DATA SECURITY ASSESMENT: ISO/IEC 27002 MODEL BASED

Rizal S[1], Cholil W[2], Widiyati Q[3]
Computer Science Faculty, Bina Darma University
Palembang, South Sumatera
syahri_rizal@binadarma.ac.id, widya@binadarma.ac.id

ABSTRACT

Most of Organization using the Information Technology is to enhance the performance of their process business and increase the productivity. There are no doubt about the successfully of using IT, but another problems that produce from this paradigm that data security awareness. This paper will describe the assessment process of data security process management and implementation at the research object which is has implementing IT as the main support in their Process Business. The assessment model based on ISO/IEC 27002, as an internal standard of cyber security issues. The result of this paper will be input to the Object in another assessment IT process business.

KEY WORDS

Data Security, Risk Assessment, ISO/IEC 27002. Information Technology.

1. Introduction

IT audit represents process of collecting and assessment of evidence based on which successfulness of information system can be estimated, or based on which it can be determined if functioning of information system is in function of safeguarding of assets and maintaining of integrity of data. Furthermore, it is also necessary to determine if information system supports effective achievement of goals and if system resources are used in effective and efficient manner. Beside its exact and analytical function, IT audit today also represents modern consulting function – "right hand" which helps management in IT governance.

1. Data Security Standards

This research was using ISO/IEC 27002 as the standardization for Data Security. This standard already recommended as the Information security standard globally which applicable to achieved the beneficial of Organization Data Security globally.

ISO / IEC 27002 published in 2009 and is the Indonesian version of the ISO / IEC 27002: 2005, contain specifications or requirements that must be met in building the Information Security Management System (ISMS). This standard is independent of information technology products, require the use of risk-based management approach, and are designed to ensure security controls been able to protect the information assets of the various risks and give confidence level of security for interested parties. The standard was developed to approach process as a model for the establishing, implementing, operating, monitoring, reviewing (review), maintenance and improvement of an ISMS. Process approach stressed to encourage users to consider some important issues such as:

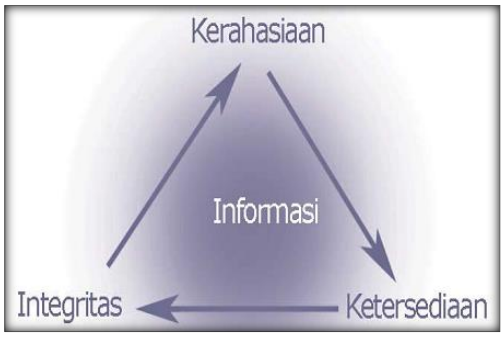
a). Understanding of the organization's information security requirements and the need for policies and objectives for information security

b). Monitoring and reviewing the performance and effectiveness of the ISMS, and

c). Continual improvement based on objective measurement of the level of achievement Security

Information security consists of protection against the following aspects:

1. Confidentiality aspects that ensure the confidentiality of data or information, ensuring that information can only be accessed by authorized persons and ensure the confidentiality of data sent, received and stored.
2. Integrity aspect which ensures that data is not modified without permission parties authorized (authorized), maintain the accuracy and integrity of information and methods of the process to ensure the integrity of this aspect.
3. Availability (availability) aspect which ensures that data will be available when needed, ensuring legitimate users can use the information and related devices (assets associated if necessary).



Picture 2.2 The elements of security information

2. The Infrastructure Network SCADA System

SCADA stands for Supervisory Control and Data Acquisition is a system for supervising and controlling of process equipment geographically dispersed. The reason the use of SCADA is because of the need to conduct direct supervision of the distribution of electricity, by collecting information on the state of equipment or devices in the field and take action on that information remotely or remotely in real time and centralized.

3.1 **Basic Functions SCADA**

The basic function of SCADA are:
1. Telemetering (TM)

Transmit information in the form of measurement of electrical quantities at a particular time, such as: voltage, current, frequency. Monitoring conducted by the dispatcher of them featuring real power in MW, MVA reactive power, voltage in KV, and the current in A.

2. Tele Signals (TS)

Sends signals indicating the status of an equipment or device. The information is sent in the form of status voltage breakers, separators, whether there is an alarm, and other signals. Telesinyal may be the condition of a single equipment, can also be the grouping of a number of conditions. Telesinyal can be expressed singly (single indication) or double (double indication).

3. Tele Control (TC)

Command to open or close the electrical power system equipment can be carried out by the dispatcher remotely, is just by pressing one button command open / close in dispatcher.

3.2 Basic Requirements of Control Center

A Control Center is a central station that should be fulfilled the following requirements:

a. Security, reliability, and availability of computer systems.

b. Convenience, continuity, accuracy of delivery, storage, and processing data.

c. Supply and support of the computer system.

d. Ease to operate and maintain.

e. Ability to develop.

4. Security Testing

4.1. Planning of Security Testing

In conducting safety testing data on the network infrastructure SCADA systems, the authors use the ISO / IEC 27002 as security standards and using CIA Triangle as a reference level of security that must meet the system so it can be said to be safe if the system fulfills the CIA Triangle and the standards of ISO / IEC 27002.

The author uses several clauses in ISO / IEC 27002 relating to research by the author. The clauses are:

1. Clause 5: Physical and environmental security.
2. Clause 6: Management of communications and operations.
3. Clause 7: Control access.
4. Clause 9: Management of information security incidents

The clause used above, the author evaluates the security level of data on the network infrastructure SCADA system by conducting interviews and penetration testing are used as evidence of safety evaluation data.

Table 3.1 Criteria for assessment index at maturity level

Status Keamanan	Kategori Pengamanan		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Perencanaan atau Diterapkan Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9

Source : ITGI (2007, p.18)

4.2. Implementation of Data Security Test

In testing the data security of network infrastructure SCADA system, the authors use the appropriate method described in data security standard ISO / IEC 27002 is an interview, examination and evidence.

In the interviews, the author interviewed the assistant manager of IT department that does have full authority over the security of the network infrastructure SCADA system.

Table 3.2 test result data security clause 5

No Klausa	Objek Kontrol	Kontol Keamanan	Penilaian						Hasil Bukti
			0	1	2	3	4	5	
5	Keamanan fisik dan lingkungan	Keamanan area perusahaan dari gangguan dari luar dan bencana alam (gempa, kebakaran, dll)					X		PT. PLN (Persero) UPB Sumbagsel terletak di kertapatih, daerah tersebut jauh dari gunung, sungai dan laut, sehingga kecil kemungkinan dari bencana ge,pa, kebanjiran. Selain itu, kantor PT.PLN (Persero) juga memiliki jarak dari gedung disekitarnya, sehingga memperkecil terjadinya kebakaran (Kecuali dari internal kantor)
5	Keamanan fisik dan lingkungan	Perlindungan peralatan perusahaan					X		Kantor PT. PLN (Persero) dikelilingi oleh pagar beton tinggi dan dijaga oleh security selama 24jam dan dilengkapi kamera CCTV untuk mengawasi seluruh area perusahaan
Total Nilai			8						
Rata-Rata			4						

4.3 Evidence of Security Test:

1) To ensure the proper application of process information. Author attach table availability of SCADA system.

Tabel 12. Asumsi Perhitungan Availability

PARAMETER ASUMSI	SATUAN	2012	2013	2014	2015	2016	2017
Kesiapan Master Station	%	99.91	99.92	99.93	99.94	99.95	99.96
Kesiapan Tele Informasi Data	%	96.10	96.20	96.30	96.40	96.50	96.60
Kesiapan Telekomunikasi	%	99.82	99.83	99.84	99.85	99.86	99.87

Tabel 13. Roadmap Availability

PARAMETER	SAT	2013	2014	2015	2016	2017
Kesiapan SCADA	%	95.00	95.20	95.40	95.60	95.80
Kesiapan Komunikasi dan Teleproteksi	%	98.00	98.10	98.20	98.30	98.40

Picture 3.1 SCADA *availability*

2) Using cryptographic controls. Author attach the monitoring packet in the data transfer from the RTU to the Master station

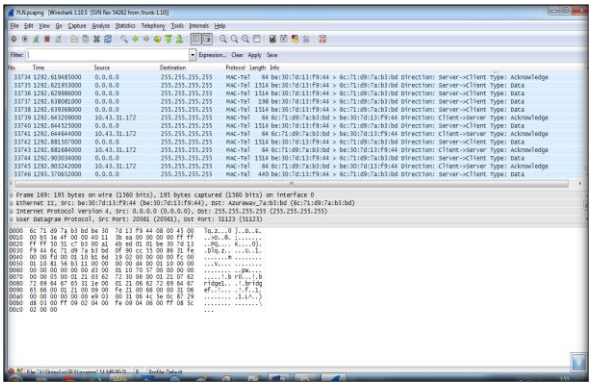


Figure 5.6 The results capture packets using wireshark

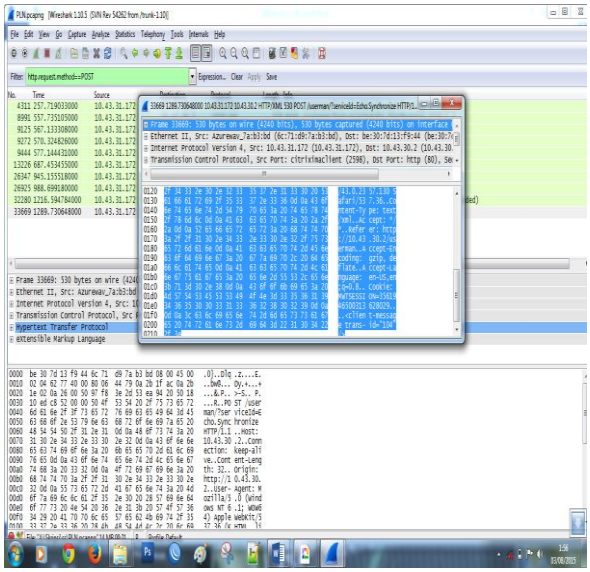


Figure 5.7 Selection of packet capture using http.request.method == POST to observe events that occurred during the input package delivery

In addition the writer suggestions are for testing clause 9, is considered safe and does not need repair or improvement of security, of the captured packet was no information that could be used in addition to SCADA server. Because as described in table testing, SCADA systems include encrypt module and the module decrypt so far possible interception.

5. Conclusion

As the results of this initial stage produced some conclusions are:

1. The level of security on the network infrastructure in the Object Research SCADA system has been included in both categories with reference to the security standard ISO / IEC 27002.
2. The level of security on the wireless network Object Research is still low. That is because there are many wireless networks in office networks do not use a password.
3. Need to build additional safeguards for media hotspot, for user management, bandwidth and performance monitoring of employees at Research Object. In addition, to avoid the use of the hotspots of the parties are not entitled and also to avoid tapping activities and loss of information on the office network Object Research

References

[1] Guldentops, E, 2003, "*Maturity Meansurement First the Purpose then the Methode*", Information Systems Control, Journal Vol. 4

[2] IT Governace Institute, 2007, "*Cobit 4.1"*, IT Governance Institute Illinois.

[3] IT Governance Institute, 2008," *Enterprise Value: Governance of It Investment*", IT Governance Institute Illinois.

[4] ISACA, 2012, "*Cobit 5 A Business Fremework for the Governace and Management of Enterprise IT*", USA, ISACA.

[5] Nugroho, Heru., "*Perancangan Model Kapabilitas Optimasi Sumber Daya TI Berdasarkan COBIT 5 Process Capability Model"*, Jurnal Teknologi Informasi Vol. 1, No. 5 (Mei 2013), hal 176-183.

[6] Sari IM., Ali, AHN., & Kurnia, I., "*Pembuatan Metode Evaluasi Kematangan Pelaksanaan Proyek dengan Menggabungkan COBIT 5 Domain BAI 1.11 dan MEA 1.04 dengan Best Practice PMBOK 4th.",* Jurnal Teknik POMITS Vol. 1, No. 1, (2013) hal. 1-8.

[7] Weber, Ron, 2000, "*Information Systems Controls and Audit*", New jersey, Pentice Hall Inc.