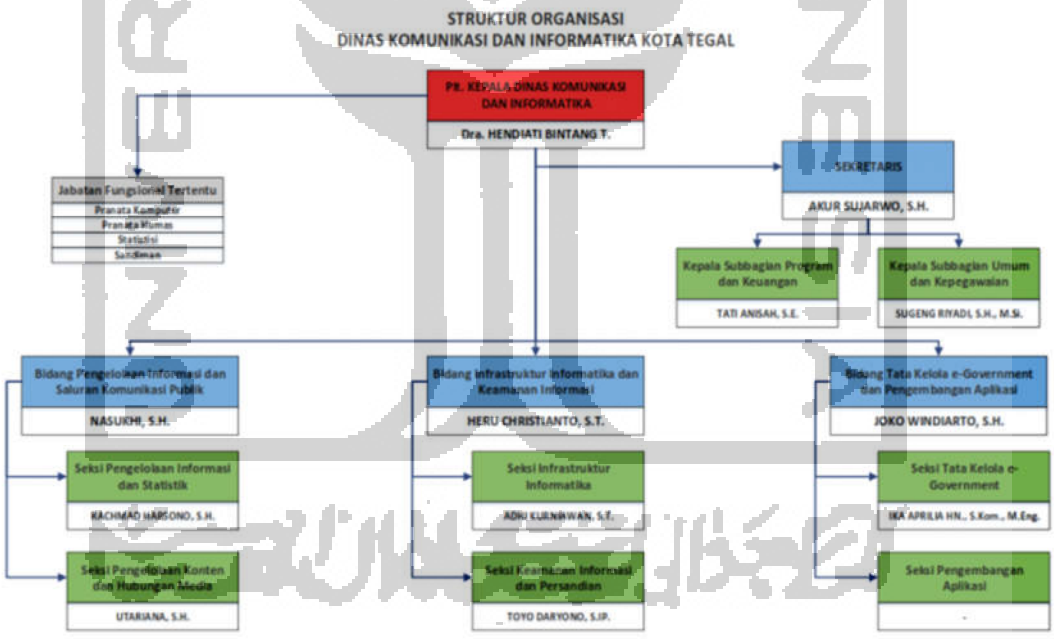
BAB 2
Tinjauan Pustaka

2.1 Gambaran Umum Dinas Komunikasi dan Informatika Kota Tegal

Berdasarkan peraturan Walikota Tegal nomor 18 tahun 2016 , Dinas Komunikasi dan Informatika Kota Tegal adalah pengelola komunikasi dan informatika di pemerintah Kota Tegal yang mempunyai tugas untuk membantu Walikota melaksanakan urusan pemerintahan yang menjadi kewenangan daerah dan tugas pembantuan di bidang komunikasi dan informatika. Dinas Komunikasi dan Informatika yang dimiliki oleh Kota Tegal masuk kriteria tipe B yang terdiri dari 3 bidang, adapun bidang yang menjadi wewenang dinas komunikasi dan informatika adalah bidang pengelolaan informasi dan saluran komunikasi publik, bidang informatikan dan keamanan informasi, bidang tata kelola e-government dan pengembangan aplikasi persandian, dan berikut merupakan struktur organisasi Dinas Komunikasi dan Informatika kota Tegal dan tupoksinya.



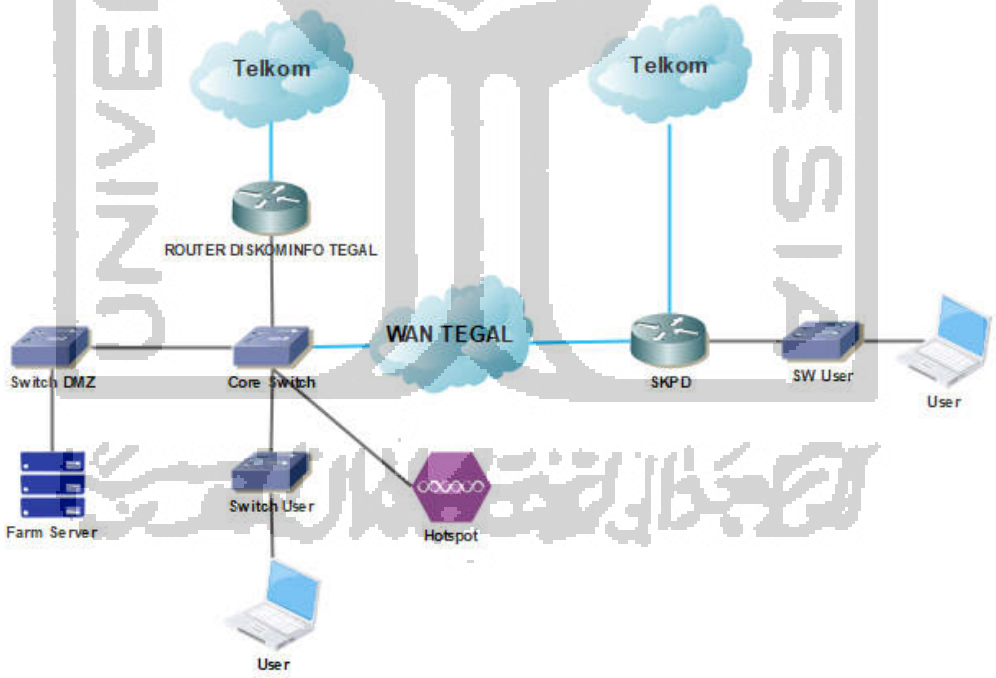
Gambar 2.1 Struktur Organisasi Dinas Komunikasi dan Informatika Kota Tegal

Tugas pokok dan Fungsi Kebijakan Pengembangan dan Pengelolaan TIK telah dibebankan sepenuhnya ke Dinas Komunikasi dan Informatika, dalam melaksanakan tugas sebagaimana dimaksud dalam Pasal 306, Dinas Komunikasi dan Informatika menyelenggarakan fungsi :

1. Perumusan kebijakan di bidang komunikasi dan informatika, bidang persandian, dan bidang statistik.
2. Pelaksanaan kebijakan di bidang komunikasi dan informatika, bidang persandian, dan bidang statistik
3. Pelaksanaan evaluasi dan pelaporan di bidang komunikasi dan informatika, bidang persandian, dan bidang statistik
4. Pelaksanaan kesekretariatan dinas komunikasi dan informatika
5. Pengendalian penyelenggaraan tugas unit pelaksana teknis dinas
6. Pelaksanaan fungsi lain yang diberikan oleh walikota sesuai dengan tugas dan fungsinya.

2.1.1 Gambaran Topologi Jaringan Kota Tegal

Secara garis besar infrastruktur Dinas Komunikasi dan Informatika berperan untuk menghubungkan antara masing-masing Satuan Kerja Perangkat Dinas (SKPD) agar dapat terhubung ke jaringan internal Kota Tegal dan berikut adalah gambaran topologi jaringan Kota Tegal.



Gambar 2.2 Gambaran Umum Jaringan Kota Tegal

Dari sisi tanggung jawab jaringan SKPD dikelola oleh masing-masing SKPD. Dinas Komunikasi dan Informatika Kota Tegal bertanggung jawan terhadap koneksi dari jaringan *backbone* mereka menuju *router* masing-masing SKPD.

2.2 Studi Pustaka

2.2.1 Penelitian Terdahulu

Rihal, Purnamasari, (2010) dalam penelitiannya melakukan implementasi dan analisis keamanan pada suatu perusahaan dengan menggunakan *Open Source Security Information Management (OSSIM) AlientVault*. Peneliti mengintegrasikan *OSSIM AlientVault* dengan perangkat keamanan jaringan *IDS* dan *firewall* (*Juniper*) dan memantau trafik yang lewat selama satu minggu dan melakukan simulasi penyerangan dengan *ICMP Flooding*, hasilnya menunjukan bahwa *OSSIM AlientVault* dapat mendeteksi serangan *ICMP Flooding* di jaringan mereka.

Arsham, K. (2016) dalam penelitiannya membangun sistem manajemen keamanan jaringan menggunakan *Open Source Security Information Management (OSSIM)* yang membantu *security officer* dalam menangani dan mengamankan sebuah jaringan. *OSSIM* diintegrasikan dengan modul *OSSEC* agen *HIDS* sebagai pendeteksi serangan *(Intrusion Detection System)* dan melakukan simulasi serangan terhadapnya dengan manggunakan *DDos, Sniffing* maupun *Exploit* ke target. Dan hasilnya *SIEM*-pun dapat mengenali serangan tersebut.

Djunaidi V. & Rifqy & Wijaya S. & Roestam R. (2014) meneliti dan menggunakan *OSSIM AlientVault* sebagai *NMS (Network Monitoring System)* di suatu perusahaan, penulis mencoba untuk menganalisa dan mengimplementasikan *OSSIM AlientVault* dengan metode *Top Down* dan mengsimulasikan serangan *Bruteforce* ke *Zimbra Email Server*, hasil penelitiannya *OSSIM AlientVault* dapat melihat serangan yang terjadi ke *E-mail Server* Zimbra dan memberikan notifikasi *e-mail* kepada *administrator*. Penelitipun menganjurkan untuk membuat *backup server* dan penambahan notifikasi keamanan berbasis *sms*.

Pratama A. & Wijaya A. & Halim RM. N. (2016) dalam penelitian menggunakan *OSSIM Alientvault* untuk *memonitoring server* Universitas Bina Darma Palembang dari sisi keamanan, penggunaan *OSSIM Alientvault* dapat melaporkan ancaman seperti *virus*, ancaman *malware* terhadap jaringan secara *realtime*.

Bachane, I. & Idrissi Khamlichi, Y. & Chaoui, H. (2016) dalam penelitiannya menggunakan *SIEM* sebagai alat *forensic* di lingkungan *cloud*, didalam *cloud* dengan berbagai macam *service* serta kombinasi berbagai macam layanan yang ada didalam lingkungan *cloud*, penulis melihat perlunya penggunaan *SIEM* untuk lingkungan *cloud* secara *realtime* agar proses penanganan masalah keamanan dalam lingkungan *cloud* dapat di proses dengan lebih cepat, dan hasil penelitian mengganggap penggunaan *SIEM* lebih efektif dibandingkan menggunakan *syslog server*.

Irfan, M. & Abbas, H. & Iqbal, W. (2015) dalam penelitian mereka menguji kelayakan penggunaan *SIEM* untuk *forensic* di lingkungan *cloud*, mereka menggunaan *USM AlientVa*ult sebagai pilihan *SIEM*-nya dan menggunaakan beberapa aset *seperti Windows 8.1, Windows 7, Windows Xp, Windows Server 2008*, dan *Solarwinds* sebagai pilihan *NMS*-nya, Peneliti melakukan simulasi serangan *Bruteforce* dan *Dos* dengan menggunakan Kali Linux, dan dari hasil implementasi tersebut didapakan bahwa serangan dan analisis yang dikumpulkan dalam *SIEM* dapat menujukan kelayakan penggunaan *SIEM* di lingkungan *cloud*.

Anastasov, I & Davcev, D. (2014) mengusulkan penggunaan model dan arsitektur baru dalam implementasi *SIEM* dengan menggunakan *Hierarchical SIEM Manager*, mekanisme yang memang diperuntukkan untuk tipe perusahaan dengan organisasi yang terdistribusi. Peneliti berhasil menggunakan *ArchSight* dalam implementasi keamanan jaringan yang besar dan terdistibusi.

Hadiansyah, C. & Iskandar, I. & Doynikova, E (2017) melakukan penelitian yang fokus untuk melakukan implementasi penggunaan *SIEM* untuk mengamankan jaringan di Dinas Komunikasi dan Informatika Provinsi Jawa Barat . Peneliti memasang *OSSIM* di jaringan Provinsi Jawa Barat dengan aset berupa *Windows Server 2003*, *Linux Redhat* dan *Email Server*. Peneliti menggunakan *OSSIM AlientVault* dan mensimulasikan serangan menggunakan *ICMP flooding*. *SIEM* dapat mengenali serangan dan menujukan *top attacker, top source* dan *top destination.*

Vianello, V. & Gulisano, V. & Jimenez-Peris, R. & Patiño-Martínez, M. & Torres, R. & Díaz, R. & Prieto, E. (2013) menggunakan *SIEM* untuk infrastruktur yang komplek dan dengan jumlah aset yang banyak dan dengan sistem *SIEM* yang tidak terdistribusi membuat *SIEM* kekurangan *resource* untuk memproses semua *event* yang ada dan mengkorelasikan dengan kemungkianan adanya serangan. Peneliti mencoba untuk melakukan pengetesan *SIEM* di sistem *Olympic Games* dengan pendekatan *distributed correlation* dan *query parallelization* dalam menyerang. Dan menggunakan D*os* dan menggunakan *Worm* sebagai alat serangan, hasil *monitoring* berupa notifikasi ke *admininistrator*. Peneliti menggunakan *OSSIM AlientVault* dan mensimulasikan serangan menggunakan *Worm* dan *Bruteforce*.

Dairinram, P. & Wongsawang, D. & Pengsart, P. (2013) melihat bahwa banyaknya jumlah *event* yang semakin meningkat di infrastruktur yang komplek membuat identifikasi terhadap ancaman yang ada dari *event* yang terkumpul menjadi salah satu masalah yang di hadapi *administrator*. Peneliti menggunakan *The Latent Semantic Analysis (LSA)* untuk menganalisa korelasi serangan dari *event-event* yang di kumpulkan oleh *SIEM*.

Tabel 2.1: ***Literature Review***

No	Nama	Uraian Singkat	Objek Penelitian	Tools	Hasil
1	Rihal, M. & Purnamasari, P. D. (2010)	Penelitiannya mengintegrasikan *OSSIM AlientVault* dengan perangkat keamanan jaringan *IDS* dan *firewall* dan metode yang dipakai penulis adalah melakukan pemantauan terhadap trafik *TCP, UDP* dan *ICMP* selama satu pekan, dan melakukan simulasi serangan. Hasil serangan dan laporanpun dianalisa.	*OSSIM AlientVault* di jaringan dengan *IDS* dan *Firewall Juniper*	Peneliti menggunakan *OSSIM AlientVault* dan *Juniper* sebagai jaringan dan mensimulasikan serangan menggunakan *ICMP flooding*	*OSSIM* dapat mendeteksi serangan secara *real-time* melalui pengamatan trafik jaringan dan laporan dari *OSSIM AlentVault*
2	Arsham, K. (2016)	Peneliti membangun sistem manajemen keamanan jaringan menggunakan *Open Source Security Information Management (OSSIM)* yang akan membantu admin dalam menangani dan mengamankan sebuah jaringan. *OSSIM SIEM (security Information and Event Mangement)* akan diintegrasikan dengan modul *OSSEC agent HIDS* sebagai pendeteksi serangan *(Intrusion Detection System)*.	Implementasi manajemen keamanan jaringan menggunakan *Open Source Security Information Management (OSSIM)*	Peneliti fokus membahas bagaimana serangan bisa terlihat dengan tipe serangan *Ddos, Sniffing, Exploit*	*OSSIM* dapat menyajikan hasil deteksi serangan dalam bentuk *real time log event* dan grafik sehingga *administrator* dapat dengan mudah mengetahui adanya sebuah serangan dengan cepat.
3	Djunaidi V. & Rifqy & Wijaya S. & Roestam R. (2014)	Peneliti mencoba menganalisis dan merancang *Network Monitoring System* dengan menggunakan *OSSIM AlienVault* pada PT METALOGIX INFOLINK PERSADA. Metode penelitian yang digunakan adalah metode *Top Down*	*OSSIM AlientVault* di jaringan sebagai alat *Networ Monitoring System* dan mengirimkan notifikasi *E-mail*	Peneliti menggunakan *OSSIM AlientVault* dan *Mail Server Zimbra* sebagai target dan serangan menggunakan *Bruteforce*	*Security Incident Event Management (SIEM*) dan dapat melihat notifikasi yang tentang apa yang terjadi pada *E-mail Server* Zimbra dan menyarankan menggunakan *server backup* serta notifikasi *sms*
4	Pratama A. & Wijaya A., &	Dengan menggunakan *metode Experimen (Experimental Research)*, penulis menggunakan *SIEM* untuk	*OSSIM AlientVault* di jaringan	Peneliti menggunakan *OSSIM AlientVault* dan Server	*OSSIM AlientVault* dapat melaporkan kejadian jika terjadi *threat* ancaman

	Halim RM. N. (2016)	melakukan *monitoring* terhadap *Server* Universitas Bina Darma Palembang yang ada pada Jaringannya.	Universitas Bina Darma Palembang untuk *monitoring server*	Universitas Bina Darma Palembang sebagai target	seperti *virus malware detection, network unstable* dan melakukan monitoring secara *real time*
5	Bachane, I. & Idrissi Khamlichi, Y. & Chaoui, H. (2016)	Dalam penelitian ini penulis melihat di *cloud* dengan berbagai macam layanan dengan kombinasi layanan yang unik, masalah di lingkungan *cloud* pun banyak, Penelitiannya fokus bagaimana tantangan untuk melakukan investigasi *forensic* dengan *SIEM* di lingkungan *cloud* dan membandingkan dengan *syslog server*	Proses *forensic* di lingkungan *cloud* dengan menggunakan *SIEM*	Peneliti menggunakan proses *forensic* dalam penelitiannya	Peneliti menganggap penggunaan *SIEM* lebih efektive dibandingkan menggunaan *syslog server*
6	Irfan, M. & Abbas, H. & Iqbal, W. (2015)	Analisis kelayakan untuk melakukan forensika digital melalui *SIEM (Security Information and Event Management)* di lingkungan *cloud*. Penelitian berfokus pada serangan pasif sementara beberapa aset dan serangan aktif serta analisis *forensic*. Diawal disajikan gambaran menyeluruh tentang berbagai hal yang dapat dipertimbangkan untuk melakukan analisis *forensic* yang mendalam di lingkungan *cloud*.	Kelayakan penggunaan *SIEM* di lngkungan *cloud* dengan aset berupa *Windows 8.1, Windows 7, Windows XP, Windows Server 2008 R2, VMware Esx, Solar winds Log and Event Manager*	Peneliti menggunakan *USM AlientVault* dan beberapa jenis *server* dan serangan menggunakan *KaliLinux OS* dengen tipe serangan *Bruteforce* dan *Dos*	Serangan dan analisis yang dikumpulkan *SIEM* menunjukkan keberhasilan dan kelayakan penggunaan *SIEM* di ingkungan *cloud*.
7	Anastasov, I & Davcev, D. (2014)	Peneliti mengusulkan model dan arsitektur baru untuk implementasi *SIEM* dengan menggunakan *Multiple Hierarchical SIEM Managers*. Modelnya disebut "*Hierarchical Managers Model*", mekanisme ini diarahkan untuk perusahaan dengan organisasi yang terdistribusi	Penerapan *SIEM* di jaringan yang terdistibusi dengan aset berupa. *Active Directory, Email Server, Database Server*	Peneliti menggunakan *ArcSight ESM*	Peneliti berhasil menggunakan *ArcSight ESM* dalam jaringan yang terdistribusi

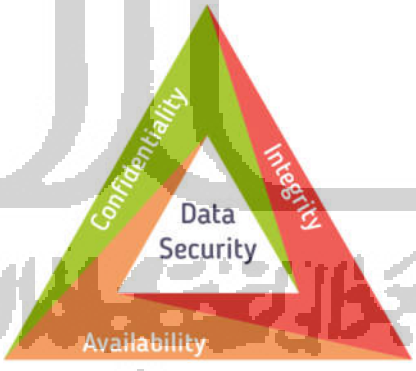
8	Hadiansyah, C. & Iskandar, I. & Doynikova, E (2017)	Peneliti fokus untuk melakukan implementasi penggunaan *SIEM* untuk mengamankan jaringan di Dinas Komunikasi dan Informatika Provinsi Jawa Barat	*OSSIM* di jaringan Provinsi Jawa Barat dengan aset berupa *Window Server 2003, Linux Redhat* dan *Email Server*	Peneliti menggunakan *OSSIM AlientVault* dan mensimulasikan serangan menggunakan *ICMP flooding*	*SIEM* dapat mengenali serangan dan menujukan *Top Attacker. Top Source* dan *Top Destination.*
9	Vianello, V. & Gulisano, V. & Jimenez-Peris, R. & Patiño-Martínez, M. & Torres, R. & Díaz, R. & Prieto, E. (2013)	Penggunaan *SIEM* untuk infrastruktur yang komplek dan dengan jumlah aset yang banyak dan dengan *SIEM* yang tidak terdistribusi membuat *SIEM* kekurangan *resource* untuk memproses semua event yang ada dan mengkorelasikan dengan kemungkianan adanya serangan. Peneliti mencoba untuk melakukan pengetesan *SIEM* dengan *distributed correlation* dan *query parallelization* dalam menyerang aset	*FTP Server, Windows Server*	Peneliti menggunakan *OSSIM AlientVault* dan mensimulasikan serangan menggunakan *Worm, Bruteforce*	*SIEM* dapat mengenali serangan yang ada dan dapat memberikan notifikasi.
10	Dairinram, P. & Wongsawang, D. & Pengsart, P. (2013)	Banyak jumlah *event* yang semakin meningkat di infrastruktur yang komplek membuat identifikasi terhadap ancaman yang ada dari *event* yang terkumpul menjadi salah satu masalah yang di hadapi *administrator*. Peneliti menggunakan *The Latent Semantic Analysis (LSA)* untuk menganalisa korelasi serangan dari *event-event* yang di kumpulkan oleh *SIEM*	Peneliti fokus menggunaakan *LSA indetification* untuk mengenali serangan yang ada pada jaringannya dan menggunakan *FTP server* sebagai target, *Windows XP, Windows 7*	*Worm, Bruteforce*	Tekniknya juga memberikan hasil yang benar dengan Keakuratan matriks yang dikurangi adalah 85,71%

2.3 Landasan Teori

Makin banyaknya organisasi yang mengunakan IT sebagai salah satu fungsi pendukung bisnis membuat ketergantungan terhadap IT semakin tinggi, dan semakin banyak pula aset informasi dan data yang ada pada organisai tersebut terkumpul. Informasi tersebut menciptakan sebuah nilai *(Value)* terhadap aset yang ada pada instansi tersebut. Sistem IT yang semakin kompleks dan terdistribusi membuat departemen IT sulit mengelola dan memonitoring aset IT dengan mudah. Padahal dari sisi bisnis sudah menjadi kebutuhan untuk departmen IT untuk dapat memonitor apa saja yang terjadi dengan jaringan atau semua aspek penyusun IT tersebut.

2.3.1 Keamanan Informasi *(Information Security)*

Keamanan informasi adalah bidang dan aktifitas profesional yang multidisiplin dan berkaitan dengan pengembangan dan implementasi mekanisme keamanan dari berbagai aspek baik teknis dan organisional. Fokus keamanan informasi adalah untuk mengamankan informasi di infrastruktur IT maupun sistem informasi dari berbagai macam serangan yang mengakibatkan informasi tersebut di akses dengan tidah sah, penggunaan informasi yang tidak sah, kebocoran data, modifikasi data serta perusakan informasi. Tindakan mengamankan informasi yang relevan saat ini meliputi beberapa aspek keamanan yaitu: *Confidentiality, Integrity, Availability, Privacy, Authenticity & Trustworthiness, Non-Repudiation, Accountability & Auditability.* (Cherdantseva dan Hilton, 2013)



Gambar 2.3 *Information Security (CIA)*

a. Kerahasiaan (*Confidentiality)*

   Dalam keamanan informasi aspek *confidentiality* adalah bagaimana meyakinkan informasi hanya dapat diakses oleh orang yang berhak dan terautorisasi terhadap informasi tersebut. (Expert ISO27000). Dalam implementasinya baik didalam jaringan

maupun di level data banyak solusi yang mengandalkan mekanisme enkripsi untuk melindungi data tersebut

b. Integritas (*Integrity)*

Dalam keamanan informasi aspek *integrity* adalah bagaimana menjamin integritas suatu data ataupun informasi agar tidak bisa dirubah oleh orang yang tidak berhak atau tidak terautorisasi (Oriyano, 2014). Contohnya: Pada saat data dikirimkan dari Sumber A menuju Tujuan B. bagaimana menjamin bahwa data yang dikirim A sama dengan data yang diterima B. Untuk menyakinkan data yang diterima sama, maka B melakukan *checksum* terhadap data yang di terimanya dan membandingkan dengan karakter *checksum* yang ada pada A. Mekanisme seperti ini sering disebut dengan nama *File Integrity Checksum.*

c. Ketersediaan (*Availability)*

Dalam keamanan informasi aspek a*vailability* adalah bagaimana menjamin suatu sistem informasi/infrastruktur yang bertugas untuk mengirim, menyimpan serta memproses informasi dapat selalu tersedia pada saat *user* membutuhkan sistem tersebut (Oriyano, 2014). Ketersediaan sistem informasi / infrastruktur menjadi hal yang penting harus selalu tersedia agak segala macam proses bisnis organisasi tersebut berjalan dengan baik. Banyak solusi yang berkaitan dengan a*vailability* baik di level *data center, network*, *server* yang tujuannya adalah membuat sistem tersebut *redundant* agar dapat bekerja dengan *availability* yang di inginkan sesuai dengan kebutuhan bisnisnya.

d. Privasi (*Privacy)*

Aspek *privacy* adalah bagaimana menjamin bahwa seseorang atau kelompok atau organisasi dapat menyembunyikan informasi yang bersifat *sensitive* bagi mereka.

e. Keaslian dan Kepercayaan (*Authenticity & Trustworthiness)*

Dalam keamanan informasi aspek a*uthenticity & trustworthiness* adalah bagaimana menjamin suatu data dapat di anggap otentik dimana ada karakter yang bersifat unik dan spesifik yang membuat data tersebut berbeda dengan data yang lain (Oriyano, 2014). Kadang istilah *authenticity & trustworthiness* sering diartikan dengan *integrity*, tapi aspek *authenticity & trustworthiness* adalah sisi yang menunjukan suatu informasi itu asli atau tidak. *Digital signature* merupakan salah satu teknologi yang menjamin bahwa data bersifat otentik.

f. Tidak ada Penolakan (*Non-Repudiation)*

Aspek n*on-repudiation* adalah aspek keamanan informasi yang menjamin bahwa pengirim data tidak dapat menolak mengirim data dan penerima tidak dapat menolak untuk menerima data tersebut sesuai dengan prosedur yang ada (Oriyano, 2014).

g. Akuntabilitas dan dapat di Audit (*Accountability & Auditability)*

Aspek ini menjamin bahwa segala macam solusi keamanan yang ada dapat di audit dan dapat dipertanggungjawabkan sesuai dengan *framework* yang organisasi tersebut ikuti.

2.3.2 *Network Threat*

Jaringan komputer sebagai salah satu komponen IT merupakan komponen infrastruktur yang menghubungkan dan membuat layanan IT bekerja dalam suatu instansi. Jaringan juga merupakan tempat dimana segala macam layanan IT berjalan untuk mendukung proses bisnis yang ada yang menunjang berjalannya proses bisnis di suatu instansi. Pada saat infrastruktur jaringan mempunya *value* tersebut maka jaringan akan mulai diserang, dan berikut merupakan beberapa contoh serangan yang ada dalam jaringan.

a. *Mac Flooding*

MAC Address Flooding, adalah metode untuk melumpuhkan jaringan. Celah keamanan yang di serang dalam teknik ini adalah keterbatasan tabel *MAC Address switch* dalam. *Switch* bisa mempelajari *MAC Address* yang masuk menggunakan *port switch* dan mencatatnya di tabel *MAC Address*. *Hacker* mengirimkan banyak *MAC Address* palsu (*Bogus*). Apabila tabel *MAC Address* penuh maka Switch akan berubah menjadi *HUB* dan mengirimkan *broadcast* kesemua *port*. Tujuan dari serangan ini adalah membuat jaringan lumpuh atau melakukan *sniffing* paket data dijaringan. Penggunaan *Mac Flooding* juga membuat komputer atau *router* mempunyai tabel *arp* yang bertambah.

b. *Arp Poisioning*

Merupakan teknik menyerang jaringan komputer yang memungkinkan *hacker* bisa menyadap komunikasi data pada jaringan atau melakukan modifikasi trafik atau bahkan menghentikan trafik. Prinsipnya serangan *ARP Poisoning* ini memanfaatkan kelemahan pada teknologi jaringan komputer itu sendiri yang menggunakan *ARP broadcast*. Teknik ini meracuni tabel *arp* suatu *pc/router* dimana *hacker* akan meracuni tabel *ARP* dengan alamat MAC yang salah. Serangan *ARP Poisoning* biasanya merupakan serangan pembuka untuk serangan *sniffing, Man in the Middle, Session Hijacking* dan serangan lainnya.

c. CDP Flooding

Flooding adalah Teknik yang digunakan untuk membanjiri trafik, sedangkan *CDP* adalah *Cisco Discover Protocol*, *CDP flooding* merupakan Teknik yang digunakan oleh *hacker* untuk membanjiri tabel *CDP* suatu *router/switch* dan membuat Tabel *CDP device* tersebut penuh melebihi kemampuannya. Penggunaan Serangan ini dapat menyebabkan *router /switch* berhenti bekerja, karena serangan ini masuk kedalam teknik *Dos (Denial of Service)*

d. *DHCP Starvation*

Serangan yang bertujuan untuk membuat *DHCP server* tidak bekerja dengan mengirim *request DHCP* dengan menggunakan *MAC address* palsu, dengan begitu *DHCP server* akan memberikan masing-masing *ip address* kepada *MAC address* palsu tersebut sampai *ip* yang tersedia habis, dengan begitu *client* tidak akan mendapatkan *ip address* dari *DHCP server* yang asli. (termasuk DOS attack).

e. *DHCP Rogue*

Salah satu pemanfaatan celah keamanan pada mekanisme konfigurasi alamat jaringan menggunakan *DHCP*. *DHCP Rogue server* memberikan konfigurasi alamat jaringan yang salah kepada *client* yang tergabung di dalam jaringan dengan tujuan menciptakan serangan jaringan berupa *man in the middle*, sehingga dapat menimbulkan ancaman terhadap *privasi client* yang tergabung di dalam jaringan.

f. *SYN Flooding*

Flooding adalah teknik yang digunakan untuk membanjiri trafik, sedangkan *SYN* adalah tipe *flag* didalam *TCP* yang digunakan pada awal proses koneksi dalam jaringan, atau yang lebih dikenal dengan *threeway hand shake. SYN flooding* merupakan Teknik yang digunakan oleh *hacker* dengan melakukan permintaan koneksi terhadap suatu *device* dengan jumlah koneksi yang tak terhingga sehingga device tersebut tidak bisa lagi memenuhi permintaan koneksi lagi. Penggunaan Serangan ini dapat menyebabkan *device* berhenti bekerja, karena serangan ini masuk kedalam teknik *Dos (Denial of Service)*

g. *Bruteforce*

Metode digunakan untuk meretas *password* dengan cara mencoba semua kemungkinan kombinasi yang ada pada "*wordlist"*. Lamanya waktu akan ditentukan oleh panjang dan kombinasi karakter *password* yang akan diretas

2.3.3 *IT Security Risk Management*

Risk Management adalah proses untuk mengidentifikasi *vulnerabilities* dan ancaman terhadap sumber informasi yang digunakan oleh sebuah organisasi dalam mencapai tujuan bisnisnya, dan menentukan tindakan/respon pencegahan apa yang perlu dilakukan jika resiko tersebut terjadi, atau dapat untuk mengurangi risiko pada tingkat yang dapat diterima, berdasarkan pada nilai sumber informasi untuk organisasi tersebut *(ISACA,2006)*

Dalam ranah *IT Security, IT Security Risk Management* adalah proses yang dilakukan oleh perusahaan/instansi untuk dapat mengidentifikasi ancaman terhadap aset-aset informasi yang dimiliki oleh organisasi tersebut , baik berupa infrastruktur, data, aplikasi dan memahami bagaimana cara untuk mencegah atau mengurangi resiko keamanan dari informasi yang dimiliki oleh perusahaan.instansi tersebut. Berdasarkan *NIST SP800-30* ada 9 tahap yang dilakukan pada saat melakukan managemen risiko

2.3.4 *Risk Assesment*

Risk Assessment merupakan tahap mengidentifikasi resiko dalam *Risk Management Process*. Sebuah organisasi atau perusahaan menggunakan *risk assessment* untuk menentukan bahaya apa saja yang berpotensi dan resiko-resiko yang akan ditimbulkan terhadap sistem IT. hasil yang diharapkan dari proses ini adalah dapat membantu mengidentifikasikan kontrol yang sesuai untuk mengurangi atau menghilangkan resiko-resiko tersebut selama proses pengurangan resiko *(risk mitigation*).

2.3.4.1 Threat Identification

Threat (ancaman) adalah potensi - potensi yang berbahaya yang dihasilkan oleh suatu sumber *(threat source)* yang dapat menyerang celah keamanan yang dimiliki suatu sistem. Suatu sumber ancaman tidak dapat menghasilkan ancaman ketika tidak ada celah keamanan.

2.3.4.2 Risk Mitigation

Pada tahap *risk mitigation*, meliputi tahap pemberian prioritas, evaluasi dan implementasi kontrol pengurangan resiko yang direkomendasikan dan diperoleh dari tahap *risk assessment*. Karena proses menghilangkan semua resiko yang mungkin terjadi mempakan hal yang sangat tidak praktis dan mendekati mustahil, maka merupakan kewajiban dari *senior management/business managers* untuk menggunakan pendekatan *least-cost* dan mengimplementasikan kontrol yang paling penting untuk mengurangi level resiko ke level

yang lebih dapat diterima, dengan mengedepankan dampak yang minimal pada sumber daya dan tujuan organisasi.

2.3.4.3 Evaluation and Monitoring

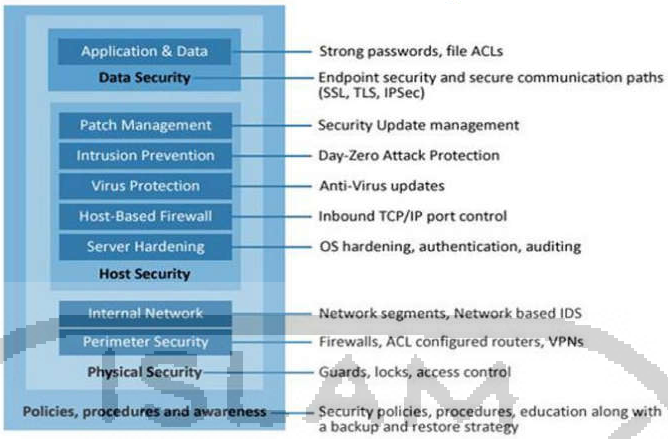
Pada sebagian besar peusahaan, jaringan yang dimiliki biasanya akan terus menerus akan mengalami perkembangan, meliputi sistem yang dimiliki, komponen-komponen yang dimiliki serta *software* atau aplikasi yang akan diganti atau mengalami *update* dengan versi terbaru. Selain itu, penambahan juga akan meliputi pergantian serta pembaharuan aturan keamanan yang dimiliki. Setiap perubahan tersebut menimbulkan permasalahan karena resiko-resiko yang akan muncul serta resiko yang sebelumnya telah dapat diatasi akan muncul kembali. Oleh karena itu, proses *risk management* harus terus berjalan dan mengalami perkembangan.

2.3.5 *Security Strategy Defence in Depth*

Dalam implementasi sistem keamanan informasi karena sangat pentingnya sebuah informasi, tidak jarang organisasi menggunakan pendekatan *defence in depth* untuk mengamankan informasi yang di milikinya.

Defence in depth merupakan mekanisme keamanan berlapis untuk meningkatkan keamanan sistem secara keseluruhan. Jika sebuah serangan menyebabkan satu mekanisme keamanan gagal, mekanisme lain mungkin masih memberikan keamanan yang diperlukan untuk melindungi sistem. contoh, bukan ide bagus untuk benar-benar mengandalkan *firewall* untuk memberikan keamanan pada aplikasi penggunaan internal saja, karena *firewall* biasanya dapat dihindari oleh *hacker* (bisa melalui serangan fisik atau serangan *social engineering*). Mekanisme keamanan lainnya harus ditambahkan untuk melengkapi perlindungan yang diberikan oleh *firewall* seperti *CCTV*, dan *security awareness* serta solusi yang lain yang menangani berbagai serangan dari vector tertentu (OWASP, 2015).

Berikut gambaran implementasi defense in depth pada suatu organisasi dengan berbagai pilihan solusi sesuai dengan layernya.



Gambar 2.4 *Defence in Depth Strategy*

2.3.6 Sistem Manajemen Keamanan Informasi (SKMI)

Sistem Manajemen Keamanan Informasi adalah kumpulan dari kebijakan dan prosedur untuk mengatur data sensitif milik instansi pemerintahan secara sistematis. Tujuan dari SMKI sendiri adalah untuk meminimalisir risiko dan menjamin kelangsungan bisnis secara proaktif untuk membatasi dampak dari pelanggaran keamanan.

Sistem Manajemen Keamanan Informasi juga harus mengacu pada standar nasional atau internasional yang ada agar kualitas pengamanan yang diberikan tinggi dan mampu menanggulangi adanya masalah. Standar internasional yang telah direkomendasikan untuk penerapan SMKI adalah ISO/IEC 27001. Standar ini telah berjalan berbasis risiko sehingga mampu mengurangi ancaman dan menanggulangi masalah dengan cepat dan tepat

Implementasi dari SMKI ini meliputi kebijakan, proses, prosedur, struktur organisasi, serta fungsi dari *software* dan *hardware*. Pelaksanaan SMKI juga harus langsung dipengaruhi oleh tujuan organisasi, kebutuhan keamanan, dan proses yang digunakan oleh organisasi. Penerapan Sistem Manajemen Keamanan Informasi pada sebuah organisasi juga harus memiliki pedoman yang ditujukan pada pimpinan organisasi. Hal ini telah dinyatakan oleh 16 Direktorat Sistem Informasi pada tahun 2007 bahwa telah ditetapkan 10 pedoman terbaik untuk penerapan SMKI, namun tidak menutup kemungkinan untuk terjadi perubahan pada pedoman-pedoman yang telah ada. Berikut ini adalah 10 pedoman yang disebutkan dalam SKMI:

1. Pedoman manajemen umum
2. Pedoman kebijakan keamanan yang memenuhi sasaran bisnis
3. Pedoman manajemen risiko keamanan informasi yang mengidentifikasi aset kritis diantaranya sistem, jaringan, dan data

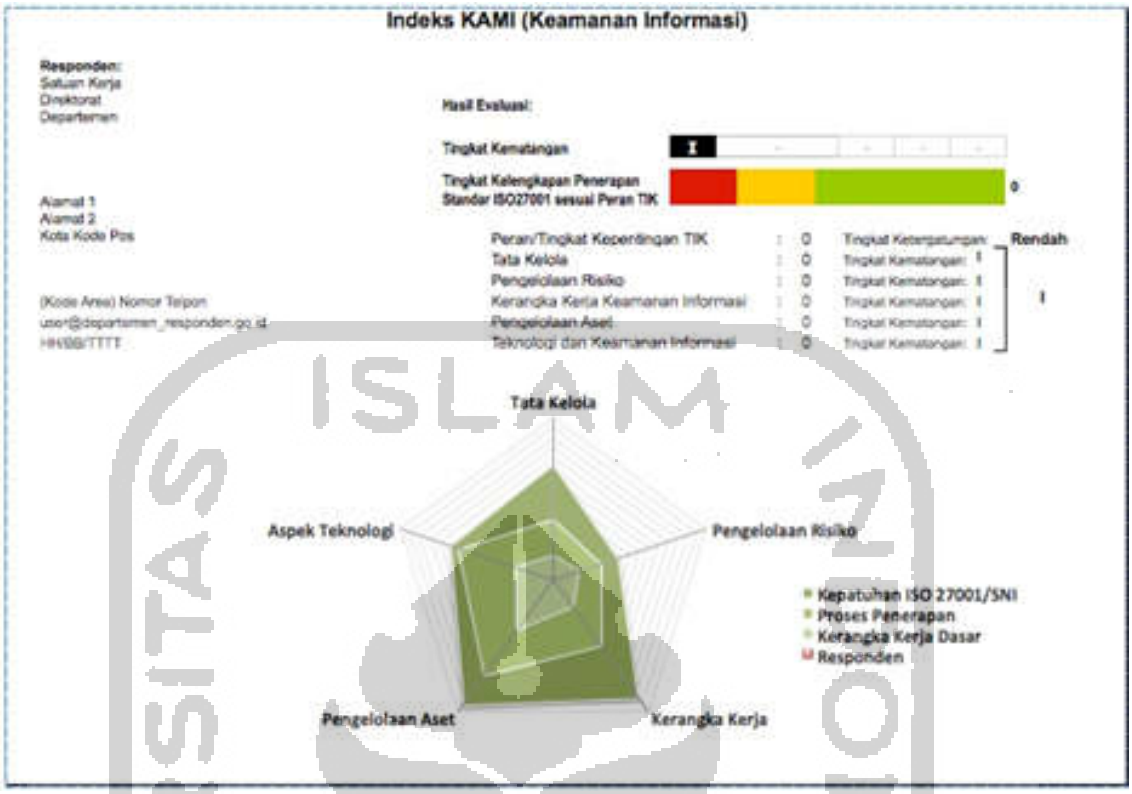
4. Pedoman arsitektur & desain keamanan berdasar kebutuhan bisnis dan perlindungan aset informasi paling kritis
5. Pedoman isu-isu pengguna yang meliputi akuntabilitas & pelatihan serta ekspertis yang memadai
6. Pedoman manajemen sistem & jaringan yang meliputi kontrol akses untuk melindungi aset dalam jaringan, integritas *software*, konfigurasi aset, dan *backup* yang terjadwal
7. Pedoman otentikasi & otorisasi bagi pengguna aset dan pihak ketiga (kontraktor & penyedia layanan)
8. Pedoman pengawasan & audit terhadap kondisi sistem dan jaringan yang ada
9. Pedoman ang keamanan fisik aset informasi dan layanan serta sumber daya IT
10. Pedoman rencana keberlanjutan bisnis & pemulihan bencana untuk aset kritis dan dilakukannya tes secara periodik dan pastikan berfungsi secara efektif

2.3.7 Indeks Keamanan Informasi (KAMI)

Indeks KAMI merupakan suatu alat untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 serta peta area tata kelola keamanan sistem informasi di suatu lembaga pemerintahan. Bentuk evaluasi yang diterapkan dalam indeks Keamanan Informasi (KAMI) dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan IT dalam mendukung terlaksananya tugas pokok dan fungsi yang ada.

Data yang digunakan dalam evaluasi ini nantinya akan memberikan gambaran indeks kesiapan keamanan informasi dari aspek kelengkapan maupun kematangan, kerangka kerja , keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi Indeks KAMI ini secara umum ditujukan untuk digunakan oleh instansi pemerintah di tingkat pusat. Akan tetapi satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat juga dapat menggunakan alat evaluasi ini untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggungjawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. Berikut merupakan contoh dan bentuk bagaimana indeks Keamanan Informasi (KAMI) direpresentasikan.



Gambar 2.5 Contoh Grafik Indeks KAMI

Evaluasi dilakukan terhadap beberapa area target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009

Alat evaluasi Indeks KAMI dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. Evaluasi yang dilakukan dengan menggunakan indeks Keamanan Informasi (KAMI) ini mencakup 5 target area, yaitu:

1. Tata Kelola Keamanan Informasi

   Pada bagian ini dilakukan evaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi serta tugas dan tanggung jawab pengelola keamanan informasi. Kontrol yang diperlukan adalah kebijakan formal yang mendefinisikan peran, tanggung jawab, kewenangan pengelolaan keamanan informasi dari pimpinan unit kerja sampai ke pelaksana operasional. Termasuk juga adanya program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.

2. Pengelolaan Risiko Keamanan Informasi

   Pada bagian ini dilakukan evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Kontrol yang diberlakukan adalah adanya kerangka kerja pengelolaan risiko dengan definisi yang eksplisit terkait ambang batas diterimanya risiko, program pengelolaan risiko dan langkah mitigasi yang secara reguler dikaji keefektivitasannya

3. Kerangka Kerja Keamanan Informasi

   Pada bagian ini dilakukan evaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Kontrol yang diperlukan adalah sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektivitas kontrol dan langkah perbaikan.

4. Pengelolaan Aset informasi

   Pada bagian ini dilakukan evaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Kontrol yang diperlukan adalah bentuk pengamanan terkait keberadaan aset informasi serta keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut

5. Teknologi dan Keamanan Informasi

   Pada bagian ini dilakukan evaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Kontrol yang digunakan adalah strategi terkait dengan tingkatan risiko dan tidak secara eksplisit menyebutkan teknologi atau merk tertentu.

Dari ke lima aspek keamanan informasi berdasarkan indeks Keamanan Informasi (KAMI) maka peran IT dalam mengamankan informasinya dapat terukur dan bias dijadikan sebagai inputan kepada pengelola layanan IT.

2.3.8 Pengukuran indeks Keamanan Informasi (KAMI)

Dalam proses pengukuran indeks Keamanan Informasi (KAMI), alat yang digunakan program berbasis Excel yang sudah disesuaikan dengan matriks yang ada pada ISO 27001. Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan kondisi penerapan keamanan informasi yang terjadi di instansi tersebut.

Dalam proses pengisian kuisioner responden diminta untuk mendefinisikan Peran IT (atau Tingkat Kepentingan IT) di Instansinya. Definisi ini bisa dijabarkan untuk tingkat Satuan Kerja baik di tingkat Kementerian/Lembaga, ataupun untuk satuan kerja yang lebih kecil, sampai ke Unit Eselon III. Responden juga diminta untuk mendeskripsikan infrastruktur IT yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik kepentingan IT yang sama.

Pertanyaan dikelompokkan untuk 2 keperluan. Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2009. Setiap jawaban diberikan skor yang nantinya dikonsolidasi untuk menghasilkan angka indeks sekaligus digunakan untuk menampilkan hasil evaluasi dalam *dashboard* di akhir proses ini. Skor yang diberikan untuk jawaban pertanyaan sesuai tingkat kematangannya mengacu kepada table dibawah ini:

Peran TIK				
Rendah		Indeks (Skor Akhir)		Status Kesiapan
0	12	0	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	588	Baik/Cukup
Sedang		Skor Akhir		Status Kesiapan
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi		Skor Akhir		Status Kesiapan
25	36	0	272	Tidak Layak
		273	392	Perlu Perbaikan
		393	588	Baik/Cukup
Kritis		Skor Akhir		Status Kesiapan
37	48	0	333	Tidak Layak
		334	453	Perlu Perbaikan
		454	588	Baik/Cukup

Gambar 2.6 Tabel Skoring Peran IT dan Status Kesiapan

Hasil dari penjumlahan skor untuk masing-masing area ditampilkan dalam diagram radar dengan latar belakang area untuk tingkat maksimal kematangan 1 s/d 3. Dalam diagram ini bisa dilihat perbandingan antara kondisi kesiapan sebagai hasil dari proses evaluasi dengan acuan tingkat kematangan yang ada.

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

Gambar 2.7 Tabel Nilai Kategori Penilaian

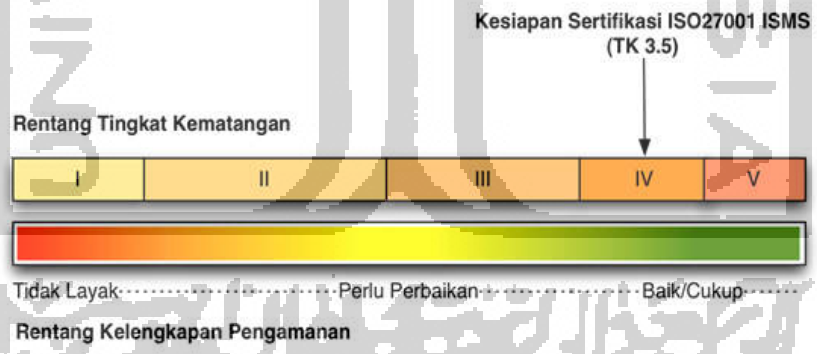
Dengan membaca diagram ini, pimpinan instansi dapat melihat kebutuhan pembenahan yang diperlukan dan korelasi antara berbagai area penerapan keamanan informasi. Adapun korelasi antara peran atau tingkat kepentingan IT dalam instansi didefinisikan melalui tabel berikut:

Pengelompokan kedua dilakukan berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga.

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

Kedua pengelompokan ini dapat dipetakan seperti pada gambar 2.8 yang memberikan dua sudut pandang yang berbeda: tingkat kelengkapan pengamanan dan tingkat kematangan pengamanan. Dan instansi responden dapat menggunakan metrik ini sebagai target program keamanan informasi.



Gambar 2.8 Tingkat Kematangan dan Kesiapain ISO 27001

Indeks KAMI sebaiknya digunakan 2 kali dalam setahun sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu.

2.3.9 *SIEM*

SIEM adalah teknologi yang dapat mendeteksi ancaman dan insiden keamanan dengan pengumpulan *log* secara *real-time* dan menganalisa *historis log* keamanan dari berbagai macam tipe *log* dan dari berbagai sumber data yang berasal dari *device* yang berbeda. *SIEM* juga mendukung analisa dan investigasi insiden melalui analisis data *historis* dari berbagai alat keamanan seperti *(Router, IDS/IPS, UTM, Server dll).* Kemampuan inti dari teknologi *SIEM* adalah cakupan pengumpulan *log* yang luas dan kemampuan untuk mengkorelasikan dan menganalisis kejadian di berbagai sumber yang berbeda (Gartner, 2017)

Gambar 2.9 *SIEM* Feature List

2.3.9.1 Fitur-Fitur *SIEM*

a. *Log/Event Collection*

   SIEM dapat mengumpulkan *log* dari berbagai sumber (*Windows, Unix / Linux*, Aplikasi, *Database, Router, Switch*, dan perangkat lainnya) dan menempatkan *log* tersebut di lokasi yang terpusat (Fernandes,2017).

b. *Log Analisys*

   Hal pokok yang dimiliki oleh solusi *SIEM* adalah analisis data *log* dari berbagai sumber dan menghasilkan analisa yang cerdas untuk *monitoring* keamanan IT secara *real time.* Data *log* mentah dianalisis dan di representasikan dalam bentuk diagram, grafik yang mudah dimengerti oleh Administrator. Administrator IT juga dengan mudah menelusuri data *log* yang ditampilkan di *dashboard* untuk mengetahui lebih banyak aktivitas pengguna, serangan di jaringan, *log event* dll (Fernandes,2017).

c. *Event Correlation*

Event correlation adalah bagaimana *SIEM* memberikan informasi ke *administrator* untuk menangani masalah secara proaktif. Fitur ini memungkinkan administrator jaringan meningkatkan keamanan jaringan mereka dengan memproses jutaan *log event* secara bersamaan untuk mendeteksi anomali pada jaringan. Hubungan antar *event* dapat didasarkan pada *log, rules,* atau *alert* pada *system*. Misalnya, sebuah komputer login menggunakan 5 *UserID* yang berbeda di hari yang sama, secara korelasi akan memiliki tingkat urgensi yang tinggi, karena hal tersebut mirip dengan pola pemakaian *password* orang lain secara ilegal dari komputer tersebut (Fernandes,2017).

d. *Log Forensics*

SIEM membantu profesional keamanan melakukan penyelidikan *log forensic* dengan membiarkan mereka melakukan analisis penyebab serangan untuk melacak penyusup jaringan atau *event* yang menyebabkan masalah jaringan. Proses *log forensic* harus sangat intuitif dan *user-friendly,* memungkinkan administrator IT untuk mencari data *log* mentah dengan mudah. Pencarian *log* harus segera menunjukkan *entry log* yang tepat yang menunjukan aktivitas pelanggaran keamanan, menemukan waktu, orang dan lokasi aktivitas itu berasal (Fernandes,2017).

e. *IT Compliance*

SIEM memberikan laporan pelanggaran *policy* untuk berbagai standar keamanan seperti *DSS PCI, FISMA, GLBA, SOX, HIPAA*. Untuk memenuhi persyaratan sesuai dengan standar keamanan yang ada, organisasi perlu memantau jaringan mereka secara real time, memastikan keamanan untuk aset penting mereka, dan memberikan laporan audit jaringan kepada auditor bila diperlukan (Fernandes,2017).

f. *Application Log Monitoring*

SIEM membantu Administrator IT untuk memantau secara efektif *log* dari berbagai aplikasi bisnis mereka seperti *Database Server, Server DHCP, Server Web,* dll. *hacker* dapat dengan mudah mendapatkan akses ke aplikasi bisnis dan menyebabkan masalah jika aplikasi bisnis tidak dipantau secara real time. *SIEM* memungkinkan administrator IT untuk memantau aplikasi penting bisnis mereka secara *real time* dan mendeteksi anomali / aktivitas yang mencurigakan pada aplikasi dijaringan mereka (Fernandes,2017).

g. *Real Time Alerting*

Notifikasi yang *real-time* adalah fitur yang ada pada *SIEM* yang berfungsi untuk mengingatkan *security officer* saat terjadi anomali dan aktivitas yang mencurigakan di

jaringan. Administrator IT perlu memantau, mendeteksi, dan merespons secara *real time* terhadap permasalahan kritis yang dapat mempengaruhi infrastruktur jaringan mereka. Respon yang lambat dalam menanggapi masalah keamanan akan memperbesar kemungkinan masalah yang lebih besar (Fernandes,2017).

h. Object Access Auditing

Sebagian besar administrator menghadapi tantangan untuk mendeteksi apa yang sebenarnya terjadi pada file dan folder mereka, siiapa yang mengakses, menghapus, mengedit, memindahkan, dan sebagainya. Kemampuan audit akses terhadap suatu objek membantu administrator memenuhi kebutuhan yang ada. Dengan Audit terhadarp akses suatu objek data, organisasi dapat mengamankan data aset bisnis penting mereka, seperti data karyawan, catatan akuntansi, kekayaan intelektual, data pasien, data keuangan, dll (Fernandes,2017).

i. User Activity Monitor

Sebagian besar pelanggaran data terjadi karena organisasi gagal memantau aktivitas pengguna mereka, terutama pengguna yang memiliki hak istimewa. Dengan *SIEM* administrator dapat memantau pengguna secara real-time, dan membantu dalam mendeteksi penyalahgunaan data (Fernandes,2017).

j. Dashboard

Dashboard pada *SIEM* membantu administrator IT melakukan tindakan cepat dan membuat keputusan yang tepat selama terjadi masalah di jaringan. Data keamanan disajikan dengan cara yang sangat *intuitif* dan *user-friendly*. *Dasboard* harus dapat disesuaikan sepenuhnya sesuai dengan kebutuhan sehingga administrator IT dapat menambahkan dan hanya melihat informasi keamanan yang mereka butuhkan (Fernandes,2017).

k. Reporting

Administrator IT membuat keputusan berdasarkan laporan keamanan yang dihasilkan oleh *SIEM*. Laporan harus tepat dan akurat. *SIEM* menyediakan beberapa laporan keamanan dan kepatuhan sesuai dengan standar keamanan yang ada. Dan *Reporting* yang *out-of-the-box* yang dapat dihasilkan satuan beberapa menit atau dapat juga dijadwalkan pada waktu tertentu. Laporan keamanan harus memiliki desain yang bagus, dan data harus terstruktur dengan baik. Pembuat laporan membantu administrator membuat laporan keamanan untuk memenuhi persyaratan keamanan internal mereka (Fernandes,2017).

l. File Integrity Monitoring

File Integrity Monitoring (FIM) membantu Administrator untuk melihat apakah ada perubahan data dan. Bila pengguna yang tidak berwenang atau mengakses dan menyalahgunakan data rahasia, seperti catatan keuangan, dan informasi sensitif lainnya dari perusahaan. *SIEM* dapat memberikan notifikasi sesuai dengan kebutuhan administrator (Fernandes,2017).

m. System & Device log Monitoring

Sistem dan perangkat jaringan merupakan bagian terpenting dari setiap infrastruktur IT. *Log* yang dihasilkan oleh *server, workstation, router, switch*, dan lain-lain berisi informasi penting yang dapat di *monitoring* untuk mengurangi ancaman jaringan, seperti mencegah pencurian data, mendeteksi anomali jaringan, dan memantau aktivitas pengguna.

Akan sulit untuk melakukan analisis *log* secara manual. Oleh karena itu, otomatisasi *monitoring log* dan analisis sistem dan *log* secara real time akan membantu administrator mengurangi *downtime* jaringan, meningkatkan kinerja jaringan, dan memperkuat keamanan jaringan (Fernandes,2017).

2.3.10 *Digital Forensic*

Forensik Digital merupakan disiplin ilmu baru didalam dunia forensik, dimana pengertian dari forensik secara umum adalah sebuah proses keilmuan yang digunakan untuk mengumpulkan, menganalisis dan menghadirkan barang bukti. Ilmu forensik sebenarnya adalah sebuah ilmu yang sangat berhubungan dengan hukum yang digunakan untuk penanganan barang bukti yang akan dihadirkan didalam sebuah persidangan, karena terdapatnya perbedaan jenis serta cara penanganan barang bukti disetiap disiplin ilmu maka ilmu forensik menjadi lebih berkembang sesuai dengan disiplin ilmu yang ada, antara lain forensik kriminal, kedokteran, psikiatri, komputer, akunting, dan masih banyak cabang ilmu forensik lainnya.

Forensik Digital dulunya lebih dikenal sebagai komputer forensik, karena perkembangan sistem komputer yang sangat pesat dan menjadikan komputer bukan hanya sebuah komputer konvensional, sehingga semua perangkat digital yang menggunakan sistem kerja komputer termasuk kedalamnya dan memiliki arti dan cakupan yang lebih luas. Forensik Digital memiliki beberapa pengertian, yang antara lain adalah sebagai berikut:

Marcella, Forensik Digital adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti digital dalam kejahatan komputer. (Asrizal, 2012)

Budhisantoso, Forensik Digital adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti didalam penegakan hukum. (Asrizal, 2012)

Dr. H. B. Wolfe, serangkaian metode teknik dan prosedur untuk mengumpulkan bukti dari peralatan dan berbagai perangkat penyimpanan media komputasi digital, yang dapat disajikan di pengadilan dalam format yang *koheren* dan bermakna. (EC-Council, 2002)

Steve Hailey, *Pemeliharaan*, identifikasi, ekstraksi, interpretasi, dan dokumentasi bukti komputer, untuk memasukan aturan bukti, proses hukum, integritas bukti, pelaporan faktual dari informasi yang ditemukan, dan memberikan pendapat ahli dalam pengadilan hukum atau lainnya hukum dan atau proses administrasif sebagaimana dengan apa yang ditemukan. (EC-Council, 2002)

2.3.11 *Network Forensic*

Menurut *Gary Palmer* dalam bukunya *Road Map for Digital Forensic Research*, *Network forensic* adalah sub cabang forensik digital yang berkaitan dengan pemantauan dan analisis lalu lintas jaringan komputer untuk keperluan pengumpulan informasi, bukti hukum, atau deteksi serangan.

Dalam *network forensic* metodologi seperti tugas forensik lainnya, memulihkan dan menganalisis bukti digital dari sumber jaringan harus dilakukan sedemikian rupa sehingga hasilnya bisa direproduksi akurat. Untuk memastikan hasil yang bermanfaat, penyidik forensik harus melakukan aktivitas yang sesuai dengan kerangka metodologis. Keseluruhan proses dan metodelogi yang direkomendasikan dalam buku ini adalah sebagai berikut:

Gambar 2.10 Metodelogi *OSCAR* (*Source: A Road Map for Digital Forensic Research*)

1. *Obtain Information*

   Dalam tahap ini investigator mencari informasi yang mendukung proses forensik, segala informasi yang berhubungan dengan proses investigasi forensik,, seperti bentuk topologi jaringan, serangan apa yang terjadi di jaringan dan *environment network* itu sendiri

2. *Strategize*

   Merupakan tahap merencanakan penyelidikan agar *investigator* bekerja secara *efisien*. Dalam tahap ini investigator melakukan prioritasi terhadap objek apa saja yang bisa dijadikan sebagai barang bukti. Dalam proses ini juga investigator menentukan bagaimana proses penanganan barang bukti. Sehingga proses ini dianggap sudah dilakukan.

3. *Collect Evidence*

   Dalam proses ini investigator mengumpulan segala macam informasi yang menjaidi barang bukti dalam investigasi seperti *capture paket, log,* dan semua barang bukti yang mengarah ke insiden yang ada.

4. *Analyze*

   Dari hasil prioritasi barang bukti, akuisisi barang bukti di tahap *strategize* serta pengumpulan barang bukti dari masing-masing sumber, selanjutnya dilakukan analisa terhadap barang bukti tersebut

5. *Report*

   Pelaporan adalah aspek terpenting dari penyelidikan. Segala macam hasil temuan dalam proses analisa seharusnya dilakukan pelaporan dan dokumentasikan.