Jurnal Teknologi dan Manajemen

ISSN (Print) 1693-2285

Artikel Penelitian

ANALISIS KEAMANAN PRIVATE CLOUD BERBASIS FRAMEWORK NISTCY DI PT XYZ

Risma Anggraini[1],

[1] *Program Studi Sistem Informasi, Politeknik STMI Jakarta, Jl.Letjen Suprapto No.26 RT.10/RW05 Cempaka Putih, Kota Jakarta Pusat, 10510, Indonesia*

INFORMASI ARTIKEL

Diterima : 1 Februari 2021
Direvisi : 29 Maret 2021
Diterbitkan : 08 April 2021

KATA KUNCI

Keamanan Sistem Informasi, Manajemen Risiko, *NIST Cybersecurity*, *Private Cloud*

KORESPONDENSI

E-mail Author Korespondensi:
arismaang@gmail.com

A B S T R A K

Cloud computing merupakan teknologi yang menjadikan internet sebagai pusat pengelolaan data. Dengan berkembangan yang pesat tak lepas dari ancaman yang mengintai. PT XYZ adalah perusahaan penyedian solusi IT yang memiliki private cloud pada data center. Tujuan dari untuk melakukan analisis keamanan sistem informasi, mengetahui kekurangan dan menghasilkan rekomentasi keamanan sistem informasi private cloud di perusahaan. Dengan mengacu kepada framework NIST Cybersecurity dan menggunakan metode observasi dan wawancara kepada pihak terkait. Hasil dari penelitian adalah merencanakan tindakan, pengelolaan sumber daya manusia dan teknologi dan perangkat keamanan sistem informasi yang ada di private cloud agar bebas dari ancaman dan serangan, serta mendeteksi secara dini berbagai ancaman yang datang sehingga dapat ditangani dengan optimal, serta segala data dan informasi yang penting atau bersifat rahasia dapat tetap terjaga di private cloud perusahaan.

PENDAHULUAN

Cloud computing menyediakan platform komputasi untuk pengguna untuk melakukan berbagai aktifitas penyimpanan secara online, penempatan aplikasi perusahaan, pengembangan dan pembentukan lingkungan jaringan. (Mozumder D M. , 2017)

Ancaman terbesar terhadap loud computing berdasarkan *survey CludPassg* (Schulze, Cloud Security Spotlight Report., 2016) adalah akses tidak sah melalui penyahgunaan control akses yang tidak standar sebesar 53%, pembajakan akun sebesar 44%, dan *Aplication Programming Interface* (API) sebesar 39%. Sehingga perlunya sistem keamanan yang dikelola dengan baik. Keamanan sistem informasi merupakan perlindungan informasi dari berbagai ancaman untuk memastikan kelangsungan bisnis, meminimalkan risiko bisnis, dan memaksimalkan peluang bisnis.

Framework keamanan sistem informasi yang paling umum digunakan adalah ISO 27001;2013 yang diterbitkan oleh International Organization for Standardization, NIST Special Publication 800-53 dan NIST Cybersecurity Framework (CSF) yang diterbitkan oleh National Institute of Standards dan Technology (NISt) (Stonerburner, 2002). Framework NIST Cybersecurity merupakan panduan berdasarkan standar, pedomaan, dan praktik yang sudah ada, yang digunakan untuk mengelola dan mengurangi risiko keamanan sistem infromasi yang lebih baik lagi serta mendorong komunikasi manajemen risiko dan *cybersecurity* antar *stakeholher*.

PT XYZ merupakan salah satu perusahaa yang bergarak dibidang penyedia solusi IT yang ada di Indonesia. PT XYZ memiliki infrastruktur *private cloud* untuk mendukung aktivitas perusahaan. *Private cloud* ini berisi berbagai aplikasi, data dan demo produk yang biasa digunakan. Data yang ada merupakan data internal perusahaan dan data yang berkaitan dengan berbagai proyek dengan klien.*Masalah* keamanan *private cloud* belom dikelola dengan baik, sehingga terjadi kebocoran bahkan kehilangan data yang menyebabkan hilangnya kepercayaan klien. para *stakeholder* merencanakan peningkatan keamanan sistem infromasi pada *private cloud* untuk mengembalikan kepercayaan dan kepuasan klien. Oleh karena itu, keamanan sistem informasi *private cloud* harus ditingkatkan dan dikelola dengan baik sesuai dengan standar sehingga ancaman dapat diminimalisir.

Penelitian ini menggunakan *NIST Cybersecurity* dikarenakan framework ini bersifat publik dan bebas digunakan yang memungkinkan manajemen dan staf IT lebih mudah memahaminya. Selain itu para *stakeholder* dapat mengetahui mengenai tatanan kemanan sistem informasi yang diimplementasikan dan apa yang ingin dicapai. Sehingga

DOI: 10.52330/jtm.v19i1.11

framework ini dianggap palang cocok digunakan untuk menghadapi tantangan keamanan ini.

Tujuan yang ingin dicapai dari penelitian ini, adalah Melakukan analisis keamanan sistem informasi di *private cloud* PT XYZ berdasarkan *framework* NIST Cybersecurity, Mengetahui kekurangan keamanan sistem informasi yang sudah ada di *private cloud* PT XYZ berdasarkan *framework* NIST Cybersecurity, dan menghasilkan rekomendasi untuk mengingkatkan kemanan sistem informasi di *private cloud* PT XYZ bedasarkan *framework* NIST Cybersecurity Mencipatakan standar keamanan sistem informasi di *private cloud* sesuai dengan *framework* NIST Cybersecurity. Serta meningkatkan keamanan sistem informasi di private cloud PT XYZ, agar dapat meminimalisir ancaman dan serangan dari pihak yang tidak berwenang dan bisa melakukan mitigasi risiko yang ada.

METODOLOGI

Cloud Computing

Terdapat empat model umum pengembangan *cloud* berdasarkan kepemilikan, ukuran dan akses, yaitu : (Brunette G, 2009)
Public Cloud : Merupakan model penyebaran yang paling popular karena dapat diakses oleh publik. Memiliki risiko paling tinggi, karena semua orang dapat mengaksesnya (Erl.Mahmood, 2013)
Private Cloud : Model ini didedikasikan untuk satu klien, dengan penggunaan *private cloud* memberikan control yang lebih tinggi dalam melindungi hal yang rahasia.
Community Cloud : Model ini adalah *private cloud* yang dibagikan di anatara komunitas tertentu, kepentingan bersama atau masalah seperti kebijakan atau persyaratan keamanan.
Hybrid Cloud : Model ini mengkombinasikan dari model *cloud* lainnya, sebuah perusahaan dapat memutuskan untuk menyebarkan data sensitinya ke *private cloud* atau sisanya di *public cloud*.

B. Keamanan Sistem Informasi

Tujuan yang berkaitan dengan keamanan sistem informasi dan *cybersecurity*, (Haynes J, 2014) yaitu :Kerahasiaan : Menjaga pembatasan resmi pada akses dan pengungkapan informasi, termasuk sarana untuk melindungi privasi pribadi dan informasi kepemilikan. *Integritas* : Menjaga terhadap modifikasi atau penghancuran informasi yang tidak semestinya, dan termasuk memastikan informasi tanpa penyangkalan dan keaslian. Ketersediaan : Memastikan akses yang tepat waktu dan dapat diandalkan untuk penggunaan informasi. (Nieles M, 2017) *Autentikasi* : Memverifikasi identitas pengguna, proses, atau perangkat, seringkali sebagai persyaratan untuk mengizinkan akses ke sumber daya dalam informasi *Non-repudiasi* : Perlindungan terhadap seseorang yang secara salah mengingkari telah melakukan tindakan tertentu. Memberian kemampuan untuk menentukan apakah individu tertentu mengambil tindakan yang tepat seperti membuat informasi, mengimkan pesan, menyetujui informasi, dan menerima pesan

Panduan Keamanan Sistem Informasi

Tabel Klasifikasi Keamanan Sistem Infrmasi (Tripwire, 2014)

	Benchmark	Standard	Framework	Regulasi
CIS Benchmarks	V			
DISA Checklists	V			
ISO 15408		V		
ISO 27001/27001		V	V	
NIST 800-53		V	V	
TOP 20 CSC		V	V	
COBIT V.5			V	
HIPAA			V	V
NERC CIP			V	V
SOX				V
GLBA				V

Terdapat satu panduan lagi dari National Institute of Standards and Technologi (NIST) yang diterbitkan tahun 2014, yaitu NIST Cybersecurity Frame works (CSF) yang dikategorikan sebagai Standard an *Framework* berdasarkan kategori diatas.

C. NIST Cybersecurity Framework

Framework NIST Cybersecurity memberikan kebijakan panduan keamanan komputer untuk bagaimana organisasi dapat menilai dan meningkatkan kemampuan untuk mencegah, mendeteksi, dan menangani serangan *cyber*. *Frameworks NIST Cybersecurity* dibuat berdasarkan *Executive Order* (EO). *Executive Order* mengarahkan NIST untuk bekerja dengan para pemangku kepentingan untuk mengembangkan *framework* berdasarkan standar, pedoman, dan praktik apa yang ada untuk mengurangi risiko cyber terhadap infrastruktur.

Gambar 2.1 Framework NISC Cybersecurity

Lima tahapan dari Framework NISC Cybersecurity : (Casey, 2015)

1. Identify : Pengembangan pemahaman organisasi untuk mengelola risiko kemanan sistem informasi ke sistem, asset dan data. Tahap ini merupakan dasar untuk penggunaan framework yang efektif, sehingga tahapanini harus dilakukan secar tepat.
2. *Protect* : Pengembangan dan penerapan perlindungan yang tepat untuk memastikan ketersediaan layanan infrastruktur penting. Fungsi protect mendukung untuk membatasi dampak potensial dari insiden *cybersecurity*. Enam kategori dalam fungsi *Protect* adalah :*Business environment* :

 DOI: 10.52330/jtm.v19i1.11

Kategori ini mencangkup prioritas dari misi, sasaran , dan kepentingan lainnya, dan pemanfaatan untuk menginformasikan peran, tanggung jawab, dan pengambilan keputusan.

3. *Detect :* Pengembang dan penerapan kegiatam untuk mengidentifikasi terjadinya insiden *cybersecurity*. Fungsi *Derect* memengkinkan penemuan insiden *cybersecurity* secra tepat waktu.
4. *Respond :* Pengembangan dan penerapan kegitan yang tepat untuk mengambil tindakan terkait insiden cybersecurity. Fungi ini mendukung kemapuan untuk menangani dampak dari insiden yang potensial. Lima kategori utama dalam fungsi
5. *Respond* adalah : *Recover :* Pengembangan dan penerapan kegiatan yang tepat untuk memepertahankan rencana untuk ketehana dan untuk pemulihan kemempuan layanan. Fungsi *Recover* mendukung pemulihan tepat waktu saat terjadi insiden.

HASIL DAN DISKUS

A. Identifikasi Aset Saat ini

Identifikasi aset merupakan langkah yang penting, dimana pada tahapan ini dilakukan penilaian dan identifikasi terhadap aset yang dinilai penting atau berpengaruh bagi proses bisnis perusahaan dalam bidang keamanan. Dengan kategori keamanan Aset (Naynes M, 2017)

Confidentiality (kerahasiaan): Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

Integrity (integritas) : Menjamin bahwa data tidak berubah (modifikasi) tanpa izin pihak berwenang, menjaga keakuratan dan keutuhan informasi serta metode proses menjamin integrity ini.

Availability(ketersediaan) : Menjamin ketersediaan data, akses dan penggunaan informasi yang tepat waktu dan dapat diandalkan

Tabel 1: Daftar Aset perusahaan

No	Aset	C	I	A	Nilai	Ket.
	Data dan Informasi					
1	Data Pelanggan	3	3	2	2.7	T
2	Data Vendor	3	3	2	2.7	T
3	Data Proyek	3	3	3	3	T
4	Data Technical	3	3	3	3	T
5	Data Finance	3	3	3	3	T
6	Data Sales dan Account Managemen	3	3	2	2.7	T
7	Data Sumber daya Manusia	2	3	3	2.7	T
8	Database aplikasi	3	3	3	3	T
Aplikasi dan Sistem						
9	Aplikasi Sales dan AM	3	3	3	3	T
10	Aplikasi Internal IT	2	2	2	2	S
11	Aplikasi Finance	3	2	3	2.7	T
12	Aplikasi Project Manegement	3	3	3	3	T
13	Aplikasi Maintenance	2	2	2	2	S
14	Aplikasi Manage Service	3	3	3	3	T
15	Virtual Server	1	1	1	1	R
16	Virtual Jaringan	1	1	1	1	R
17	Virtual Serurity	1	1	1	1	R
18	Cloud file server	3	3	3	3	T
19	Load Balancer	2	2	2	2	S
20	DNS Server	2	2	2	2	S
21	Video Conference Server	1	1	1	1	R
Server dan Jaringan						
22	Server Cisco UCS	3	3	3	3	T
23	Server Cisco Blade	3	3	3	3	T
24	Server HP Proliant	3	2	3	2.7	T
25	Server IBM	2	3	3	2.7	T
26	Switch core Cisco Catalyst	3	3	3	3	T
27	Switch access HP	3	3	3	3	T
28	Switch Cisco Fabric	3	3	3	3	T
Penyimpanan						
29	Storage EMC	3	3	3	3	T
30	Vmware VCenter	3	3	3	3	T
31	Strorage Hitachi	3	3	3	3	T
32	Hypervisor Ms. Hyper V	3	3	3	3	T
33	Hypervisor Vmware ESX	3	3	3	3	T
Keamanan						
34	IP address	2	2	1	1.7	S
35	Log collector	3	3	2	2.7	T
36	Firewall PaloAlto	3	3	3	3	T
37	NMS	2	3	3	2.7	T
38	Antivirus	3	3	3	3	T
39	Security Infromastion & Event Managemen	3	3	3	3	T
Lain-Lain						
40	CCTV	3	3	2	2.7	
41	Ruang Server	3	3	3	3	T
42	Access Door	2	3	3	2.7	S
43	PC Monitoring				3	T

C : Confidentiality, I ; Integrity, A: Availability

B. Kondisi Saat Ini

Melakukan pendekatan *cybersecurity* dan hasilnya dikategorikan kedalam fungsi dari *framework* NIST *Cybersecurity*. Fungsi *Identify* merupakan fondasi dari f*ramework* NIST *Cyebersecurity.*

Fungsi *Protect* digunakan untuk membatasi dan mengendalikan akses aman kesistem baik fisik maupun digital.

Fungsi *Detect* sabagai pengembangan dan implementasi kegiatan identifikasi kejadian *cybersecurity.* berfokus mendukung penentuan waktu dan peristiwa.

Fungsi *Respond* sabagai penetap dan menempatkan procedure yang digunakan untuk mengambil keputusan terkait kejadian *cybersecurity* yang dialami

Fungsi *Recover* sebagai digunakan untuk membantu mengurangi dampak dari keamanan sistem informasi.

Tabel 2. Kondisi Saat ini

Fungsi	Kategoti	Nilai
Identify	Asset Management	1.8
	Business Environment	1.4
	Governance	2.0
	Risk Assessment	1.0
	Risk Management Strategy	1.3
Protect	Access Control	2.4
	Awareness and Training	1.6
	Data Security	2.3
	Information Protection Processes and Procedures	1.8
	Maintenance	1.0
	Protective Technology	2.3
Detect	Anomalies and Events	2.2
	Security Continuous Monitoring	2.8
	Detection Processes	3.2
Respond	Response Planning	1.0
	Communications	1.6
	Analysis	2.0
	Mitigation	2.7
	Improvements	1.5
Recovery	Recovery Planning	1.0
	Improvements	1.5
	Communications	2.0

C. Pengkajian Risiko

Ditahap pengkajian risiko dilakukan identifikasi, prioritas dan mitigasi yang dilakukan pada *private cloud* PT XYZ. Identifikasi dilakukan dengan mengidentifikasi risiko terhadap asset serta dampaknya terhadap perusahaan. Selanjurnya dilakukan analisis kontrol yang telah ada. Dilanjutkan dengan melakukan penilaian kecendrungan risiko. Dimana risiko ditentukan peringkatnya, dimulai dari jarang(0.1) yaitu kemungkinan terjadi kurang dari 5 dalam 1 tahun , sedang(0.5) kemungkinan terjadi 6-10 dalam 1 tahun, dan sering kemungkinan terjadi lebih dari 10 kali dalam 1 tahun (1).

Tabel 3 Kriteria Dampak Risiko

	Rendah (10)	Sedang(50)	Ttinggi (100)
Reputasi	Tidak memperngaruhi reputasi	Reputasi negative hanya di internal perusahaan	Reputasi negative diinternal dan ekternal perusahaan
Gangguan Operasional	Downtime 0 – 30 menit	Downtime > 30 menit < 1 jam	Downtime >1 jam
Pengaraguh Operasional	Tidak mempengaruhi operasional	Sedikt mempengaruhi operasional	Sangat mempengaruhi operasional
Nilai Kerusakan	Nilai kerusakan tidak penting bagi perusahaan	Nilai kerusakan penting bagi perusahaan	Nilai kerusakan menjadi perhatian utama perusahaan
Financial	< Rp 1.000.000	> Rp. 1.000.000 < Rp 10.000.000	>Rp. 10.000.000

Tabel 4 Tingkat Risiko

	KECENDRUNGAN			
		Jarang (0.1)	Sedang (0.5)	Sering (1)
DAMPAK	Rendah (10)	Rendah (1)	Rendah (5)	Rendah (10)
	Sedang (50)	Rendah (5)	Sedang (25)	Sedang (50)
	Tinggi (100)	Rendah (10)	Sedang (50)	Tinggi (100)

Tabel 5 Daftar Dokumen yang harus dipenuhi

No	Dokumen	Kategori
1	Daftar Inventaris Aset	Asset Management
2	Daftar Arus, klasifikasi dan pengelolaan data	Data security, Information Protection processes and procedures
3	Daftar Komunikasi	Asset Management
4	Kebijakan Invemtaris aset	Asset Management
5	Daftar Inventaris sistem informasi ekstrelnal	Asset Management
6	Kebijakan keamanan sistem informasi	Business Environment, Governance

DOI: 10.52330/jtm.v19i1.11

7	Kebijakan dan daftar risiko organisasi	Business Environment, Risk Assessment, Information protection processes and procedures
8	Kebijakan dan daftra risiko asset	Business Environment, Risk Assessment, Information protection processes and procedures
9	Kebijakan keamanan pihak ketiga	Business Environment, Aeareness dan Training
10	Daftar peran dan tanggungjawab	Governance, Awareness dan Training
11	Daftar Ancaman dan Kerentanan	Risk Assessment , Mitigation
12	Daftar Kepatuhan Regulasi dan Peraturan	Governance
13	Kebijakan Keamanan Fisik	Information Protection Processes and Procedures , Maintenance
14	Kebijakan Pengelolaan Aset	Maintenance , Security Continuous Monitoring
15	Kebijakan Kredensial dan Hak Akses	Access Control, Security Continuous Monitoring
16	Kebijakan Akses Jarak Jauh	Access Control
17	Topologi Infrastruktur Jaringan dan Aplikasi	Access Control , Data Security
18	Kebijakan Pelatihan Keamanan Sistem Informasi	Awareness and Training
19	Kebijakan Perlindungan Data dan Sistem Informasi	Data Security
20	Kebijakan Pemantauan dan Deteksi	Security Continuous Monitoring
21	Kebijakan Media Portabel	Protective Technology
22	Kebijakan Penilaian Kerentanan dan Pengujian Penetrasi	Security Continuous Monitoring , Information Protection Processes and Procedures
23	Kebijakan Pengelolaan Sumber Daya Manusia	Information Protection Processes and Procedures
24	Kebijakan Pemulihan	Business Environment , nformation Protection Processes and Procedures, Communications
25	Kebijakan Penanganan	Anomalies and Events, Detection Processes
26	Kebijakan Audit dan Evaluasi	Information Protection Processes and Procedures
27	Kebijakan Backup Data	Information Protection Processes and Procedures
28	Kebijakan Pengelolaan Perubahan	Information Protection Processes and Procedures
29	Kebijakan Konfigurasi Perangkat	Information Protection Processes and Procedures
30	Kebijakan Pengembangan Sistem	Data Security, Information Protection Processes and Procedures

Melihat dari jaringan dan keamanann yang sudah ada , proses pengelolaan keamanan sistem informasi perangkat dan teknologi yang dapat di rekomendasikan untuk diintegrasikan (Government, 2015)
:

A. *Next Generation Instrusion Prevention System* (NGIPS) *trusion Prevention System* difokuskan untuk mengidentifikasi kemungkinan insiden, mencatata informasi tentang insiden, mencoba menghentikan dan melaporkan ke administrator keamanan, sedangkan NGIPS menambahkan fitur antivirus dan anti malware dan keamanan internet.

B. Data Loss Prevention (DLP) *Software* mendeteksi potensi pelanggaran data dan mencegah dengan memantau, medeteksi danmemblokir data sensitive ketika data digunakan, dat adalm lalu lintas jaringan dan saat penympanan data.

C. Web Application Firewall (WAF) *Web Application Firewall* merupakan teknologi yang relative baru, dibandingkan dengan teknologi firewall lainnya, dimana jenis ancaman yang dimitigasi masih sering berubah. WAF berfungsi untuk menyaring, memantau dan memblokir lalu lintas HTTP ke dalam aplikasi dari aplikasi berbasis web. WAF berbeda dengan firewall biasa dikarenkan WAF dapat melakukan filter terhadap konten aplikasi web tertentu dan sebagai gerbang keamanan antar server.

D..Vulnerability Scanner, *Vulnerability Scanner* mengidentifikasi port jaringan dan identifikasi layanan *host*,

artibut *host*, dan mengidentifkasi kerentanan lainnya. Digunakan untuk membantu mengidentifikasi versi perangkat lunak rusak, *patch* yang hilang kesalahan konfigurasi dan memvalidasi kepatuhan atau penyimpanan terhadap kebijakan keamanan.

E. *Network Access Control* (NAC), NAC memungkinkaakses berdasarkan kredensial pengguna dan hasil dari melakukan pemeriksaan kesesuaian di computer pengguna. Dilakukan pemeriksaan kesesuaian dan verifikasi sesuai dengan kebijakan keamanan seperti pengaturan dan membaruan perangkat lunak *firewall* dan anti *malware*.

F. *Identity & Access Management* (IAM) IAM digunakan untuk mendefinisikan dan mengeola peran dan hak akses pengguna jaringan dan keadaan dimana pengguna diberikan atau dibatasi hak – hak istimewa.

G. APT *Prevention Advanced persistent threats* (APT) melakukan pengawasan dalam jangka waktu lama. Teknologi APT *Prevention* digunakan untuk mendeteksi dan juga menangka malwave yang bisa berujung pada serangan APT yang mengakibatkan kehilanagn data perusahaan bahkan mematikan seluruh infrastruktur teknologi informasi perusahaan atau biasa disebut serangan *zero-day*.

H. *Distributed Denial of Service* (DDoS) *Protection*
DDoS merupakan teknik *Denail of Sevice* (DoS) yang menggunakan banyak *hos*t untuk melakukan srangan. DDoS Protection berfungsi untuk memberikan proteksi aset kepada serangan DoS dan DDoS yang mengganggu ketersedian infrastruktur aplikasi dan jaringan.

I. *Penetration Testing Tool*,
Penetration Testing Tool merupakan pengujian keamanan yang dimana penilai meniru rerangan untuk mengidentifikasi metode mitigasi yang harus diterapkan

KESIMPULAN

Belum dilakukannya audit dan evaluasi kerkait kemanan sistem informasi secara berkala. Dengan penggunaan *framework* NIST *Cybersecurity* cocok digunakan untuk perusahaan skala menengah karena proses bisnis berjalan secara dinamis mengikuti perkembangan yang terjadi. Dari hasil penelitian dapat digunakan oleh perusahaan sejenis yang mempunyai private cloud dengan menentukan standar keamanan yang akan digunakan. Sehingg perlunya penelitian lanjutan untuk membandingkan pengelolaan keamanan sistem informasi dan *cybersecurity* dengan standar lain dalam pengelolaan keamanan system informasi perusahaan, sehingga semua infrastruktur penting dapat terlindungi dengan baik, dan pengeolaan keamanan dapat direncanakan dan dilakukan secara berkala, mengingat pentingnya informasi dalam perusahaan. Dan kedepannya diharapakan perusahan dapat lebih peduli tehadap keamanan dan pentingnya data dan informasi, sehingga dapat menggunakan metedo yang lain untuk memastikan keamana data dan informasi dan dilakukan secara berkala.

UCAPAN TERIMA KASIH

Alhamdulillah puji dan syukur kepada Allah swt, karena atas kehendak dan ridhonya jurnal ini dapat diselesaikan, dan tidak lupa atas segala dukungan semua pihak terutama keluarga, teman seperjuangan dan industri yang telah banyak membantu saya sehingga jurnal ini dapat rampung. Dan tak lupa terimakasih kepada STMI dan tim P2M yang telah memfasilitasi penerbitan jurnal.

Daftar Pustaka

Brunette G, M. R. (2009). Security guidance for critical areas of focus in cloud computing v.2.1. *Cloud Computing Top*

Casey, T. F. (2015). *The Cybersecurity fremework in Action: An Intel Use Case*. Intel Corporation.

Erl.Mahmood, Z. &. (2013). *Cloud Computing Conce[ts, TEchnology and ARCHITECTURE*.

Government, U. (2015). *Public Printing and Documents Chapter 35*. Retrieved april 15, 2019, from - Coordination of Federal Information Policy Subchapter II - Information Security Dec. 3552 Definition.

Haynes J, N. (2014). Cybersecurity/Information Assurance (IA).

Mozumder D, M. M. (2017). *Cloud Computing Security Breaches and Threats Analysis*. International Journal of Scientific & Engineering Research, Volume 8 Ussue 1.

Naynes M, D. K. (2017). *An Introduction to Information Security* . National Institude of Standarsd and Technology.

Nieles M, D. K. (2017). *An Introduction to Information Security*. National Institute of Standards and Technology.

Schulze. (2016). *Cloud Security Spotlight Report*. CloudPassage.

Stonerburner, G. &. (2002). *Risk Management Guide for Information Technology System*. National Institute of Standards and Technology.

Tripwire. (2014). *PCI DSS and The "TOP 20" Critical Security Control*. Tripwire,Inc: Company Security Frameworks Series .

 DOI: 10.52330/jtm.v19i1.11