DESIGN AND ANALYSIS PHYSICAL AND LOGICAL SECURITY USING TIA-942 AND ISO/IEC 27000 SERIES IN DATA CENTER OF PDII-LIPI

Mukhlis Anugrah Pratama[1], Mochammad Teguh Kurniawan[2].

[1]Information System Major, Industrial Engineering Faculty, Telkom University
[2]Information System Major, Industrial Engineering Faculty, Telkom University
Telekomunikasi Street 1, Dayeuh Kolot, Bandung, 40257
Phone: (022) 7564108, Fax: (022) 7565200.
E-mail: mukhlis.pratama17@gmail.com[1], teguhkurniawan@telkomuniversity.ac.id[2]

ABSTRACT (80-100 words)

By the growing of need for information technology, data center should provide optimal service for the company especially security. Pusat Dokumentasi and Informasi Ilmiah (PDII-LIPI) has implemented data center to support its business process. But there are problems that arise from weaknesses related to the implementation of data center planning in PDII-LIPI. Based on these, it's needed physical and logical security design of the data center in accordance withTIA-942 for physical security and ISO/IEC 27000 series for logical security and using PPDIOO Network Life-cycle methods with result the ideal design of data center security for PDII-LIPI.
Key words: Data center, Physical and Logical security of data center, TIA-942.

1. INTRODUCTION

The times driven by globalization is increased significantly. One of the effects of globalization is the development of information technology is very fast. The continued development of information technology, it will be a supporting element for enterprise information systems, not least the government (Fathinuddin, Teguh Kurniawan, & Kurniawati, 2014). For companies, the passage of business processes aligned with corporate goals is a basic requirement. The role of data center is vital for the company especially as a achievement component of the company's objectives. The data center should provide optimal service as the center of business services companies. Design criteria of the data center design must meet several aspects, like Availability, Scalability, Security, Performance, and Manageability (Arregoces, 2004).

One of the important aspect in design of the data center issecurity aspect. Information Security is the measures adopted to prevent unauthorized use, abuse modification, or denial of knowledge, facts, data, or the ability (Maiwald, 2011). Two to three percent of the organization's annual revenue is lost due to an incident that occurred on information security especially caused by human behavior (Alnatheer, 2015). It reinforced that network security is needed physically and logically.

Pusat Dokumentasi andInformasi Ilmiah (PDII) is an organization under the Indonesian Institute of Sciences (LIPI). PDII-LIPI principal task of carrying out the development and provision of documentation services information (LIPI, 2011). Based on observations of current conditions, PDII-LIPI has been using the data center. However, there are problems that arise from the weakness related to the implementation of data center planning in PDII-LIPI. The problems such as the placement of data center that does not fit, no security for the data center room, logical data center security services is still minimal, and the lack of security of the data center to the disaster, such as fire. From the problems in PDII-LIPI, it can be concluded that, the main problems on the implementation of the data center in PDII-LIPI is no standard used to manage the data center, especially the physical and logical security standards.

In performing this research, methods used is the method Prepare, Plan, Design, Implement, Operate, Optimize (PPDIOO) and refers to the TIA-942 for physical security and ISO / IEC 27000 Series for logical security. Method PPDIOO approach focuses on how to design a good network, including its life cycle. This method helps companies to succeed in the development of technology end-to-end aligned with the core business of the CISCO. This method aligning business and technical requirements of each phase (Cisco 2005). This research resulted the design of data center security, both physically and logically in accordance withTIA-942 and ISO / IEC 27000 series for data center PDII-LIPI.

2. THEORETICAL BACKGROUND

2.1. Data Center

According to the definition of the Telecommunications Industry Association (TIA-942), the data center is a building or part of a building which has a primary function as a computer room and supporting areas (Telecommunications Industry Association, 2005).

According Arregoces&Portolani in the book Fundamentals Data Center, Data Center is a place that contains critical computing resources located in a controlled environment and under the control of a centralized by enabling organizations to use it as a support business continuity (Arregoces, 2004).

2.2. Physical Attack on Data Center

According to John Kingsley-Hefty in the book Physical Security Strategy and Process Playbook (Kingsley-Hefty, 2013) physical attack that often occurs in the data center, which is as follows (Kingsley-Hefty, 2013):

1. Environmental Factors
2. Acts of nature
3. Uninvited guests
4. infrastructure theft

2.3. Logical Attack on Data Center

According Arregoces and Portolani, attacks on the logical common are as follows (Arregoces, 2004):

1. Scanning / Probing
2. Denial of Service (DoS)
3. Unauthorized Access
4. Eavesdropping
5. Malware
6. Layer 2 Attack

2.4. Telecommunication Standard for Data Center (TIA-942)

Telecommunications Industry Association (TIA-942) is an American national standard that specifies minimum requirements for telecommunications infrastructure of data centers and computer rooms. Topology prepared in this standard is intended to be applied in all types of data centers. TIA-942 discusses the procedures for Network architecture, Electrical design, file storage, backup and archiving, system redundancy, network access control and security, database management, Web hosting, Application hosting, content distribution, Environmental control, Protection against physical hazards (fire, flood, Windstorm), and Power management (Telecommunications Industry Association, 2005).

2.5. Information Security Management Systems (ISMS)

ISMS, or Information Security Management System consists of policies, procedures, guidelines and related resources and activities are collectively managed by an organization in the form of asset protection of its achievement. ISMS is a systematic approach for determining, implementing, operating, monitoring, reviewing, maintaining and improving information security of an organization to achieve its business objectives (ISO/ IEC, 2014).

2.6. PPDIOO Method

The following explanation of each stage of the lifecycle PPDIOO Network (Cisco 2005):

1. Prepare Phase

In this stage, the determination of business needs and vision of appropriate development strategies and identify technologies that are used to support the growth plan, as well as the proposed architecture with high level design through testing.

2. Stage Plan

In this stage, the determination of whether the condition is currently able to support the proposed system, ensuring resources are available to manage the technology company from design to implementation.

3. Stage Design

In this stage of detailed design development and comprehensive according to business

needs and technical requirements to support availability, reliability, security, scalability, and performance.

4. Implement Phase

In this stage, the integration of the device without disrupting the continuity of business processes, testing the proposed system, perform the installation, configuration and integration of the results of the design that has been made.

5. Operate Phase

In this stage, network operations, maintain the network, and monitoring the performance, capacity, availability, security and reliability. The researcher also associated management problems that occur on the system.

6. Optimize Phase

In this stage, checks whether the system has been running already meet the objective and ensure that the system improves operational performance.

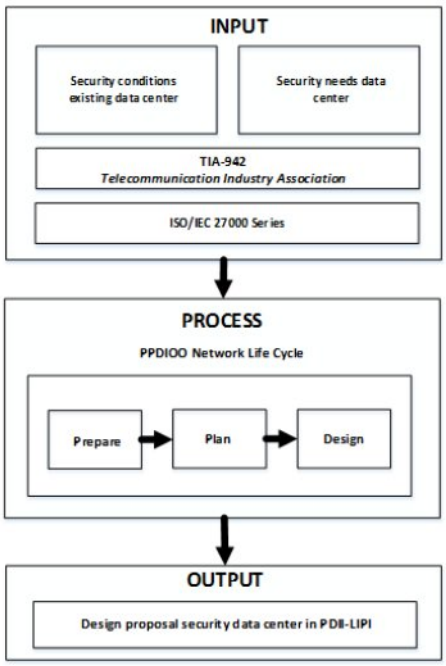

Figure 1. Conceptual Model

3. RESEARCH METHOD

3.1 Conceptual Model

The conceptual model describes the concept of logic description to help solving the problems that will be designed in this study. In this research used methods PPDIOO. In the framework of the conceptual model described research Design and Analysis of Physical and Logical Security at the Data Center of PDII-LIPI.

3.2 Research Systematic

This research used research systematic to determine the flow of the stages of research for problem resolution. Stages of research conducted in accordance with the stages available on the network development methods PPDIOO.In this research conducted several stages of the prepare phase, plan phase, and the design phase for the method PPDIOO and added two stages for the completion of this research is the analysis phase, and the final stage. Based on problem definition, application methods PPDIOO only reached the stage of design.

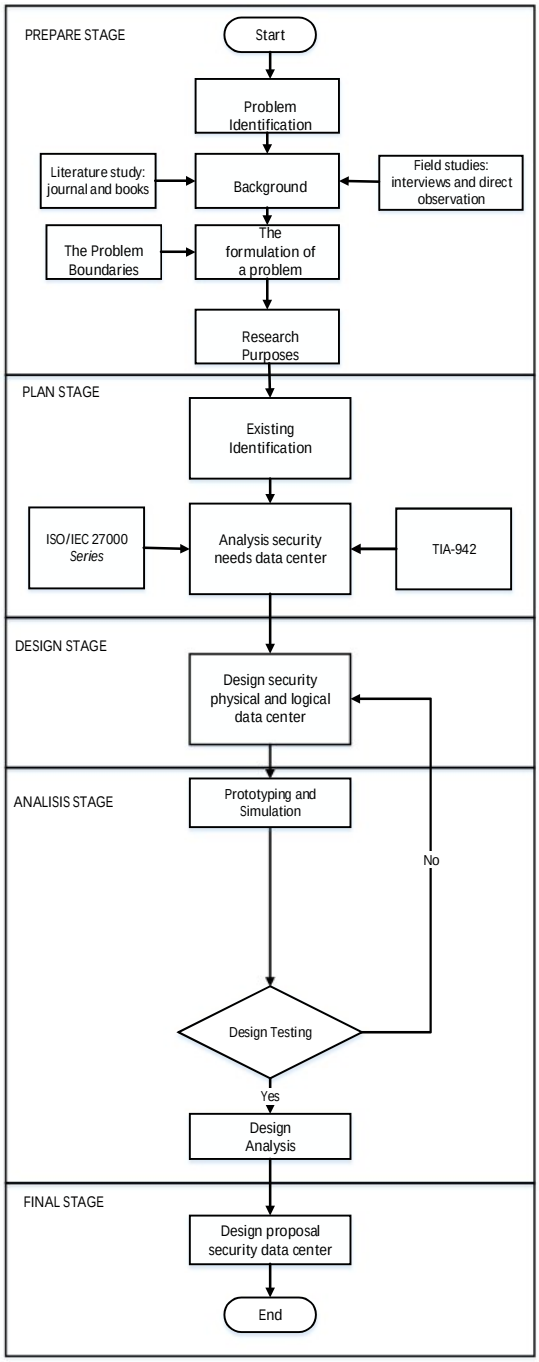

Figure 2. Research systematic

4. RESULT AND DISCUSSION

4.1 Result

In this research conducted the identification of physical and logical security of the data center PDII-LIPI with the following results:

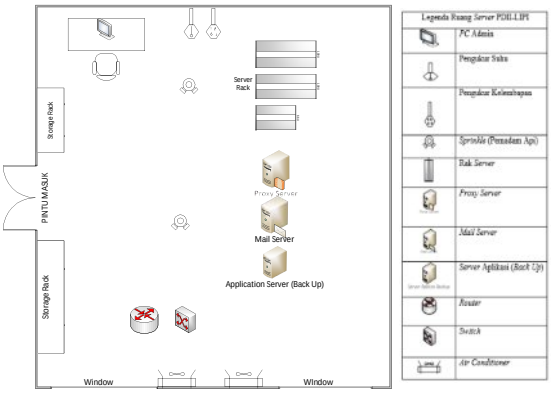

Figure 3. Plan Space Server

Figure 3 shows the plan space of PDII-LIPI server. It simply uses the server room work space be transformed to enable the server room. Based on observation, physical security of data center space was minimal when referring to the TIA-942. Data center room is adjacent to the workspace and make it unsafe because it allows unauthorized access to the data center room. The space does not have security, in addition to the storage room keys were put in the room that can be accessed by anyone. The room also unsupervised data center in real time because there is no surveillance cameras or CCTV installed in the data center room. To safeguard against disaster, data center space in PDII-LIPI also very minimal with only providing fire extinguishers that are corrective controls without special sensors.

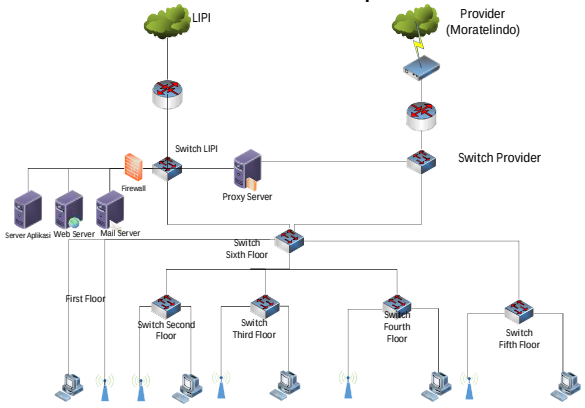

Figure 4. Network Infrastructure PDII-LIPI

Figure 4 show that the PDII-LIPI has two internet networks, from LIPI and provider (Kurniawan, Nurfajar, Dwi, and Yunan, 2016). Based on observations, the current condition of PDII-LIPI already using a firewall, proxy and antivirus, antimalware as

logical security. In addition, the PDII-LIPI has been running a backup procedure and has implemented a VPN. PDII-LIPI also apply Demilitarized Zone or DMZ is used to interact with outside networks PDII-LIPI. Based on observations of the logical data center security PDII-LIPI still not in accordance with ISO / IEC 27002. PDII-LIPI does not has a policy on information security, doesn't has automatically updates procedures and the lack of security-related security services. The lack of security created vulnerabilities on servers that can disrupt business processes of PDII-LIPI. It proves the logical data center security PDII-LIPI has not completely worked well.

Then conducted gap analysis to theidentification results of the current conditions with the physical and logical security standards used in the data center with the following results.

The first analysis is compare the gap between physical data center security conditions with the TIA-942 standard. The reasons for selecting the standard TIA-942 is due to TIA-942 provides minimum requirements of data center infrastructure that is discussed in detail in TIA-942 and can be applied to any type of data center.

Table 1. Gap Analysis between TIA-942 and Current Physical Security

No	*Checklist*	TIA-942 (Yes/No)	Existing Condition
Domain: ***Architectural***			
Subdomain: *CCTV Monitoring*			
1	Door	Yes	No
2	Computer Room	Yes	No
Subdomain: CCTV			
1	CCTV record all activity	Yes	No
2	Bitrate record (fps)	Yes	No
Subdomain: *Security Access Control/Monitoring*			
1	Access control to data center room	Yes	No
Domain: ***Mechanical***			
Subdomain: *Fire Suppression*			
1	Pre-action Fire Suppression	Yes	No
2	Clean-agent Fire Suppression	Yes	No

Table 1 shows that the 100% gap between physical security data centerof PDII-LIPI with TIA-942. The absence of CCTV and access control to the data center room can cause potential damage and theft of assets increases. In addition, the selection of existing fire suppression are not pre-action (preventive) and use materials that are not clean-agent can cause damage to the data center or the loss of data saved in the data center.

The second analysis is compare the gap between logical data center security conditions with ISO / IEC 27002. The reason for selection of standard ISO / IEC 27002 is a standard because that standard is commonly used in information security technology and can be used by all types and sizes of organizations.

Table 2. Gap Analysis between TIA-942 and Current Logical Security

No	*Checklist*	ISO/IEC 27002(Yes/No)	Existing Condition
Domain: ***Information Security Policies*** **(5)**			
1	Information security policy (5.1.1)	Yes	No
Domain: ***Operations Security*** **(12)**			
1	Malware protection (12.2.1)	Yes	Yes
2	Back up policy (12.3.1)	Yes	Yes
3	Procedure operating system update (12.5.1)	Yes	No
Domain: ***Communications Security*** **(13)**			
1	IDS(Intrusion Detection System) Implementation (13.1.2)	Yes	No
2	VPN(Virtual Private Network) Implementation (13.1.2)	Yes	Yes
3	Firewall Implementation (13.1.2)		
a	Technology for security services	Yes	No
b	Technical parameter for safe connections	Yes	Yes

Table 2 shows that 50% gap between logical data center security of PDII-LIPI with ISO / IEC 27002. PDII-LIPI as a manager of a data center, isn't implement policies related to information security. PDII-LIPI also not apply operating system updates regularly. This make the server vulnerable to attacks that exploit the information resources on the server. IDS has not led to the implementation of unsupervised data traffic and scanning services can still be done. Some checklist that has been applied to the PDII-LIPI is the installation of a firewall as protection against unauthorized access, but the application firewall in PDII-LIPI only as technical parameters, namely by setting a rule for security of the connection is applied to the server'soperating system. PDII-LIPI has also implemented antimalware and auto back up to protect the data that exist in the data center PDII-LIPI. Besides the

implementation of Virtual Private Network (VPN) already implemented by PDII-LIPI because of different needs and priorities of access to the network or data center.

4.2 Discussion

In this research, based on the identification and gap analysis results be designed the proposed design of data center physical and logicalsecurity. In the proposed design of the data center's physical security is need implementation of CCTV, access control data center room using fingerprint and fire extinguishers which is preventive and clean-agents.

Based on analysis of the gap between the current conditions with the TIA-942 standard, required a surveillances for physical securityin PDII-LIPI data center like Closed Circuit Television (CCTV) in accordance with the TIA-942 standard. The design of this CCTV camera placement is accordance with the TIA-942 standard.

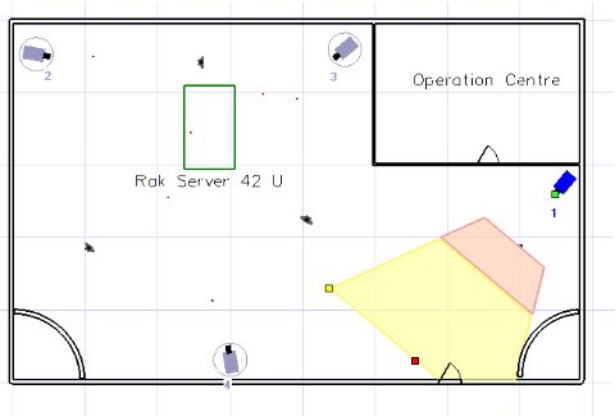

Figure 5. The laying of the Position Camera

Based on camera placement in Figure 5, then the camera coverage is like Figure 6.

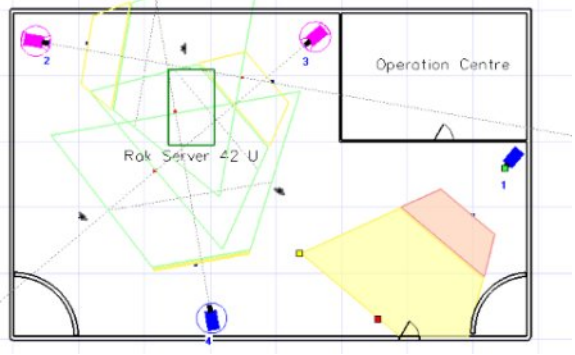

Figure 6. Coverage Observation Camera

Based on observations, obtained coverage comprehensive view. There is no blank spot in the observation coverage. For the calculation of bandwidth and disk space used to store the results of CCTV per day as shown in Table 3

Table 3. Bandwidthand Hard Disk Space Used Per Day

Resolution (pixel)	Compress Type	FPS	Frame Size (kB)	Bandwidth (Mbit/s)	Disk Space (GB)	Bitrate Record (kbit/s)
1280x1024	H.264	20	16	2.62	28.3	2621
640x480	H.264	20	3.8	1.25	13.4	623
640x480	H.264	20	3.8	1.87	20.2	623
640x480	H.264	20	3.8	2.49	26.9	623
Total				8.23	88.8	

Bandwidth and hard drive space to store the results of monitoring for a day is 8.23 Mbit / s and 88.8 GB. The bandwidth calculation is done for each connected user on the network requires a bandwidth corresponding to the activity of the work done (Fathinuddin, TeguhKurniawan, &Kurniawati, 2014). CCTV cameras used an IP camera so that the calculation required bandwidth for CCTV cameras connected to the network. While the hard drive calculation is performed to determine the needs of storage required to store the results of the CCTV footage.

Based on analysis of the gap between the current conditions with the TIA-942 standard, required an access control for PDII-LIPI's data center room as physical security like card or biometric access to the entrance and exit the data center room in accordance with the TIA-942 standard. For the proposed access control data center room is access control using biometric fingerprint access. The reasons for selecting biometric access is using biometric access that is very effective and can't possibly lose the biometric access device.

Based on analysis of the gap between the current conditions with the standard TIA-942, required a fire-extinguishing systems for physical security of the fire disaster for data center PDII-LIPI in the form of fire suppression are pre-action and clean agents for data center room in accordance with the TIA-942. Clean-gas is fire extinguishing agents are non-conductive, volatile and leaves no residue. This is done to minimize the possibility of fire in the data center room that result in damage to assets or loss of important data stored on the company's data center.

Furthermore, in designing the logical security of the data center proposed the information

security policies, automatic updatesprocedures of the operating system, and communications security technology implementations.

Based on analysis of the gap between the current conditions with ISO / IEC 27002, there is need a policy related to information security for the security of logical data center PDII-LIPI is policy information security should be defined, approved by management, published and communicated to all employees and external parties Related accordance with ISO / IEC 27002. An information security policy is useful for defining and agreeing the level of control over the implementation of activities related to data and information. Some of the information security policy must be defined and approved PDII-LIPI management related logical data center security, namely:

Table 4. Information Security Policy Proposal

No	Policy Topic
1	Access Control
2	Security physical and environment
3	Restrictions installation software and its use
4	Back Up
5	Information Transfer
6	Malware Protection
7	Vulnerability Management
8	Cryptography Control
9	Communications Security
10	Relationship with Supplier

With the implementation of the policy is expected to provide direction and support for security-related information in accordance with the needs of PDII-LIPI and can be used as reference material for all the activities related to data and information.

Based on analysis of the gap between the current conditions with ISO / IEC 27002 requires a procedure related to the operating system update periodically to ensure operational integrity of the system in accordance with ISO / IEC 27002. In this procedure periodically update the operating system can eliminate or reduce vulnerability that may occur in the operating system before it is updated so can create a secure server. In this proposed operating system updates automatically on a regular basis using the features in the Ubuntu operating system that is using one of the features in the facility package management system that can update automatically. This feature is called Unattended Upgrades that can be used to automatically update the operating system (Ubuntu, 2014).

Based on analysis of the gap between the current conditions with ISO / IEC 27002 requires an implementation of intrusion detection system or IDS to monitor data traffic on the data center that is used as one of the proposed security logic data center of PDII-LIPI in accordance with ISO / IEC 27002.Implementation of IDS is part of the security services that is security of communication is one of the criteria that should be applied to the data center network. Based on ISO / IEC 27002, Implementation of IDS has the objective of ensuring the protection of information in networks and supporting information processing facilities. Proposed IDS is applied to the PDII-LIPI is the application of IDS to detect attacks on web applications and detect DoS attacks. The reasons for selecting a proposal for a solution to PDII-LIPI use web applications to support business processes and to avoid a theft of data by a user who is not authorized.

Based on analysis of the gap between the current conditions with ISO / IEC 27002, there is need a firewall implementation as one logical data center security-related packet filtering in accordance with ISO / IEC 27002. For the proposed firewall packet filtering is implemented as a hardware firewall. The reasons for selecting a hardware firewall is a technology for security of network services and network management that is placed between the internal network and the Internet in this case acts as a hardware firewall packet filtering firewall works at the network layer so that unauthorized access is reduced. It can minimize the possibility of unauthorized access to the data center PDII-LIPI.

5. CONCLUSION

The following are conclusions from the research:

1. Servers located in the data center room PDII-LIPI not been well managed in terms of physical security. Data center physical security PDII-LIPI not in accordance with the TIA-942. The layout of the data center room is adjacent to the workspace and

have no security. In addition the data center room also unsupervised in real time using a surveillance camera. For security-related disasters, is available only fire-extinguisher which is corrective without special sensor

2. Servers located in the data center room PDII-LIPI not been well managed in terms of security logic. Logical security data center has not implemented a policy on information security, the absence of the operating system update procedure automatically and periodically, and the absence of security implementation services.
3. Physical security of the proposed data center is the implementation of the CCTV cameras. In addition it is proposed also control access to the data center room by using fingerprint and proposed also a fire extinguishing system for physical security against fire disaster using fire extinguisher which is pre-action and use materials that are clean agents.
4. Security logic of the proposed data center is to identify the policies on information security that is used as a control in the implementation of activity-related data and information. In addition, the proposed procedures also update the operating system regularly to reduce the vulnerability on the server. For the security of data center services PDII-LIPI, the proposed implementation of intrusion detection system (IDS) and firewall implementations as packet filtering.

6. REFERENCES

(a) Alnatheer, M. A. (2015). Information Security Culture Critical Success Factors. *Information Security Culture*, 1.
(b) Arregoces, M. a. (2004). *Data Center Fundamentals.* Indianapolis: Cisco Press.
(c) Cisco. (2005). CREATING BUSINESS VALUE AND OPERATIONAL EXCELLENCE. 4.
(d) Fathinuddin, M., Teguh Kurniawan, M., & Kurniawati, A. (2014). Perancangan Topologi Jaringan Pada Pemerintah Kabupaten Bandung Dengan Metodologi NDLC Menggunakan GNS3. *SENTIA 2014-Polinema* (p. 1). Malang: SENTIA-Polinema.
(e) ISO/IEC. (2014). *Information Technology - Security Techniques - Information Security Management Systems - Overview Vocabulary 3rd Ed.* International Organization for Standarization.
(f) Kingsley-Hefty, J. (2013). *Physical Security Strategy and Process Playbook.* Oxford: Elsevier.
(g) LIPI. (2011). *Tentang Kami*. Retrieved 2015, from http://www.pdii.lipi.go.id/tentang-kami/
(h) Maiwald, E. (2011). *Network Security : A Beginner's Guide.* New York: McGraw-Hill.
(i) Telecommunications Industry Association. (2005). *Telecommunications Infrastructure Standard for Data Centers - TIA 942* (ANSI/TIA-942-2005 ed.). Arlington: Telecommunications Industry Association.
(j) Ubuntu. (2014). *Automatic Updates*. Retrieved 2016, from https://help.ubuntu.com/lts/serverguide/automatic-updates.html