2.6 IT Security

IT security is a collection of policies, procedures, model, theories, personnel and technologies responsible for protecting the IT assets of an entity (Jourdan et al., 2010). In the meantime, it can also be referred to as the protection and recovery from unwanted or undesirable damage, alteration, disclosure or use, unintentional or deliberate, of IT assets and resources (Alnatheer and Nelson, 2009; Bozkus and Caliyurt, 2018)

2.6.1 IT Security Breach

Vulnerability, threat, and attack are the three kinds of security breaches or hazards that endanger the security of data in a digital environment or IT system (Beebe and Clark, 2005; Bozkus and Caliyurt, 2018). All of the vulnerabilities and threats in

the information technology infrastructure arise passively at first. However, before it becomes an active mode, it is essential to address and overcome these passive vulnerabilities and dangers (Kim et al., 2012). The assault is shown as a danger that occurs on a regular basis (Simmonds and Sandilands, 2004; Bozkus and Caliyurt, 2018).

H2: IT security breach significantly positive influences the IT security maintenance for IT infrastrucure.

Further following discussion is about each kind of security breach that may jeopardize the information technology infrastructure's security. All of the dangers, as shown in Figure 2.4, may transcend beyond data security, which is very important to an organization or business.

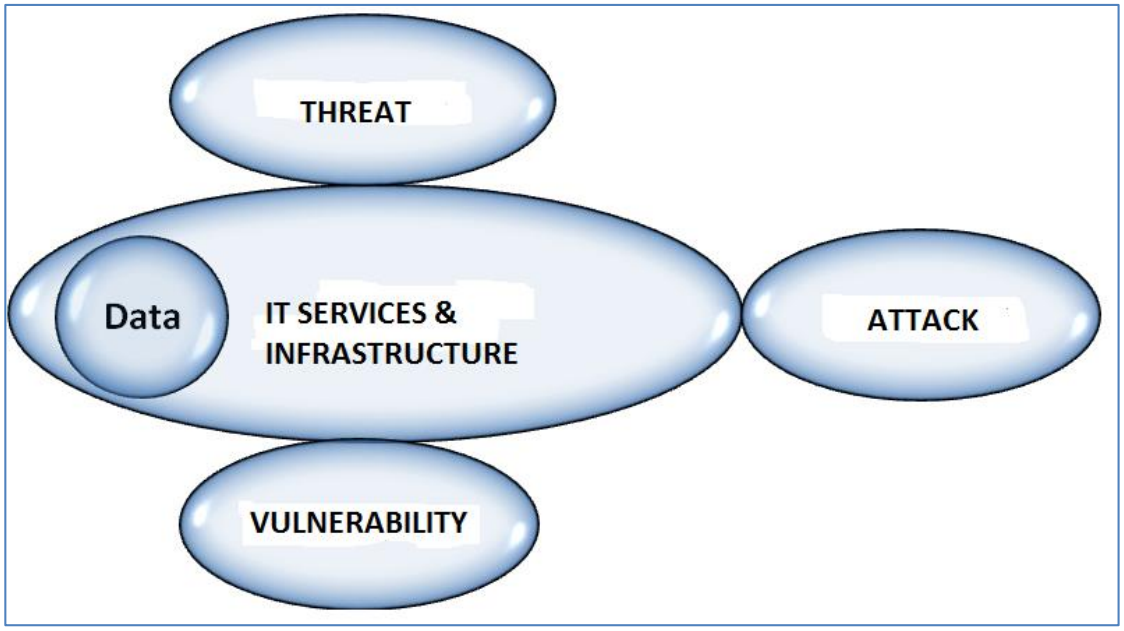

Figure 2.4: IT Security Breach

Threat in the cyber world is anything that can be interferes with the operation, function, integrity, availability of all types of IT infrastructure and services. Threats can be occurring in any type of form (Straub & Nance, 1990; Bozkus and Caliyurt, 2018).

Threats can be happening as an evil action by those who are not responsible or by accident due to natural events or human errors. (Khorshed and Ali, 2012).

Different forms for data breaches have been interpreted within the context. According to Jaeger (2013), missing paper files accounted for 38% of cyber-attacks, lost transportable storage media accounted for 27%, and attackers accounted for just 11%. Insiders who are malevolent pose a significant danger to data security because they have more expertise, tools, and accessibility than outside hackers (Vance et al., 2013).

Another significant insider danger is access policy violations, particularly when they are combined with malevolent intents such as fraud, copyright infringement, sale or exposure of confidential material, and identity theft (Rubenstein and Francis, 2008). According to the Poneman Institute, in 2012, 39% of all events were caused by irresponsible workers or contractors, 37% were caused by hackers or criminals inside, and 24% were caused by system "glitches" (Ebad, 2020). As a result, it's possible to argue that the human element is the weakest link in information security (Yeniman et al., 2011). As a result, a written risk management framework, as well as higher levels of policy literacy and skills, are required, particularly for software companies (Whitman, 2017).

Those for achieving the threat of security breach is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H2a: Threat significantly positive influences the IT security breach of IT security maintenance for IT infrastrucure.

Vulnerability refers to any flaws in the usage of information technology infrastructure and services. This vulnerability may occur in a variety of circumstances,

such as in the design, configuration, implementation, or administration of information technology infrastructure, exposing it to attacks (Trcek, 2008; Bozkus and Caliyurt, 2018). The disadvantage is that it exposes information technology infrastructure to data loss and downtime problems or downtime.

Cyber-attacks increase worries about possible privacy intrusions, which supports a similar trend in contemporary society. Internet users are exposed to ever-increasing privacy concerns as they rely more on computers to store and transmit private data. Despite rising security issues, studies have discovered that individuals continue to reveal an ever-increasing amount of sensitive data online (Barnes, 2006), and this trend shows no indications of going backwards. According to popular social media data, Fb users share over 300 million photos each day on the site. With the increasing frequency of security events and the rising amount of technological advancements influence subsequent, the issue of how to encourage computer organizations to monitor oneself arises (Daigle, 2020).

Refusing to disclose details is other type of threat avoidance. The act of exchanging data to all is known as self-disclosure. Soul is an essential component of personal and plays a vital role in the formation of social connections (Livingstone et al., 2020). Reciprocal self-disclosure aids in the discovery of mutual understanding and the development of trust in relationships (Rubin, et al., 2020). Self-disclosure may have an effect that extends beyond the person, in addition to fulfilling performance targets. A feature of online product evaluations on Amazon.com, for example, discovered that disclosing individual data in customer reviews had an impact on review assessment and following identity by other users (Forman et al., 2008).

Those for achieving the vulnerability of security breach is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H2b: Vulnerability significantly positive influences the IT security breach of IT security maintenance for IT infrastrucure.

The term "possible attack" refers to a method for exploiting existing vulnerabilities in information technology infrastructure (Yang and Wang, 2011). A kind of threat known as a denial of service, or DoS, is an example. Actually, this flaw exists in the architecture of operating systems, and one kind of attack that may be carried out as a result of the flaws is known as Ping of Death assaults (Vivo et al., 1998; Yang & Wang, 2011). There are two types of attacks: passive attack and aggressive attack (Yegneswaran et al., 2005; Yang & Wang, 2011).

Previous work on pc interaction indicated that, in order to solve technological constraints, individuals may enhance identity in innovation settings. Online communication forums are one of the few sociological phenomenon that seem to reflect people's seeming readiness to share confidential info. According to assessments, Facebook members share almost 3 million bits of content every minute (Karim, et al., 2020). Mamonov and Benbunan-Fich (2018) suggests that most of the information provided by users via the service indicates anything private about them.

Facebook has declared intentions to monetize the wealth of data shared by users thru the platform. Impressions of a privacy danger linked to computer security breaches will prompt an instinctive reaction to the threat and action to mitigate the risk to individual personal data. It's worth noting that, although security breaches and privacy infractions are theoretically different, both dangers often coexist in reality.

A cyber-attack occurs when unauthorized computer entry occurs, regardless of the reason for the access or if real data is exposed. A privacy breach, on the other hand, arises when private data acquired for one reason is utilized for other even without permission of the subject (Mamonov & Benbunan-Fich, 2018).

Those for achieving the possible attack of security breach is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H2c: Possible attack significantly positive influences the IT security breach of IT security maintenance for IT infrastrucure.

Protecting data using protective methods such as credentials and assessing the release dangers of new evidence are two examples of proactive security measures. Login details may provide you some influence over your confidential data. In both study and practise by Taddei and Contena (2013), more subjective norm over data has been related to increased willingness to reveal personal data (Cavusoglu et al., 2016).

Users may feel greater standards of safety and reduced chances of data breaches when a novel control method is applied to safeguard data. According to a meta-analysis of conscience in computer-mediated settings, felt safety is highly correlated to personal data sharing (Weisband and Kiesler, 19196; Cavusoglu et al., 2016).

Personal self-evaluation, according to the Pattern Recognition paradigm, happens after automated advice people as a long slog aimed at assessing and modifying one's degree of self-efficacy. Nevertheless, detailed work in data from legacy systems suggests that self-efficacy represents one's expertise in a certain area, and thus it may lead to rapid and effectiveness of spontaneous actions (Mamonov, & Benbunan-Fich, 2018).

While most of the study on the influence of self-efficacy in overall social behavior has concentrated on the straightforward effect of self-efficacy on behavioural intention, information protection researches (Johnston et al., 2015) have emphasised that self-efficacy also has straightforward effects on behavioural intention, but also mediates the range of specific dangers (Woon, et al., 2005; Johnston et al., 2015).

This impact was verified in an observational research that found that security-related identity mediates the desire to avoid computer safety violations in the face of a security danger (LaRose et al., 2008; Yar, 2018).

2.6.2 IT Security Offensive Protection

IT security offensive protection is activities on analysis and testing the IT infrastructure security. It has three types of testing that includes: -

- Vulnerability Assessment - Study to locate security vulnerabilities and identify the corrective action should be taken to improve the network.
- Penetration testing – Subjects a system to the real world attacks selected and conducted by testing personnel.
- IT Security Audit - Compares current practices against a set of standards.

H3: IT security offensive protection significantly positive influences the IT security maintenance for IT infrastrucure.

2.6.2.1 Vulnerability Assessment

Vulnerability assessment is a study to locate security vulnerabilities in the network or system (Koivunen, 2012). In this method, it need full of cooperation from the targeted organization in term of grants access to its facilities, providing the network access, detailed information about the network and others (Radianti and Gonzalez,

2006; Koivunen, 2012). The main objective in this study is to identify weaknesses in the system and make improvements in to the security the systems and network. It is very useful things among of all network security assessment but it's very hard to truly define (Lee et al., 2002; Koivunen, 2012)

Rather than security audit that had specified standard to measure against, in vulnerability assessment there is no standard (Kostina et al., 2009; Jun and Punit, 2011). It may be a vulnerability assessment for internal, external, host, network, perimeter, non-technical and others (Guha and Mukherjee, 1997; Jun and Punit, 2011). So, this practice is higher level than penetration tests and audits and the successful and usefulness of this result it depends on the skill of the tester.

The usefulness and cost effectiveness of such testing is limited and the quality of the people will determine the quality of this methodology (Yu et al., 2009; Yunos et al., 2015). The scope of the vulnerability assessment is depending on things that need to be assessed (Yuill et al., 2000; Yunos et al., 2015).

Those things that need to be assesses can be including examine the specific systems that may the most vulnerable or contain the most valuable information or maybe the vulnerability assessment is needed at firewall or web site (Killcrece, 2003; Yunos et al., 2015). Maybe the client wants a firewall or Web site assessed or examine in non-technical security posture, which may warrant walkthroughs to all the facilities (US-CERT, 2015).

However, the goals or objectives in certain vulnerability assessment must be determining the tasks that are need to perform. An assessment is also more beyond than security audit is because it will look the past checklist if exist (Jun and Punit, 2011). In vulnerability assessment is not only addressing the specific issues by using the scanning tools but it will perform to examine the extent of the system's vulnerabilities and explore

the implications of the vulnerabilities disclosed by the tools (Yunos et al., 2015). Then, the report will produce within more detail of recommendations.

Those for achieving the vulnerability assessment of security offensive is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H3a: Vulnerability assessment significantly positive influences the IT security offensive protection of IT security maintenance for IT infrastrucure.

Scholars in software engineering, finance, operational research, and allied fields have lately focused on data protection asset allocation. The growing field of data security economy attempts to formalise these choices, but there is still a gap between theoretical frameworks and actual interactions. Data collecting possibilities for central computer guards, in especially, vary from other situations. The topic of our article, penetrating test (short: pentesing), is an instance of active data record options unique to computer networks. Vulnerability assessment is frequently utilised in practise, but its impacts have not been documented in the literature on data security expenditure (Bouveret, 2018; Leszczyna, 2019).

Vulnerability assessment is sometimes known as "ethical hacking" since hired ethical hackers examine the target network from the perspective of a hacker, revealing instead of exploiting flaws. The goal of this research is to look at the additional advantages and costs of security research for overall system protection. Because hepatomegaly and attacks are so similar, it's natural to assume that data uncovered by pentests should be represented similarly to data uncovered by strikes. However, there are cost distinctions: pentests incur predictable upfront expenses, while costs related to

successful assaults are more unpredictable, considerably greater, and borne ex post (Böhme et al., 2019).

2.6.2.2 Penetration testing

Penetration testing has the most sizzle and the testing is what the professionals use to ensure that a system or network is secure condition (Kohn et al., 2013). However, it's actually the least useful of the various network systems diagnostics.

Firstly, correct action that to perform penetration testing is a covert the test. This means that consultant or tester inside the organization plays the role like a hostile attacker that tries to compromise the network systems security (Zambon et al., 2010; Böhme and Moore, 2016). Within the term of penetration, the testing will carry out without warning in situation that closes to complete secrecy (Zhang & Wang, 2011).

Ideally, there should be no support from the organization that had being tested. Any of the guidance from the organization should be restricted to the penetration team (Zhang et al., 2012). However, if the penetration testing is outsourcing to other organization, that organization should let the consultant only know their objective and goals in doing this penetration testing (Zan et al., 2010).

This penetration testing can be conducted to relate to the real inside or outside attackers (Zhang et al., 2011). The penetration testing is also can be technical or non-technical form (Zielińska et al., 2014). For example, in “social engineering" method is not technical testing that need tester to get information maybe by telephone or other.

So, from inside the target organization, there are only a several people that should know about the execution of penetration testing. Another important thing is any critical aspect of the penetration testing should be to see and involve by the staffs in

target organization that had authorized in this area (Zhou and Yao, 2012). They can react with his authorized on the penetration attempts.

Then, penetration testing is useful because of its goal to compromise the network security in target organization. In this situation, the consultant will identify the potential holes that in believe it's become a pot of honey and very likely to be detected by the real attacker's perspective (Bing and Hai-Feng, 2012). According to this scenario, the target organization should be known and see the potential damage that can be produce from the exploitation of these vulnerabilities.

Those for achieving the penetration testing of security offensive is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H3b: Penetration testing significantly positive influences the IT security offensive protection of IT security maintenance for IT infrastrucure.

Even in a high-security system, a hacker may still target a number of vulnerabilities. WPA2-AES is still considered a strong security protocol, however it only pertains to time slots and not administration frames at this time. A hacker attempts to insert a forged control frames into the platform in order to launch a Denial-of-Service (DoS) attack (Dacosta, et al., 2012). Wireless Network Overload Attack, Identification Flood Attack, De-authentication Attack, Affiliation Flood Assault, and Disconnection Strike are the most common wireless DoS assaults nowadays. These assaults will cause a wireless connection to become overwhelmed, resulting in service interruptions, increased packet loss rates, and the necessity to resume the stopped Access Point (AP) (Wang, et al.,2016).

2.6.2.3 Security audit

Usually an audit is generally known when the organization wants to know the real level and tasks of this organization to measure up to meet the specific standards. This type of testing will provide a good guidance to the organization on improving its adherence to the specific standards (Kurowski and Frings, 2011; Malik et al., 2019). This will implicate to organization to have the better security-though. So, an audit is when taking a set of rules and measures it with the current practices (Zimmerman and Glavach, 2011; Malik et al., 2019). This task is very straightforward security testing but it has a concentrated purposes and limitations.

The process on usual audit in general situation is same to the information systems security audits. In a security audit, it is also having a set of security guidelines, standards or policies that will be measures against the current system or network (Zissis and Lekkas, 2012; Malik et al., 2019). Then, the quality and content in security audit standards must be very greatly items. So, the standard must be addressing the physical including the technical security (Zonouz and Haghani, 2013; Malik et al., 2019).

In security audit, it's cover on all how the staffs treat the information and the physical resources in organization (Balduzzi and Zaddach, 2012; Line and Albrechtsen, 2016). Then, it's also including the levels of computer protection and maintenance, system configuration, password strength and other usual aspects of technical security. So, the standard must be representing a continuing network security process or practices and definitely not a one-time measurement (Zonouz et al., 2014; Line and Albrechtsen, 2016).

In organization site, a standard must already have in place to determine whether the standard itself is acceptable by the security auditor. Then, the standard must acceptable to the actual environment. If the organization is not having the standards, the

auditor will measure it by their own standards. So, the organization needs to determine the acceptable of the auditor's standard.

Those for achieving the security audit of security offensive is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H3c: Security audit significantly positive influences the IT security offensive protection of IT security maintenance for IT infrastrucure.

A audit committee of a data system is performed to determine how well a company can secure its valuable or essential assets. Furthermore, complex assaults have been created to discover fresh weaknesses in great sources as technological advances and Internet-enabled applications become available. As a consequence, businesses must adapt their system security methods to meet changing data security needs. A good security plan nowadays requires a thorough procedure (Onwubiko, 2009; Susanto and Almunawar, 2018).

Regular data security audit performance assessment is one method to evaluating an institution's data systems practises and activities. An auditing procedure will allow you to see whether your integrated planning rules are in place, if your assets are secure, private, and available, and if your data analytics are working quickly and successfully to meet your security goals (Pereira and Santos, 2010; Susanto and Almunawar, 2018)

2.6.3 IT Security Defensive Protection

For data protection or security of information technology, it should be done in proactively which mean that there should be a plan for implementing the rules of preventive to secure IT infrastructure. However, the limitation of this case is it requires high capital and skilled labor. So, with that, whatever the outcome of security breach is difficult to expected or demonstrated to management until there are some attacks or security breach happen in real situation (Tripathi and Singh, 2012; Nwankwo, 2020).

In this situation, the IT staff needs to be prudent in extending the scheme along with the figures of return on investment to the company. This is because the cost to restore backs any data or information that has been lost or damaged is very high compared to the cost of the investment for security prevention in IT infrastructure (Baskerville and Spagnoletti, 2014; Nwankwo, 2020). It should be analyzed and compared more closely to the return on investment for the company's need.

Generally, to secure the IT infrastructure, it should be the three most basic implementation of IT security practices which is IT security policy and guidelines, IT security education and awareness and IT security perimeter (Arcy & Hovav, 2009; Baskerville and& Spagnoletti, 2014; Nwankwo, 2020).

First of most important in IT security defensive protection factor is about IT security policy and guidelines. In IT security policy and guideline, it will be clearly state that, what can be done and what cannot be done by any person in control or mange of an IT infrastructure and services for a company or organization. Any usage of IT infrastructure components such as computers, Internet, information systems, computer networks and others must be having specific policies in addition to general IT security

policy. IT security policy is an important factor that controls the usage of IT infrastructure for a company or organization (Baskerville and Spagnoletti, 2014).

Within the IT security policy, IT security guideline is add value on it. It is important to ensure that whatever IT security services are use, it will be used in safe and secure manner.

Those for achieving the IT security policy of defensive secuity is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H4a: IT Security policy significantly positive influences the IT security defensive protection of IT security maintenance for IT infrastrucure.

The risk management framework must be updated on a regular basis. It should evolve and expand with the company at all regularly to make that it fits the business's vision and purpose. Restarting the protection policies offers a number of benefits. Maintaining good with organisational changes and guaranteeing that the documentation does not become stagnant and out-of-date are two of them (Briney, 2000; Rostamiet et al., 2020)

The different supporting actions must be carefully examined and executed in order to create an efficient data security policy. These auxiliary activities contribute to the overall creation of a successful data security policy. If people are unaware of an data protection policy, it will be ineffective. As a result, it's critical that the data security policy be implemented properly and effectively across the company, as well as communicated to users (Höne and Eloff, 2002; Rostamiet et al., 2020)

Those for achieving the IT security guideline of defensive secuity is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H4b: IT Security guideline significantly positive influences the IT security defensive protection of IT security maintenance for IT infrastrucure.

IT security policy and guideline will make a balance in any unsecure situation happen in IT infrastructure usage. For an example, the employees are not allowed to surf any porn, social networking and others certain website during working time. So, if this thing happens in organization, there will be follow-up actions according to the IT security policy for the involved employees such as warning, suspension, fines and others.

Then, second important factor to secure the IT infrastructure is about education and awareness of all employees, customers and whoever involved in usage of computers, information systems and IT of a company. They need to be educated and aware with the right to use it in wisely and safely. This is very important part because within the usage of sophisticated security perimeter system is not necessarily guaranteed to protect the security of data, information or IT infrastructure. As an example of the situation of an invasion to the internet banking user's account, the bank said they have a very strong security system and blame the customers which do not operate their own internet banking account in properly (Jang-Jaccard and Nepal, 2014).

Whereas, the user's bank account is not properly and wise educated by the banks involved. They only promote intensely concerned with internet banking for consumers but not how to use internet banking wisely and safely.

Users and customers whose cannot use information technology infrastructure in properly and safely manner will be subjected to the invaders with a variety of fraud techniques such as social engineering, scams, phishing, fraud and others. The department of information technology should make a lot of awareness campaigns by providing cyber security guidelines posters and others. Like what was done by CyberSecurity Malaysia during this campaign of safely uses Internet among peoples in Malaysia. The company or organization can also collaborate with the CyberSecurity Malaysia on cyber security awareness program.

Those for achieving the IT security education of defensive security is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H4c: IT Security education significantly positive influences the IT security defensive protection of IT security maintenance for IT infrastrucure.

Our computer infrastructures security and reliability is becoming a major priority. University qualification increasingly integrated computer and data safety concepts into the conventional post - secondary software engineering curriculum to meet this need. Educational protection concepts must be based in practice in order to accomplish successful instruction (Du and Wang, 2008; Rostamiet et al., 2020). Using appropriate attack tools, hackers may effectively infiltrate and manipulate mobile devices, as well as beat defenses such as virus scan engines, by leveraging system weaknesses or a lack of protection. As a result, stability issues and risks should be thoroughly investigated and managed (Wang, et al., 2017).

Data safety expert and vendor credentials verify abilities and skills, but they do not replace experiences or qualifications. Professionals certificates may be useful in a restricted operating market, whereas academic credentials promote wide skills and abilities in generally (Hentea, et al.,2006; Whitman, 2018)

Those for achieving the IT security awareness of defensive security is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H4d: IT Security awareness significantly positive influences the IT security defensive protection of IT security maintenance for IT infrastrucure.

The way people utilise data analytics has evolved significantly over time. The user account has shifted as well, from a scenario in which all clients were computing or computer science experts to one where the lot of consumers are barely internet savvy today (Thomson and Von Solms, 1998; Whitman, 2018) Every firm must implement a data protection awareness programme in order to attain this. This software will teach customers on data safety problems while also reminding them of the problems as well as any new ones that may have arisen. Because the goal of this preventive maintenance program is to alter the user's thinking and behavior, it must be designed in such a manner that the user's actions and thoughts are changed to guarantee that their activities are safety conscious (Siponen et al, 2014; Whitman, 2018).

The rise in computer technology (IT) protection measures around the world is primarily due to (1) a rise in online records, (2) a boost in smart phones, (3) a boost in organised cybersecurity groups, (4) a boost in smart local and global IT security threats, (5) complexity in detecting hackers, (6) restricted cyber - crime laws, and (7) limited IT

threat intelligence among web users. Pirates are also driven to carry out an attack for a variety of purposes (Aloul, 2012).

The security perimeter are the tools and techniques that are necessary to secure IT infrastructures such as firewalls, Intrusion Detection System, Intrusion Prevention System, anti-virus software, DMZ (Demilitarized Zone) technique and others (Böhme et al, 2016). Besides that, high demand for IT experts and trained IT staff are needed to well manage and control all the security perimeters of IT infrastructure. An overall and centralized IT security system should be implemented on all the IT infrastructure, services and facilities that are used and available within a company or organization.

These security solutions may be software or hardware, but the technique of management and security on the Internet and networks is the most essential factor. This firewall, whether it be software or hardware, must contain the following features.

A network firewall serves as a gatekeeper for the computer system, acting as a filter and safe transit route for accessibility to and from the Internet and networks to secure the organization's IT facilities on the network from intrusion (Norton, 2016).

It will examine all network traffic for appropriate password and other security code use. Only authorized transmissions into and out of the network are permitted. Because of its susceptibility and lack of security, it has become important to every company that connects to the Internet (Killcrece et al. 2003; Jang-Jaccard and Nepal, 2014). It can totally discourage unwanted access to computer networks, but it can't completely prohibit it (Klein et al., 2010). As a result, it may enable access to the computers within it only from trusted Internet sites, and it may only allow secure information to flow (Norton, 2016).

Those for achieving the IT security parameter firewall of defensive security is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H4e: IT Security parameter firewall significantly positive influences the IT security defensive protection of IT security maintenance for IT infrastrucure.

The numerous benefits of enhanced meters, monitoring, and analytics come with additional tech issues when the electricity grid adopts Smart Grid technology (Lyu and Lau, 2010; Brewer, 2019). The network is becoming increasingly prone to hacking as the power grid becomes more digitalized and reliant on communication technologies. Computer hackers, if not discovered and rectified in a timely manner, may result in system controllers receiving misleading data and the power grid potentially collapsing (Zou, et al.,2020)

The intrusion detection system (IDS) is an essential part of the security protection measures for IT infrastructure (Anuar and Papadaki, 2010; Brewer, 2019). IDS has to be precise, adaptable, and extendable. The systematic and automated IDS development process, rather than pure knowledge encoding and engineering methods, are required to meet these criteria and the complexity of today's digital surroundings (Lorena, 2015; Zou, et al.,2020).

The primary goal of IDS is to detect potential events, record information about them, and try to report them (Lorena, 2015). Then, businesses utilize IDS for a variety of reasons, such as detecting issues with security rules, discouraging people, and recording current risks from violating security policies (Gritzalis and Furnell, 2012).

Nearly every organization's IT security architecture now includes an intrusion detection system (IDS) (Kheir & Debar, 2009; Jang-Jaccard & Nepal, 2014).

Those for achieving the IT security parameter IDS of defensive security is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H4f: IT Security parameter IDS significantly positive influences the IT security defensive protection of IT security maintenance for IT infrastrucure.

Many protection measures for IoT have been suggested to solve scale and resource-constrained safety problems, such as web app firewalls. An IDS is capable of monitoring network activity among linked objects and issuing alerts if a violation is discovered. Because of its surveillance and warning capabilities, an IDS is regarded as a critical defensive tool for conventional IP networks.

Despite the fact that IDS functions effectively in conventional networks, creating IDS for Iot system is a difficult job. This is due to the features of Iot systems, such as the IDS agent nodes' low process and storage capacities (Thakkar, & Lohiya, 2020). Nevertheless, the IoT's linked architecture and devices' capacity to interact with one another create security concerns in IoT networks. As a result, a suitable data protecting IoT computers and systems, such as an Intrusion Detection System (IDS), must be created (Thakkar, & Lohiya, 2021).

The typical IT infrastructure depends on various forms of protection software, including anti-virus and anti-spyware applications (Zhang et al., 2010). The anti-malware tools safeguard persistent state on the IT infrastructure to provide protection.

These tools rely on rules and signatures developed based on knowledge of malware, attacks, and software vulnerabilities (Zhang, 2020).

In IT infrastructure, causing the computer client and server, which executes anti-malware software for detecting and removing the malware and virus, to monitor all the computer client and server that is served on the IT infrastructure (Zhao and White, 2014). The anti-malware software will execute and monitor one or more application program, periodically storing a state of the nodes as snapshot, suspending the first node from which the virus is detected if the anti-malware software executed on the second node detects the virus, and restoring the first node at a state of a point in time when the snapshot is stored by using the snapshot of the suspended first node.

Those for achieving the IT security parameter anti-malware software of defensive security is important for IT infrastrucure security maintenance significantly. With that, thus following hypothesised is needed.

H4f: IT Security parameter anti-malware software significantly positive influences the IT security defensive protection of IT security maintenance for IT infrastrucure.

Because neural networks and data centers have many parallels, authors have described a modified version of the basic SIR infected individual to investigate the behaviour of particularly undesirable and how their grow in multiple channels such as peer-to-peer networking and wsns (Mishra and Keshri, 2013). Several methods for detecting malware in network infrastructures have been suggested (Watson et al., 2014). Malware authors, on the other hand, attempt to make them invisible by using polymorphism methods to remain undetected. Malware activity duration should be kept

to a minimum, and malware dissemination should be limited in cloud networks (Shahin, 2014).

Suarez-Tangil and Stringhini, (2018) performed the biggest study of Malware detection behaviors to comprehend the nonlinear response of malware. They used VirusTotal testing data to examine malware strains discovered between 2010 and 2017. To detect target Android apps, they presented an operational flow analysis method. Their method divides apps into categories related to network flow and creates intrusion prevention characteristics.

The key of the protection on user data for a certain organization should be known with respect to where and how the data is stored, whose can access it, how to protect the data from being stolen, distributed and shared among unauthorized person (Barske & Stander, 2010; Zhang, 2020). Then, how to protect users from fraud's attacks such as spamming, fake e-mails, fake web site and others.

2.6.4 IT Security Management

Information security, according to ISO/IEC 17799:2005, is defined as "the protection of information's confidentiality, integrity, and availability, as well as additional characteristics such as authenticity, accountability, non-repudiation, and dependability."

There are many definitions for information, including the following:

i) Information is about someone or something is made up of facts about that person or thing.

ii) By processing input data using a programme, important or valuable information may be retrieved as output from a computer.

iii) Information is a valuable corporate asset that, like other significant company assets, must be adequately safeguarded (Melara & Sarriegui, 2003; Tehranipoor & Wang, 2012).

iv) Information may take many different forms. It may be printed or written on paper, saved electronically, sent through mail or electronic means, seen on film, or uttered in a dialogue.

The main goals of IT security management are to guarantee that IT assets can meet the following security goals.

i) Confidentiality

ii) Integrity

iii) Availability

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (Landwehr, 1981; Tehranipoor and Wang, 2012). Some examples of breach of confidentiality are "Unauthorized personnel can read the classified documents", "Remote access to the system without approval", and "Shared folders without consent of the owners".

Those for achieving the objective of confidentiality is important for IT security maintenance for IT infrastrucure in significantly. With that, thus following hypothesised is needed.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

H5a: Confidentiality significantly positive influences the IT security objective of IT security maintenance for IT infrastrucure.

The implementation of input validation that depend on encryption to guarantee data secrecy has long been seen as incompatible with the fundamental security concept of clear distinction of laws and regulations. While using a nonlinear transfer network and tokens significantly simplifies access control, it also creates a new risk in terms of policy secrecy (Mattei, 2017).

Indeed, the major trend of tokens, and thus the associated nonlinear transfer hierarchy, makes the connection among customers and the assets they are allowed to access apparent, and thus reveals the edition. Nevertheless, in certain cases, the strategy must be treated as secret since administrators do not want to fully reveal to whom they provide (or do not grant) access to the data.

An examination of the policy may also enable analysts to rebuild the aspects of the proposed networks of authorized users as well as their true identity. The safety of the security policy it seems to be a natural necessity that processes will be willing to support, as long as energy efficiency is ensured, since the overarching objective of these fresh ideas is to allow an effective nondisclosure method for asset dispersal (Alabady, et al.,2020).

Integrity separates into data integrity and system integrity (Butian, 2015). Data integrity means the property that data has not been altered or destroyed in an unauthorized manner (Chen & Nazareth, 2010). System integrity means the property that a system performs its intended function in an unimpaired manner, free from

deliberate or accidental unauthorized manipulation of the system (Trcek, 2006; Tehranipoor & Wang, 2012).

Those for achieving the objective of integrity is important for IT security maintenance for IT infrastrucure in significantly. With that, thus following hypothesised is needed.

H5b: Integrity significantly positive influences the IT security objective of IT security maintenance for IT infrastrucure.

The protection policy in a "secure" computing device, such as protection and privacy, communicate with one another and were n't self-contained. When it comes to maintaining secrecy, honesty is a must. Sophisticated systems that rely only on secrecy for safety might not even be capable to provide this function and, as a result, may not be safe by design. Information security in a computing system is determined by the microsoft's handling of the data rather than its substance (Nelson, 1994; Zhang, 2020).

In computing networks, change is inevitable; data preparation entails altering the data or utilising it to create new data. As a result, authenticity in a production facility is determined by the accuracy of new data rather than the avoidance of change.

Authenticity is dependent on the accuracy of programming and the proper connection among the system and the information on which it works, since information in a computing device is modified by users via software programmes. (Limoges et al., August 1994; Zhang, 2020). Authenticity is defined as the absence of contamination or manipulation that has a negative impact on a system's functionality.

This term indicates "correctness of processing" between the program's consumers, programmes, and data components for a computing device. This description is the result of looking at a multitude of scenarios where strong consistency is valued and identifying security criteria that are similar to all of them in the most significant of which is operational accuracy (Eckel and Laffey, 2020).

The definition of Availability is the property of being accessible and usable upon demand is obtainable from an authorized entity (Landwehr, 1981; Tehranipoor and Wang, 2012).

Those for achieving the objective of availability is important for IT security maintenance for IT infrastrucure in significantly. With that, thus following hypothesised is needed.

H5c: Availability significantly positive influences the IT security objective of IT security maintenance for IT infrastrucure.

As a result, data protection is very important in everybody's life. In addition, many companies engaged in utilising technological services to operate more effectively must be worried about the problem of confidential data being put at danger. The three goals of cybersecurity are confidentiality, integrity, and availability, which guarantee security and privacy (Alkhudhayr et al., 2019). The companies must be able to handle data security risks such as tampering, security breaches, and service disruption. Every industry has a duty to improve data security expertise in order to protect network environments. The word "availability" refers to giving authorised users access to the assets and data they need when they need it.

An sovereignty private information technique may be used to ensure remote regulatory compliance (Khidzir et al. 2018). This method shows that the data is secure and that it can be utilised in an actual world. It may also efficiently verify data security without downloading and installing the real data. Furthermore, a public key token is a shared erasure-coded information and scalable stockpiling technique (Kumar and Bhatia, 2020).

2.6.5 Information Security Management Model Review

IT infrastructure security is a state which protects a system or object from risk (Anuar and Furnell, 2011). It consists of systems, operations and internal controls in order to ensure the confidentiality, availability and integrity of data, knowledge and ICT infrastructure of an organization. User's roles in ICT systems have evolved from IT specialists for accessing information facilities, non-IT personnel for daily operation, unspecified individuals which is interested parties from outside organization. Establishment of organization information security policy (ISP) is the first step to protect organizations from security threats. Table 2.1 summarized procedures for building a set of ISP through the comparison of six standards in information security management standard.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

Table 2.1: International standard for ISP

International standard	Guidelines
BS 7799 (Code of practice for ISM) ISO/IEC 17799	Describe the minimum contents in an ISP Explain what should do with an ISP An ISP should be approved by management, published and communicated throughout the organization An ISP should be evaluated and updated periodically
BSI IT baseline protection manual	Description of drawing up an ISP Coverage topics Contents Review
COBIT (The information system audit and control association and foundation, ISACAF)	Describes the process and control needs for implementing an ISP Brief section on the security and internal control framework policy Writing and maintaining a document
GASSP (Generally accepted system security principles)	Minimal requirements for an ISP and principles behind it The different processes needed for defining, maintaining and implementing the policy The hierarchy concept of an ISP
GMITS (ISO/IEC PDTR 13335-1)	Provide a comprehensive guidance on information security with planning, management and implementation
ISFs Standard of good practice (The globally representation information security forum, ISF)	Performance evaluation List the contents of ISP The characteristics of the policy Explain the acceptable user behavior

As a pioneer, UK Department of Trade & Industry (DTI) firstly developed Code of Practice (CoP) PD0003 on information security in September 1993, with the assistance of a group of leading UK organizations. This Code of Practice was later retitled and published as BS 7799 Part 1 "Code of Practice for Information Security Management" in February 1995 by British Standards Institution (BSI). BS 7799 provides a common basis for developing organizational security standards and effective information security management practices. It enhances confidence in inter-organizational dealings.

Then, a new standard BS 7799 Part 2 "Information Security Management System – Specification with guidance for use" was released in 1998. The structure of this standard was the same as Part 1, in addition to defining a Code of Practice based on

a set of key controls. As BS 7799 was a theoretical control standard and not a technical standard of practice, it might not solve ISMS problems effectively. Therefore, ISO further developed ISO/TR 13335 (Information Technology – Guideline for the Management of IT Security) and ISO/IEC 18044 (Information Security Incident Management) standards (ISO/IEC FDIS 17799:2005; ISO/IEC 27001:2005. Both standards are helping ICT industry to implement information security management.

A scheme for accreditation of BS 7799 entitled "c:cure" was launched at InfoSecurity 1998 by UK Accreditation Certification Service (UKAS) and the British Standards Institution (BSI). The accreditation procedure for ISO 9001 was adopted such as independent accredited certification body required for the purpose. This scheme initiated the further adaptation from national standard (BS) to international standard (ISO). Following the revisions of BS 7799 part 1 in 1999, the standard was transferred to ISO/IEC 17799:2000 (Part 1) – Code of Practice for Information Security Management. Finally, ISO/IEC 27001 Part 1 and Part 2 were issued in 2005, making them official and recognized standards both locally and internationally. ISO/IEC 27001:2005 is directly related to the original BS 7799.

ISO/IEC 27002:2005 is a generic and advisory document, not a formal specification standard. It provides a well-structured and comprehensive set of controls to address information security risks, covering confidentiality, integrity and availability aspects. Organizations that adopt ISO/IEC 27002 must assess their own information security risks and apply suitable controls, by following the standard for guidance.

2.6.5.1 ISO 27001

ISO 27001 is an international standard that lays out the criteria for developing, implementing, operating, monitoring, evaluating, maintaining, and upgrading a documented Information Security Management System (ISMS) that addresses an organization's entire business risks. ISMS is intended to verify that the security measures chosen are sufficient and proportional in order to safeguard the organization's information assets and instil trust in its customers.

2.6.5.2 ISO/IEC 27001:2017 (Information Security Management System - Requirements)

The international standard ISO/IEC 27001:2017 has its roots in the technical content derived from BSI standard BS7799 Part 2:2002. This standard is generally applicable to all types of organizations, including business, enterprises, government agencies, institution and healthcare.

The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS. The PDCA cycle has four phases:

1. Plan – Establishment of the ISMS. The first step is to define risk assessment, in which risks shall be identified, analysed and evaluated. Identification and evaluation of the risk treatment options are then followed. After the control objectives and controls are selected, management needs to approve residual risks and authorize implementation of ISMS.

2. Do – Implementation and operating the ISMS. Management actions, resources, priorities, roles and responsibilities shall be defined in this step. It needs to determine the risk treatment plan to the respective risks, and to implement controls accordingly.
3. Check – Monitoring and reviewing the ISMS. Monitoring and reviewing procedures should be developed and executed. The effectiveness of ISMS and controls, as well as the risk assessment methodology and residual risks, should be included and reviewed.
4. Act – Maintaining and improving the ISMS. Implementing both preventive and corrective actions in this step could further improve the ISMS. It also enforces document and record control, and reviews information security incidents for lessons learning, so as to improve the ISMS.

Often, ISO/IEC 27001:2017 is implemented together with ISO/IEC 27002:2005. ISO/IEC 27001 and ISO/IEC 27002 assist in defining the requirements and outlining the most suitable information security controls for the ISMS respectively. However, there are complicated and confusing guidelines of risk assessment mechanism and ISMS implementation are included; those standards are only stated what is needed to do but it does not mention properly how to do it.

2.6.5.3 ISO/IEC 27002:2013 (Code of Practice for Information Security Management)

ISO/IEC 27002:2013 (replacing ISO/IEC 17799:2005 in April 2007) is an international standard that originated from the BS7799-1 standard originally laid down by the British Standards Institute (BSI). ISO/IEC 27002:2013 refers to a code of practice for information security management, and is intended to be a common basis

and practical guideline for developing organizational security standards to facilitate the effectiveness of management practices.

By adopting the standard, an organization can address information security risks comprehensively. This standard consists of several guidelines and the best practices in 11 security domains shown as follows:

1. Security policy.
2. Organization of information security.
3. Asset management.
4. Human resources security.
5. Physical and environmental security.
6. Communications and operations management.
7. Access control.
8. Information systems acquisition, development and maintenance.
9. Information security incident management.
10. Business continuity management.
11. Compliance.

Among these 10 security domains, a total of 39 control objectives and 133 best practice information security control measures are recommended for organizations to satisfy the control objectives and protect information assets against threats to confidentiality, integrity and availability.

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

2.6.5.4 ISO/IEC 13335 (IT Security Management)

Initially, ISO/IEC 13335 was a Technical Report (TR) before becoming a full ISO/IEC standard. It consists of a series of guidelines for technical security control measures:

1. ISO/IEC 13335-1:2004 documents the concepts and models for information and communications technology security management.
2. ISO/IEC TR 13335-3:1998 provides the techniques for the management of IT security. It was superseded by ISO/IEC 27005:2008.
3. ISO/IEC TR 13335-4:2000 covers the selection of safeguards (for example technical security controls). It was superseded by ISO/IEC 27005:2008.
4. ISO/IEC TR 13335-5:2001 suggests management guidance on network security. It has been under review, and may merge with ISO/IEC 18028-1 and ISO/IEC 27033.

Information security is a multi-dimensional discipline that can be viewed from different perspectives. The conceptual models are presenting security element relationship that shows how assets are potentially subjected to a number of threats. The threats and environment change over time and it may have impacts on the probability of risk occurrence.

The model has been developed with the assumption of an environment containing constraints and threats that change constantly and are only partially known, including the assets of an organization, the vulnerabilities associated with those assets, safeguards selected to protect assets and residual risks acceptable to the organization.

2.6.6 Information Technology Security Maintenance

Upon the successful implementation and testing of a new and improved IT security profile, an organization might feel more confident of the level of protection it is providing for its information assets (Whitman & Mattord, 2018). By the time the organization has completed implementing the changes mandated by an upgraded IT security program, a good deal of time has passed.

In that time, everything that is dynamic in the organization's environment has changed (Whitman & Mattord, 2018). Some of the factors that are likely to shift in the information technology security environment are:

- New assets are acquired.
- New vulnerabilities associated with the new or existing assets emerge.
- Business priorities shift.
- New partnerships are formed.
- Old partnerships dissolve.
- Organizational divestiture and acquisition occur.
- Employees who are trained, educated, and made aware of the new policies, procedures, and technologies leave.
- New personnel are hired possibly creating new vulnerabilities.

If the program is not adjusting adequately to change, it may be necessary to begin the cycle again. That decision depends on how much change has occurred and how well the organization and its program for information technology security maintenance can accommodate change (Whitman & Mattord, 2018). If an organization deals successfully with change and has created procedures and systems that can flex

with the environment, the IT security program can probably continue to adapt successfully (Kundu and Ghosh, 2014).

The CISO determines whether the information security group can adapt adequately and maintain the information technology security profile of the organization or whether the macroscopic process of the SecSDLC (Security System Development Life Cycle) must start a new to redevelop a fundamentally new information technology security profile.

It is less expensive and more effective when an information technology security program is designed and implemented to deal with change (Whitman & Mattord, 2018). It is more expensive to reengineer the information technology security profile again and again.

Management model must be adopted to manage and operate ongoing security program (Alnatheer, 2014). Models are frameworks that structure tasks of managing particular set of activities or business functions (May, 2008; Alnatheer, 2014). With that, by assist the information security community to manage and operate the ongoing security program, a management model must be adopted (Guo &Yuan, 2012). In general, management models are frameworks that structure the tasks of managing a particular set of activities or business functions. A maintenance model is intended to complement the chosen management model and focus organizational effort on maintenance.

2.7 Theoretical Conceptual Framework

This research is focusing on the issue of information technology security maintenance in IT infrastructure. A conceptual framework can be well-defined as the

outcome of combining numerous related concepts from various theories in order to explain, provide a better understanding or predict a particular event, phenomenon or research problem (Imenda, 2014). In order to develop the conceptual framework, several selected concepts are derived from IT security management model and literature review. Then, all the concepts are combined into the conceptual framework.

Based on these several selected IT security management models, theories and concepts, the conceptual framework for this research is proposed. In the conceptual framework of this research, the inputs are all the components of IT security maintenace collected throughout the using of the components of IT security management models, theories and concepts.

As a result, there is a pressing need to investigate and comprehend the difficulties of managing the conceptual security maintenance process for IT infrastructure via improved IT security management. Although software maintenance is considered to be one of the lifecycle processes that is better suited for a distributed environment, software development activities typically necessitate extensive customer contact, quick development cycles, and quick response times, all of which are hampered by communication delays, misinterpretations of requirements, and indirect responsibilities that are common in distributed environments.

These also need exposing the connections between difficulties, since various challenges may result in the occurrence of other issues. (Ulziit et al., 2015). To the best of our knowledge, despite the fact that a few studies have focused on the problems of IT infrastructure in general, no thorough research has been conducted in the context of improving IT security management for IT infrastructure.

This is critical since there are obvious differences between software maintenance and IT security management, as well as a method for improving IT security management for IT infrastructure. It's essential to note that this research is focused on outsourcing. That is, all of the settings examined in this research are separated by cultural, chronological, and geographic barriers. Our contributions consist of a conceptual framework (Wieringa, and Daneva, 2015) that explains the problems and solutions associated with conceptual security maintenance (Ulziit et al., 2015). We contribute the following sub-contributions to the conceptual framework:

- Using the grounded theory approach, identify difficulties in managing conceptual security maintenance and characterize them.
- Identifying and categorizing options for managing security and infrastructure maintenance.
- A map depicting the problems and their solutions.

The conceptual framework for this study is provided based on these few chosen IT security management models, ideas, and concepts. The inputs to this study's conceptual framework are all the components of IT security maintenance gathered via the use of IT security management models, theories, and ideas.

The suggested conceptual model for security maintenance in a campus network's IT infrastructure is an amalgamation of IT access control models, ideas, and concepts that encompass a wide range of elements and activities related to information technology security. Software vulnerability, risk assessment, attack motive, threat detection, deterrent, and security goal are all part of the framework. It is built on an

older model, ideas, and principles for information security management. To guarantee that potentially anomalous circumstances are avoided, the framework has been improved with the addition of a mixture of constructs and refined via the recalibration of IT security management model, theories, and ideas. Figure 2.5 illustrates the suggested framework.

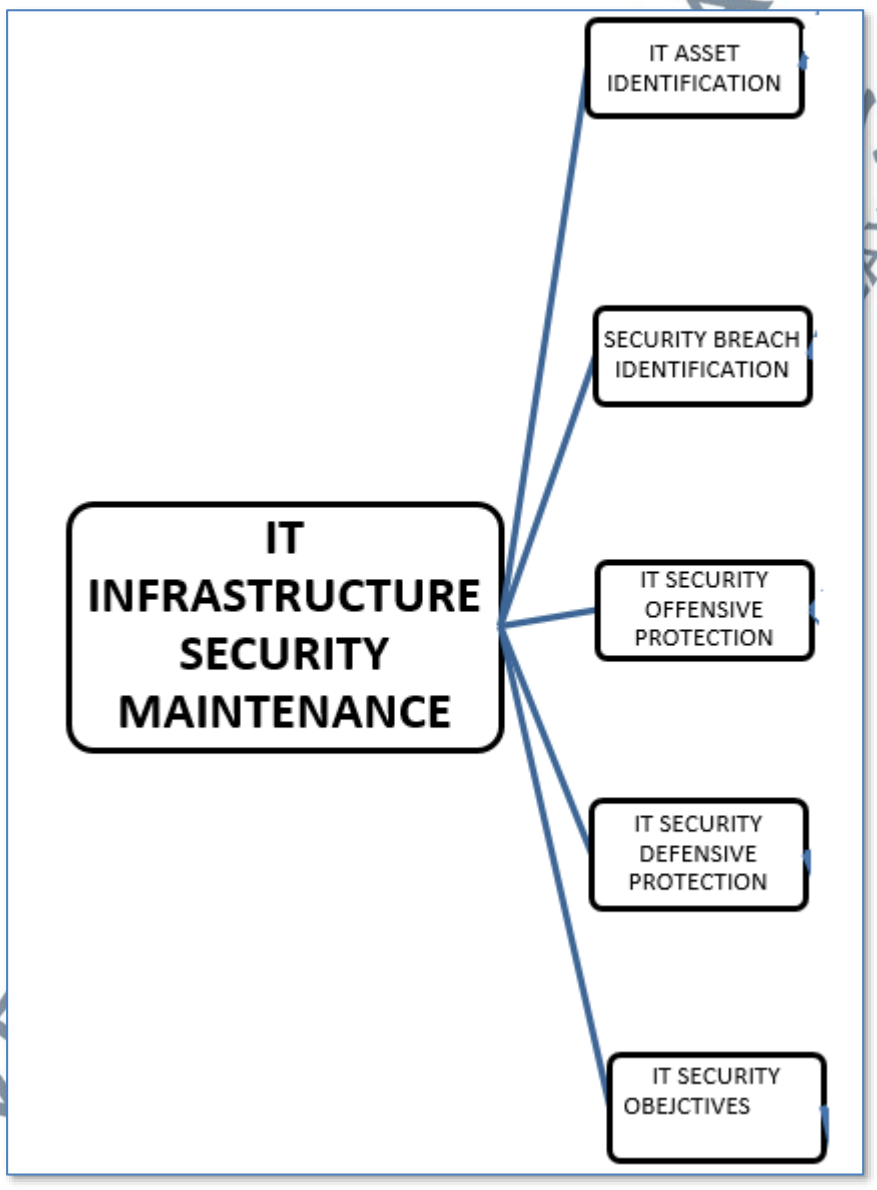

Figure 2.5: Proposed IT Security Maintenance Framework

2.8 Chapter Summary

After review of IT security management, this provides foundation knowledge and supporting evidences to develop an IT security maintenance framework for IT infrastructure. The development on Information Security Management System (ISMS) had a long development history in any organization and low adoption of ISO 27001 was observed (Mirtsch et al., 2020). The high cost and lengthy implementation time of ISMS are clear deterrents to organizations adopting the standard.

Therefore, an IT security maintenance framework for IT infrastructure based on putting the core and compatible requirements of ISO 27001 ISMS for reducing the redundancy of the existing usage of ICT security safeguards and aimed to reduce domain's barriers. The development of an IT security maintenance framework for IT infrastructure is proposed as a common framework and overcome the limitations of integrated system theory, as well as adopting the key concepts from IT security management model, theories and concepts (Bandura, 1977; Chadwick & Hibbert, 2013).

Moreover, the PDCA approach was observed in ISO 27001 ISMS model. Combination of all the advantages in each model as example like understanding customer requirements, value-added processes, processes performance and effectiveness, continually improvement and others to develop the IT security maintenance framework for IT infrastructure.

A review on different approaches of IT security management model was performed such as ISO/IEC 27005:2018 and PDCA framework. This is combined with PDCA and IT security management model to fulfill ISO 27001:2017 standard. Lastly,

the different implementation models for ISMS and IT security management model had reviewed.

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA