RISK MANAGEMENT ANALYSIS OF NETWORK SECURITY USING SNI ISO / IEC 27001 APPROACH IN TVRI JAWA BARAT

Muhamad Rizki Fadillah[1], Angga Setiyadi[2]
[1,2] UNIKOM
Jalan Dipatiukur No. 112-116, Lebakgede, Coblong, Kota Bandung, Jawa Barat 40132
E-mail : rizkifadillah418@gmail.com[1], angga.setiyadi@email.unikom.ac.id[2]

ABSTRACT

TVRI West Java is one of the station broadcast area's Television of the Republic of Indonesia. At the operational aspects of the daily, the level of awareness about the security of information in TVRI West Java still less so that the necessary analysis of risk management to determine and identify the risk that arises and it'll happen in the TVRI West Java and testing network to find vulnerabilities that may emerge on the services and the network itself, the impact of the vulnerability of measured in accordance with the level of critical in business process in TVRI West Java. The approach SNI ISO/IEC 27001 to the requirements of the information security management system are encouraged by the Ministry of Communications and Information Technology in the regulation number 4 in 2016.

Keyword: RISK MANAGEMENT, NETWORK SECURITY, INFORMATION SECURITY, ISO 27001, TVRI Jawa Barat

1. PRELIMINARY

TVRI West Java is a regional television station established by Televisi Republik Indonesia for the West Java Province. Each agency requires good management of data and data / information security, so that the level of data and information security can be guaranteed. Because if it refers to the regulation of the minister of communication and information technology number 4 of 2016 that agencies must apply the SNI ISO / IEC 27001 standard. with Mr. Adit, as the IT coordinator, that employees of TVRI West Java are not yet aware of information security so events such as damage to networks that interfere to business processes can occur. Handling the risks that occur and that will occur on TVRI West Java has not been documented. So if there is an incident of loss, damage from both physical and digital assets has not met the standards imposed by the Ministry of Communication and Information. There has never been a test of network security on TVRI in West Java which can lead to business processes if the existing network on West Java TVRI is experiencing interference.

To overcome the problems that currently occur in West Java TVRI, an analysis of the risks that have occurred and will occur will be carried out so that the risks that exist on TVRI West Java can be identified and documented, and make a risk assessment that exists on TVRI West Java to find out the level of damage caused by existing risks, and testing the computer network to determine the vulnerability and the level of damage contained in computer networks on TVRI West Java.

It is expected that the implementation of SNI ISO / IEC 27001 parameters can be a solution to the problems that occur where SNI ISO / IEC 27001 becomes a requirement in the application of Information Security Management System to ensure the security, integrity and availability of data managed by TVRI West Java.

2. RESEARCH CONTENTS

2.1 2.1 Supporting Theories

1) Computer Network Security

Network security is the protection of corporate networks and services from unauthorized alteration, destruction or disclosure of data / information which aims to provide assurance that the network carries out important security related functions. In network security, organizations / companies must secure all aspects of their network resources. After resources are connected to the network, all host-based security attributes must be reviewed to understand how they are affected by the network environment. Servers on the network can contain sensitive data and information about how to access internal resources [2].

2) Information Security

Information security is protection of information from various threats to ensure the continuity of business processes, reduce the level of business risk, and increase opportunities for the business itself. In designing information system security systems there are information security aspects that must be considered. Aspects that must be considered are:

1. Confidentiality

Aspects that guarantee the confidentiality of data and information that can only be accessed by those who have authority over the information..

2. Integrity

Aspects that guarantee data and information cannot be changed without the knowledge of the competent

authorities, guarantee the completeness of information, and ensure that data is not damaged which can cause changes to the original data.

3. Availability

Aspects that guarantee data availability if data is needed and ensure users can access information without interference [2].

3) SNI ISO / IEC 27001

SNI ISO / IEC 27001 is a standard for establishing requirements for determining, implementing, monitoring, operating, improving, reviewing and maintaining an Information Security Management System (ISMS) which is documented in the viewpoint of overall business risk. The ISMS is designed to ensure the selection of adequate and proportional security controls to protect information assets and provide trust to related parties [4].

4) Risk

Risk is a danger or consequence that occurs as a result of an ongoing process or future event. Risk always blocks every individual or various institutions, including business organizations. in risk management, there are several levels, namely large risks and small risks [2].

5) Risk Management

Risk management is the process of identifying the level of vulnerability and threats to information used by an organization to achieve business objectives, and decide on countermeasures to minimize risk to an acceptable level, based on the value of information sources for organizations / companies [2].

6) Risk Management

Risk management needs to be planned and considered all alternative solutions, before mitigation is carried out, so that the expected results are effective and efficient. Some alternatives can be considered to use the likelihood table to determine the handling of risks can be seen in table 2.1 [2].

Table 1 Likelihood

Probability Factor	Impact				
	Very Low	Low	Medium	High	Critical
Very rarely	Low	Low	Medium	High	High
Rarely	Low	Low	Medium	High	Extreme
Sometimes	Low	Medium	High	Extreme	Extreme
Often	Medium	High	High	Extreme	Extreme
Very often	High	High	Extreme	Extreme	Extreme

7) Asset

Information is an asset for a company or organization, other assets have a certain value for each company or organization that must be protected, to ensure continuity in the company or organization, reduce damage caused by leakage of information security systems, increase return on investment and expand opportunities effort [2].

8) Computer Networks

A computer network is a group of interconnected computers using communication protocols through communication media. With the computer network then between computers, can exchange data and information, applications, Information Systems and other programs [1].

2.2 Risk Management Analysis

1) Risk Management Analysis Methodology

The research method used in this study is the PPDIOO method (Prepare, Plan, Design, Implement, Operate, and Optimize). This PPDIOO network development method was created by Cisco Systems Inc. to support the business processes carried out. This method has continuous phases, and each phase has steps to succeed in planning, designing, implementing, and operating a computer network system [9].

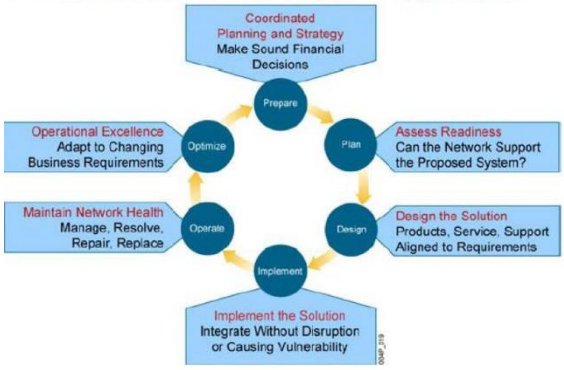


Figure 1 PPDIOO Method

a) *Prepare*

Research in this final project is to analyze the risks that occur and will occur on TVRI West Java. There are various problems that occur in handling the risks that occur in West Java TVRI, including the employees of West Java TVRI have not been concerned about information security, the West Java TVRI does not have documentation related to the handling of existing risks, and the West Java TVRI has never done computer network testing.

b) *Plan*

The solution that will be offered to deal with the problems that occur is to facilitate West Java TVRI in increasing awareness of information security, facilitate West Java TVRI in making documentation related to the risks that occur and that will occur and facilitate West Java TVRI in knowing computer network vulnerabilities.

c) *Design*

Network security testing scenario on TVRI West Java is by identifying the presence and possible exploitation of security vulnerabilities on the network, which includes server devices on TVRI West Java. Test scenario can be seen in Figure 2.

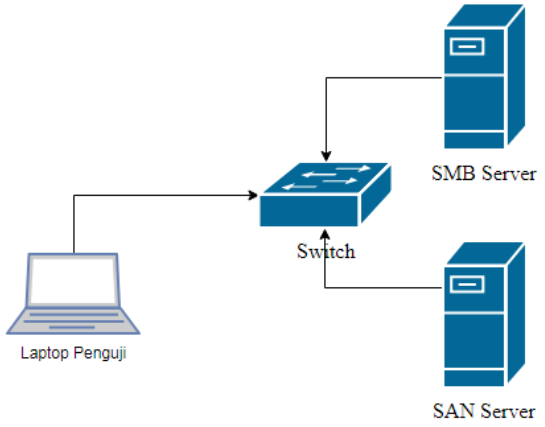


Figure 2 Network Testing Scenario

For computer network topology on TVRI West Java consists of 2 main networks; 1 SAN network, and 1 main network connects all parts of the work. SAN networks consist of storage units, and service provider servers. This SAN network is then connected to the main network via the PC Router. The main network is a combination of several small networks in each part, which are connected to the PC Router. Computer network topology on TVRI West Java can be seen in Figure 3.

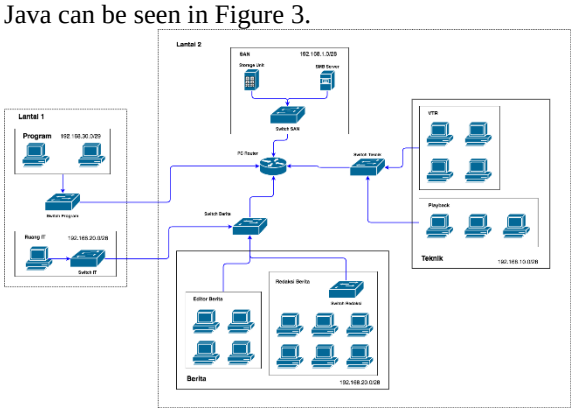


Figure 3 computer network topology

d) *Implement*

This stage is carried out the analysis and testing of computer networks to determine the vulnerabilities and impacts that affect the business processes of West Java TVRI, testing computer networks carried out on SMB servers and Storage servers where the two servers are the main servers that support business processes in West Java TVRI. What is done in this implementation includes network control analysis on TVRI West Java, security analysis of network services, and analysis of separation in the network.

2.2 Test Result

After the design and implementation phase is carried out, the next stage is testing the network control, testing the security of network services and testing the separation in the network, and making recommendations regarding network control testing, network service security testing and network separation testing.

1) Network control testing

Testing network control to test the compliance of TVRI West Java in managing network control over the requirements contained in SNI ISO / IEC 27001. Network control testing can be seen in table 2

Tabll 2 Network Control Test Results

No	Information	Applied	Documented	Not Applied
1	Is the network managed and controlled to protect information in systems and applications?	v		
2	Are security mechanisms, service levels and management requirements of network services identified and included in network service agreements?		v	
3	Are information services, users and information systems separated on the network?	v		
4	Are there official transfer policies, procedures and controls to protect the movement of information through the use of all types of	v		

	communication facilities.			

Based on Table 2, it can be concluded that TVRI West Java has carried out network control in accordance with SNI ISO / IEC 27001, but it has not been documented so that TVRI West Java must document the control of the existing network.

2) Analysis and Recommendations of Network Control

The results of network control testing, TVRI West Java has several aspects related to network control. The recommendation of network control testing is to document and implement network control aspects.

3) Network Service Security Testing

Network service security testing is carried out on a computer network on TVRI West Java to identify the existence and possibility of exploiting security vulnerabilities on the network, which includes server devices on TVRI West Java. The computer network security testing process has several security loopholes and tries to exploit these vulnerabilities. There are several findings on network security vulnerabilities on SAN and SMB servers on TVRI West Java, as follows:

a) Weak password, this vulnerability is found on both servers with the IP Address 192.168.10.2 and 192.168.10.3. The use of this weak test allows passwords to log in to the server. Test verification results can be seen in Figures 4 and 5.

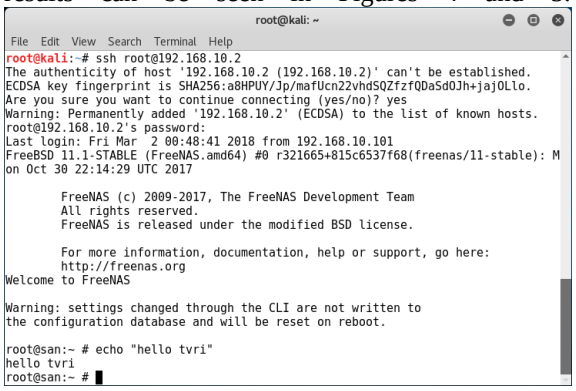


Figure 4 Weak Password Test Results on ip 192.168.10.2

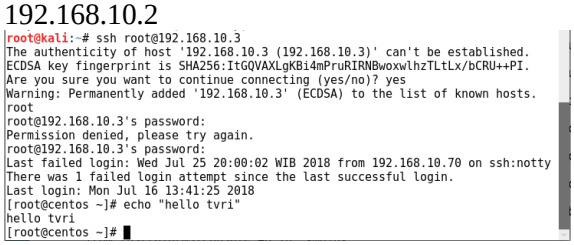


Figure 5 Weak Password Test Results on ip 192.168.10.2

a) *iSCSI Unauthinticated Target Detection, this vulnerability is found on the SAN server with ip 192.168.10.2. iSCSI configurations that have not used authentication mechanisms allow testers to access iSCSI without authentication* terlebih dahulu. Test verification results can be seen in Figure 6.

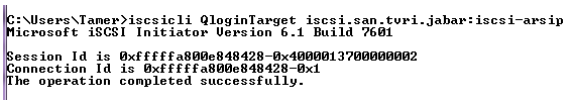


Figure 6 Unauthenticated Target Detection iSCSI Test Results

4) Network Service Security Analysis and Recommendations

From the description of the test results in the network service security testing section, the following is a table of analysis and recommendations for testing network security services on TVRI West Java. Analysis and recommendations can be seen in table 3.

IP	Vulnerability	Category	Impact	Recommendation
192.168.10.2	*Weak Password*	*Security Misconfiguration*	There is the use of weak password on the server so that the system can be taken over (root compromised)	Change SSH password in accordance with the password policy conditions on TVRI West Java
192.168.10.3	*Weak Password*	*Security Misconfiguration*	There is the use of weak password on the server so that the system can be taken over (root compromised)	Change SSH password in accordance with the password policy conditions on TVRI West Java
	iSCSI Unauthinticated Target Detection	*Security Misconfiguration*	There is a default configuration that does not use	Add an authentication mechanism in the iSCSI

			an authentication mechanism so that testers can access iSCSI without prior authentication	configuration

5) separation testing in the network

Testing of separation in the network to test the compliance of TVRI West Java in managing the separation in the requirements contained in SNI ISO / IEC 27001. Testing of separation in the network can be seen in Table 4.

	SAN	Teknik	Berita	Program
Subnet Mask	255.255.255.240	255.255.255.240	255.255.255.240	255.255.255.240
Number of hosts	2^4-2=14	2^4-2=14	2^4-2=14	2^3-2=6
Network Address	192.168.1.0/28	192.168.10.0/28	192.168.20.0/28	192.168.30.0/29
First host address	192.168.1.1	192.168.10.1	192.168.20.1	192.168.30.1
Last host address	192.168.1.15	192.168.10.15	192.168.20.15	192.168.30.7
Broadcast address	192.168.1.16	192.168.10.16	192.168.20.16	192.168.30.8

6) Analysis and recommendations

The results of testing the separation in the network, the West Java TVRI has implemented all aspects of separation in the network. The recommendation of testing the separation in the network is to make documentation related to separation in the network.

3. CLOSING

1) Conclusion

Based on the description in the previous chapters, some conclusions can be drawn from this study, including:

1. This research has proven to facilitate the IT field in identifying, analyzing, and documenting risks to computer networks on TVRI West Java.
2. This research can help the task of IT in securing computer networks on TVRI West Java.
3. This research can provide direction for the preparation of the implementation of the Information Security Management System which is based on the regulation of the Minister of Communication and Information Technology number 4 of 2016 that agencies must apply the SNI ISO / IEC 27001 standard.

2) Suggestions

This research still has all the limitations and disadvantages both in terms of readiness, and the completeness. Therefore, suggestions are needed to improve these limitations and shortcomings, including:

1. Required readiness from all elements of staffing of West Java TVRI to apply all parameters of SNI ISO / IEC 27001.
2. Information security information dissemination is needed for all West Java TVRI employees.
3. Periodic testing / auditing is needed to maintain the security of all aspects for the smooth running of business processes on West Java TVRI.

BIBLIOGRAPHY

[1] B. A. Forouzan and S. C. Fegan, Data Communications and Networking, 4th ed., McGraw-Hill, 2007.

[2] B. G. Ragard, Information Security Management: Concepts and Practice, CRC PRESS, 2010.

[3] *CISA Review Manual*, 2006.

[4] SNI ISO/IEC 27001, BSN, 2013.

[5] https://nmap.org/, diakses pada tanggal 7 Juni 2018

[6] https://tenable.com/, diakses pada tanggal 5 juni 2018

[7] S. Wilkins, "PPDIOO Stages > Cisco's PPDIOO Network Cycle," 2011. [Online]. [Accessed 27 Oktober 2017].