Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893
p-ISSN: 2089-3787

Penilaian Tingkat Keamanan Teknologi Informasi Menggunakan Metode Keamanan Informasi (KAMI) Dan *Vulnerability Assessment*

Dewa Gede Anom Atmaja[1*], I Gede Putu Krisna Juliharta[2], Ketut Queena Fredlina[3]
[1,2,3]Teknik Informatika, STMIK Primakara, Denpasar
[1,2,3]Jalan Tukad Badung No.135, Renon, Denpasar (0361) 8956085
**Corresponding Author email*: *anom.atmaja@live.com*

Abstrak

Diskominfostatistik atau Dinas Komunikasi, Informatika, dan Statistik Kota Denpasar merupakan intansi pemerintah yang bergerak sebagai pengawas dan penerapan TIK di wilayah Kota Denpasar dalam menangani permasalahan teknologi informasi dan sistem informasi yang dimiliki. Semua kegiatan teknologi informasi dan sistem informasi dipusatkan dan dikembangkan di Dinas Komunikasi, Informatika, dan Statistik Kota Denpasar. Dalam hal ini pemerintah berperan penting dalam meningkatkan mutu kualitas yang ada sesuai prosedur standarisasi keamanan yang layak. Paper ini menganalisis tingkat keamanan Teknologi Informasi menggunakan kombinasi Metode Keamanan Informasi dan *Vulnerability Assessment,* studi kasus pada Dinas Komunikasi, Informatika, dan Statistik Kota Denpasar. Hasil analisis tingkat kesiapan menunjukkan dari 5 mesin yang melingkupi E-Pajak, AkuWaras, Aplikasi, Eproc, dan Bursakerja terdapat 1 level critical, 10 level high, 24 level medium dan 16 level low.
Kata Kunci: *Keamanan Teknologi Informasi, Metode Vulnerability Assessment, Metode Kemanan Informasi*

Abstract

"Diskominfostatistik" of Denpasar City is a government agency that operates as a supervisor and application of ICT in the Denpasar City area in dealing with problems of information technology and information systems owned. All information technology and information system activities are centralized and developed at the Denpasar City Office of Communication, Informatics and Statistics. In this case, the government plays an important role in improving the quality of existing quality according to proper safety standardization procedures. This paper analyzes the security level of Information Technology using a combination of Information Security Methods and Vulnerability Assessment, a case study at the Denpasar City Office of Communication, Informatics, and Statistics. The results of the readiness level analysis show that of the 5 machines covering E-Tax, AkuWaras, Applications, Eproc, and Bursakerja, there are 1 critical level, 10 high levels, 24 medium levels and 16 low levels.
Keywords*: Information Technology Security, Vulnerability Assessment Method, Information Security Method*

1. Pendahuluan

Instansi pemerintahan di Indonesia juga perlu menerapkan keamanan informasi untuk menghindari adanya pencurian data dan hilangnya data secara sengaja maupun tidak sengaja. Hal ini juga perlu diterapkan dan diperhatikan di Dinas Komunikasi, Informatika dan Statistik Kota Denpasar dimana sebagai pengawas dan penerapan TIK di wilayah Kota Denpasar dalam menangani permasalahan teknologi informasi dan sistem informasi yang dimiliki. Semua kegiatan teknologi informasi dan sistem informasi dipusatkan dan dikembangkan di Dinas Komunikasi, Informatika, dan Statistik Kota Denpasar.

Saat ini perkembangan teknologi informasi sangat luar biasa pesatnya dan juga memberikan pengaruh di sektor-sektor penting seperti pendidikan, sektor usaha maupun pelayanan publik dari pemerintah. Karena begitu pesatnya, saat ini informasi maupun pesan sangat mudah untuk dapat dikirim maupun diunduh menggunakan sistem elektronik.

Kemudahan yang diberikan dalam menggunakan teknologi berpengaruh terhadap rentannya tingkat kerawanan dan kebocoran dari informasi tersebut.
Oleh karena itu, kita sebagai pengguna teknologi perlu memperkaya diri dengan pengetahuan tentang bagaimana mengamankan informasi-informasi penting agar tidak terjadi kebocoran data. [1]

Keamanan informasi pada suatu organisasi merupakan hal yang sangat penting dan harus menjadi perhatian utama. Namun apakah kriteria penerapan keamanan informasi di organisasi anda telah memenuhi kelengkapan dan kematangan yang sesuai dengan standar?
Indeks KAMI (Keamanan Informasi) merupakan aplikasi yang digunakan sebagai alat bantu untuk menganalisa dan mengevalusi tingkat kesiapan (kelengkapan dan kematangan) penerapan keamanan informasi di sebuah organisasi sesuai dengan kriteria pada SNI ISO/IEC 27001.

Vulnerability Assessement adalah sebuah metode untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu sistem atau infrastruktur yang berbasis teknologi informasi. Metode ini telah digunakan dalam analisis sistem keamanan Web [2]-[4], sistem kemanan jaringan komputer [5], mengkaji data untuk memperoleh informasi kerentanan lingkungan dan fisik non-alami [6][7], dan bidang lainnya.

Paper ini bertujuan untuk menganalisis tingkat keamanan Teknologi Informasi menggunakan *Vulnerability Assessement,* studi kasus pada Dinas Komunikasi, Informatika, dan Statistik Kota Denpasar

3. Tinjauan Pustaka

Penelitian mengenai analisis tingkat keamanan informasi telah dilakukan dengan menggunakan berbagai metode. Akhirina [8] mengevaluasi keamanan teknologi informasi di perusahaan menggunakan Indeks Keamanan Informasi (KAMI). Penilaian ini digunakan untuk melihat seberapa jauh tingkat kematangan tingkat kematangan keamanan informasi di lingkungan keamanan informasi di perusahaan PT Indotama Partners Logistics. Hasil pengukuran tingkat kematangan keamanan teknologi informasi pada perusahaan tersebut berada di lavel I+ sampai dengan II+. Total skor peran TIK adalah 26 (Tinggi), dan hasil pengukuran lima area dalam Indeks KAMI sebesar 391, yang berarti tingkat kematangan TIK nya masih perlu diperbaiki diperbaiki. Hasil dari penelitian ini dapat digunakan sebagai media evaluasi dalam rangka meningkatkan keamanan informasi dari perusahaan di masa yang akan datang

Ikhsan [9] menganalisis risiko keamanan Teknologi Informasi menggunakan metode Octave Allegro. Octave Allegro digunakan untuk mengidentifikasi dan mengevaluasi dari risiko keaman sebuah informasi. OCTAVE melakukan penilaian risiko berdasarkan pada tiga prinsip dasar administrasi keamanan, yaitu: *confidentiality, integrity,* dan *availability. Pada penelitian tersebut,* penilaian risiko hanya sampai tahapan ketiga yaitu menentukan Identify Threats dimana tahap pertama estabilsh drivers, yaitu menetapkan apa yang menjadi arahan organisasi. Tahap kedua Membuat profile assets, yaitu membuat profil aset yang telah dimiliki organisasi. Tahap ketiga identify threats, yaitu mengidentifikasi ancaman untuk setiap aset informasi dalam kontek wadahnya.

Umar [10] menganalisis keamanan sistem informasi berdasarkan *Framework* COBIT 5 Menggunakan *Capability Maturity Model Integration*. Kombinasi antara kedua standar tersebut dalam sistem informasi mampu memberikan nilai tingkat pencapaian teknologi informasi. Hasil yang didapat nilai maturity level 4,458 yang berarti institusi berada di level *Managed and Measurable*. Pada level ini, institusi semakin terbuaka terhadap perkembangan teknologi.

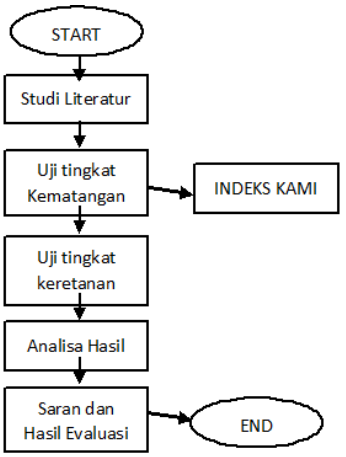
Pada penelitian ini, Penilaian Tingkat Keamanan Teknologi Informasi dilakukan Menggunakan kombinasi Metode Keamanan Informasi (KAMI) dan *Vulnerability Assessment*

3. Metode Penelitian

3.1 Rancangan Penelitian

Alur penelitian ini dibagi menjadi beberapa tahap dimulai dengan melakukan persiapan jurnal, melakukan studi literatur dengan membaca buku-buku, jurnal-jurnal, referensi yang berkaitan dengan penelitian ini dan penelitian terdahulu yang berkaitan dengan penelitian yang sedang dilakukan. Kemudian melakukan pengumpulan data mengenai penelitian ini dengan melakukan wawancara, observasi dan studi dokumentasi ke kantor Dinas Komunikasi, Informatika dan Statiska Kota Denpasar. Data yang didapatkan dari hasil pengumpulan data

dikumpulkan sebagai bahan untuk melakukan pengolahan data. Langkah selanjutnya melakukan analisa dari hasil pengolahan data sebelumnya untuk mengidentifikasi dan mengevaluasi semua permasalahan, hambatan yang terjadi serta kebutuhan-kebutuhan yang diharapkan. Alur penelitian ditutup dengan memberikan kesimpulan, saran untuk penelitian selanjutnya dan membuat laporan.



Gambar 1. Alur Penelitian

3.2 Instrumen Penelitian

Alat penelitian yang digunakan dikategorikan menjadi 2 sebaga berikut:

a. Perangkat Lunak

Perangkat lunak yang digunakan menjadi tiga, yaitu:

1) Sistem Operasi: Kali Linux dan Windows 10.
2) Microsoft Office Excel: Indeks Kami v3.1
3) *Network Security Tools*

Network security tools yang digunakan tersedia di internet dan tools tersebut bersifat *freeware.*

Tabel 1. *Network Security Tools*

TOOLS	**FUNGSI**
Ping	*Network enumeration* dan identifikasi ip address yang aktif
Nessus	*Port scanner dan penetration testing TCP, UDP, SNMP, URL serta Network Secuirty Scanner dan Vulnerability*
Traceroute	Menganalisa jalur paket data mengalir

b. Perangkat Keras

Perangkat keras yang digunakan pada penelitian ini berupa laptop, sebagai berikut:

1) Processor AMD A8-7410 APU 2,2 GHz
2) Memory RAM 4,00 GB
3) HDD 500 GB
4) GPU AMD Radeon R5 Graphics

4. Hasil dan Analisis

4.1 Indeks KAMI

a. Hasil Identifikasi Kategori SE (Sistem Elektronik)

Bagian pertama dari indeks kami adalah penilaian sistem elektronik yang terdapat 10 pertanyaan. Dan jawaban yang diberikan Dinas Komunikasi, Informasi dan Statistik Kota Denpasar yang terdapat nilai 2 atau jawaban b berjumlah 4 pertanyaan, dan nilai 5 atau jawaban A berjumlah 3 pertanyaan dan sisanya nilai 1 atau jawaban c berjumlah 3 pertanyaan dengan total yang dimiliki skor 26. Skor tersebut memiliki arti bahwa sistem elektronik memiliki kategori Tinggi. Tinggi berarti Diskominfostatistik Kota Denpasar teknologi informasi dan computer merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan.

b. Hasil Identifikasi Kategori Tata Kelola Keamanan Informasi

Bagian kedua adalah penilaian tata kelola keamanan informasi. Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi tugas dan tanggung jawab pengelola keamanan informasi. Total pertanyaan 22 yang ditanyakan Dinas Komunikasi, Informasi dan Statistik Kota Denpasar menjawab 3 jawaban ditetapkan secara menyeluruh dan menjawab 6 jawaban dalam perencanaan serta 7 jawaban dalam penerapan/penerapan sebagian. Skor untuk proses penilaian tata kelola keamanan informasi adalah 40. Skor rekapitulasi tahap 1 dan tahap 2 adalah 40 sedangkan skor validasi ke tahap 3 adalah 48 sehingga status akhir "I+" dan dikategorikan tidak valid.

c. Hasil Identifikasi Kategori Pengelolaan Risiko Keamanan Informasi

Bagian ketiga adalah penilaian pengelolaan resiko keamanan informasi, bagian ini mengevaluasi tingkat kesiapan penerapan pengelolaan resiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Terdapat 16 pertanyaan dengan 14 jawaban dalam perencanaan dengan skor 1 dan 2 jawaban tidak dilakukan dengan skor 0. Total skor adalah 18 dan skor penerapan tahap 1 dan 2 adalah 18, sedangkan skor untuk validasi tahap penerapan 3 adalah 36. Maka bagian ketiga pengelolaan resiko memiliki status akhir "I" dan dikategorikan tidak valid.

d. Hasil Identifikasi Kategori Kerangka Kerja Pengelolaan Keamanan Informasi

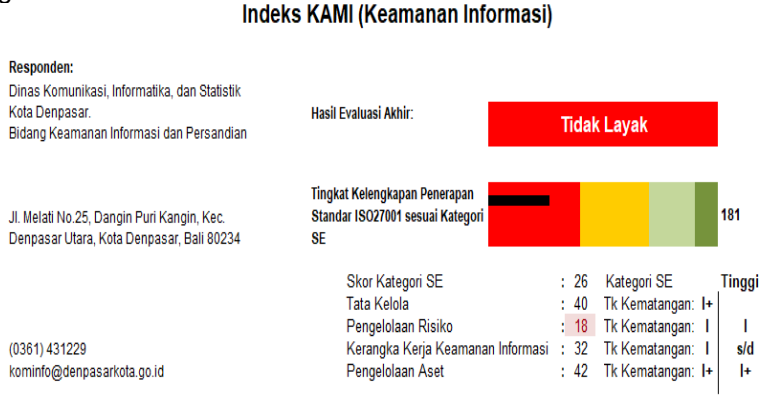
Bagian keempat adalah penilaian kerangka kerja pengelolaan keamanan informasi. Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Terdapat 29 pertanyaan dan Diskominfostatistik Kota Denpasar menjawab 22 jawaban dalam perencanaan dan 7 jawaban tidak dilakukan, sehingga total skor adalah 32. Sedangkan skor tahap penerapan 1 & 2 adalah 32. Skor minimum tahap penerapan 3 adalah 64, sehingga Dinas Komunikasi, Informatika, dan Statistik Kota Denpasar memiliki status akhir "I" dan dikategorikan tidak valid.

e. Hasil Identifikasi Kategori Pengelolaan Asset Informasi

Bagian kelima adalah pengelolaan asset informasi. Bagian ini mengevaluasi kelengkapan pengamanan asset informasi, termasuk keseluruhan siklus penggunaan asset tersebut. Terdapat 38 pertanyaan, dan Dinas Komunikasi, Informasi dan Statistik Kota Denpasar memberikan jawaban 2 jawaban diterapkan secara menyeluruh, 4 jawaban dalam penerapan/diterapkan sebagian. Serta 22 jawaban dalam perencanaan dan sisanya 10 jawaban tidak dilakukan. Total skor adalah 42 dan skor tahapan 1 dan 2 adalah 40. Skor minimum tahap penerapan 3 adalah 68, sehingga Diskominfostatistik mendapatkan status akhir "I+" dan dikategorikan tidak valid.

f. Hasil Identifikasi Kategori Teknologi dan Keamanan Informasi

Bagian keenam adalah teknologi informasi, bagian ini mengevaluasi kelengkapan, konsistensi, efektifitas penggunaan teknologi dalam pengamanan informasi. Terdapat 26 pertanyaan, dan Dinas Komunikasi, Informasi dan Statistik Kota Denpasar menjawab 4 jawaban diterapkan secara menyeluruh, 9 jawaban dalam penerapan/diterapkan sebagian. Serta 6 jawaban dalam perencaan dan 7 jawaban tidak dilakukan. Status akhir yang didapatkan adalah "I+" dan dikategorikan tidak valid.



Gambar 2 Indeks Keamanan Informasi

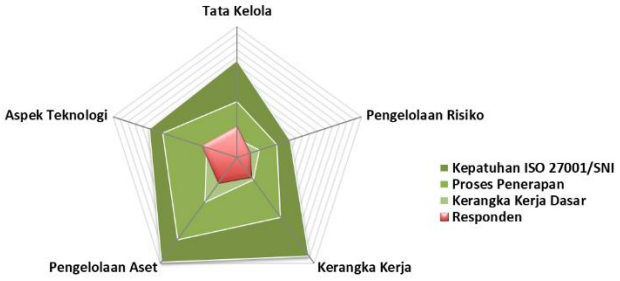
Berdasarkan hasil evaluasi gambar diatas, tingkat penerapan sistem elektronik di Dinas Komunikasi, Informasi dan Statistik Kota Denpasar masuk dalam kategori tinggi. Hal ini dilihat dari posisi kategori 1 dan 2. Namun hasil evaluasi dengan kategori yang tinggi sistem elektronik di Dinas Komunikasi, Informasi dan Statistik Kota Denpasar mendapatkan hasil evaluasi yang tidak layak dengan nilai tingkat kelengkapan penerapan standar ISO 27001 dinilai 181.

Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai:

- Tingkat I - Kondisi Awal
- Tingkat II - Penerapan Kerangka Kerja Dasar
- Tingkat III - Terdefinisi dan Konsisten
- Tingkat IV - Terkelola dan Terukur
- Tingkat V - Optimal

Untuk membantu memberikan uraian yang lebih detil, tingkatan ini ditambah dengan tingkatan antara I, I+, II, II+, III, III+, IV, IV+ dan V, sehingga total terdapat 9 tingkatan kematangan.

Pada kategori tata kelola diperoleh skor 40 dengan tingkat kematangan I+ yang artinya bahwa dalam ketogeri tata kelola ini masih dalam tahap kondisi awal. Untuk kategori pengelolaan resiko diperoleh skor 18 dengan tingkat kematangan I yang artinya kategori ini masih dalam tahap kondisi awal. Pada Kerangka kerja keamanan informasi diperoleh skor 32 dengan tingkat kematangan I yang artinya kondisi pada Kerangka Kerja masih dalam tahapan Kondisi Awal, sedangkan Pengelolaan Aset diperoleh skor 42 dengan tingkat kematangan I+ yang artinya masih dalam Kondisi Awal. Sehingga dari seluruh kategori tersebut harus mencapai III+ untuk dikategorikan Terdifinisi dan konsisten sehingga semua area tersebut bisa dikategorikan baik.



Gambar 3 Aspek Penilaian

Dari radar diatas menunjukkan sejauh mana respon Dinas Komunikasi, Informatika, dan Statistik Kota Denpasar (warna merah muda) terhadap penerapan SMKI (sistem manajamen keamanan informasi). Dari lima kategori terlihat aspek teknologi dan tata kelola lebih baik dibandingkan pengelolaan resiko, pengelolaan asset serta kerangka kerja.

4.2 *Network Security Assessment*

Tabel 2 Target Keamanan Jaringan

	KETERANGAN
Nama Domain	Denpasarkota.go.id
Instansi	Dinas Komunikasi, Informatika dan Statistik Kota Denpasar
Alamat	Jl. Melati No.25, Dangin Puri Kangin, Kec. Denpasar Utara, Kota Denpasar, Bali 80234
Email	kominfo@denpasarkota.go.id
Telepon	(0361) 431229

Mapping pada jaringan yang akan diuji. Pada tabel ini dijelaskan tentang status IP Address yang berkaitan dengan denpasarkota.go.id serta memberikan nama dan tipe IP yang digunakan.

Tabel 3 Mapping Domain denpasarkota.go.id

NO	IP ADDRESS	NAMA MESIN	TYPE	FUNGSI
1	222.124.29.196	Aplikasi.denpasarkota.go.id	Public	DNS Server
2	118.97.144.182	E-pajak.denpasarkota.go.id	Public	DNS Server
3	223.27.147.139	Eproc.denpasarkota.go.id	Public	DNS Server
4	180.250.189.39	Akuwaras.denpasarkota.go.id	Public	DNS Server
5	180.250.189.40	Bursakerja.denpasarkota.go.id	Public	DNS Server

Tabel 4. Proses Ping

NO	IP ADDRESS	NAMA MESIN	PING STATUS
1	222.124.29.196	Aplikasi.denpasarkota.go.id	Reply
2	118.97.144.182	E-pajak.denpasarkota.go.id	Reply
3	223.27.147.139	Eproc.denpasarkota.go.id	Reply
4	180.250.189.39	Akuwaras.denpasarkota.go.id	Reply
5	180.250.189.40	Bursakerja.denpasarkota.go.id	Reply

Proses traceroute merupakan langkah untuk memastikan pada tiap IP yang ada apakah memang benar server dan semua server yang dideteksi memang hidup atau mati.

Tabel 5. Proses Traceroute

NO	IP ADDRESS	HASIL TROUCEROUTE	
1	180.250.189.40	Lokasi	Indonesia
		Firewall	Ping diizinkan
		Route length	7 Hops
		Loss	0%
		Status	Up
2	222.124.29.196	Lokasi	Indonesia
		Firewall	Ping diizinkan
		Route length	7 Hops
		Loss	0%
		Status	Up
3	180.250.189.39	Lokasi	Indonesia
		Firewall	Ping diizinkan
		Route length	7 Hops
		Loss	0%
		Status	Up
4	223.27.147.139	Lokasi	Indonesia
		Firewall	Ping diizinkan
		Route length	12 Hops
		Loss	0%
		Status	Up
5	118.97.144.182	Lokasi	Indonesia
		Firewall	Ping diizinkan
		Route length	6 Hops
		Loss	0%
		Status	Up

Dari tabel diatas bisa dilihat proses traceroute dari tiap IP, dari hasil diatas didapat beberapa fakta yaitu pada IP server Aplikasi (222.124.29.196), IP server E-Pajak (118.97.144.182), IP server Eproc (223.27.147.139), IP server Akuwaras (180.250.189, dan IP

server Bursakerja (180.250.180.40) untuk proses *PING* statusnya *reply* dan untuk proses traceroute juga up (menyala). Dari kesimpulan diatas dapat dipastikan kelima IP yang dites hidup dan memberikan respon/layanan.

Setelah dipastikan aktif, maka proses selanjutnya yaitu melakukan pengecekan/analisa kerentanan (*Vulnerabilities*) dan *Business Impact Analysis* serta *Risk Factor,* penulis akan melakukan analisa perangkat yang digunakan pada tiap server IP. Pada tabel dibawah akan dijelaskan analisa perangkat yang ada menggunakan tools NMAP.

Tabel 6. Analisa Perangkat Menggunakan tools Nmap

Nama Perangkat	Fungsi	Software	IP Addreess
Server Aplikasi	Server	Kaspersky	222.124.29.196
		Cisco-SCCP	
		Mysql	
Server E-Pajak	Server	Postgresql	118.97.144.182
		Mysql	
Server Eproc	Server	MobileMe Mail	223.27.147.139
Server Akuwaras	Server	Microsoft SQL-Server	180.250.189.39
		Cisco-SCCP	
Server Bursakerja	Server	Utilistor	180.250.189.40
		Mysql	
		Cisco-SCCP	

Proses ini merupakan proses terakhir yang dilakukan dalam aktivitas *Network Security Assessment* dimana pada proses ini melakukan *Vulnerabilities* atau analisa kerentanan.

Dari aktivitas ini IP yang akan dilakukan analisa kerentanan pada tabel dibawah ini, sebagai berikut:

Tabel 7. Analisa Kerentanan

No	IP Address	Nama Mesin
1.	222.124.29.196	Server Aplikasi
2.	118.97.144.182	Server E-Pajak
3.	223.27.147.139	Server Eproc
4.	180.25.189.39	Server AkuWaras
5.	180.25.189.40	Server Bursakerja

Pada tabel diatas merupakan IP Address yang akan dilakukan Scanning menggunakan tools Nessus untuk mendapatkan *Vulnerabilities Assessment* atau Hasil Kerentanannya pada tiap mesin IP. Dan hasil daripada *Vulnerabilities Assessment* tersebut dapat diliat pada tabel dibawah ini sebagai berikut:

Tabel 8. Kerentanan Server eproc.denpasarkota.go.id

NO	VULNERABILITY	JENIS KERENTANAN
1	NTMail3 Arbitrary Mail Relay	SMTP problems
2	mDNS Detection (Remote Network)	Service Detection

Tabel 9. Kerentanan Server aplikasi.denpasarkota.go.id

NO	VULNERABILITY	JENIS KERENTANAN
1	MikroTik RouterOS < 6.40.7 or 6.41.x < 6.41.3 SMB Buffer Overflow	Misc.
2	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.	Misc.
3	Unencrypted Telnet Server	Misc.

NO	VULNERABILITY	JENIS KERENTANAN
4	DNS Server Cache Snooping Remote Information Disclosure	DNS
5	DNS Server Spoofed Request Amplification DdoS	DNS
6	DNS Server Recursive Query Cache Poisoning Weakness	DNS

Tabel 10. Kerentanan Server akuwaras.denpasarkota.go.id

NO	VULNERABILITY	JENIS KERENTANAN
1	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.	Misc.
2	Unencrypted Telnet Server	Misc.
3	MikroTik RouterOS Unauthenticated Intermediary	Misc.
4	DNS Server Cache Snooping Remote Information Disclosure	DNS
5	DNS Server Spoofed Request Amplification DdoS	DNS
6	DNS Server Recursive Query Cache Poisoning Weakness	DNS

Tabel 11. Kerentanan Server bursakerja.denpasarkota.go.id

NO	VULNERABILITY	JENIS KERENTANAN
1	PHP Unsupported Version Detection	CGI abuses
2	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.	Misc.
3	SSL Certificate Cannot Be Trusted	General
4	SSL Self-Signed Certificate	General
5	Unencrypted Telnet Server	Misc.
6	MikroTik RouterOS Unauthenticated Intermediary	Misc.
7	SSL Medium Strength Cipher Suites Supported (SWEET32)	General
8	DNS Server Cache Snooping Remote Information Disclosure	DNS
9	DNS Server Spoofed Request Amplification DdoS	DNS
10	DNS Server Recursive Query Cache Poisoning Weakness	DNS
11	SSH Weak Algorithms Supported	Misc.
12	SSH Server CBC Mode Ciphers Enabled	Misc.
13	SSH Weak MAC Algorithms Enabled	Misc.

Tabel 12. Kerentanan Server e-pajak.denpasarkota.go.id

NO	VULNERABILITY	JENIS KERENTANAN
1	SSL Version 2 and 3 Protocol Detection	Service Detection
2	SSL Certificate Cannot Be Trusted	General
3	SSL Medium Strength Cipher Suites Supported (SWEET32)	General
4	SSL Certificate Expiry	General
5	DNS Server Cache Snooping Remote Information Disclosure	DNS
6	DNS Server Spoofed Request Amplification DdoS	DNS
7	DNS Server Recursive Query Cache Poisoning Weakness	DNS
8	HTTP TRACE / TRACK Methods Allowed	Web Servers
9	SSH Weak Algorithms Supported	Misc.
10	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General
11	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.
12	SSH Server CBC Mode Ciphers Enabled	Misc.
13	SSH Weak MAC Algorithms Enabled	Misc.

4.3 Business Impact Analysis dan Risk Factor

Dari hasil vulnerability yang sudah dianalisa sebelumnya, maka data yang telah didapatkan selanjutnya dilakukan proses Network Security Assessment yaitu menghitung Business Impact Analysis (BIA).

Tabel 13. Business Impact Analysis server Eproc

NO	VULNERABILITY	AV	AC	AU	C	I	A	SCORE	LEVEL	JENIS KERENTANAN
1	NTMail3 Arbitrary Mail Relay	1.0	0.71	0.704	0	0	0.660	7.8	HIGH	SMTP problems
2	mDNS Detection (Remote Network)	1.0	0.71	0.704	0.75	0	0	5.0	MEDIUM	Service Detection

Tabel 14. Business Impact Analysis server Aplikasi

NO	VULNERABILITY	AV	AC	AU	C	I	A	SCORE	LEVEL	JENIS KERENTANAN
1	MikroTik RouterOS < 6.40.7 or 6.41.x < 6.41.3 SMB Buffer Overflow	1.0	0.71	0.704	0.660	0.660	0.660	10.0	CRITICAL	Misc.
2	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.	1.0	0.71	0.56	0.660	0.660	0.660	9.0	HIGH	Misc.
3	Unencrypted Telnet Server	1.0	0.61	0.704	0.275	0.275	0	5.8	MEDIUM	Misc.
4	DNS Server Cache Snooping Remote Information Disclosure	1.0	0.71	0.704	0.275	0	0	5.0	MEDIUM	DNS
5	DNS Server Spoofed Request Amplification DdoS	1.0	0.71	0.704	0	0	0.275	5.0	MEDIUM	DNS
6	DNS Server Recursive Query Cache Poisoning Weakness	1.0	0.71	0.704	0	0.275	0	5.0	MEDIUM	DNS

Tabel 15. Business Impact Analysis Server Akuwaras

NO	VULNERABILITY	V	C	U				CORE	LEVEL	JENIS KERENTANAN
1	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.	.0	.71	.56	.660	.660	.660	.0	IGH	Misc.
2	Unencrypted Telnet Server	.0	.61	.704	.275	.275		.8	EDIUM	Misc.
3	MikroTik RouterOS Unauthenticated Intermediary	.0	.71	.704	.275			.0	EDIUM	Misc.
4	DNS Server Cache Snooping Remote Information Disclosure	.0	.71	.704	.275			.0	EDIUM	DNS
5	DNS Server Spoofed Request Amplification DdoS	.0	.71	.704			.275	.0	EDIUM	DNS
6	DNS Server Recursive Query Cache Poisoning Weakness	.0	.71	.704		.275		.0	EDIUM	DNS

Tabel 16. Business Impact Analysis Bursakerja

NO	VULNERABILITY	AV	AC	AU	C	I	A	SCORE	LEVEL	JENIS KERENTANAN
1	PHP Unsupported Version Detection	1.0	0.71	0.704	0.660	0.660	0.660	10.0	HIGH	CGI abuses
2	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.	1.0	0.71	0.56	0.660	0.660	0.660	9.0	HIGH	Misc.
3	SSL Certificate Cannot Be Trusted	1.0	0.71	0.704	0.275	0.275	0	6.4	MEDIUM	General
4	SSL Self-Signed Certificate	1.0	0.71	0.704	0.275	0.275	0	6.4	MEDIUM	General
5	Unencrypted Telnet Server	1.0	0.61	0.704	0.275	0.275	0	5.8	MEDIUM	Misc.
6	MikroTik RouterOS Unauthenticated Intermediary	1.0	0.71	0.704	0.275	0	0	5.0	MEDIUM	Misc.
7	SSL Medium Strength Cipher Suites Supported (SWEET32)	1.0	0.71	0.704	0.275	0	0	5.0	MEDIUM	General
8	DNS Server Cache Snooping Remote Information Disclosure	1.0	0.71	0.704	0.275	0	0	5.0	MEDIUM	DNS
9	DNS Server Spoofed Request Amplification DdoS	1.0	0.71	0.704	0	0	0.275	5.0	MEDIUM	DNS
10	DNS Server Recursive Query Cache Poisoning Weakness	1.0	0.71	0.704	0	0.275	0	5.0	MEDIUM	DNS
11	SSH Weak Algorithms Supported	1.0	0.61	0.704	0.275	0	0	4.3	MEDIUM	Misc.

NO	VULNERABILITY	AV	AC	AU	C	I	A	SCORE	LEVEL	JENIS KERENTANAN
12	SSH Server CBC Mode Ciphers Enabled	1.0	0.35	0.704	0.275	0	0	2.6	LOW	Misc.
13	SSH Weak MAC Algorithms Enabled	1.0	0.35	0.704	0.275	0	0	2.6	LOW	Misc.

Tabel 17. Business Impact Analysis server e-pajak

NO	VULNERABILITY	AV	AC	AU	C	I	A	SCORE	LEVEL	JENIS KERENTANAN
1	SSL Version 2 and 3 Protocol Detection	1.0	0.61	0.704	0.660	0	0	7.1	HIGH	Service Detection
2	SSL Certificate Cannot Be Trusted	1.0	0.71	0.704	0.275	0.275	0	6.4	MEDIUM	General
3	SSL Medium Strength Cipher Suites Supported (SWEET32)	1.0	0.71	0.704	0.275	0	0	5.0	MEDIUM	General
4	SSL Certificate Expiry	1.0	0.71	0.704	0	0.275	0	5.0	MEDIUM	General
5	DNS Server Cache Snooping Remote Information Disclosure	1.0	0.71	0.704	0.275	0	0	5.0	MEDIUM	DNS
6	DNS Server Spoofed Request Amplification DdoS	1.0	0.71	0.704	0	0	0.275	5.0	MEDIUM	DNS
7	DNS Server Recursive Query Cache Poisoning Weakness	1.0	0.71	0.704	0	0.275	0	5.0	MEDIUM	DNS
8	HTTP TRACE / TRACK Methods Allowed	1.0	0.71	0.704	0.275	0	0	5.0	MEDIUM	Web Servers
9	SSH Weak Algorithms Supported	1.0	0.61	0.704	0.275	0	0	4.3	MEDIUM	Misc.
10	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	1.0	0.35	0.704	0.275	0	0	2.6	LOW	General
11	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	1.0	0.35	0.704	0	0.275	0	2.6	LOW	Misc.
12	SSH Server CBC Mode Ciphers Enabled	1.0	0.35	0.704	0.275	0	0	2.6	LOW	Misc.
13	SSH Weak MAC Algorithms Enabled	1.0	0.35	0.704	0.275	0	0	2.6	LOW	Misc.

Dari keseluruhan hasil yang didapatkan, didapatkan jumlah *vulnerabilities* masing-masing mesin yang ada di Dinas Komunikasi, Informatika, dan Statistik Kota Denpasar dengan review tabel sebagai berikut:

Tabel 18. Hasil Analisa Vulnerability

NO	Nama IP Jaringan	Jumlah Vulnerability
1.	Aplikasi	6
2.	Akuwaras	6
3.	Bursakerja	13
4.	E-Pajak	13
5.	Eproc	2

Dari tabel diatas dapat disimpulkan bahwa setiap IP Jaringan memiliki rata-rata *vulnerability* sebanyak 8 *vulnerability.* Untuk server Bursakerja dan E-Pajak adalah yang paling banyak memiliki *vulnerability* yaitu sebanyak 13 dengan kategori cukup tinggi kerentanannya. Dengan angka segitu resiko yang dimiliki cukup tinggi sehingga perbandingannya sangat berbeda dengan *vulnerability* yang dimiliki oleh Aplikasi, Akuwaras sebanyak 6, sedangkan yang paling sedikit memiliki *vulnerability* yaitu Eproc sebanyak 2.

5. Kesimpulan

Beberapa kesimpulan yang dapat diambil dari penelitian yang telah dilakukan adalah sebagai berikut:

1. Sistem manajemen keamanan informasi di Dinas Komunikasi, Informatika, dan Statistika Kota Denpasar sudah dilakukan walau masih belum berjalan secara optimal karena belum mencapai tingkat kematangan yang diharapkan. tingkat kematangan saat ini pada data subyektif mendapatkan hasil evaluasi yang tidak layak dengan nilai tingkat kelengkapan penerapan standar ISO 27001 dinilai 181.
2. Tingkat kesiapan menunjukkan dari 5 mesin yang melingkupi E-Pajak, AkuWaras, Aplikasi, Eproc, dan Bursakerja terdapat 1 level critical, 10 level high, 24 level medium dan 16 level low.

DAFTAR REFERENSI

[1] Ngurah. Budaya Keamanan Informasi, 09 Mei 2018. [Online]. Available: https://denpasarkota.go.id/baca-berita/13720/Berikan-Edukasi-Cegah-Penyalahgunaan-Teknologi-Informasi-Pemkot-Denpasar-Gelar-Seminar-petikBudaya-Keamanan-Informasipetik.

[2] Tania, A. M., Setiyadi, D., & Khasanah, F. N. Keamanan Website Menggunakan Vulnerability Assessment. *INFORMATICS FOR EDUCATORS AND PROFESSIONAL: Journal of Informatics*, 2018; *2*(2): 171-180.

[3] Riadi, I., Yudhana, A., & Yunanri, W. Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 2020; *7*(4): 853-860.

[4] Laksmiati, D. Vulnerability Assessment Pada Situs Www. Hatsehat. Com Menggunakan Openvas. *Jurnal Akrab Juara*, 2020; *5*(3): 240-246.

[5] Gadran, A. N. Desain Dan Testing Keamanan Jaringan Komputer Dengan Network-Based Intrusion Prevention System (NIPS) Menggunakan Metode Vulnerability Assessment Dan Penetration Testing, Tugas Akhir, Universitas Bakrie, 2019

[6] Suhana, M. P., Nurjaya, I. W., & Natih, N. M. (2016). Analisis Kerentanan Pantai Timur Pulau Bintan, Provinsi Kepulauan Riau Menggunakan Digital Shoreline Analysis System dan Metode Coastal Vulnerability Index. *Jurnal Teknologi Perikanan dan Kelautan*, *7*(1), 21-38.

[7] Adiputra, A., Rasminto, R., & Khausar, K. Vulnerability Assessment of Environmental and Non-Natural Physical by Subsidence in Sub-Unity of Peatland Hydrology at Jangkang River-Liong River Bengkalis Island. *Genta Mulia: Jurnal Ilmiah Pendidikan*, 2020; *11*(1): 13-21

[8] Akhirina, T. Y., & Arif, S. M. Evaluasi Keamanan Teknologi Informasi pada PT INDOTAMA PARTNER LOGISTICS Menggunakan Indeks Keamanan Informasi (KAMI). *Jurnal Nasional Teknologi dan Sistem Informasi*, 2016; *2*(2): 53-62.

[9] Ikhsan, H., & Jarti, N. Analisis Risiko Keamanan Teknologi Informasi Menggunakan Octave Allegro. *JR: JURNAL RESPONSIVE Teknik Informatika*, 2018; *2*(1): 31-41

[10] Umar, R., Riadi, I., & Handoyo, E. Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*, 2019; *1*: 47-53