Security Analysis of Grr Rapid Response Network using COBIT 5 Framework

By SUNARDI

KONTAR KOMPUTER VOL. 10, NO. 1 APRIL 2019
DOI : 10.24843/LKJITI.2019.v10.i01.p04
Accredited B by RISTEKDIKTI Decree No. 51/E/KPT/2017

p-ISSN 2088-1541
e-ISSN 2541-5832

Security Analysis of GRR Rapid Response Network using COBIT 5 Framework

Imam Riadi[a1], Sunardi[b2], Eko Handoyo[c3]

[a] Department of Information System, Universitas Ahmad Dahlan
Jln. Prof. Dr. Soepomo, S.H. Janturan, Yogyakarta, Indonesia
[1]imam.riadi@is.uad.ac.id

[b] Department of Electrical Engeneering of, Universitas Ahmad Dahlan
Jln. Prof. Dr. Soepomo, S.H. Janturan, Yogyakarta, Indonesia
[2]sunardi@mti.uad.ac.id

[c] Department of Informatics, Universitas Ahmad Dahlan
Jln. Prof. Dr. Soepomo, S.H. Janturan, Yogyakarta, Indonesia
[3]eko1707048003@webmail.uad.ac.id (Corresponding author)

Abstract

Connection from the Internet is required to always be maintained under any conditions, but not always connectivity will run smoothly, lots of crowds or problems that require connections do not run smoothly. Application of security systems to overcome all problems and difficulties, both technical and non-technical which can affect system performance. GRR Rapid Response is the answer to internet network security. GRR asks for a client-server model, agents installed on the machine (client) to be able to communicate with the Grr server to access and provide unique client IDs. After setting this active and running, the server can send a request to the client who collects information, and the client sends a response to the request. After Grr is made, it is necessary to do a system evaluation and evaluation. The COBIT 5 framework is a good standard for determining the level of maturity of network security. The maturity level obtained is 2.899 can be decided at an institutional maturity level defined. The level of support the institution has agreed to, supports and supports all activities related to network security.

Keywords: *COBIT 5, Grr Rapid Response, Maturity Level, Network Security, Defined*

1. Introduction

Today, rapid technological developments have caused many companies to change the way they do business. Companies without using technology are sure to lag behind in many aspects such as efficiency, connectivity and effectiveness[1]. The Internet can be obtained by searching for the desired information[2]. Connection from the network is required under any circumstances, but connectivity is not always going well, a lot of complexity or problems related to the connection are not going well[3]. The penetration of internet and computer networks has increased rapidly in addition to providing convenience, but also has security problems for companies and individual database users[4]. Along with the development of technology, it is often misused by some irresponsible parties that can cause threats[5]. The application of security systems aims to overcome all problems and constraints, both technically and non-technically which can affect the performance of the system such as availability, confidentiality and integrity factors so that the level of security[6]. Security experts need to investigate the root of the problem, and reduce the threats that are being faced that might arise in the future, so digital forensics must be considered by security experts[7] is shown in Figure 1.

DOI : 10.24843/LKJITI.2019.v10.i01.p04
Accredited B by RISTEKDIKTI Decree No. 51/E/KPT/2017
p-ISSN 2088-1541
e-ISSN 2541-5832

Figure 1. Security aspects

GRR is a quick response procedure for an incident, using the Python language with the aim of conducting live forensics remotely. GRR can be used on hosts running different operating systems. GRR currently has no other competition in using live forensics [8]. The way GRR works are to collect non-synchronized client artifacts, requests with enabled IDs are sent to clients who are interested in collecting the sought artifact data, then serialized and saved to the GRR server. [9].Is shown in Figure 2.

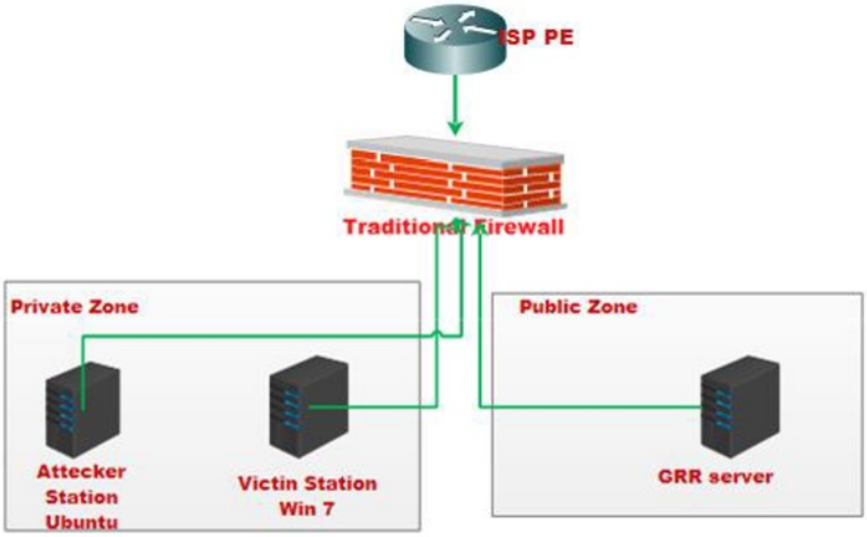

Figure 2. Experiment Setup Topology

Technology network security will get what effective results if it uses good governance in its use and is capable of value and evaluation. Network security can be evaluated with various standards su17as COBIT, COSO, ITIL, CMM, BS779, ISO 9000. The standard used in security in America is NIST Special Publication 800-30 Revision 1[10]. The standard, commonly used in Indonesia is ISO 27001[11]. While for this study us9g standards COBIT is a standard guide to information technology management practices and a set of documentation for best practices for IT governance that can help auditors, management, and users to bridge the gap among business risk, control needs, and technical issues[12]. This study aims to conduct an evaluation related to network security management that has been implemented with. This study aims to get the value of the level of network security that GRR Rapid Response has been designed by adding an

institutionalized GRR Rapid Response, so that recommendations and innovations can be made for information system security in the institution. So that institution can provide security and comfort for users of the network.

2. Research Methods

The method in this study consists in several stages. as shown in Figure 3.

Figure 3. Step method

The stages of the method are divided into six, namely observation, COBIT5 mapping framework, structuring questionnaires, calculating maturity level, gap analysis, and collecting data. The full description is as follows:

a. Observation

   This stage is doing obsession with internet networks that GRR Rapid Response has given so that we can know the work processes and procedures of GRR Rapid Response.

b. Mapping the COBIT5 Framework

   This stage is to carry out an activity statement in accordance with the framework COBIT 5 so that the activity compatibility can be obtained.

c. Preparation of questionnaires

   This stage is the making of a questionnaire that will be used to assess the ongoing security process.

d. Calculate Maturity level

   This stage is to calculate the maturity level from the results of the questionnaire that has been obtained so that the maturity level value can be obtained at this time.

e. Gap analysis.

   This stage is to analyze the gap between the current maturity level and the desired maturity target.

f. Compilation of recommendations

   This stage is to formulate recommendations that will be given to the agency so that they can be proposed as improvements to the existing network security.

LONTAR KOMPUTER VOL. 10, NO. 1 APRIL 2019 p-ISSN 2088-1541
DOI : 10.24843/LKJITI.2019.v10.i01.p04 e-ISSN 2541-5832
Accredited B by RISTEKDIKTI Decree No. 51/E/KPT/2017

3. Result and Discussion

In the results section and this discussion in full the stages of the research carried out are explained. As in the previous section this study has four stages. This section will discuss the results obtained at each stage.

3.1. Observation GRR Rapid Response Network

GRR is a procedure that consists of different modules, which focus on acquiring various types of live forensic information from client machines [13]. Additionally, GRR is an integral part of this particular model in order to aggregate data and provide forensic evidence[14]. Digital evidence analysis needs to be carried out in accordance with special procedure, procedures and according to forensic analysis, to obtain good digital evidence, so that from digital evidence in the form of valid information to support legal decisions in the trial[15]. This framework is also capable working with large networks as scalability is one of them motivation for the creation of GRR and has several methods to maintain privacy. After observing the network with GRR rapid response, the network topology can be obtained as shown in Figure 4.

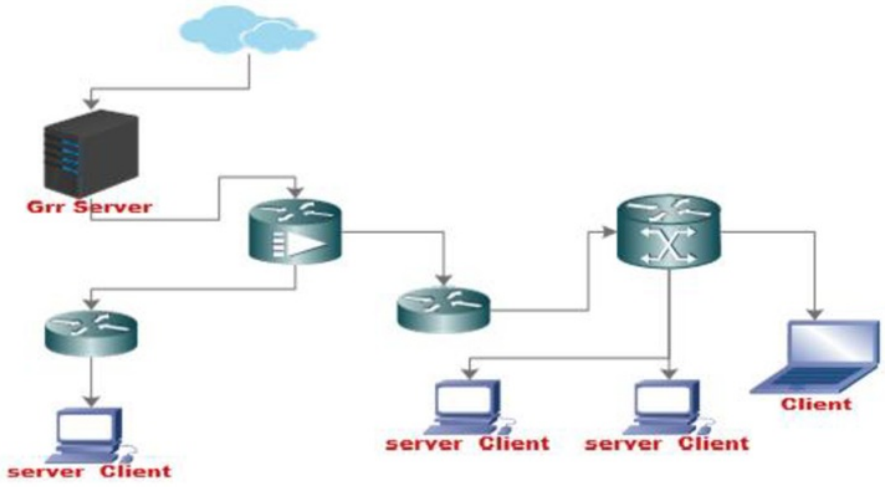

Figure 4. Network topology GRR rapid response

3.2. Mapping the COBIT5 Framework

This stage is mapping the COBIT 5 framework standard with the needs of existing network security evaluations. COBIT 5 framework consists of 5 main domains[16], as in Figure 5.

DOI : 10.24843/LKJITI.2019.v10.i01.p04
Accredited B by RISTEKDIKTI Decree No. 51/E/KPT/2017
p-ISSN 2088-1541
e-ISSN 2541-5832

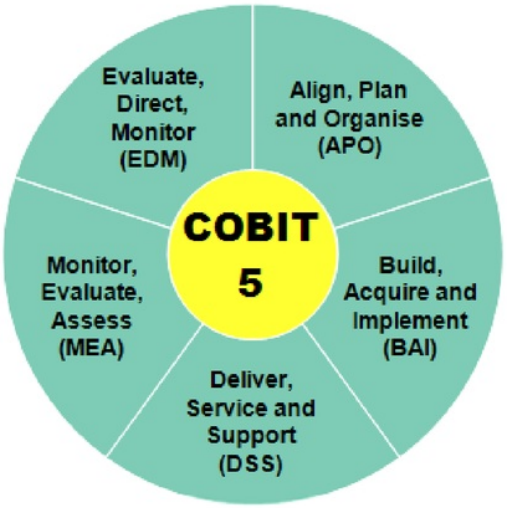

Figure 5. COBIT 5 Domain Framework

Of the 5 existing domains that collect evaluations related to network security is the DSS domain (Deliver, Service and Support). Where in this domain set 6 processes in information technology management[17], as in Figure 6.

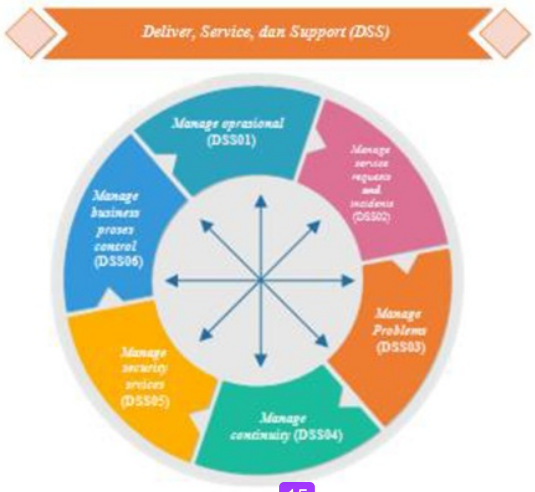

Figure 6. Domain DSS COBIT 5 Framework

DSS domain (Deliver, Service and Support) has sub-domains, namely managing security services (DSS05), this sub-domain is more focused on network security by having 7 processes and 49 activities, as in Figure 7.

KONTAR KOMPUTER VOL. 10, NO. 1 APRIL 2019
DOI : 10.24843/LKJITI.2019.v10.i01.p04
Accredited B by RISTEKDIKTI Decree No. 51/E/KPT/2017
p-ISSN 2088-1541
e-ISSN 2541-5832

Figure 7. Domain DSS05 COBIT 5 Framework

The next process is to compile the DSS05 domain suitability activities with the activities that will be made in the questionnaire. due to the limitations of our writing, we only included one of the 7 DSS05 sub-domain processes, namely DSS05.01. The DSS05.01 process consists of 6 activities, as in Table 1.

Table 1 Protect against malware activity

Protect against malware (DSS05.01)	
No	**Activity Questions**
1	Obtain information about malicious software and how to handle it.
2	Install and activate anti-virus on your PC.
3	Is antivirus on the PC always updated.
4	Regularly review and evaluate information about potential malware threats.
5	Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information.
6	Conduct periodic training on malware in the use of e-mail and the Internet.

3.3. Preparation of questionnaires

Questionnaires are used in the process of determining maturity values. There are 4 respondents in the institution that are related to the system, namely, Network Engineer, Developer Engineer, Admin, and client. To assess the DSS05 domain, a mapping between sub-control objectives and human resources is carried out in the implementation of information systems[18]. RACI is a diagram consisting of Responsible, Accountable, Consulted, and Informed [19]. The mapping is done for all control objectives that are in the DSS05 domain. As in Table 2.

Table 2 Diagram RACI

DSS05	Network Engineer	Devops Engineer	Admin	Client
01	R	C	A	I
02	R	A	I	I
03	I	A	I	R
04	C	I	A	R
05	C	A	I	R

06	I	I	R	I
07	R	C	A	I

This stage is to determine the scale of value for the ongoing network security process so that it can evaluate the network security activity process in the institution. As in Table 3.

Table 3 Scale value level

Value	Information
1	Are not done
3	Do
5	Done with SOP

From Table 3 it will be combined with Table 2 to get the activity process with DSS05 that will be formed in the questionnaire.

3.4. Calculate Maturity level

This stage is to calculate the data from the questionnaire with reference to maturity level. The questionnaire of this study was conducted on 4 respondents, where respondents were directing people who had direct responsibility for network security. While the absolute value which is the value of the maturity model can be seen in Table 4 below.

Table 4 Absolute value of the maturity model

Value	Information
0	There is no
1	Initialization
2	Can be repeated
3	Defined
4	Regulated
5	Optimized

Furthermore, the correlation between level values and absolute values that are done by calculation in the form of an index uses a mathematical formula. The mathematical equations to determine index values are as follows:

$$Index = \frac{\sum Most\ Question\ Answers}{\sum Questionnaire\ Questions} \quad (1)$$

The results of these measurements are converted into the maturity level with the scale as follows in Table 5.

Table 5 Scale of maturity level

Range	Maturity Level
0.00 – 0.50	0 (No Existent)
0.51 – 1.50	1 (initial)
1.51 – 2.50	2 (Managed)
2.51 – 3.50	3 (Defined)
3.51 – 4.50	4 (Managed and Measurable)
4.51 – 5.00	5 (Optimized)

The results of the questionnaire calculation to determine the level of model maturity of each control process. With calculations using mathematical equations and the scale of rounding the index in the previous table. The results of calculating the maturity level Existing. As in Table 6.

Table 6. Maturity Level Existing

DSS05	Total Question	Total Answer	Maturity level Existing
01	24	76	3.167
02	36	108	3.000
03	36	116	3.222
04	32	92	2.875
05	28	68	2.429
06	20	50	2.500
07	20	62	3.100

3.5. Gap analysis

Once the existing Maturity Level values are obtained and Maturity The recommendation level (target) has been determined, then the gap between the current condition and the target to be achieved will be analyzed and identified opportunities from the gap to be optimized, as in Table 7.

Table 7. Value of Maturity Level gap

DSS05	Target	*Index Maturity Level Existing*
01	5	3.167
02	5	3.000
03	5	3.222
04	5	2.875
05	5	2.429
06	5	2.500
07	5	3.100

From Table 7 is a comparison between the desired target and the achievement of the value of Maturity. The existing level of information technology security process has been done so far. So that it can be described as a graph Maturity Level gap as in Figure 8.

p-ISSN 2088-1541
e-ISSN 2541-5832

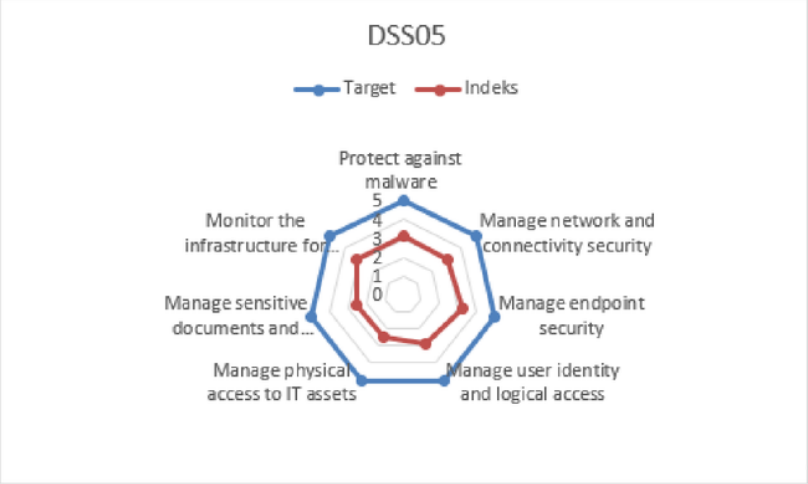

Figure 8 Gap analysis

Based on Gap analysis obtained from the results of the target level to be achieved and the level achieved on DSS05, as in Figure 8, then here is some Gap Maturity Level Analysis. As in Table 8 as follows.

Table 8 Gap Maturity Level Analysis

DSS05	*Maturity Level*
01	Defined
02	Defined
03	Defined
04	Defined
05	Managed
06	Managed
07	Defined

The overall value of Maturity Level on DSS05 will be calculated on average so that it will get the level of Maturity Level in the organization or institution[20].

$$\textbf{\textit{Maturity Level DSS05}} = \frac{\sum \textbf{\textit{Maturity Level}}}{\textbf{\textit{many processes}}} \quad (2)$$

$$DSS5 = \frac{i(DSS05.01) + i(DSS05.02) + i(DSS05.03) + i(DSS05.04) + i(DSS05.05) + i(DSS05.06) + i(DSS05.07)}{mp}$$

$$MLDSS05 = \frac{3{,}167 + 3{,}000 + 3{,}222 + 2{,}875 + 2{,}429 + 2{,}500 + 3{,}100}{7}$$

$$Maturity\ Level\ DSS05 = 2{,}899$$

From the calculation results obtained the value of achievement is 4,458 so that it can be set Maturity Level of organization or institution is at the Defined level.

3.6. Compilation of recommendations

After Maturity Level has been determined, the recommendation preparation process will be carried out. Recommendations that can be given to improve the quality of information system security in the agency:

1) Protect against malware (DSS05.01) is on a Defined level where in this level institutions have implemented network security properly, documented and monitored related to malware. It's just that it still needs a process of development, evaluation and innovation related to network security. So that the maximum results obtained in the next evaluation.
2) Manage network and connectivity security (DSS05.02) is on a Defined level where in this level institutions have implemented security related to network security. Establishing a system used to evaluate threats that will arise, documented and monitored. It's just that it still needs a process of development, evaluation and innovation related to network security.
3) Manage endpoint security (DSS05.03) is on a Defined level where at this level the institution has implemented a network security only that agency must carry out routine evaluations, at least once a month for information systems that are feared to be potential new threats related to the endpoints.
4) Manage user identity and logical access (DSS05.04) is on a Defined level where at this level the institution has implemented network security against the user identity and logical access. In this condition, the implementation of the regulation has been implemented and monitored. It's just that it still needs a development process, evaluation and innovation related to user identity and logical access.
5) Manage physical access to IT assets (DSS05.05) at the Managed level where at this level the institution implements physical network security. Where the process is only carried out with SOP standards. So it still needs activities to document and monitor the security of physical networks.
6) Manage sensitive documents and output devices (DSS05.06) is in a Managed level where at this level the institution provides security related to sensitive document management and output service, in its performance performance has been implemented with SOP. It's just that you need to do an increase in administration and monitoring related to the security of sensitive documents.
7) Monitor the infrastructure for security-related events (DSS05.07) is on a Defined level where at this level the institution implements, documents and monitors every security process infrastructure related events. So that it requires evaluation and innovation in the next step of the process to minimize future threats.

4. Conclusion

DSS05 Sub-domain Manage security services is a good procedure to be used in the implementation and mega-audit related to network security with GRR Rapid Response. Based on the research conducted by the institution, get the Maturity Level 2.899. So, it can be decided that the institutional maturity level is in Defined. This level stipulates that the institution has implemented, supported and monitored all activities related to network security. However, institutional performance needs to be improved in evaluating and innovating management of existing activities, so that being able to make institutions reach the desired level is Optimized.

References

[1] R. E. Tarigan, "A Study Of Customer Satisfaction On Online Trading System Application Of Securities Company In Indonesia Using," *CommIT (Communication and Information Technology*, vol. 9, no. 1, pp. 19–22, 2015.
[2] I. P. A. Darmawan, I. N. Piarsa, and I. P. A. Dharmaadi, "Ekstrak Hirarki Data Dari Situs

Web A-Z Animals Menggunakan Web Scraping," *Lontar Komputer: Jurnal Ilmiah Teknolohi Informasi*, vol. 8, no. 3, pp. 166–177, 2017.

[3] M. Haryanto and I. Riadi, "Analisis dan Optimalisasi Jaringan Menggunakan Teknik Load Balancing (Studi Kasus : Jaringan UAD Kampus 3)," *Journal Sarjana Teknik Informatika*, vol. 2, pp. 1370–1378, 2014.

[4] A. Susila, I. Riadi, and Y. Prayudi, "Wi-Fi Security Level Analysis for Minimizing Cybercrime," *International Journal of Computer Applications*, vol. 164, no. 7, pp. 35–39, 2017.

[5] A. D. E. Kurniawan, I. Riadi, and A. Luthfi, "Forensic Analysis And Prevent Of Cross Site Scripting In Single Victim Attack Using Open Web Application Security Project (OWASP) Framework," *Journal of Theoritical and Applied Information Technology*, vol. 95, no. 6, pp. 1363–1371, 2017.

[6] Rosmiati, I. Riadi, and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance Imam Riadi," *International Journal of Computer Applications*, vol. 141, no. 8, pp. 975–8887, 2016.

[7] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *International Journal On Advance Science Engineering and Information Technology*, vol. 8, no. 3, p. 949, 2018.

[8] S. Sunardi and I. Riadi, "Forensic Analysis of Docker Swarm Cluster using Grr Rapid Response Framework," *International Journal of Advance Computer Science and Applications*, vol. 10, no. March, pp. 459–466, 2019.

[9] H. Rasheed, A. Hadi, and M. Khader, "Threat Hunting using GRR Rapid Response," *International Conference on New Trends in Computing Science*, 2017.

[10] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," *J. Inform. J. Pengemb. IT*, vol. 2, no. 2, pp. 1–8, 2017.

[11] M. Wahyudi, "Audit Keamanan Informasi Pada Pdam Tirta Tarum Karawang Menggunakan Indeks Kami SNI ISO/IEC 27001:2009 Dan Fishbone," *Jurnal Ilmu Pengetahuan dan Teknologi Komputer*, vol. 2, no. 1, pp. 15–26, 2016.

[12] E. Hicham, B. Boulafdour, M. Makoudi, and B. Regragui, "Information security, 4TH wave," *Journal of Theoritical and Applied Information Technology*, vol. 43, no. 1, pp. 1–7, 2012.

[13] W. Glenn and M. Carr, "A GRReat Framework for Incident Response in Healthcare Subrata Acharya (IEEE Member)," *IEEE Int. Conf. Bioinforma. Biomed. A*, pp. 776–778, 2015.

[14] Z. Reichert, "Automated Forensic Data Acquisition in the Cloud," 2014.

[15] I. Riadi, R. Umar, and I. M. Nasrulloh, "Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods," *LONTAR Komputer: Jurnal Ilmiah Teknologi Informasi*, vol. 9, no. 3, pp. 169–181, 2018.

[16] ISACA, *A Business Framework for the Governance and Management of Enterprise IT*, no. September. 2011.

[17] Wella, "Audit Sistem Informasi Menggunakan Cobit 5.0 Domain DSS pada PT Erajaya Swasembada, Tbk," *Ultima InfoSys*, vol. VII, no. 1, pp. 38–44, 2016.

[18] B. B. Wahono, "Peningkatan Layanan Sistem Informasi Kesehatan (Studi Kasus Dinas Kesehatan Kabupaten Jepara)," *Jurnal SIMETRIS*, vol. 6, no. 1, pp. 101–110, 2015.

[19] R. G. Mufti and Y. T. Mursityo, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN 2548-964x*, vol. 1, no. 12, pp. 1622–1631, 2017.

[20] G. Waluyan, A. D. Manuputty, F. Teknologi, I. Universitas, and K. Satya, "Evaluasi Kinerja Tata Kelola TI Terhadap Penerapan Sistem Informasi Starclick Framework COBIT 5 (Studi Kasus : PT . Telekomunikasi Indonesia , Tbk Semarang)," *TEKNOSI*, vol. 02, no. 03, pp. 157–166, 2016.

Security Analysis of Grr Rapid Response Network using COBIT 5 Framework

ORIGINALITY REPORT

15%

SIMILARITY INDEX

PRIMARY SOURCES

1	garuda.ristekdikti.go.id Internet	207 words — 7%
2	ejournal.undip.ac.id Internet	34 words — 1%
3	Fifin - Sonata. "STRATEGI PENGUATAN IKNB MELALUI AUDIT TATA KELOLA DAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA USAHA START UP MENGGUNAKAN COBIT FRAMEWORK (STUDI KASUS : OTORITAS JASA KEUANGAN)", Jurnal Komunika : Jurnal Komunikasi, Media dan Informatika, 2018 Crossref	25 words — 1%
4	Subrata Acharya, William Glenn, Matthew Carr. "A GRReat framework for incident response in healthcare", 2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2015 Crossref	24 words — 1%
5	www53.homepage.villanova.edu Internet	23 words — 1%
6	media.neliti.com Internet	22 words — 1%
7	Imam Riadi, Rusydi Umar, Arizona Firdonsyah. "Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements", International Journal of Electrical and Computer Engineering (IJECE), 2018	20 words — 1%

Crossref

8	Zachary Reichert, Katarina Richards, Kenji Yoshigoe. "Automated Forensic Data Acquisition in the Cloud", 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems, 2014 Crossref	19 words — 1%
9	"An Analysis of IT Assessment Security Maturity in Higher Education Institution", Lecture Notes in Electrical Engineering, 2016. Crossref	19 words — 1%
10	www.jatit.org Internet	16 words — 1%
11	tci-thaijo.org Internet	13 words — < 1%
12	Mushlihudin Muslihudin. "Perancangan Sistem Pengingat Aktifitas Akademik Dosen dengan JSON", Jurnal Komtika, 2017 Crossref	12 words — < 1%
13	www.gti.co.cr Internet	10 words — < 1%
14	dwisafitrilestari-potter.blogspot.com Internet	10 words — < 1%
15	kinetik.umm.ac.id Internet	9 words — < 1%
16	id.123dok.com Internet	8 words — < 1%
17	www.fda.gov Internet	8 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		