MENINGKATKAN KEHANDALAN TEKNOLOGI INFORMASI MELALUI REKAYASA KEAMANAN SIBER MENUJU POLRI PRESISI DI ERA POLICE 4.0

NASKAH AKADEMIK

OLEH:
ALUMNI S2 KOICA*
KOREAN NATIONAL POLICE UNIVERSITY; INSTITUT TEKNOLOGI BANDUNG

PENULIS

1. Kompol Achmad Kolbinus, S.T.
2. Kompol Yudho Arif Wibowo, S.Si.
3. AKP Audy Joize Oroh, S.Kom., S.I.K.
4. AKP Nugrahadi Kusuma, S.Sos., S.I.K.
5. AKP Grawas Sugiharto, S.Kom., M.Si.
6. AKP Victor Berliyantho, S.I.K.
7. AKP Ruzi Gusman, S.H., S.I.K., M.Si.
8. Iptu Ericson Siregar, S.Kom.
9. Iptu Muhammad Hafif, S.I.K.
10. Iptu I Made Martadi Putra, S.Kom.
11. Iptu Muhammad Yasin, S.I.K., M.A.P.
12. Ipda Tri Boy Alvin Siahaan, S.Tr.K.
13. Ipda Ariq Taufiqorrahman Arsyam, S.Tr.K.
14. Ipda Prima Pringgo Putra, S.Tr.K.
15. Ipda Muhammad ImamFadhil, S.Tr.K.
16. Ipda Dimas Robin Alexander, S.Tr.K.
17. Ipda Ryan Kushervian Rasyid, S.Tr.K., M.H.
18. Ipda Eristu Rizqi Prananda, S.Sos.
19. Ipda Sarlendra Satria Yudha, S.Kom.
20. Ipda Frentina Yuliana, S.T.

RINGKASAN EKSEKUTIF

Teknologi informasi (TI) turut berkembang sejalan dengan perkembangan peradaban manusia. Perkembangan teknologi informasi meliputi perkembangan infrastruktur TI. Banyaknya sistem dan teknologi baru yang muncul menuntut Polri mengikuti perkembangan teknologi yang ada. Salah satunya adalah pemanfaatan big data untuk mendukung data yang diperlukan dalam sistem pemerintahan, organisasi maupun perusahaan. Salah satu implementasi big data pada Kepolisian Negara Republik Indonesia (Polri), yaitu penggunaan data personel Polri melalui Sistem Informasi Personel Polri (SIPP) sebagai rangka penyelenggaraan pembinaan sumber daya manusia Polri yang bersih, transparan, akuntabel dan humanis sebagai sarana pendukung berupa data personel yang akurat, tepat, dan tersedia setiap saat. Hal ini tentunya sejalan dengan Rencana Pembangunan Jangka Panjang Polri tahap IV (periode 2021-2025) yaitu menjadi organisasi yang unggul (Excellent) dengan pemanfaatan big data guna penguatan kelembagaan Polri yang merupakan bagian dari Taksonomi Bloom Polri. Taksonomi Bloom ini merujuk pada kategori tatanan pemikiran terentang mulai dari higher-order thinking hingga lower-order thinking dalam konteks pengembangan kepemimpinan dan pendidikan

Penggunaan data yang memanfaatkan big data memerlukan keamanan informasi dari serangan siber agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab, mengingat pentingnya informasi SIPP yang menjadi rujukan utama mengenai informasi personel Polri. Dalam mengelola keamanan informasi pada satuan kerjannya, SSDM Polri telah menerapkan mekanisme pengamanan data dan informasi yang masih bersifat teknis. Keamanan informasi adalah usaha untuk meyakinkan terlindunginya sifat kerahasiaan, ketersediaan, dan keutuhan informasi. Untuk menjamin kelangsungan keamanan informasi ini, pemerintah telah menetapkan beberapa aturan, salah satunya adalah Peraturan Kementerian Komunikasi No. 4 Tahun 2016 yang mewajibkan sistem elektronik yang bersifat strategis menerapkan keamanan informasi.

Menindaklanjuti peraturan tersebut, naskah akademik ini tata kelola keamanan informasi berdasarkan SNI ISO 27001:2013, OCTAVE Allegro, dan COBIT 2019 yang khusus dibuat untuk penggunaan data center, penyedia serta pengelola sistem elektronik dalam konsep kerangka kerja deteksi, pencegahan, respon, kontrol, dan evaluasi. Kerangka kerja ini diharapkan mampu diterapkan pada data center, penyedia serta pengelola sistem elektronik

sehingga kerangka kerja ini dapat digunakan pada Big Data Polri untuk meningkatkan kehandalan teknologi informasi guna mewujudukan Polri presisi di era Police 4.0.Naskah akademik ini berkontribusi untuk mengembangkan suatu rangkaian sistem yang terstruktur mulai dari deteksi serangan siber yang aplikatif melalui sistem keamanan jaringan Honeypots guna mendukung tata kelola keamanan informasi.

DAFTAR ISI

Ringkasan Eksekutif 2
Daftar Isi 4
Daftar Gambar 6
Daftar Tabel 7
BAB I 8
A. Latar Belakang 9
B. Permasalahan 12
C. Maksud dan Tujuan 13
D. Metodologi 14
BAB II 15
A. Kajian Teoritis 15
A.1 Keamanan Siber 15
A.1.1 Ruang Siber 15
A.1.2 Kejahatan Siber 18
A.1.3 Deteksi Ancaman Siber 20
A.2 Tata Kelola Keamanan Informasi 22
A.2.1 Manajemen Keamanan Informasi 22
A.2.2 SNI ISO 27001:2013 tentang Sistem Manajemen Keamanan Informasi 24
A.2.3 Octave Allegro 26
A.2.4 Control Objective for Information and related Technology (COBIT) 29
B. Kajian Empiris 37
B.1 Honeypot Sebagai Perangkat Deteksi 37
B.2 Tata Kelola Teknologi Informasi Berbasis COBIT 38
B.3 Keamanan Informasi Berbasis SNI ISO 27001:2013 39
B.4 Penilaian Resiko Berbasis Octave Allegro 41
B.5 Indeks KAMI 4.1 43
BAB III 45
A. Kondisi Umum 45
B. Perangkat Keamanan Informasi 47
B.1 Perangkat lunak (software) keamanan teknologi Informasi 47
B.1.1 Honeypot 47
B.1.2 Anti Virus 48

B.1.3 Operating System (OS) Hardening 48
B.1.4 Enkripsi 48
B.1.5 Anti Keylogger 48
B.1.6 Anti Phishing 49
B.1.7 Endpoint Protection 49
B.1.8 Data Lost Protection (DLP) 49
B.1.9 Virtual Private Network (VPN) 50
B.2 Perangkat Keras (hardware) keamanan teknologi Informasi 50
B.2.1 Firewall 50
B.2.2 Intrusion Detection System (IDS) 50
B.2.3 Intrusion Prevention System (IPS) 50
B.2.4 Token Authentication 51
B.2.5 Proxy 51
C. Sistem Manajemen Keamanan Informasi 51
D. Audit Keamanan Informasi 53
BAB IV 55
A. Kondisi Umum 55
B. Pengembangan dan Pengujian Distro Linux Presisi Sebagai Metode Keamanan Server 61
B.1 Perancangan IPS (Intrusion Prevention System) 61
B.2 Perancangan Honeypot 61
B.3 Distro Linux Presisi 62
C. Pengembangan Tata Kelola Keamanan Informasi Berbasis COBIT, SNI ISO 27001:2013 dan Octave Allegro 63
C.1 Rancangan Integrasi SNI ISO 27001 dan OCTAVE Allegro 63
C.1.1 Tahapan Kerangka SNI ISO 27001:2013 64
C.1.2 Tahapan Kerangka OCTAVE Allegro 65
C.1.3 Integrasi SNI ISO 27001:2013 – OCTAVE Allegro 65
D. Penggunaan Indeks KAMI 4.1 Sebagai Tools Audit Keamanan Informasi 84
Daftar Pustaka 88

DAFTAR GAMBAR

Gambar 1 Implementasi honeypots 2 layer (Spitzner, 2003) 21
Gambar 2 Langkah-langkah OCTAVE Allegro (OCTAVE Approach, 2003) 27
Gambar 3 COBIT 2019 core model (ISACA, 2018) 32
Gambar 4 Komponen sistem tata kelola COBIT 2019 (ISACA, 2018) 33
Gambar 5 Level kapabillitas pada proses COBIT 2019 (ISACA, 2018) 35
Gambar 6 Tingkat Kematangan Untuk Focus Area (ISACA, 2018) 37
Gambar 7 Sirklus PDCA 52
Gambar 8 Kerangka Kerja SMKI 57
Gambar 9 Struktur Organisasi Tata Kelola Keamanan Informasi 58
Gambar 10 Struktur organisasi CISO 59
Gambar 11 Intrusion Prevention System 61
Gambar 12 Multi-Honeypot 62
Gambar 13 Distro Linux Presisi 63

DAFTAR TABEL

Tabel 1 Area dan Sasaran Pengendalian ISO/IEC 27001:2013 25
Tabel 2 Rating level COBIT 2019 (ISACA, 2018) 35
Tabel 3 Tahapan SNI ISO 27001:2013 64
Tabel 4 Tahapan Metode OCTAVE Allegro 65
Tabel 5 Pemetaan Metode OCTAVE Allegro pada SNI ISO 27001:2013 65
Tabel 6 Pemetaan Metode OCTAVE Allegro pada Klausul 6.1 SNI ISO 27001:2013 67
Tabel 7 Pemetaan ISO/IEC 27001:2013 ke COBIT 2019. 68
Tabel 8 Pemilihan domain model inti COBIT 2019 71
Tabel 9 Isi Komponen Kebijakan. 82

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

A. Latar Belakang

Teknologi informasi (TI) turut berkembang sejalan dengan perkembangan peradaban manusia. Perkembangan teknologi informasi meliputi perkembangan infrastruktur TI, seperti *hardware*, *software*, teknologi penyimpanan data (*storage*), dan teknologi komunikasi. Perkembangan TI tidak hanya mempengaruhi dunia bisnis, tetapi juga bidang-bidang lain, seperti kesehatan, pendidikan, pemerintahan, dan lain-lain (Laudon dan Laudon, 2012). Banyaknya sistem dan teknologi baru yang muncul menuntut Polri mengikuti perkembangan teknologi yang ada. Salah satunya pemanfaatan big data seperti pemanfaatan media sosial facebook, twitter, instagram, sistem kependudukan untuk mendukung data yang diperlukan dalam sistem pemerintahan, organisasi maupun perusahaan (Nugroho dkk., 2019). Big data adalah aset informasi bervolume tinggi, berkecepatan tinggi, dan beragam yang menuntut bentuk pemrosesan informasi inovatif yang hemat biaya yang memungkinkan peningkatan wawasan, pengambilan keputusan, dan otomatisasi proses (Glossary, 2007).

Salah satu implementasi big data pada Kepolisian Negara Republik Indonesia (Polri), yaitu penggunaan data personel Polri melalui Sistem Informasi Personel Polri (SIPP) sebagai rangka penyelenggaraan pembinaan sumber daya manusia Polri yang bersih, transparan, akuntabel dan humanis sebagai sarana pendukung berupa data personel yang akurat, tepat, dan tersedia setiap saat. SIPP adalah sistem berbasis komputer yang dikelola oleh Bag Infopers SSDM Polri, yang dapat menerima, mengirim, menyimpan, mengolah, menyajikan data dan informasi tentang Pegawai Negeri pada Polri secara online maupun manual secara akurat, berkualitas, dan tepat waktu. Hal ini sebagai upaya mendukung penyelenggaraan pembinaan sumber daya manusia Polri. Sistem tersebut dikembangkan guna mengolah dan menyajikan data tentang personel Polri yang tepat dan akurat sebagai sarana pendukung dalam menetapkan kebijakan dan pengambilan keputusan di bidang pembinaan sumber daya manusia di lingkungan Polri untuk menciptakan *e-government* yang ideal. Hal ini tentunya sejalan dengan Rencana Pembangunan Jangka Panjang Polri tahap IV (periode 2021-2025) yaitu menjadi organisasi yang unggul (Excellent). Yakni dengan pemanfaatan big data guna penguatan kelembagaan Polri yang merupakan bagian dari Taksonomi Bloom Polri. Taksonomi Bloom ini merujuk pada kategori

tatanan pemikiran terentang mulai dari higher-order thinking hingga lower-order thinking dalam konteks pengembangan kepemimpinan dan pendidikan (Haryatmoko, 2020).

Penggunaan data yang memanfaatkan big data memerlukan keamanan informasi dari serangan siber agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab, mengingat pentingnya informasi SIPP yang menjadi rujukan utama mengenai informasi personel Polri. Dalam mengelola keamanan informasi pada satuan kerjannya, SSDM Polri telah menerapkan mekanisme pengamanan data dan informasi yang masih bersifat teknis. SSDM Polri saat ini belum menerapkan sistem manajemen keamanan informasi (SMKI) secara komprehensif sehingga ancaman bagi aset-aset informasi organisasi masih memungkinkan untuk terjadi dan dapat mengancam operasional dari institusi. Beberapa potensi ancaman yang mungkin terjadi pada SSDM Polri seperti kejadian kehilangan, perusakan, pencurian, hingga penyadapan terhadap data sensitif personel akan menimbulkan dampak negatif pada operasional Polri yang secara tidak langsung mengancam keamanan Negara. Sehingga hal ini perlu mendapatkan atensi utama dari institusi.

Keamanan informasi adalah usaha untuk meyakinkan terlindunginya sifat kerahasiaan, ketersediaan, dan keutuhan informasi. Keamanan informasi ini juga meliputi aplikasi dan manajemen kontrol yang berhubungan dengan hal yang mengancam informasi itu sendiri, sehingga dapat mempengaruhi kesuksesan sebuah organisasi dalam mencapai tujuan (Chazar dan Ramdhani, 2016). Untuk menjamin kelangsungan keamanan informasi ini, pemerintah telah menetapkan beberapa aturan, salah satunya adalah Peraturan Kementerian Komunikasi No. 4 Tahun 2016 yang mewajibkan sistem elektronik yang bersifat strategis menerapkan keamanan informasi. Pada peraturan ini disebutkan bahwa negara mewajibkan penyelenggara sistem elektronik strategis dan tinggi menerapkan SNI ISO 27001:2013 tentang sistem manajemen keamanan informasi.

SNI ISO 27001:2013 merupakan standar yang dibuat Badan Standar Nasional (BSN) Indonesia yang mengadopsi ISO/IEC 27001. ISO/IEC 27001:2013 sebagai dasar dari SNI tersebut merupakan framework paling popular dan banyak digunakan dengan presentase 27% dibanding framework lainnya, yaitu COBIT (26%), ITIL (8%), BS7799 (18%), dan PCIDSS (21%) (Susanto dkk., 2011). Selain itu pada pengembangan Dedy Achmadi, dkk (2018), tentang pengembangan kerangka kerja SMKI berdasarkan ISO 27001 yang khusus dibuat untuk data center guna memenuhi aspek aspek *confidentiality*, *integrity*, dan *availability* pada

keamanan informasi menjelaskan bahwa pada data center terdapat tiga komponen penting, yaitu sumber daya manusia, proses, dan teknologi. Kerangka kerja ini diharapkan mampu diterapkan pada data center sehingga framework ini dapat digunakan pada SIPP yang merupakan bagian dari big data SSDM Polri untuk meningkatkan kehandalan teknologi informasi guna mewujudukan Polri presisi di era Police 4.0. Kerangka kerja ini juga mendukung penyempurnaan Pedoman dan Standard Operasional Prosedur kepolisian berbasis data dan teknologi informasi. Sebagaimana konsep Kapolri mengenai Presisi (Prediktif, responsibilitas, transparansi, berkeadilan) yang dilaksanakan dalam bidang transformasi organisasi. Transformasi organisasi merupakan salah satu dari empat bidang prioritas Kapolri Jenderal Polisi Drs. Listyo Sigit Prabowo, M.Si., dalam konsep Transformasi Menuju Polri yang presisi.

Keberhasilan dari SMKI bergantung dari proses manajemen risiko dengan mengidentifikasi aset kritis untuk memproritaskan mitigasi risiko yang tepat (Keating, 2014). Selain itu, Manajemen Risiko Keamanan Informasi (MRKI) adalah salah salah satu elemen penting dari proses SMKI pada organisasi yang membutuhkan MRKI untuk melakukan penilaian risiko dan menjadikan panduan untuk mengurangi risiko tersebut. Terdapat banyak tipe dari pendekatan penilaian risiko yang tersedia. Banyak organisasi masih kesulitan memilih metode ideal untuk kebutuhan yang spesifik untuk organisasinya (Shameli-Sendi dkk., 2016). Dalam mendukung manajemen keamanan informasi, framework yang dapat diterapkan yaitu OCTAVE Allegro yang merupakan metodologi untuk merampingkan dan mengoptimalkan proses penilaian risiko keamanan informasi sehingga organisasi dapat memperoleh hasil yang cukup dengan investasi kecil dalam waktu, orang, dan sumber daya terbatas (Humaira, 2012). Hasil identifikasi dan penilaian risiko tersebut akan menjadi bahan acuan dengan SNI ISO 27001:2013 untuk menjadi yaitu kontrol keamanan informasi guna mendukung kesesuaian dengan aturan terkait keamanan informasi, mengurangi biaya insiden, dan meningkatkan kepercayaan publik.

Pengembangan selanjutnya menghasilkan sistem pendeteksi serangan siber yang aplikatif melalui sistem keamanan jaringan *Honeypots* guna mendukung keamanan informasi dan tata kelola keamanan informasi. Honeypots adalah suatu sistem keamanan jaringan komputer yang didesain untuk diserang/disusupi oleh cracker, dan bukan untuk menyediakan suatu layanan produksi. Seharusnya hanya sedikit atau bahkan tidak ada sama sekali trafik jaringan yang berasal atau menuju honeypots. Oleh karena itu, semua trafik *honeypots* patut dicurigai sebagai aktivitas yang tidak sah atau tidak terautorisasi. Jika cukup informasi pada *log file honeypots*,

maka aktivitas mereka dapat dimonitor dan diketahui pola serangannya tanpa menimbulkan risiko kepada *production system* (Spiztner, 2003). Implementasi sistem tersebut dengan melakukan pencegahan atas serangan yang akan dilakukan oleh hacker dengan menekankan pada pendeteksian atas serangan yang dilakukan hacker sehingga administrator dapat mempelajari serangan tersebut dan mencari solusi untuk mencegahannya melalui tata kelola keamanan informasi berbasis COBIT, SNI ISO 27001:2013 dan Octave Allegro.

Berdasarkan hasil identifikasi dan analisa dari kerentanan, risiko, dan ancaman dengan sistem *Honeypot* tersebut, ditindaklanjuti dengan suatu tata kelola keamanan informasi pada big data Polri yang memenuhi kriteria struktur organisasi tata kelola keamanan informasi, sumber daya manusia, kebijakan serta prosedur tata kelola keamanan informasi. Tata kelola keamanan informasi tersebut dirancang dengan menggabungkan framework COBIT 2019, ISO/IEC 27001:2013 dan OCTAVE Allegro. COBIT 2019 dan ISO/IEC 27001:2013 juga digunakan untuk melakukan penilaian terhadap *capability level* (tingkat kemampuan) SSDM Polri dalam mengelola keamanan informasi dan melakukan analisis kesenjangan (gap) antara tingkat kemampuan keamanan informasi SSDM Polri saat ini (eksisting) dengan yang ideal dengan capaian target tingkat kemampuan 3. Capaian tingkat kemampuan 3 bersumber dari Peraturan Menteri Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi yang kemudian dimplementasikan pelaksanaannya dalam Indeks KAMI (Keamanan Informasi) sehingga dapat dilakukan perancangan rekomendasi dan roadmap untuk memenuhi tata kelola keamanan informasi Polri.

B. Permasalahan

Berdasarkan latar belakang sebagaimana tersebut diatas, dapat dirumuskan permasalahan yang akan dikaji adalah bagaimana peningkatan kehandalan teknologi informasi melalui rekayasa keamanan siber dalam rangka terwujudnya Polri Presisi di era Police 4.0. Untuk menjawab permasalahan tersebut, terdapat tiga hal pokok persoalan yaitu:

1. Bagaimana pemanfaatan *honeypot* dalam merancang dan mengembangkan sistem keamanan pada Big Data Polri?
2. Bagaimana merancang tata kelola keamanan informasi berbasis COBIT, SNI ISO 27001:2013 dan OCTAVE Allegro?
3. Bagaimana audit keamanan informasi pada big data polri dengan memanfaatkan indeks KAMI 4.1?

C. Maksud dan Tujuan

1. Maksud

   Maksud dari penulisan naskah akademik ini adalah untuk memberikan gambaran kepada pimpinan tentang konsep, argumentasi ilmiah, serta perancangan secara aplikatif dan manajemen, berkaitan dengan kondisi kehandalan teknologi informasi dalam keamanan informasi pada Polri yang ada saat ini. Disamping itu juga perlunya rekayasa keamanan siber pada Big Data Polri yang diharapkan dapat mengoptimalkan pelaksanaan pembinaan karir personel sehingga mewujudkan Polri Presisi di Era Police 4.0.

2. Tujuan

   Adapun tujuan penulisan naskah akademik ini adalah untuk memperoleh dukungan pimpinan dan *stakeholder* lainya dalam melaksanakan pemanfaatan Big Data Polri yang ada saat ini, menjadi Big Data yang aman melalui peningkatan kehandalan teknologi informasi melalui rekayasa keamanan siber sebagai suatu bentuk strategi dalam rangka pembinaan karir personel guna penguatan kualitas pelayanan publik pada Polri.

D. Batasan Masalah

Dalam penelitian ini, agar pembahasan terhadap permasalahan lebih fokus, permasalahan akan dibatasi dalam beberapa aspek yang diantaranya:

1. Studi penerapan naskah akademik ini dilakukan pada SSDM Polri, dengan pertimbangan kebutuhan keamanan informasi terhadap pengelolaan dan manajemen keamanan informasi pada aplikasi layanan sistem elektronik sehingga diharapkan hasil pengembangan keamanan informasi dapat yang digunakan pada Satuan Kerja Polri lain;
2. Perancangan dan pengembangan sistem keamanan pada Big Data Polri menggunakan *honeypot* dengan mengedepankan metode deteksi;
3. Perancangan tata kelola keamanan informasi berbasis COBIT, SNI ISO 27001:2013, dan OCTAVE Allegro pada Big Data Polri terkait proses bisnis pada SIPP yang dikelola oleh SSDM Polri dalam menghadapi ancaman dan risiko yang akan terjadi berdasarkan risiko; dan
4. Audit keamanan informasi pada Big Data Polri dengan memanfaatkan indeks KAMI 4.1. pada SSDM Polri dalam mengelola SIPP.

E. Metodologi

Bahwa untuk mencapai tujuan sebagaimana tersebut diatas, kajian ini dilakukan dengan menggunakan metodologi penelitian kualitatif yang bersifat deskriptif dengan menguraikan teori dan sumber data yang relevan terhadap peningkatan kehandalan teknologi informasi melalui rekayasa keamanan informasi menuju Polri yang presisi di era Police 4.0. Sumber data primer diperoleh dari peraturan perundang-undangan dan eksperimen kepada pihak terkait yang bertujuan untuk menggali pendapat dan pandangan terhadap kondisi kehandalan teknologi informasi saat ini serta kehandalan teknologi informasi melalui rekayasa keamanan siber pada Big Data Polri yang diharapkan. Sumber data sekunder diperoleh dari buku, jurnal, laporan dan dokumen lainnya yang terkait.

Penulisan hasil kajian diuraikan dalam lima bagian. *Pertama*, merupakan pengantar kajian tentang latar belakang, pokok permasalahan, tujuan dan metodologi terkait peningkatan kehandalan teknologi informasi melalui rekayasa keamanan informasi pada Big Data Polri. *Kedua*, merupakan kajian teoritis tentang keamanan siber yang berisikan ruang siber, kejahatan siber, serta deteksi ancaman siber. Pada kajian teoritis juga terdapat penjelasan mengenai tata kelola keamanan informasi yang terdiri dari manajemen keamanan informasi, SNI ISO 27001:2013 terkait Sistem Manajemen Keamanan Informasi, Octave Allegro, serta *Control Objective for Information and related Technology (COBIT).* Pada bagian *Kedua*, dijelaskan juga mengenai kajian empiris tentang *Honeypot* sebagai perangkat deteksi, tata kelola teknologi informasi berbasis COBIT, dan keamanan informasi berbasis SNI ISO 27001:2013, serta Indeks Kemanan Informasi (KAMI) 4.1. *Ketiga*, merupakan pembahasan tentang kondisi penerapan keamanan siber saat ini, dimulai dari kondisi umum, perangkat keamanan informasi, manajemen keamanan informasi, dan audit keamanan informasi. *Keempat*, merupakan kondisi penerapan keamanan siber yang diharapkan baik kondisi umum, pengembangan dan pengujian *Honeypot* sebagai metode deteksi, hingga pengembangan tata kelola keamanan informasi berbasis COBIT, SNI ISO 27001:2013 dan Octave Allegro, dan penggunaan indeks KAMI 4.1 sebagai tools audit keamanan informasi. *Kelima*, merupakan kesimpulan dalam menjawab permasalahan pokok kajian serta mengusulkan rekomendasi yang dapat disampaikan kepada Pimpinan Polri.

BAB II
KAJIAN TEORITIS DAN EMPIRIS

A. Kajian Teoritis

A.1 Keamanan Siber

A.1.1 Ruang Siber

Perkembangan globalisasi dan teknologi informasi telah membawa perubahan besar dalam kehidupan manusia. Teknologi Informasi menjadikan hubungan komunikasi antar manusia dan antar bangsa semakin mudah dan cepat tanpa dipengaruhi oleh ruang dan waktu. Globalisasi adalah suatu proses perubahan dinamika lingkungan global sebagai kelanjutan dari situasi yang pernah ada sebelumnya yang ditandai dengan ciri kemajuan teknologi dan informasi, menimbulkan saling ketergantungan, pengaburan terhadap batas-batas negara (*borderless*). Dampak dari perkembangan teknologi dan informasi mengubah haluan perang yang terjadi saat ini.

Era globalisasi mendorong sebagian negara tidak lagi menggunakan cara perang tradisionaldankonvensional. Akibatnya, kekuatan negara tidak lagi dilihat pada kekuatan persenjataan, tetapi juga pada segi budaya, perekonomian, politik, dan teknologi. Hal ini membuat persaingan dan peperangan menjadi semakin tidak terlihat batasannya. Peperangan dan konflik yang terjadi di suatu negara tidak hanya didominasi oleh kekuatan militer, tetapi kekuatan nirmiliter juga dilakukan oleh aktor nonnegara (*non state actor*) (Nasution, 2021).

Bentuk peperangan yang tidak lagi menggunakan cara perang tradisional menimbulkan ancaman baru di ruang siber. Ancaman yang berevolusi menjadi serangan siber bukan sekadar konsep saja. Rentannya pertukaran informasi di ruang siber (*cyberspace*) didorong sebuah negara untuk membangun sistem keamanan yang dapat mengatasi ancaman tersebut. Peristiwa Estonia pada tahun 2007 dan Georgia pada tahun 2008 merupakan contoh serangan kejahatan siber (*cybercrime*) dengan pemanfaatan *Distributed Denial of Service* (DdoS), sehingga melumpuhkan aktivitas negara karena banyak sektor kritis yang diserang. Serangan yang tercatat cukup mengkhawatirkan adalah serangan Stuxnet. Stuxnet adalah contoh malware yang sangat canggih dan berhasil melumpuhkan seperlima sistem kendali pengayaan nuklir dari pembangkit listrik tenaga nuklir milik Iran (B. Kelley, 2013).

Ruang siber (*cyberspace*) adalah ruang dimana komunitas saling terhubung menggunakan jaringan (misalnya intenet) untuk melakukan berbagai kegiatan sehari-hari. *Cyber* diartikan sebagai istilah lain, yaitu *cyberspace* yang diambil dari data *cybermetics*. Pada mulanya istilah *cyberspace* tidak ditujukan untuk menggambarkan interaksi yang terjadi melalui jaringan komputer. John Perry Barlow pada tahun 1990 mengaplikasikan istilah siber (*cyber)* yang dihubungkan pada jaringan internet. Dalam perkembangannya, *cyber* dapat membawa dampak positif dan negatif yang bisa menimbulkan suatu kejahatan dalam perkembangan dunia *cyber*. Kejahatan yang lahir sebagai suatu dampak negatif dari perkembangan aplikasi pada internet ini disebut dengan kejahatan siber (*cybercrime*) yang mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet.

Menurut pendapat Mcdonnell dan Sayers, ancaman siber terdiri atas tiga jenis, yaitu:

1. Ancaman perangkat keras (*hardware threat*).
   Ancaman ini merupakan ancaman yang disebabkan oleh pemasangan perangkat tertentu yang berfungsi untuk melakukan kegiatan tertentu didalam suatu sistem, sehingga peralatan tersebut merupakan gangguan terhadap sistem jaringan dan perangkat keras lainnya.
2. Ancaman perangkat lunak (*software threat*).
   Ancaman ini merupakan ancaman yang disebabkan masuknya perangkat lunak tertentu yang berfungsi untuk melakukan kegiatan pencurian, perusakan, dan manipulasi informasi.
3. Ancaman data/informasi (data/ *information threat*).
   Ancaman ini merupakan ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu.

Ancaman di ruang siber (*cyberspace*) didominasi oleh aktor non-negara (*non-state actor*) seperti individu hacker, kelompok hacker, kegiatan para hacker, *non-government organization* (NGO), terorisme, kelompok kejahatan terorganisir (*organized criminal groups*) dan sektor swasta (seperti internet *companies and carries, security companies*) juga dapat mengancam pertahanan dan kedaulatan negara. Sasaran ancaman kejahatan siber (*cybercrime*) pernah terjadi pada kasus penyadapan komunikasi pribadi Presiden Indonesia dan beberapa pejabat tinggi negara yang dilakukan Australia berdasarkan dokumen yang dibocorkan oleh Edward Snowden mantan kontraktor *National Security Agency* (NSA) dari Amerika. Selain itu, salah

satu situs resmi unit kerja Kementerian Pertahanan Republik Indonesia (Kemhan RI) dibobol oleh hacker, yakni website milik Direktorat Jenderal Potensi Pertahanan (Ditjen Pothan) yang mengalami perubahan laman yang disebut defacing. Situs tersebut dibobol oleh CVT (Cyber Vampire Team) dengan menuliskan laman situs "Oops Myanmar Hacker was here". Kemudian menuliskan kalimat dalam bahasa Inggris, yaitu "*Hello Indonesia Government, you should be proud with uneducated Indo script kiddies. Coz they believe (defacing/ Ddosing) to other country website is the best solution for them. If you would sympathize the white programmers/ developers of your country and how they are feeling. You can catch such script kiddies. Coz CVT are ready to provide those kiddies information".*

Ancaman global, kemajuan teknologi dan informasi tidak hanya ditujukan untuk menyerang instansi pemerintah dan militer. Namun dapat pula mengancam seluruh aspek kehidupan manusia, seperti ekonomi, politik, budaya, dan keamanan suatu negara. Baru-baru ini, serangan siber juga terjadi pada website industri telekomunikasi milik pemerintah. Ancaman kejahatan siber (*cybercrime*) dapat terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu. Ancaman inidalam aspek kehidupan masyarakat menimbulkan berbagai ancaman fisik baik nyata ataupun tidak nyata dengan menggunakan kode-kode komputer (*software*) untuk melakukan pencurian informasi dan data yang dapat mengancam suatu negara.

Peningkatan terhadap ancaman kejahatan siber (*cybercrime*)yang dilakukan baik oleh negara ataupun aktor non-negara (*non state actor*) berdampak terhadap terjadinya cyber warfare atau gangguan cyber (*cyber violence*). Ketergantungan negara terhadap jaringan komunikasi membawa tantangan dan ancaman tersendiri. Oleh sebab itu, dibutuhkan analisis manajemen risiko dalam menghadapi serangan kejahatan siber (*cybercrime*) dengan tujuan menjaga pertahanan dan kedaulatan NKRI dalam mewujudkan tujuan nasional. Manajemen risiko dapat artikan sebagai serangkaian prosedur dan metodologi yang digunakan untuk mengidentifikasi, mengukur, memantau dan mengendalikan risiko yang timbul dari kegiatan organisasi. Manajemen risiko yang dibuat dalam bidang informasi dan komunikasi yang berhubungan dengan kehidupan banyak warga negara ataupun yang bersifat rahasia, merupakan hal yang dilakukan untuk mengurangi tingkat kerawanan penyalahgunaan informasi dan data di ruang siber (*cyberspace*) (Lestari, 2013).

Risiko yang terjadi dalam menghadapi ancaman kejahatan siber (*cybercrime*) berasal dari dalam maupun luar negara dengan memanfaatkan kondisi sosial, politik, budaya, ideologi, dan perkembangan teknologi. Banyak cara yang dilakukan oleh berbagai macam pihak untuk mendapatkan informasi yang ada dalam Sistem Informasi Pertahanan Negara (Sisfohanneg). Beberapa aksi penyerangan bahkan telah dilakukan, misalnya aksi peretasan dengan melakukan defacing terhadap situs Dirjen Pothan Kemhan. Bocornya informasi terkait pertahanan negara yang terdapat didalam Sisfohanneg dapat mengancam kedaulatan negara, khususnya kedaulatan informasi. Konsep manajemen risiko dalam pertahanan merupakan unsur penting untuk menganalisis seberapa besar ancaman berdampak kepada pertahanan negara (Lestari, 2013).

Dalam konteks menghadapi ancaman serangan kejahatan siber (*cybercrime*), tidak dapat diselesaikan dengan hanya menggunakan kekuatan senjata. Namun membutuhkan integrasi seluruh kekuatan nasional dibawah komando dan kendali (Kodal) Kementerian Pertahanan (Kemhan).10 Risiko yang dihadapi dalam mengatasi ancaman kejahatan siber (*cybercrime*) tidak kalah dengan perang konvensional. Penggunaan teknologi cyber berdampak luas karena bisa mencakup berbagai aspek kehidupan bermasyarakat dan bernegara, diantaranya bidang ideologi, politik, ekonomi, sosial budaya, dan keamanan. Kejahatan siber (*cybercrime*) semakin meningkat yang dimanfaatkan pihak-pihak tertentu baik secara individu atau kelompok maupun negara dengan tujuan tertentu untuk dapat melemahkan lawannya. Kondisi ini perlu diwaspadai karena tidak menutup kemungkinan suatu negara dapat dilumpuhkan dan dihancurkan dengan perang teknologi atau melalui *cyber*.

Sebagai bangsa yang berdaulat dan beradab tentu perlu upaya untuk mempertahanan keutuhan suatu negara dengan membangun pertahanan negara yang kuat demi tercapainya tujuan kepentingan nasional. Berbagai kondisi diatas menggambarkan betapa pentingnya identifikasi manajemen risiko dalam menghadapi ancaman kejahatan siber (*cybercrime*) dalam pengeloaan pembangunan pertahanan negara (Rahmawati, 2017).

A.1.2 Kejahatan Siber

Teknologi merupakan kegiatan yang dilahirkan oleh manusia dengan merencanakan dan menciptakan benda-benda material yang bernilai praktis, seperti mobil, pesawat, televisi adalah hasil dari pengembangan teknologi. Dilihat dari fungsi dan pentingnya teknologi, semua kalangan masyarakat dan instansi pemerintah sangat tergantung terhadap teknologi baik yang

digunakan untuk hal positif maupun negatif. Kata *cyber* dan teknologi diuraikan dari asal kata technique, dari kata Yunani Technikos yang berarti kesenian atau keterampilan dalam dan logos adalah limo atau asas-asas utama pada cyber (*software*) (Rahmawati, 2017). Meningkatnya pemanfaatan pada ruang siber (*cyberspace*) di seluruh lini kehidupan masyarakat pada era globalisasi saat ini secara parallel, akan menghubungkan pada pemanfaatan suatu jaringan teknologi internet pada obyek atau sektor tertentu sesuai dengan tujuan dari pengawakannya.

Dalam kajian Strategis Keamanan Siber Nasional, mendefinisikan ancaman kejahatan siber (*cybercrime*) sebagai setiap kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan atau gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan sehingga mengancam kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) sistem dan informasi (Iwan, 2012). Ancaman siber dapat terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu dalam aspek kehidupan masyarakat dapat menimbulkan berbagai ancaman fisik, baik nyata ataupun yang tidak nyata dengan menggunakan kode-kode komputer (*software*) untuk melakukan pencurian informasi (*information theft*), kerusakan sistem (*system destruction*), manipulasi informasi (*information corruption*) atau perangkat keras (*hardware*) untuk melakukan gangguan terhadap sistem (*network instruction*) ataupun penyebaran data dan informasi tertentu untuk melakukan kegiatan propaganda (Iwan, 2012).

Sumber-sumber ancaman siber dapat berasal dari berbagai sumber, seperti intelijen asing (*foreign intelligence service*), kekecewaan (*disaffected employees*), investigasi jurnalis (*investigatives journalist*), organisasi ekstremis (*extremist organization*), aktivitas para hacker (*hacktivist*), dan kelompok kejahatan terorganisir (*organized crime groups*).

Risiko kejahatan siber (*cybercrime*) berpotensi terhadap kehilangan sistem informasi data, kegiatan militer dan gangguan lainnya yang menggunakan jaringan komputer dan internet. Dalam melihat sumber-sumber ancaman di atas, pemerintah melalui Kementerian Pertahanan (Kemhan) perlu mempersiapkan diri dalam menghadapi ancaman siber ini. Kemhan perlu mempersipakan Sumber Daya Manusia yang handal dalam menguasai teknologi, sistem infrastruktur yang handal, dan didukung oleh perundang-undangan atau kebijakan dalam melaksanakan operasi cyber warfare (International Telecommunication Union (ITU), 2017).

A.1.3 Deteksi Ancaman Siber

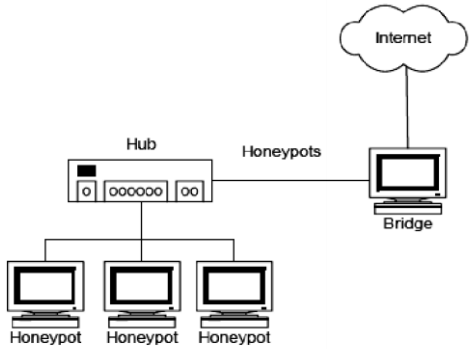
Banyak aspek yang bisa mengancam keamanan sistem jaringan komputer, yaitu ancaman yang bersifat *interruption* dimana informasi dan data dalam system dirusak dan dihapus sehingga jika dibutuhkkan data atau informasi tersebut telah rusak atau hilang. Kemudian ancaman yang bersifat *interception* yaitu informasi yang ada disadap oleh orang yang tidak berhak mengakses informasi yang terdapat pada sistem ini. Selanjutnya *modifikasi* yaitu ncaman terhadap integritas dari sistem informasi tersebut. Dan yang terakhir adalah *fabrication* yaitu orang yang tidak berhak berhasil memalsukan suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari yang dikehendaki oleh penerima informasi tersebut. Dengan sistem ini diharapkan dapat mengetahui akan sistem keamanan jaringan komputer, khususnya mendeteksi segala sesuatu yang akan mengancam web server (Sumarno, 2015).

Spitzner, Lance (2003*) Honeypot* merupakan salah satu jenis teknologi terbaru di bidang keamanan sistem dan jaringan komputer yang digunakan sebagai pelengkap teknologi keamanan sebelumnya. Teknologi keamanan sebelumnya seperti firewall dan IDS *(Intrusion Detection System)* merupakan teknologi konvensional dimana sistem pertahanan di bangun untuk mencegah penyerang menembus masuk ke dalam area yang di lindungi. *Honeypot* berbeda dari teknologi pertahanan konvensional sebelumnya dimana sistem pertahanan akan bernilai apabila penyerang telah masuk ke dalam sistem. Sistem honeypot akan melakukan monitoring terhadap aktivitas penyerang dengan menggunakan berbagai macam teknologi sehingga penyerang merasa aktivitas yang dilakukannya telah berhasil dan mengira sedang melakukan interaksi dengan sistem yang sebenarnya (Spitzner, 2003).

Honeynet mengimplementasikan Data Control dan Data Capture secara sederhana namun efektif. *Honeynet* yang menjadi gateway adalah firewall layer 3 (tiga). Firewall digunakan untuk memisahkan sistem *Honeynet* menjadi tiga jaringan yaitu Internet, *Honeypots* dan *Administrative.* Setiap paket yang menuju ataupun meninggalkan sistem Honeynet harus melewati firewall. Firewall tersebut yang juga berfungsi sebagai Data Control akan diset untuk mengatur koneksi inbound dan outbound. Dikarenakan firewall tersebut merupakan bagian dari sistem Honeynet, maka konfigurasi firewall tersebut sedikit berbeda dengan konfigurasi firewall pada umumnya yaitu mengizinkan setiap koneksi inbound untuk masuk dan mengontrol / membatasi setiap koneksi outbound yang keluar dari sistem (Spitzner, 2003).

Data Capture yang diterapkan pada Honeynet terdiri dari beberapa layer / bagian. Layer pertama adalah log yang terdapat pada firewall itu sendiri. Firewall log akan mencatat setiap koneksi yang menuju atau meninggalkan Honeynet. Layer kedua adalah sistem IDS. Fungsi IDS adalah untuk menangkap setiap aktivitas yang terjadi pada jaringan dan juga karena pada umumnya IDS mempunyai signature database maka IDS dapat memberikan informasi yang lengkap dari suatu koneksi yang terjadi. Layer ketiga adalah pada honeypot honeypot itu sendiri. Ini dilakukan dengan cara mengaktifkan system log pada honeypot honeypot yang digunakan. System log kemudian diset agar tidak hanya melakukan pencatatan secara lokal, tetapi juga secara remote ke sebuah remote log server.

Remote log server ini harus didisain lebih aman daripada *honeypot honeypot* yang ada agar data data yang didapat tidak hilang. Untuk membuat suatu solusi yang lebih mudah untuk diterapkan tetapi lebih susah untuk dideteksi oleh penyerang. Pada GenII *Honeynet* semua kebutuhan Honeynet (Data Control dan Capture) diterapkan hanya pada satu sistem saja (gateway) dan yang menjadi gateway adalah bridge layer 2 (dua). Keuntungan menggunakan gateway berupa bridge layer 2 (dua) adalah layer 2 bridge tidak mempunyai IP stack sehingga ketika paket melewatinya tidak terjadi routing ataupun pengurangan TTL yang mengakibatkan gateway akan semakin sulit untuk dideteksi.



Gambar 1 Implementasi honeypots 2 layer (Spitzner, 2003)

Honeypot merupakan sebuah sistem atau komputer yang sengaja dikorbankan untuk menjadi target serangan dari attacker. Komputer tersebut melayani setiap serangan yang dilakukan oleh attacker dalam melakukan penetrasi terhadap server tersebut. Metode ini ditujukan agar administrator dari server yang akan diserang dapat mengetahui trik penetrasi yang dilakukan oleh attacker serta agar dapat melakukan antisipasi dalam melindungi server yang sesungguhnya. Setiap tindakan yang dilakukan oleh penyusup yang mencoba melakukan

koneksi ke honeypot tersebut, maka honeypot akan mendeteksi dan mencatatnya (Spitzner, 2003).

Peran dari honeypot bukanlah menyelesaikan suatu masalah yang akan dihadapi server, akan tetapi memiliki kontribusi dalam hal keseluruhan keamanan. Dan besarnya kontribusi tersebut tergantung dari bagaimana Polri menggunakannya. Intinya, walaupun tidak secara langsung melakukan pencegahan terhadap serangan (firewall) tetapi dapat mengurangi dari intensitas serangan yang akan dilakukan oleh penyusup ke server yang sesungguhnya (Spitzner, 2003).

A.2 Tata Kelola Keamanan Informasi

A.2.1 Manajemen Keamanan Informasi

Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalisasi resiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis. Keamanan bisa dicapai dengan beberapa cara atau strategi yang bisa dilakukan secara simultan atau dilakukan kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. Contoh dari keamanan informasi antara lain (Whitman dan Mattord, 2012):

1. *Physical Security* adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi dan bencana alam;
2. *Personal Security* adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup *physical security*;
3. *Operational Security* adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan;
4. *Communication Security* adalah keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi; dan
5. *Network Security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan

untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. Kebanyakan orang mungkin akan bertanya, mengapa "keamanan informasi" dan bukan "keamanan teknologi informasi". Kedua istilah ini sebenarnya sangat terkait, namun mengacu pada dua hal yang sama sekali berbeda. Keamanan teknologi informasi mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan.

Berbeda dengan "keamanan informasi" yang fokusnya justru pada data dan informasi milik perusahaan. Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan. Berdasarkan penjelasan tersebut, "kemananan teknologi informasi" merupakan bagian dari keseluruhan aspek "keamanan informasi". Karena teknologi informasi merupakan salah satu alat penting yang digunakan untuk mengamankan akses serta penggunaan dari data dan informasi perusahaan. Dari pemahaman ini pula, Polri akan mengetahui bahwa teknologi informasi bukanlah satu-satunya aspek yang memungkinkan terwujudnya konsep keamanan informasi di perusahaan.

Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut (Whitman dan Mattord, 2013):

1. *Confidentiality* (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan;
2. *Integrity* (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini; dan
3. *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan, praktek, prosedur, struktur organisasi dan piranti lunak. Selain dari aspek kerahasiaan, integritas dan ketersediaan terdapat beberapa aspek lain dari keamanan informasi, yaitu:

1. *Privacy*.

   Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari orang lain.

2. *Identification*.

   Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi umumnya dilakukan dengan penggunaan *user name* dan *user ID*.

3. *Authentication*.

   Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang di klaim.

4. *Authorization*.

   Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia dan komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari informasi.

5. *Accountability*.

   Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu.

A.2.2 SNI ISO 27001:2013 tentang Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) atau disebut juga dengan *Information Security Management System* (ISMS), merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (*plan*), mengimplementasikan dan mengoperasikan (*do*), memonitor dan meninjau ulang (*check*) serta memelihara dan meningkatkan atau mengembangkan (*act*) terhadap keamanan informasi perusahaan (Disterer, 2013). Pada pelaksanaannya, ISO (*International Organization for Standardization*) dan IEC (*International Electrotechnical Commission*) mengeluarkan standar keamanan informasi dalam satu rumpun Sistem Manajemen Keamanan Informasi (SMKI) yang biasa dikenal

sebagai rumpun standar ISO/IEC 27000 yang salah satu diantaranya adalah ISO/IEC 27001 tentang Sistem Manajemen Keamanan Informasi (SMKI).

ISO/IEC 27001 merupakan suatu standar Internasional yang menerapkan sistem manajemen kemanan informasi atau lebih dikenal dengan *Information Security Management Systems* (ISMS). Dengan menerapkan standar ISO/IEC 27001 akan membantu organisasi atau perusahaan dalam membangun dan memelihara Sistem Manajemen Keamanan Informasi (SMKI). Karena, ISMS merupakan seperangkat unsur yang saling terkait dengan organisasi atau perusahaan yang digunakan untuk mengelola dan mengendalikan risiko keamanan informasi dan untuk melindungi serta menjaga kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) informasi.

Pada ISO/IEC 27001 terdapat 7 klausul mulai dari nomor 4 sampai dengan 10.yang berisi tentang ketentuan yang harus dipatuhi oleh organisasi ataupun perusahaan dalam penerapan SMKI. Kemudian pada bagian A (*Annex A*) berisi kumpulan sasaran pengendalian (*control objective*) dan pengendalian keamanan informasi (*information security control*) yang terdiri dari 14 area, 35 sasaran pengendalian dan 114 kontrol, sebagaimana ditunjukkan pada Tabel II.1 Area dan Sasaran Pengendalian ISO/IEC 27001:2013 (Disterer, 2013).

Tabel 1 Area dan Sasaran Pengendalian ISO/IEC 27001:2013

Area		Sasaran Pengendalian	
1.	Kebijakan keamanan informasi.	1.	Arahan manajemen untuk keamanan informasi.
2.	Organisasi keamanan informasi.	2.	Organisasi internal.
		3.	Perangkat bergerak (*mobile device*) dan *teleworking*.
3.	Keamanan sumber daya manusia.	4.	Sebelum dipekerjakan.
		5.	Selama bekerja.
		6.	Penghentian dan perubahan kepegawaian.
4.	Manajemen asset.	7.	Tanggung jawab terhadap asset.
		8.	Klasifikasi informasi.
		9.	Penanganan media.
5.	Kendali akses.	10.	Persyaratan bisnis untuk kendali akses.
		11.	Manajemen akses pengguna.
		12.	Tanggung jawab pengguna.

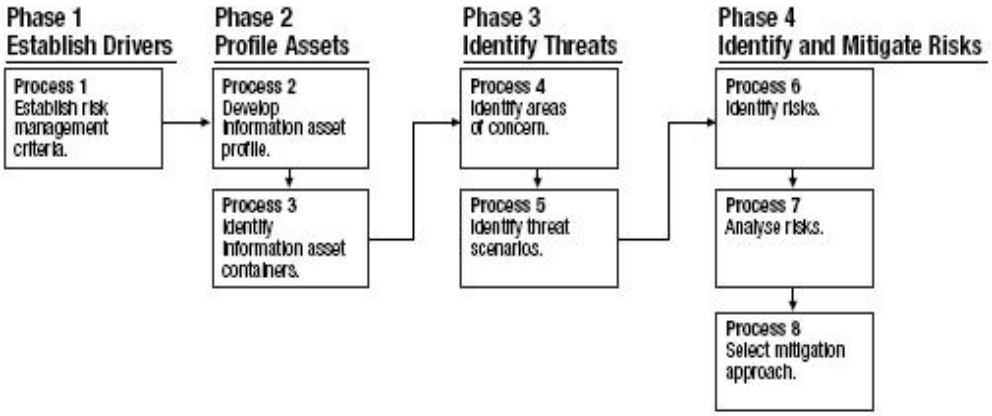
Area		Sasaran Pengendalian	
		13.	Kendali akses sistem dan aplikasi.
6.	Kriptografi.	14.	Kendali kriptografi.
7.	Keamanan fisik dan lingkungan.	15.	Daerah aman.
		16.	Peralatan
8.	Keamanan operasi	17.	Prosedur dan tanggung jawab operasional.
		18.	Perlindungan dari *malware*.
		19.	Cadangan (*Backup*).
		20.	Pencatatan (*logging*) dan pemantauan.
		21.	Kendali perangkat lunak operasional.
		22.	Manajemen kerentanan teknis.
		23.	Pertimbangan audit sistem informasi.
9.	Keamanan komunikasi.	24.	Manajemen keamanan jaringan.
		25.	Perpindahan informasi.
10.	Akuisisi, pengembangan dan perawatan system.	26.	Persyaratan keamanan sistem informasi.
		27.	Keamanan dalam proses pengembangan dan dukungan.
		28.	Data uji.
11.	Hubungan pemasok	29.	Keamanan informasi dalam hubungan pemasok.
		30.	Manajemen penyampaian layanan pemasok.
12.	Manajemen insiden keamanan informasi	31.	Manajemen insiden keamanan informasi dan perbaikan.
13.	Aspek keamanan informasi dari manajemen keberlangsungan bisnis.	32.	Keberlangsungan keamanan informasi.
		33.	Redundansi.
14.	Kesesuaian.	34.	Kesesuaian dengan persyaratan hukum dan kontraktual.
		35.	Reviu keamanan informasi.

A.2.3 OCTAVE Allegro

Software Engineering Institute (SEI) di Carnegie Mellon University mengembangkan Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE). Tujuan utama dalam mengembangkan OCTAVE adalah untuk membantu organisasi meningkatkan

kemampuan mereka untuk mengelola dan melindungi diri dari risiko keamanan informasi (Elky, 2007). Metode OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S, dan OCTAVE Allegro (Caralli dkk., 2007), sebagai berikut:

1. OCTAVE: Metode OCTAVE dirancang untuk organisasi dengan ukuran besar yang memiliki hirarki berlapis-lapis dan mempunyain infrastruktur komputasi yang mereka miliki sendiri. Aspek organisasi, teknologi, dan analisis dievaluasi oleh risiko keamanan informasinya dengan tiga cara tahap pendekatan dengan delapan proses.
2. OCTAVE-S: Lebih disesuaikan untuk organisasi yang berukuran lebih kecil dengan struktur hirarkirs datar dan tidak berlapis. Metode ini mirip dan didasari tiga tahap yang dijelaskan dalam metode OCTAVE, namun pada OCTAVE-S disederhanakan pada bagian proses yaitu hanya menjadi empat proses.
3. OCTAVE Allegro: seperti metode sebelumnya, OCTAVE Allegro lebih fokus pada penilaian risiko dalam konteks organisasi. Metode ini juga memberikan pendekatan didalam meningkatkan kemampuan organisasi disaat melakukan pengukuran risiko secara lebih efisien dan efektif. Salah satu filosofi yang mendorong adanya Allegro adalah ketika informasi menjadi inti dari penilaian keamanan risiko, semua aset terkait lainnya dianggap sebagai '*information containers*' yang menyimpan, memproses atau mengirim aset informasi. Sehingga ancaman terhadap aset informasi dapat dianalisis dengan cara mempertimbangkan '*information containers*' tersebut dan secara efektif membatasi jumlah dan jenis aset yang dibawa ke dalam proses.



Gambar 2 Langkah-langkah OCTAVE Allegro (OCTAVE Approach, 2003)

Pendekatan ini sedikit berbeda dari pendekatan OCTAVE, dimana OCTAVE Allegro fokus terhadap aset informasi, bagaimana informasi digunakan, yaitu informasi disimpan, dipindahkan, dan diolah, dan bagaimana informasi terkena ancaman, kerentanan, dan gangguan sebagai hasil yang ditimbulkan.

Terdapat empat tahap yang digunakan pada OCTAVE Allegro (Caralli dkk, 2007), yaitu:

1. Membangun *drivers*, dimana perusahaan membangun kriteria pengukuran risiko yang konsisten dengan *drivers/*hal-hal yang mendorong organisasi.
2. Membuat profil aset informasi, dimana aset informasi yang akan menjadi fokus dari pengukuran risiko diidentifikasi dan diperjelaskan, dan *asset container* yang diidentifikasikan.
3. Mengidentifikasi ancaman-ancaman, yaitu ancaman terhadap aset informasi diidentifikasikan dan didokumentasikan melalui proses yang terstruktur.
4. Mengidentifikasi dan mengecilkan risiko, dimana risiko yang telah diidentifikasikan kemudian dianalisis yang didasari dari informasi ancaman, dan rencana mitigasi yang dibangun untuk menanggapi risiko tersebut.

Dari tahapan tersebut, terdapat delapan langkah OCTAVE Allegro yang digunakan, yaitu:

1. Membangun kriteria pengukuran risiko:

   Pada langkah pertama ini, organizational driver yang akan digunakan untuk mengevaluasi akibat dari sebuah risiko terhadap misi dan tujuan bisnis perusahaan diidentifikasi. Kriteria pengukuran risiko digunakan untuk mengevaluasi akibat dalam masing-masing area dan memprioritaskannya.
2. Membangun profil aset informasi:

   Langkah kedua adalah mengembangkan profil aset informasi atas aset-aset perusahaan. Profil tersebut adalah representasi dari aset informasi yang menggambarkan fitur, kualitas, karakteristik, dan nilai yang unik.
3. Mengidentifikasi *container* dari aset informasi:

   Container adalah tempat dimana aset informasi tersebut disimpan, dikirim, dan diproses. Pada langkah ketiga, semua container yang menyimpan, mengirim, dan memproses, baik internal maupun eksternal dianalisis.
4. Mengidentifikasikan area yang diperhatikan:

   Langkah keempat merupakan proses identifikasi risiko melalui cara *brainstorming* mengenai kondisi atau situasi yang memungkinkan yang dapat mengancam aset informasi perusahaan. Tujuan dari proses ini adalah secara cepat mengetahui situasi atau kondisi yang terlintas secara tiba-tiba dalam benak tim analisis.
5. Mengidentifikasi skenario ancaman:

Dalam langkah kelima ini, area-area ancaman yang telah diidentifikasi pada langkah sebelumnya didetailkan menjadi sebuah skenario ancaman yang lebih jauh mendetailkan properti dari sebuah ancaman. Langkah ini berguna untuk memberikan pertimbangan atas kemungkinan dalam skenario ancaman.

6. Mengidentifikasi risiko:

   Pada langkah keenam, adalah konsekuensi yang didapat organisasi jika sebuah ancaman terjadi dicatat, dalam mendapatkan perkiraan risiko secara lengkap.

7. Menganalisa risiko:

   Pada langkah ketujuh adalah melakukan pengukuran kuantitatif sederhana dari sejauh mana organisasi terkena dampak dari ancaman yang telah dihitung. Nilai risiko relatif tersebut diperoleh dengan cara mempertimbangkan sejauh mana konsekuensi atas dampak risiko terhadap berbagai *impact area*, dan memperkirakan kemungkinan-kemungkinan yang dapat terjadi.

8. Memilih pendekatan pengurangan risiko:

   Dalam langkah terakhir dari proses OCTAVE Allegro ini, organisasi menentukan risiko yang memerlukan mitigasi dan mengembangkan pendekatan untuk mengurangi risiko tersebut. Hal ini dilakukan dengan cara memprioritaskan risiko-risiko berdasarkan nilai risiko relatif.

A.2.4 Control Objective for Information and related Technology (COBIT)

COBIT (*Control Objective for Information and related Technology*) merupakan suatu panduan standar praktik manajemen teknologi informasi. Standar COBIT dikeluarkan oleh IT *Governance Institute* yang merupakan bagian dari ISACA. COBIT adalah satu-satunya kerangka kerja untuk tata kelola dan pengelolaan perusahaan teknologi informasi yang menggabungkan pemikiran terbaru dalam teknik tata kelola dan manajemen, menyediakan prinsip, praktik, alat analisis, serta model yang dapat diterima secara global untuk membantu meningkatkan kepercayaan dan menilai dari suatu sistem informasi (ISACA, 2017).

COBIT merupakan suatu kerangka menyeluruh yang dapat membantu perusahaan dalam mencapai tujuannya pada area tata kelola dan manajemen teknologi informasi perusahaan. Secara sederhana, COBIT membantu perusahaan menciptakan nilai optimal dari TI dengan cara menjaga keseimbangan antara mendapatkan keuntungan dan mengoptimalkan tingkat resiko, serta penggunaan sumber daya (ISACA, 2017).

COBIT 2019 merupakan versi terbaru dari pendahulunya yaitu COBIT 5. Beberapa varian dari COBIT 2019 diantaranya *Framework: Introduction and Methodology* yang pengantar konsep kunci COBIT 2019. *Framework Governance and Management Objectives* yang menggambarkan secara komprehensif 40 (empat puluh) inti tata kelola dan tujuan manajemen, proses yang terkandung di dalamnya, dan komponen terkait lainnya. Panduan ini juga merujuk standar dan kerangka kerja lain. *Design Guide Designing an Information and Technology Governance Solution* panduan ini mengeksplorasi faktor-faktor desain yang dapat memengaruhi tata kelola dan mencakup alur kerja untuk merencanakan sistem tata kelola yang disesuaikan untuk perusahaan. 2019 *Implementation Guide Implementing and Optimizing an Information and Technology Governance Solution* yang merupakan evolusi dari panduan implementasi COBIT 5 dengan mengembangkan peningkatan tata kelola yang berkelanjutan (ISACA, 2017).

Tata kelola dan manajemen dalam COBIT 2019 dikelompokkan menjadi 5 (lima) domain sebagaimana ditunjukkan pada Gambar II.4. Domain tersebut memiliki nama dengan kata kerja yang mengungkapkan tujuan utama dan bidang aktivitas dari tujuan yang terkandung di dalam domain tersebut yang diantaranya sebagai berikut:

1. Tujuan tata kelola dikelompokkan dalam domain *Evaluate, Direct and Monitor* (EDM). Dalam domain ini, pengelola organisasi mengevaluasi opsi-opsi strategis, mengarahkan manajemen senior pada opsi-opsi strategis yang dipilih dan memantau pencapaian strategi. Pada domain ini terdiri dari 5 (lima) objektif yang diantaranya :
    a. EDM 01 *Ensure governance framework setting and maintenance*;
    b. EDM 02 *Ensure benefits delivery*;
    c. EDM 03 *Ensure risk optimization*;
    d. EDM 04 *Ensure resource optimization*; dan
    e. EDM 05 *Ensure stakeholder engagement*.
2. Tujuan manajemen dikelompokkan ke dalam 4 (empat) domain yang diantaranya:
    a. *Align, Plan and Organize* (APO) membahas keseluruhan organisasi, strategi, dan kegiatan pendukung untuk teknologi informasi. Pada domain ini, memiliki 14 (empat belas) *objective* yang diantaranya:
        1) APO 01 *Manage I&T management framework*;
        2) APO 02 *Manage strategy*;
        3) APO 03 *Manage enterprise architecture*;
        4) APO 04 *Manage innovation*;

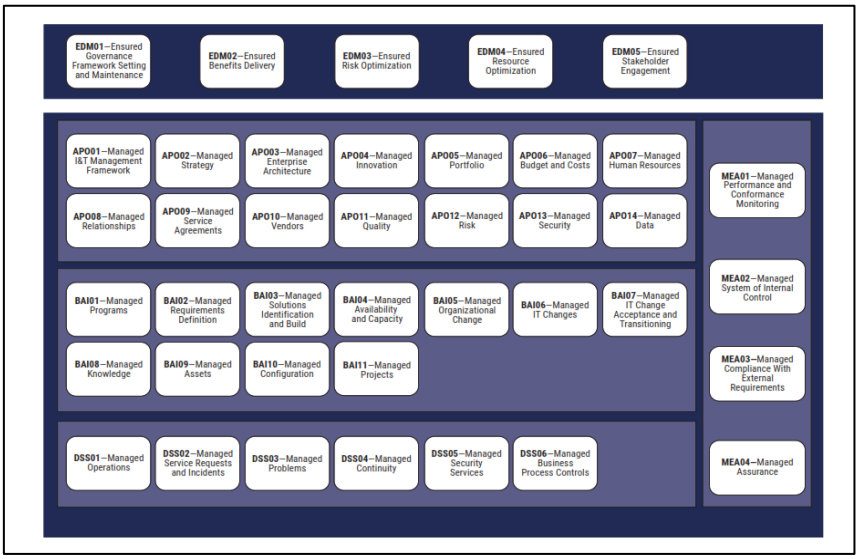
5) APO 05 *Manage portfolio*;
6) APO 06 *Manage budget and cost*;
7) APO 07 *Manage human resources*;
8) APO 08 *Manage relationships*;
9) APO 09 *Manage service agreement*;
10) APO 10 *Manage vendors*;
11) APO 11 *Manage quality*;
12) APO 12 *Manage risk*;
13) APO 13 *Manage security*; dan
14) APO 14 *Manage data*.

b. *Build, Acquire and Implement (BAI*) membahas definisi, akuisisi, dan implementasi solusi teknologi informasi dan integrasinya dalam proses bisnis. Pada domain ini, memiliki 11 (sebelas) *objectives* yang diantaranya:
1) BAI 01 *Manage programs*;
2) BAI 02 *Manage requirements definition*;
3) BAI 03 *Manage solutions identification and build*;
4) BAI 04 *Manage availability and capacity*;
5) BAI 05 *Manage organizational change*;
6) BAI 06 *Manage IT changes*;
7) BAI 07 *Manage IT change acceptance and transitioning*;
8) BAI 08 *Manage knowledge*;
9) BAI 09 *Manage assets*;
10) BAI 10 *Manage configuration*; dan
11) BAI 11 *Manage projects*.

c. *Deliver, Service and Support* (DSS) membahas pengiriman operasional dan dukungan layanan teknologi informasi termasuk keamanan. Pada domain ini, memiliki 6 (enam) *objective* yang diantaranya:
1) DSS 01 *Manage operations*;
2) DSS 02 *Manage service requests and incidents*;
3) DSS 03 *Manage problems*;
4) DSS 04 *Manage continuity*;
5) DSS 05 *Manage security services*; dan
6) DSS 06 *Manage business process controls*.

d. *Monitor, Evaluate and Assess* (MEA) membahas pemantauan kinerja dan kesesuaian teknologi informasi dengan target kinerja internal, tujuan kontrol internal, dan persyaratan eksternal. Pada domain ini, memiliki 4 (empat) *objective* yang diantaranya:

1) MEA 01 *Manage performance and conformance monitoring*;
2) MEA 02 *Manage system of internal control*;
3) MEA 03 *Manage compliance with external requirements*; dan
4) MEA 04 *Manage assurance*.

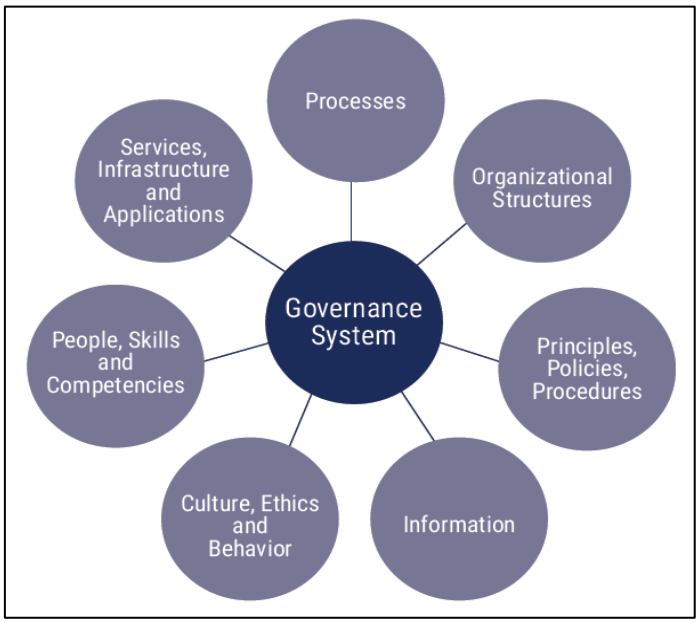


Gambar 3 COBIT 2019 core model (ISACA, 2018)

Pada COBIT 2019 untuk memenuhi tata kelola dan tujuan manajemen, setiap perusahaan perlu membangun, menyesuaikan dan mempertahankan sistem tata kelola yang dibangun dari sejumlah komponen. Komponen tersebut adalah faktor yang, secara individual dan kolektif, berkontribusi pada operasi yang baik dari sistem tata kelola perusahaan berdasarkan teknologi informasi. Komponen berinteraksi satu sama lain yang menghasilkan sistem tata kelola yang holistik untuk teknologi informasi. Komponen tersebut dari berbagai jenis dan yang palig sering ditemui adalah komponen proses. Pada COBIT 2019 terdapat 7 (tujuh) komponen sistem tata kelola sebagaimana yang ditunjukkan pada Gambar II.5 komponen system tata kelola COBIT 2019 yang diantaranya:

1. *Processes*, yang menggambarkan serangkaian praktik dan kegiatan yang terorganisir untuk mencapai tujuan tertentu dan menghasilkan serangkaian *output* yang mendukung pencapaian tujuan terkait teknologi informasi secara keseluruhan.
2. *Organizational structure*, merupakan entitas pengambilan keputusan utama dalam suatu perusahaan.

3. *Principles, policies, and framework*, menerjemahkan perilaku yang diharapkan kedalam panduan praktis untuk sebagai manajemen sehari-hari.
4. *Information*, tersebar di seluruh organisasi dan mencakup semua informasi yang diproduksi dan digunakan oleh perusahaan. COBIT 2019 berfokus pada informasi yang diperlukan untuk berfungsinya sistem tata kelola perusahaan secara efektif.
5. *Culter, etnic, and behavior*, merupakan bagian terpenting yang harus tertanam pada setiap individu dan perusahaan untuk menjalankan aktivitas manajemen dan tata kelola.
6. *People, skills, and competencies*, diperlukan untuk keputusan yang baik, pelaksanaan tindakan korektif, dan penyelesaian semua kegiatan agar berhasil.
7. *Services, infrastructure and applications*, termasuk infrastruktur, teknologi, dan aplikasi yang menyediakan perusahaan dengan sistem tata kelola untuk pemrosesan teknologi informasi.



Gambar 4 Komponen sistem tata kelola COBIT 2019 (ISACA, 2018)

Selain itu komponen juga terbagi dalam 2 (dua) yaitu komponen generik yang terdapat dalam COBIT 2019 *core model* dan *variants* yang didasarkan pada komponen generik tetapi dirancang untuk tujuan atau konteks tertentu dalam *focus area*. Pada pengembangan ini akan menggunakan komponen generik dan *variants* yang berfokus pada area keamanan informasi.

Model penilaian tingkat proses kapabilitas proses pada COBIT 2019 telah mendukung skema proses kababilitas yang berbasis CMMI. Model ini mengukur performansinya tiap-tiap proses tata kelola (*governance*) pada domain EDM atau proses manajemen (*management*) pada domain *Plan, Build, Run, Monitor* (PBRM), dan dapat menindentifikasi area-area yang perlu

ditingkatkan performansinya. Tingkat kapabilitas merupakan ukuran seberapa baik suatu proses diimplementasikan dan dijalankan. Pengukuran proses kapabilitas pada COBIT 2019 di mulai dari level 0 (nol) s.d level 5 (lima) sebagaimana ditunjukkan pada Gambar II.6 level kapabillitas pada proses COBIT 2019 dengan karakteristik yang berbeda dalam setiap tingkatannya yaitu:

1. Level 0.

   Pada level ini memiliki karakteristik penilaian berupa kurangnya pelaksanaan atau implementasi kemampuan dasar, penanganan yang tidak lengkap untuk menangani tata kelola dan tujuan manajemen, dan tidak memenuhi proses pada praktik apapun.

2. Level 1.

   Pada level ini memiliki karakteristik penilaian berupa, proses yang terjadi kurang lebih dapat mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap dan dapat dikategorikan sebagai awal atau intuitif tidak terlalu terorganisir.

3. Level 2.

   Pada level ini memiliki karakteristik penilaian berupa, proses telah mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap yang dapat dikategorikan telah dilakukan.

4. Level 3.

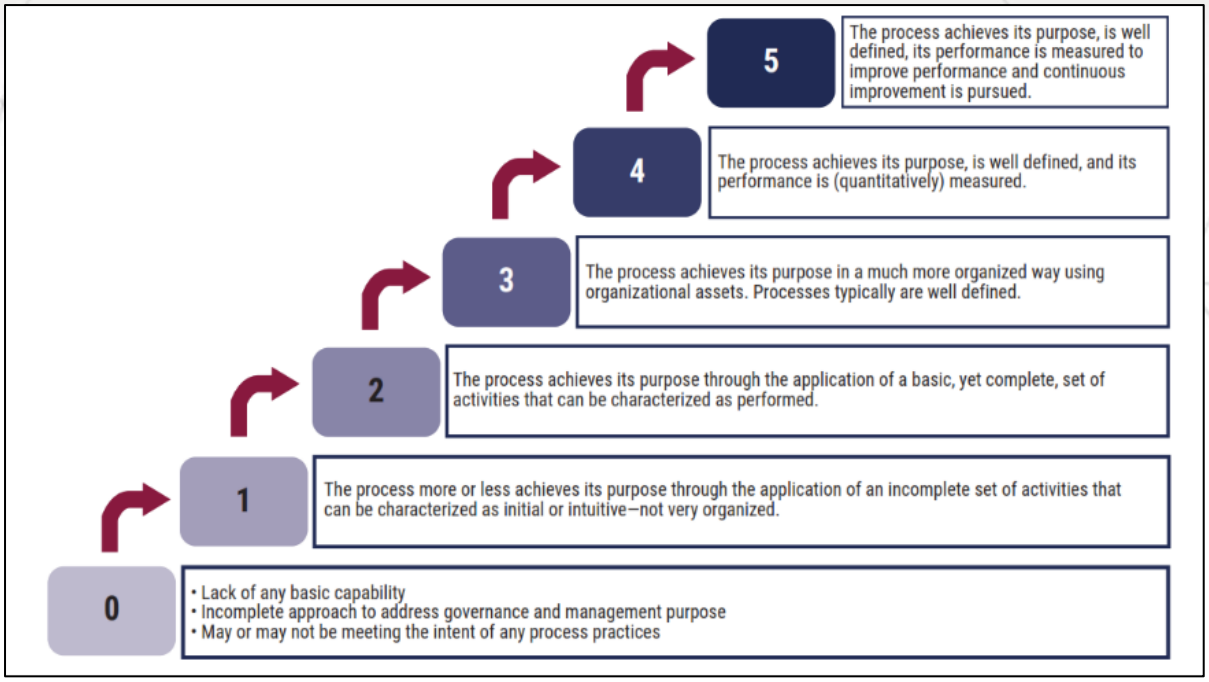
   Pada level ini memiliki karakteristik penilaian berupa, proses telah mencapai tujuannya dengan cara yang jauh lebih terorganisir menggunakan aset organisasi. Proses biasanya dapat didefinisikan dengan baik.

5. Level 4.

   Pada level ini memiliki karakteristik penilaian berupa, proses mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya diukur (secara kuantitatif).

6. Level 5.

   Pada level ini memiliki karakteristik penilaian berupa, proses mencapai tujuannya, didefinisikan dengan baik, kinerjanya diukur untuk meningkatkan kinerja dan perbaikan terus menerus dilakukan.



Gambar 5 Level kapabillitas pada proses COBIT 2019 (ISACA, 2018)

Dengan *rating level* yang merupakan pendefinisian seberapa jauh proses tersebut telah dilakukan, dinyatakan dalam persentase. Dengan skala yang digunakan untuk menilai proses yaitu N (*not achived*), P (*partially achived*), L (*largely achived*), dan F (*fully achieved*) sebagaimana ditunjukkan pada Tabel II.1.

Suatu proses dapat dinilai dengan *rating* N (*not achived*) jika penilian yang dilakukan terhadap tingkat kemampuan memiliki nilai pencapaian kurang dari 15 %. Nilai *rating* P (*partially achieved*) dapat ditentukan jika penilian yang dilakukan terhadap tingkat kemampuan memiliki nilai pencapaian diantara 15 % s.d 50 %. Nilai *rating* L (*lagerly achieved*) dapat ditentukan jika penilian yang dilakukan terhadap tingkat kemampuan memiliki nilai pencapaian diantara 50 % s.d 85 %, dan nilai *rating* F (*fully achieved*) dapat ditentukan jika penilaian yang dilakukan terhadap tingkat kemampuan memiliki nilai pencapaian lebih dari 85 persen. Untuk nilai rating F harus dapat dibuktikan dengan pemeriksaan atau penilaian komponen *enabler*, seperti kegiatan proses, tujuan proses atau struktur organisasi praktik yang baik.

Tabel 2 Rating level *COBIT 2019 (ISACA, 2018)*

N	*Not Achived*	0-15% *achievement*
P	*Partially Achived*	>15%-50% *achievement*
L	*Lagerly Achived*	>50%-85% *achievement*
F	*Fully Achived*	>85-100% *achievement*

Selain itu, terkadang pada tingkat yang lebih tinggi diperlukan suatu penilaian untuk mengekspresikan kinerja tanpa perincian berdasarkan proses kemampuan individu. COBIT 2019 mendefinisikan tingkat kematangan sebagai ukuran kinerja pada tingkat area fokus dengan menyediakan penilaian berdasarkan proses kemampuan individu seperti pada Gambar II.7 Tingkat Kematangan Untuk *Focus Area* dengan penilaian sebagai berikut (ISACA, 2018):

1. Level 0 *Incomplete*.

   Pada level ini, suatu pekerjaan dapat dikatakan *incomplete* atau tidak lengkap jika suatu pekerjaan tersebut mungkin diselesaikan atau mungkin tidak untuk mencapai tujuan tata kelola dan tujuan manajemen di *focus area*.
2. Level 1 *Initial*.

   Pada level ini, suatu pekerjaan dapat dikatakan *initial* atau rintisan jika suatu pekerjaan tersebut selesai, tetapi tujuan dan maksud penuh dari *focus area* belum tercapai.
3. Level 2 *Managed*.

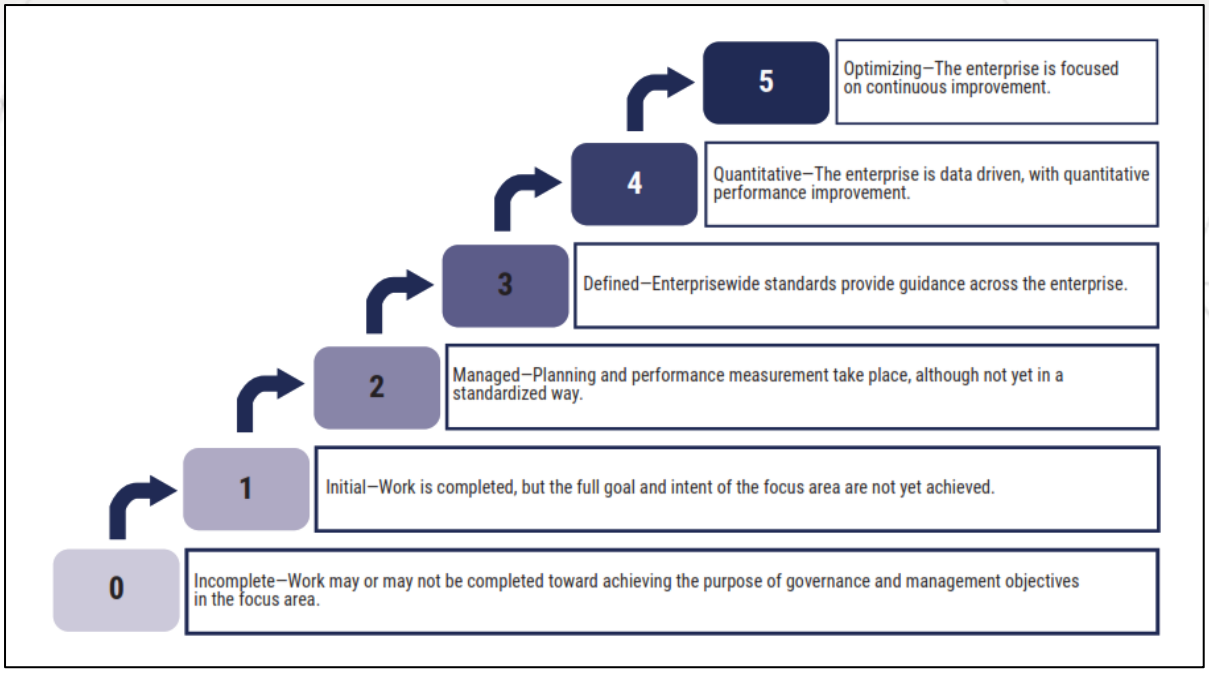
   Pada level ini, suatu pekerjaan dapat dikatakan *managed* atau dikelola jika suatu perencanaan dan pengukuran kinerja telah dilakukan, meskipun belum dengan metode atau cara yang sesuai dengan standar.
4. Level 3 *Defined.*

   Pada level ini, suatu pekerjaan dapat dikatakan *defined* atau terdefinisikan jika perusahaan telah memberikan panduan di seluruh perusahaan mengenai standar perusahaan didalam mencapai *focus area*.
5. Level 4 *Quantitative.*

   Pada level ini, suatu pekerjaan dapat dikatakan *quantitative* atau kuantitatif jika perusahaan didukung oleh data yang kuantitaif untuk meningkatkan kinerja.
6. Level 5 *Optimizing.*

   Pada level ini, suatu pekerjaan dapat dikatakan *optimizing* atau mengoptimalkan jika perusahaan telah berfokus pada peningkatan berkelanjutan sesuai dengan *focus area*.

COBIT 2019 juga mendefinisikan jika tingkat kematangan dikaitkan dengan area fokus yaitu kumpulan tujuan tata kelola dan manajemen serta komponen yang mendasarinya dan tingkat kematangan tertentu akan dicapai jika semua proses yang terdapat dalam area fokus mencapai tingkat kemampuan tertentu.



Gambar 6 Tingkat Kematangan Untuk Focus Area (ISACA, 2018)

B. Kajian Empiris

B.1 *Honeypot* Sebagai Perangkat Deteksi

Terkait dengan *honeypot* dan perkembangannya, telah banyak peneliti yang melakukan pengembangan untuk mengembangkan metode deteksi serangan siber menggunakan honeypot. Pertama, penelitian yang dilakukan oleh Baykara, 2018 dengan judul *A Novel Honeypot Based Security Approach for Real-time Intrusion Detection and Prevention Systems*. Pada pengembangan ini untuk memastikan keamanan sistem informasi, berbagai sistem digunakan teknik dan teknologi, termasuk enkripsi, otorisasi, *firewall*, sistem berbasis *honeypot*. Dalam studi ini, pendekatan berbasis honeypot untuk deteksi intrusi / sistem pencegahan (ID / PS) diusulkan. Aplikasi server *honeypot* yang dikembangkan digabungkan dengan IDS untuk menganalisis data secara real-time dan beroperasi secara efektif. Selain itu, dengan mengaitkan keunggulan *honeypot* interaksi rendah dan tinggi, sistem *honeypot* hibrida unggul dilakukan. Oleh karena itu, untuk mengurangi biaya konfigurasi, pemeliharaan, dan manajemen, setelah melihat penggunaan honeypots di jaringan perusahaan, teknologi virtualisasi digunakan. Sistem yang dikembangkan adalah jenis sistem deteksi intrusi dan pencegahan (IDPS) berbasis honorer dan mampu menampilkan lalu lintas jaringan pada server secara visual secara animasi *real-time*. Dengan demikian, ini memberikan informasi sistem dengan mudah. Terakhir, sistem yang dikembangkan dapat mendeteksi serangan *zero-day* karena konfigurasi deteksi intrusi,

yang membuatnya lebih unggul dalam performa dibandingkan IDS lainnya. Sistem ini juga membantu mengurangi tingkat positif palsu di IDS.

Kedua, penelitian yang dilakukan oleh Sumarno, 2017 dengan judul Solusi *Network Security Dari Ancaman* SQL *Injection* dan *Denial of Service* (DOS). Pada penelitian ini, dibangun suatu sistem *honeypots* yang menyerupai production system yang sesungguhnya. Layanan yang diemulasikan pada *honeypots* adalah *web server*. Mekanisme pengawasan/*monitoring* pada sistem *honeypot* ini dilakukan dengan menggunakan *log*. Digunakannya *log* ini adalah untuk memudahkan pemeriksaan kembali data (analisis forensik) yang diterima oleh sistem *honeypots*. Implementasi dalam penelitian ini, sistem honeypot dirancang berdasar kepada *high interaction honeypot*, yaitu sistem *honeypot* yang yang mengemulasikan *service* dengan alamat IP tersendiri. Rancangan *honeypot* dalam penelitian ini dipergunakan untuk memberikan *service security* terhadap layanan http (*web server*).

Ketiga, penelitian yang dilakukan moore, 2016 dengan judul *Detecting Ransomware with Honeypot Techniques*. Penelitian ini menyelidiki metode untuk mengimplementasikan *honeypot* untuk mendeteksi aktivitas *ransomware*, dan memilih dua opsi, layanan Penyaringan File dari fitur Manajer Sumber Daya *Server File Microsoft* dan *EventSentry* untuk memanipulasi *log* Keamanan Windows. Penelitian mengembangkan respons bertahap terhadap serangan ke sistem bersama dengan ambang batas ketika ada yang dipicu. Penelitian memastikan bahwa *file tripwire* saksi menawarkan nilai terbatas karena tidak ada cara untuk mempengaruhi malware untuk mengakses area yang berisi file yang dipantau.

B.2 Tata Kelola Teknologi Informasi Berbasis COBIT

Penggunaan kerangka kerja berbasis COBIT dalam mengelola teknologi informasi telah banyak diterapkan. Karena secara konsep, COBIT mampu diselarasakan dengan tujuan bisnis dari organisasi dan mampu diselaraskan dengan berbagai macam kerangka kerja yang telah di adopsi oleh organisasi. Untuk mengetahui penelitian terkini tentang penggunaan COBIT sebagai kerangka kerja tata kelola teknologi informasi, terdapat beberapa penelitian terkait. Pertama, Kasma, 2019 *Design of e-Government Security Governance System Using COBIT 2019*. Penelitian ini bertujuan untuk memberikan masukan tentang kinerja sistem manajemen dan tata kelola e-Government Security dengan harapan desain pengendalian e-Government Security dapat terpenuhi. Hasil dari penelitian ini adalah e-Government Security Governance System yang diambil dari 28 model inti COBIT 2019. 28 model inti diambil menggunakan CSF dan risiko. Selanjutnya, pengelolaan kinerja untuk sistem tata kelola ini terdiri dari tingkat

kapabilitas dan kematangan yang merupakan perpanjangan dari proses evaluasi dalam Pedoman Evaluasi e-Government yang diterbitkan oleh Kementerian PAN & RB. Evaluasi desain dilakukan dengan menentukan kondisi kapabilitas dan tingkat kematangan saat ini di Badan XYZ. Hasil evaluasi menunjukkan bahwa desain memungkinkan untuk diimplementasikan dan dibutuhkan.

Kedua, Nachrowi, 2020 *Evaluationof Governance and Management of Information Technology Services Using Cobit 2019 and ITIL4*. Penelitian ini, mengevaluasi tata kelola dan pengelolaan pelayanan pada Direktorat Kelembagaan Ditjen Dikti menggunakan COBIT 2019, dengan mengukur tingkat kapabilitas proses berdasarkan design factor yang merekomendasikan prioritas perbaikan pada 11 domain COBIT 2019 dan tingkat kepuasan pengguna aplikasi layanan menggunakan model E-govqual. Hasil penilaian level kapabilitas TI memiliki 3 level 0 proses atau tidak ada pendekatan yang ada, 6 level 1 proses atau pendekatan tidak lengkap, 1 level 2 proses atau pendekatan awal memenuhi maksud area praktik dan 1 Proses level 3 atau pencapaian tujuan jauh lebih terorganisir. Pengukuran tingkat Kepuasan Pelayanan mendapatkan 3 kriteria pada Kuadran A atau peningkatan prioritas, 13 kriteria pada kuadran B atau dipertahankan, 12 kriteria pada kuadran C atau prioritas kurang dan 3 kriteria pada Kuadran D atau kurang diharapkan. Rekomendasi perbaikan disusun berdasarkan model SWOT, mengacu pada COBIT 2019 dan ITIL 4. Hasil rekomendasi tersebut antara lain peningkatan kompetensi SDM dan integrasi pelayanan dengan PDDIKTI.

Ketiga, Andrianti 2020 Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses DSS05 (Studi Pada RS Bhayangkara Jambi). Penelitian ini bertujuan untuk tata kelola keamanan teknologi informasi menggunakan COBIT 5. Metode analisis dalam penelitian ini menggunakan framework COBIT 5 dengan menggunakan sub domain DSS05 dan menggunakan metode hasil evaluasi tingkat kapabilitas (capability level) dari COBIT (level 0-5). Penelitian ini menghasilkan rekomendasi perbaikan pada keamanan teknologi informasi sesuai dengan tingkat kapabilitas yang dicapai. Kesimpulan yang diambil dari penelitian ini yaitu perbaikan level tingkat kapabilitas dan rekomendasi tata kelola keamanan informasi.

B.3 Keamanan Informasi Berbasis SNI ISO 27001:2013

Terkait dengan SNI ISO 27001:2013 dan perkembangannya, telah banyak peneliti yang melakukan penelitian untuk menggunakan keamanan informasi berbasis SNI ISO 27001:2013.

Pertama, penelitian yang dilakukan oleh Nugroho dengan judul Metode Silogisme And Untuk Validitas Jawaban Dari Responden Dalam Analisis Maturity Level Keamanan Informasi Berbasis SNI ISO 27001:2013 Pada Dinas Kependudukan Dan Pencatatan Sipil Kota XYZ pada tahun 2018. Pada penelitian ini, berbagai ancaman yang menyerang data dan informasi dari organisasi kian marak terjadi seperti serangan *malware*, *hacker* dan bencana alam. Jika ancaman-ancaman dari informasi tersebut tidak segera ditanggulangi, maka akan menimbulkan risiko hilangnya data, informasi berserta infrastrukturnya pada aspek *confidentiality*, *integrity* dan *availability*. Akibatnya proses bisnis organisasi akan terhenti baik untuk sementara waktu bahkan dapat menyebabkan kehancuran sebuah organisasi. Salah satu metode dalam mencegah dan meminimalisir ancaman keamanan informasi adalah metode *Maturity Level*. Metode tersebut berfungsi mengukur tingkat kematangan dari penerapan keamanan informasi pada organisasi. Metode *Maturity Level* adalah metode yang sangat tepat jika digunakan untuk mengukur seberapa matang organisasi dalam memanajemen keamanan informasi yang akhirnya dapat memberikan rekomendasi untuk meningkatkan keamanan informasi sesuai dengan kebutuhan organisasi akan tetapi tergantung dengan data yang didapatkan ketika melaksanakan proses identifikasi data. Banyak metode yang digunakan agar data yang diberikan responden terjamin kevalidannya seperti metode observasi. Kelemahan metode observasi adalah tidak semua responden akan mau menunjukkan informasi misalkan informasi yang terkandung dalam aset informasi dikarenakan beberapa sebab seperti regulasi batasan daerah aman dan lain sebagainya.

Kedua, penelitian yang dilakukan oleh Rahmat dengan judul Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar SNI ISO/IEC 27001:2013 pada tahun 2019. Penelitian ini bertujuan untuk mengetahui Perencanaan Sistem Manajemen Keamanan Informasi (SMKI) menggunakan Standar SNI ISO/IEC 27001:2013 di Universitas Muhammadiyah Sukabumi. Menggunakan metode penelitian deskriptif kualitatif, dan data dikumpulkan melalui metode survey dan wawancara. Hasil yang diperoleh yaitu perencanaan SMKI menggunakan standar SNI ISO/IEC 27001:2013 di Universitas Muhammadiyah Sukabumi, sebagai berikut: Merancang dokumen 1 yang meliputi kebijakan, penilaian risiko, ruang lingkup, dan *Statement Of Applicability* (SOA) untuk menanggulangi insiden pihak luar; dan merancang dokumen 2 yang berisi prosedur keamanan informasi dengan menggunakan model *Plan-Do-Check-Act* (PDCA).

Ketiga, penelitian yang dilakukan oleh Ritzkal dengan judul Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) Pada Fakultas Teknik UIKA-Bogor pada tahun 2016. Pada penelitian ini, telah dilakukan analisis terhadap sistem manajemen keamanan informasi pada lingkungan Fakultas Teknik Universitas Ibn Khaldun (UIKA) Bogor berdasarkan ISO/IEC 27001: 2013 Klausal 11 Kontrol Akses. Standardisasi ISO/IEC 27001:2013, adalah suatu standar berkenaan dengan Sistem Manajemen Keamanan Informasi (SMKI, *ISMS*: *Information Security Management System*) yang dipublikasikan pada 25 September 2013. Sistem Manajemen Keamanan Informasi (SMKI), adalah pendekatan sistematis untuk pengelolaan informasi sensitif institusi, agar tetap dalam kondisi aman. Di dalamnya termasuk orang, proses, dan sistem teknologi informasi melalui penerapan proses manajemen risiko. Analisis terhadap SMKI pada penelitian ini dimaksudkan untuk memperoleh tingkat keamanan pada jaringan *hotspot* Fakultas Teknik berdasarkan standar tersebut. Dilakukan pembuatan suatu kuesioner dengan pendekatan *Plan-Do-Check-Act* (*PDCA*). Pengisian kuesioner dikenakan terhadap 2 jenis responden, yaitu pengguna dan manajemen. Responden pengguna dibatasi pada 20 orang dengan sistem sampling dalam pengisian kuesioner, sedangkan manajemen menunjuk satu orang pengelola jaringan *hotspot*. Diperoleh hasil, yaitu (1) pengguna hanya mempercayai tingkat keamanan sebesar 49% dan (2) pihak manajemen hanya mempercayai tingkat keamanan sebesar 45%. Berdasarkan hal itu ditunjukkan, bahwa SMKI pada jaringan *hotspot* di Fakultas Teknik kurang aman menurut Standarisasi ISO/IEC 27001:2013.

B.4 Penilaian Resiko Berbasis Octave Allegro

Terkait dengan Octave Allegro dan perkembangannya, telah banyak peneliti yang melakukan penelitian untuk mengembangkan penilaian resiko berbasis Octave Allegro. Pertama, penelitian yang dilakukan oleh Wagiu dengan judul *Information System Security Risk Management Analysis in Universitas Advent Indonesia Using Octave Allegro Method* pada tahun 2019. Pada penelitian ini dilakukan analisis terhadap manajemen risiko sistem informasi di Universitas Advent Indonesia dengan OCTAVE ALLEGRO. OCTAVE ALLEGRO merupakan metode yang sering digunakan untuk melakukan analisis di bidang manajemen risiko dan penilaian risiko. Tujuan dari penelitian ini adalah untuk mengidentifikasi risiko yang berpotensi mengancam proses bisnis di Universitas Advent Indonesia dengan terlebih dahulu mengidentifikasi dampak kawasan, menentukan skala prioritas dll. Hasil penelitian menggunakan OCTAVE Allegro adalah pendekatan pengurangan risiko untuk masing-masing.

Bidang perhatian masing-masing aset informasi kritis UNAI yaitu informasi keuangan mahasiswa, informasi keuangan dosen, informasi nilai mahasiswa, informasi transkrip nilai mahasiswa, dan data absensi kelas. UNAI membuat aturan tertulis mengenai tanggung jawab dalam menjaga keamanan informasi dan sanksi bagi pelanggar serta melakukan sosialisasi aturan tersebut secara bertahap kepada karyawan Universitas Advent Indonesia. Evaluasi kembali keamanan informasi dengan menggunakan metode OCTAVE Allegro secara berkala, misalnya 2 tahun sekali.

Kedua, penelitian yang dilakukan oleh Suroso dengan judul *Assessment of Information System Risk Management with Octave Allegro at Education Institution* pada tahun 2018. Pada penelitian ini, Manajemen Risiko dapat mengurangi risiko seperti proses bisnis yang tidak optimal, kerugian finansial, reputasi perusahaan yang menurun, atau hancurnya bisnis perusahaan. Untuk mengurangi kerusakan sistem informasi proses bisnis perusahaan, maka perlu dilakukan penilaian manajemen risiko. Penggunaan sistem informasi diperlukan untuk menunjang proses bisnis perusahaan, khususnya di institusi pendidikan, serta MH. Universitas Thamrin. Dalam penggunaan sistem informasi, akan muncul risiko-risiko yang berdampak negatif pada institusi. Untuk mengurangi dampak negatif tersebut, perlu dilakukan penilaian risiko. Metode yang digunakan dalam tugas akhir ini adalah OCTAVE Allegro. Data dianalisis menggunakan 8 langkah di OCTAVE Allegro, dan menyebarkan kuesioner kepada pengguna sistem informasi. Hasilnya, ada 34 area yang menjadi perhatian dimitigasi, dan umpan balik pengguna secara keseluruhan menyatakan menyetujui langkah-langkah mitigasinya. Disimpulkan bahwa penilaian risiko bermanfaat untuk mengurangi risiko sistem informasi.

Ketiga, penelitian yang dilakukan oleh Prananda, 2021 dengan judul Perancangan Rekomendasi Kontrol Keamanan Informasi Berbasis Manajemen Risiko Keamanan Informasi Menggunakan Octave Allegro dan SNI ISO 27001:2013 (Studi Kasus: Organisasi Staf Sumber Daya Manusia Polri). Pada penelitian ini menerapkan manajemen resiko keamanan informasi dengan menggunakan kerangka kerja OCTAVE Allegro dalam penilaian dan analisa risiko, kemudian hasil tersebut dikelola dengan kontrol SNI ISO 27001:2013. Penelitian ini menghasilkan rancangan kontrol keamanan informasi untuk SIPP Polri berdasarkan kontrol yang dipersyarakatkan SNI ISO 27001:2013 pada klausul 4 hingga 10 dan kontrol berdasarkan hasil penilaian risiko menggunakan OCTAVE Allegro. Pada penelitian ini yang dipilih berdasarkan hasil penilaian risiko merupakan kontrol pada lampiran dari Annex A SNI ISO 27001:2013. Berdasarkan hasil penelitian, terdapat 12 skenario risiko dari 3 aset kritis SIPP

Online yang dikelola oleh SSDM Polri, diantaranya terdiri dari 3 kategori risiko rendah, 5 kategori risiko sedang, dan 4 kategori risiko tinggi. Dengan jumlah kontrol keamanan informasi berjumlah 46 rekomendasi kontrol. Berdasarkan validasi hasil penelitian, kontrol keamanan informasi dengan SMKI yang dilengkapi dengan MRKI yang sesuai dengan kebutuhan organisasi dapat menjadi rekomendasi komprehensif bagi institusi.

B.5 Indeks KAMI 4.1

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009. Hasil evaluasi indeks KAMI menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di instansi pemerintah.

Terkait dengan indeks KAMI 4.1 dan perkembangannya, telah banyak peneliti yang melakukan penelitian untuk mengembangkan metode evaluasi keamanan informasi menggunakan indeks KAMI 4.1. Pertama, penelitian yang dilakukan oleh Wijatmoko dengan judul Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Kementerian Hukum Dan HAM DIY tahun 2020. Pada penelitiian ini, penggunaan Indeks KAMI digunakan untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi dan diikuti dengan penerapan ISO 27001 sebagai standar keamanan internasional yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif. Hasil dari penggunaan Indeks KAMI versi 4.1 di Kantor Wilayah Kementerian Hukum dan HAM DIY ini adalah tingkat ketergantungan penggunaan sistem pemerintahan berbasis elektronik (*e-government*) sebesar 32 dari total skor 50 dan masuk kedalam kategori Tinggi dimana sistem pemerintahan berbasis elektronik (*e-government*) adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 314 dari 645 dan berada pada kategori pemenuhan kerangka kerja dasar. Rekomendasi dari penelitian ini dapat dijadikan sebagai bahan pertimbangan dan evaluasi bagi instansi dalam melakukan perbaikan yang

berkaitan dengan mitigasi atau pencegahan kerentanan keamanan informasi, serta memastikan regulasi dapat dicapai dengan baik dan kebijakan keamanan institusi di masa yang akan datang.

Kedua, penelitian yang dilakukan oleh Arman dengan judul Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI) tahun 2019. Pada penelitian ini, dilakukan evaluasi sistem manajemen keamanan informasi dengan instrument kuisioner berdasarkan Indeks Keamanan Informasi (KAMI) untuk mengetahui tingkat kelengkapan dan tingkat kematangan keamanan informasi di lima area, tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, dan teknologi. Dari hasil evaluasi dapat diketahui bahwa pada tingkat kelengkapan mendapatkan skor 334 dan rata rata tingkat kematangan keamanan informasi berada pada level II. Dari hal ini dapat dinyatakan bahwa Dinas Komunikasi dan Informatika Kabupaten Sidoarjo perlu perbaikan untuk melakukan sertifikasi ISO27001. Hasil tersebut menjadi dasar pembuatan rekomendasi yang didapatkan dari hasil perbandingan antara Indeks KAMI dengan kontrol ISO27001. Salah satu rekomendasi yang diberikan ialah prosedur manajemen risiko tindakan perbaikan ketidakpatuhan berdasarkan kontrol A.18.2.

Ketiga, penelitian yang dilakukan oleh Gunawan dengan judul Pengukuran Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Studi Kasus di PUSTIPD UIN Raden Fatah Palembang tahun 2018. Penelitian ini bertujuan untuk melakukan penilaian secara internal terhadap sistem manajemen keamanan informasi di PUSTIPD UIN Raden Fatah Palembang. Standar yang digunakan yaitu indeks keamanan informasi (KAMI) sebagai alat evaluasi untuk mengukur kesiapan pengamanan informasi di PUSTIPD UIN Raden Fatah Palembang. Hasil dari pengukuran tingkat ketergantungan terhadap penggunaan sistem elektronik yaitu sebesar 25 yang termasuk dalam kategori tinggi, kemudian hasil pengukuran dari kelima area yaitu sebesar 211 yang termasuk ke dalam kategori Tidak Layak. Selanjutnya dalam penelitian ini diberikan rekomendasi perbaikan untuk masing-masing pertanyaan yang mendapat skor buruk (tidak dilakukan). Rekomendasi ini sebagai bahan pertimbangan dan perbaikan bagi pihak PUSTIPD UIN Raden Fatah Palembang sebelum nantinya melakukan pengukuran keamanan informasi kembali menggunakan Indeks KAMI.

BAB III
KONDISI PENERAPAN KEAMANAN INFORMASI SAAT INI

A. Kondisi Umum

Urgensi keamanan informasi ditujukan untuk mengantisipasi dan mengamankan informasi dari segala ancaman dan serangan yang terjadi baik secara online maupun offline. Untuk mengantisipasi hal tersebut, diperlukan kesiapan dan ketanggapan dalam mendeteksi, mencegah, merespon, mengontrol, dan mengevaluasi ancaman sehingga tidak berdampak luas dan menyebabkan kerugian dikarenakan proses inti dari suatu organisasi berhenti beroperasi dan hilangnya asset informasi. Hal ini dimaksudkan untuk mewujudkan layanan publik dan administrasi yang andal serta menjamin aspek kerahasiaan, integritas, serta ketersediaan informasi yang disimpan pada sistem-sistem elektronik tersebut.

Sampai dengan saat ini belum ada undang-undang yang secara khusus mengatur terkait dengan keamanan informasi namun secara implisit terdapat beberapa undang-undang dan atau peraturan yang mengatur hal tersebut diantaranya:

1. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU No. 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik;
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
3. Peraturan Pemerintah Republik Indonesia 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; dan
4. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.

Pada konteks keamanan informasi, setiap Penyelenggara Sistem Elektronik (SPE) harus menyelenggarakan sistem elektronik secara handal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana dimaksud dalam Pasal 15 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU No. 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik. Dalam hal ini, Kepolisian Negara Republik Indonesia (Polri) termasuk SPE yang menyediakan sistem elektronik dengan tujuan memberikan pelayanan kepada masyarakat dan proses kegiatan organisasi Polri.

Secara umum, Divisi Teknologi Informasi dan Komunikasi (Div TIK) Polri merupakan SPE pada setiap sistem elektronik. Div.TIK dibentuk berdasarkan Perkap nomor 6 tahun 2017. Dari sejumlah fungsi penting, Div.TIK memperoleh amanat untuk membina dan mengelola keamanan informasi yang melayani seluruh satuan kerja dan satuan kewilayahan. Secara detail, kedudukan, tugas, dan fungsi Div. TIK berdasarkan Perkap tersebut meliputi:

1. Div TIK Polri merupakan unsur pengawas dan pembantu pimpinan di bidang informatika yang meliputi teknologi informasi dan komunikasi elektronika yang berada di bawah Kapolri;
2. Div TIK Polri bertugas menyelenggarakan fungsi manajemen, pembinaan dan pengembangan sistem teknologi informasi dan komunikasi elektronika serta pengawasan TIK di lingkungan Polri;
3. Dalam melaksanakan tugas, Div TIK Polri menyelenggarakan fungsi:
    a) Pembinaan dan pengembangan Sistem Teknologi Informasi dan Komunikasi Elektronika (Sistekinfokomlek) di lingkungan Polri yang meliputi:
        1) perencanaan, pembangunan, pengembangan, dan pemeliharaan Sistekinfokomlek;
        2) penyusunan sistem dan metode berupa petunjuk teknis dan pelaksanaan dalam bentuk Peraturan Kepolisian untuk pengoperasian Sistekinfokomlek;
        3) pemantauan dan supervisi serta pemberian arahan dan bimbingan teknis untuk menjamin terlaksananya Sistekinfokomlek;
        4) pemberian pertimbangan dan saran untuk penempatan personel dalam rangka pembinaan karir pengemban fungsi Sistekinfokomlek;
        5) penyusunan standardisasi terhadap perangkat keras; dan
        6) perangkat lunak Sistekinfokomlek di lingkungan Polri untuk mewujudkan Sistekinfokomlek Polri yang terpadu dan tepat guna.
    b) Pembinaan dan pengembangan Sistekinfokomlek yang meliputi sistem pengumpulan dan analisis data, program aplikasi, website, sistem keamanan dan infrastruktur teknologi informasi
    c) Pembinaan dan pengembangan Sistekinfokomlek guna menunjang kelancaran dalam pelaksanaan tugas Polri; dan
    d) Pembinaan dan pengembangan sistem dan aplikasi teknologi yang berkaitan dengan informasi operasional dan informasi pembinaan yang bersifat nasional dan terpusat.

Kebijakan terkait dengan keamanan informasi pada Polri, secara implisit telah mulai dilakukan sesuai dengan Keputusan Kepala Kepolisian Negara Republik Indonesia Nomor:

Kep/88/I/2016, tentang Master Plan Teknologi Informasi Polri Tahun 2015-2019 dengan penilaian awal terhadap tingkat kematangan dari Arsitektur Tata Kelola dan SDM Teknologi Informasi pada nilai 0,59 dengan kondisi ideal pada nilai 3.0. Dengan pemenuhan terhadap analisis kesenjangan terhadap keamanan informasi yang harus dilakukan diantaranya:

1. Penerapan standar terkait dengan Sistem Manajemen Keamanan Informasi (SMKI);
2. Ketidaktersediaan kebijakan terkair dengan keamanan informasi;
3. Penerapan teknologi keamanan jaringan yang belum optimal;
4. Monitoring keamanan TIK dilakukan manual;
5. Manajemen user dan password;
6. SDM teknologi informasi.

Secara umum penyediaan layanan sistem elektronik dilakukan oleh Div TIK Polri. Namun pengelolaan terhadap layanan sistem elektronik sepenuhnya diserahkan kepada masing-masing Satuan Kerja (Satker) yang ada pada Polri. Hal ini yang memperkuat indikasi, jika analisis kesenjangan terhadap keamanan informasi yang harus di penuhi saat ini juga harus dipenuhi oleh setiap Satker yang mengelola layanan sistem elektronik didalamnya.

B. Perangkat Keamanan Informasi

Keamanan teknologi informasi telah menjadi suatu keharusan. Jika dipresentasekan, sebesar 30% keamanan informasi didukung oleh perangkat keamanan teknologi informasi dan 70% didukung oleh kegiatan manajemen (Rahayu,2020) yang digunakan untuk mengamankan asset informasi. Perangkat teknologi informasi ini bertujuan untuk mencegah dan mengurangi dampak dari ancaman yang terjadi sehingga ancaman dapat dicegah atau diminimalisir. Secara umum perangkat keamanan teknologi informasi ini terbagi menjadi 2 (dua) bagian besar, yaitu *hardware* (perangkat keras) dan *software* (perangkat lunak) bahkan dalam suatu kondisi tertentu ada yang menggunakan perpaduan dari keduanya (Aliy, 2020).

B.1 Perangkat lunak (software) keamanan teknologi Informasi

B.1.1 Honeypot

Honeypot merupakan perangkat lunak khusus yang didesain memiliki kelemahan di dalam sistemnya. Tujuan dari perangkat ini untuk mengetahui, mendeteksi, dan mencatat aktivitas atau upaya untuk melakukan akses langsung ke dalam sistem. Biasanya honeypot di pasang terpisah dari sistem utama sehingga ketika perangkat ini ditembus, maka sistem utama masih dalam keadaan aman. Selain fungsi tersebut, honeypot dapat digunakan juga untuk meneliti

celah keamanan yang rentan diserang oleh attacker. Dengan adanya honeypot, banyak organisasi bisa selangkah di depan dalam menangkal serangan hacker. Oleh karena itu, menggunakan honeypot merupakan langkah bijak dalam mengamankan jaringan atau perangkat teknologi informasi.

B.1.2 Anti Virus

Virus komputer merupakan program yang bisa menggandakan diri ketika sudah masuk ke dalam sistem komputer dengan tujuan tertentu. Ada banyak jenis varian virus yang dapat menyerang sistem, mulai dari yang menyebabkan kerusakan ringan sampai berat. Sedangkan anti virus merupakan program yang didesain khusus untuk mendeteksi, mengkarantina, dan menghapus virus komputer. Pada anti virus terdapat database berbagai varian virus dan program jahat lainnya sehingga anti virus dapat mendeteksi banyak virus yang ada.

B.1.3 Operating System (OS) Hardening

Merupakan tindakan untuk membuat sistem operasi menjadi lebih aman. Entimologi *hardening* sendiri adalah mengeraskan sehingga OS *hardening* dapat disebut juga meningkatkan kemampuan keamanan sistem operasi. Sistem operasi yang menjadi server sangat perlu *hardening* atau diamankan. Karena setiap sistem operasi, pasti memiliki celah keamanan yang harus diamankan. Celah keamanan tersebut yang membuat host komputer atau server menjadi mudah diretas oleh attacker. Semua layanan, *software*, *port* dan berbagai aplikasi juga dapat menjadi celah keamanan yang menyediakan jalan masuk bagi attacker untuk meretas sistem operasi atau *server* sehingga dengan menutup layanan yang tidak dibutuhkan akan mempersempit pergerakan attacker untuk memanfaatkan celah tersebut.

B.1.4 Enkripsi

Merupakan tindakan untuk mengamankan informasi dengan merubah informasi tersebut menjadi suatu informasi yang tidak dapat dibaca bahkan dimengerti secara langsung. Pada awalnya enkripsi dilakukan secara manual, yaitu menggunakan pengacakan huruf dan lainnya. Tetapi setelah berkembangnya penggunaan komputer ke dalam berbagai lini kehidupan, enkripsi mulai menggunakan perangkat komputer.

B.1.5 Anti *Keylogger*

Keylogger merupakan perangkat yang diciptakan untuk mencatat atau merekam apapun yang diketik pada keyboard. Keylogger sendiri merupakan singkatan dari *keystroke* dan *logger*.

Sedangkan anti *keylogger* merupakan perangkat yang didesain khusus untuk mendeteksi keberadaan *keylogger* dan memutus proses perekaman yang diketik di papan ketik atau media lainnya. Selain keyboard, *keylogger* dapat merekam dan mencatat beberapa perangkat. Misalnya, layar komputer, web cam, suara, dan file clipboard.

B.1.6 Anti Phishing

Phishing merupakan aktifitas untuk mendapatkan data sensitif dan informasi dari seseorang melalui email atau website secara illegal. Tehnik *phishing* ini dilakukan dengan menggunakan email atau website palsu yang dimodifikasi sehingga menyerupai dengan website aslinya. Anti phishing merupakan *software* yang dirancang khusus untuk mendeteksi konten *phishing* yang ada di email, *website* dan media lainnya. Selain dengan menggunakan *software*, cara manual yang dapat dilakukan untuk mendeteksi phishing adalah dengan mengenali dari tampilan dan tautan atau url dari umpan *phishing* dimana tautan atau url akan mengarah kepada pembuat media *phishing*.

B.1.7 Endpoint Protection

Endpoint protection merupakan bentuk perlindungan terhadap perangkat-perangkat yang terhubung dengan sistem. Perangkat *endpoint* misalnya komputer desktop, perangkat mobile, printern, faximile, dan lain lain. *Endpoint protection* atau *endpoint security* adalah bentuk pengamanann perangkat *endpoint*. Perlindungan perangkat *endpoint* dapat dipasang langsung pada perangkat melalui proses instalasi manual ataupun secara *cloud*.

B.1.8 Data Lost Protection (DLP)

Data Lost Protection (DLP) atau *data lost prevention* merupakan perangkat yang didesain untuk melindungi data dari pencurian, penyalahgunaan, dan pengaksesan oleh pihak yang tidak berhak. Data dan informasi asset yang berharga bagi sebuah organisasi yang perlu dilindungi. Mekanisme *Data Lost Protection* (DLP) adalah dengan mengawasi pengiriman data pada perangkat *endpoint*. Perangkat DLP ini memindai lalu lintas jaringan dan perangkat *endpoint* dengan mendeteksi anomali dalam pengiriman atau lalu lintas data. Perangkat DLP ini mampu mendeteksi, membuat laporan dan memblokir jika terjadi anomali pada lalu lintas atau perangkat *endpoint*.

B.1.9 Virtual Private Network (VPN)

Virtual Private Network adalah sebuah koneksi yang memungkinkan terhubung dengan jaringan local menggunakan jaringan internet. Koneksi jaringan ini memungkinkan penggunanya untuk berkomunikasi secara aman karena karena jalur komunikasinya adalah privat. Disebut dengan jaringan *end to end* atau *point to point*. Karena menggunakan salah satu protokol keamanan seperti PP2P, L2TP, dan Sock.

B.2 Perangkat Keras (hardware) keamanan teknologi Informasi

B.2.1 Firewall

Firewall adalah perangkat keamanan yang berfungsi untuk memonitor lalu lintas data yang masuk dan keluar jaringan apakah akan diteruskan atau di blokir. *Firewall* telah menjadi perangkat yang sangat penting dan selalu digunakan untuk mengamankan perangkat ketika berhubungan dengan jaringan komputer dan internet. Secara garis besar, *firewall* ada yang berbentuk *hardware* dan *software*. Kemudian terbagi lagi menjadi *network firewall* dan *host firewall*. *Network firewall* adalah *firewall* yang digunakan untuk memonitor jaringan komputer. *Host firewall* adalah *firewall* yang memonitor komputer secara mandiri.

B.2.2 Intrusion Detection System (IDS)

Intrusion Detection System adalah perangkat yang digunakan untuk mendeteksi adanya aktifitas yang menjadi ancaman untuk jaringan komputer. Perangkat ini menjadi perangkat andalan administrator jaringan untuk mendeteksi adanya ancaman pada jaringan. Setelah mendeteksi adanya ancaman pada jaringan, IDS akan mengirimkan pesan yang berisi peringatan kepada administrator jaringan. IDS sendiri terbagi menjadi 2 (dua) jenis yaitu *network base* IDS dan *host base* IDS. Dimana *network base* IDS adalah perangkat IDS yang mendeteksi ancaman dalam skala jaringan komputer. *Host base* IDS adalah perangkat yang mendeteksi ancaman khusus pada komputer personal.

B.2.3 Intrusion Prevention System (IPS)

Intrusion Prevention System adalah perangkat gabungan antara *firewall* dan IDS atau *Intrusion Detection System*. Selain mendeteksi adanya ancaman pada jaringan, IPS mampu memblokir ancaman tersebut. Fitur yang dimiliki lebih *powerfull* dari fitur IDS. Jika IDS hanya pada mendeteksi dan memberikan peringatan jika ada ancaman, maka IPS mampu memblokir ancaman tersebut. IPS terbagi menjadi 2 (dua) yaitu *Network base* IPS dan *Host base* IPS. *Network base* IPS adalah perangkah IPS yang mendeteksi, memonitor, memblokir ancaman

pada jaringan komputer. *Host base* IPS adalah perangkat yang mendeteksi, memonitor, dan memblokir ancaman pada tingkatan personal komputer.

B.2.4 Token *Authentication*

Merupakan perangkat yang memastikan bahwa *request* yang diajukan ke server merupakan permintaan yang berasal dari *user* yang sah. Untuk menjadi toker yang terpercaya maka sebuah token harus diverifikasi oleh *server*. Token ini akan menambah *layer* atau lapisan keamanan sehingga data yang diminta atau dikirimkan akan lebih aman. Dalam pelaksanaannya token autentikasi memerlukan perangkat *dongle* yang memberikan kode verifikasi. Kode autentifikasi dapat berasal dari perangkat berbentuk *dongle* atau dari aplikasi berbasis web dan juga dikirimkan via email atau sms.

B.2.5 *Proxy*

Merupakan perangkat yang menjadi penengah antara client dengan server. Fungsi utama dari proxy sendiri diantaranya:

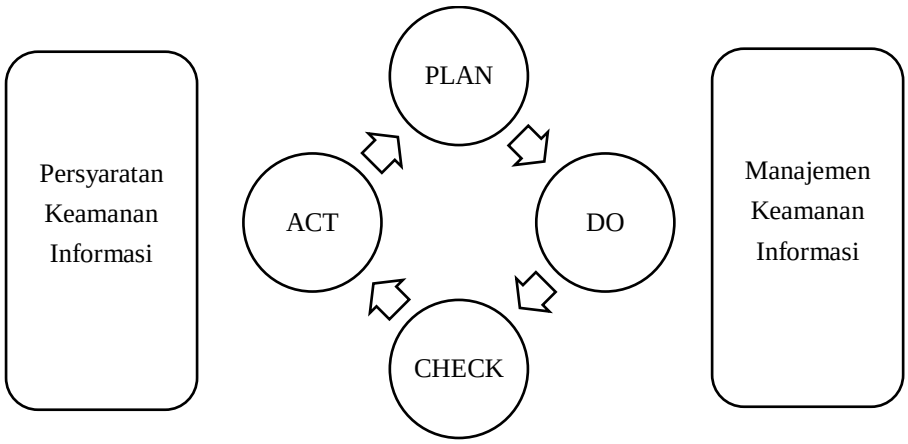
1. *Connection sharing* atau membagi koneksi internet;
2. *Filtering* yaitu menyaring koneksi yang terhubung dengan jaringan; dan
3. *Caching* yaitu sebagai memori cache yang berfungsi tempat penyimpanan sekunder ketika menggunakan internet.

Dalam praktiknya, proxy sering digunakan untuk mengamankan jaringan dari koneksi tertentu. Terutama untuk membatasi koneksi dari dalam ke luar jaringan. Misalnya untuk membatasi pengguna internet yang ada di dalam untuk mengakses domain atau konten tertentu. Selain itu beberapa *proxy* memiliki fitur untuk menyembunyikan IP Address pengguna, proxy ini disebut *anonymous proxy*. *Proxy* juga sering digunakan bersama *proxy* lain dengan alasan menjadi lebih aman. Akan tetapi kekurangannya jika melakukan hal itu adalah koneksi akan menjadi lebih lambat karena menggunakan berbagai lapisan proxy.

C. Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) merupakan sekumpulan kebijakan-kebijakan yang berhubungan dengan manajemen keamanan informasi. Konsep kunci dari SMKI adalah agar organisasi merancang, menerapkan, dan memelihara rangkaian yang berkaitan dari proses dan sistem untuk secara efektif mengelola aksesibilitas informasi, kemudian memastikan confidentiality, integrity and availability dari aset-aset informasi dan meminimalkan resiko-resiko keamanan informasi (ISO 27001, 2013).

SMKI disusun berdasarkan pendekatan resiko bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitor dan mengkaji ulang (*Check*) serta memelihara dan meningkatkan (*Act*) keamanan informasi. Adapun hubungan SMKI dan Teknologi Informasi dalam menerapkan keamanan informasi tidak dapat terpisahkan. Dalam artian, jika suatu organisasi ingin mempertimbangkan keamanan informasi, harus mengerti proses penerapan SMKI. SMKI ditujukan untuk menjaga aspek kerahasiaan (Confidentially), Keutuhan (Integrity), dan Ketersediaan (Avaibillity) dari informasi. (Sarno, 2009). Dalam membangun SMKI mengadopsi siklus PDCA (*Plan–Do–Check–Act*) yang dapat dilihat pada gambar 3.1 berikut:



Gambar 7 Sirklus PDCA (ISO 27001, 2013)

Keterangan:

1. *Plan* merupakan tahap perencanaan perancangan SMKI. Pada tahapan implementasinya adalah membangun komitmen, kebijakan, kontrol, prosedur, instruksi kerja dan lain sebagainya sehingga terciptalah SMKI sesuai dengan yang di inginkan.
2. *Do* merupakan tahapan pengimplementasian dan operasi dari kebijakan, kontrol, proses dan prosedur SMKI yang sudah direncanakan pada tahap sebelumnya.
3. *Check* merupakan tahapan mengenai kegiatan pelaksanaan SMKI termasuk peninjauan dan tahapan pra-audit.
4. *Act* merupakan tahapan perbaikan dan pengembangan SMKI dan langkahlangkah PDCA akan dilakukan sesuai dengan siklusnya, sehingga SMKI dapat tercapai dengan baik.

Untuk mengimplementasikan SMKI, pada Polri sampai dengan saat ini belum ada standar di adopsi sebagai best practice dalam mengelola SMKI. Namun pimpinan pada level top manager telah berkomitmen untuk mengimplementasikan SMKI pada penyediaan sistem elektronik pada Polri sesuai dengan tentang Master Plan Teknologi Informasi Polri Tahun 2015-2019.

D. Audit Keamanan Informasi

Audit dapat didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokementasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (Cannon, 2006).

Audit keamanan informasi adalah proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif. Beberapa elemen utama tinjauan penting dalam audit sistem dan teknologi informasi yaitu dapat diklasifikasikan sebagai berikut (Riyanarto, 2009):

1. Tinjauan terkait dengan fisik dan lingkungan, yakni: hal-hal yang terkait dengan keamanan fisik, suplai sumber daya, temperatur, kontrol kelembaban dan faktor lingkungan lain.
2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen database, seluruh prosedur administrasi sistem dan pelaksanaannya.
3. Tinjauan perangkat lunak. Perangkat lunak yang dimaksud merupakan aplikasi bisnis. Mencakup kontrol akses dan otorisasi ke dalam sistem, validasi dan penanganan kesalahan termasuk pengecualian dalam sistem serta aliran proses bisnis dalam perangkat lunak beserta kontrol secara manual dan prosedur penggunaannya. Sebagai tambahan, tinjauan juga perlu dilakukan terhadap siklus hidup pengembangan sistem.
4. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan sistem, batasan tingkat keamanan, tinjauan terhadap firewall, daftar kontrol akses router, port scanning serta pendeteksian akan gangguan maupun ancaman terhadap sistem.
5. Tinjauan kontinuitas bisnis dengan memastikan ketersediaan prosedur backup dan penyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana/kontinuitas bisnis yang dimiliki.
6. Tinjauan integritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

Secara umum kegiatan pengawasan dilingkungan polri dilakukan oleh Itwasum Polri. Itwasum Polri bertugas melaksanakan pengawasan untuk memberikan penjaminan kualutas dan memberikan konsultasi serta pendampingan kegiatan pengawasan lembaga pengawas eksternal dilingkungan Polri. Itwasum Polri bertugas membantu Kapolri dalam menyelenggarakan pengawasan internal, pemeriksaan umum, perbendaharaan, dan akuntabilitas serta pemeriksaan dengan tujuan tertentu, penelahaan ulang (review) laporan keuangan Polri serta memfasilitasi lembaga pengawasan eksternal dalam lingkungan Polri.

BAB IV
KONDISI PENERAPAN KEAMANAN INFORMASI YANG DIHARAPKAN

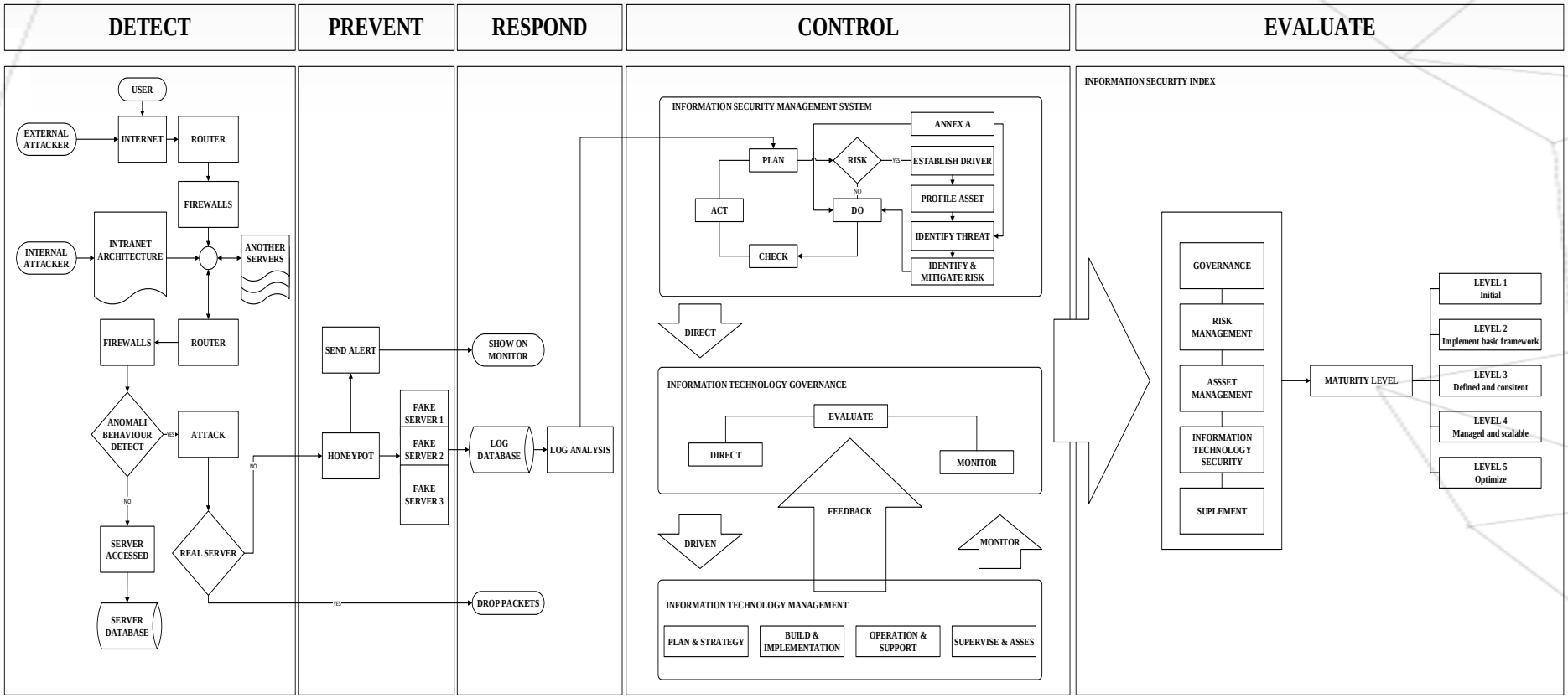
A. Kondisi Umum

Pengembangan dan implementasi keamanan informasi memerlukan kerangka kerja yang akan menjadi acuan agar implementasi dapat terjadi secara berkesinambungan dan dapat diukur kinerjanya setiap saat. Kebutuhan ini dipenuhi dengan pengembangan kerangka kerja yang meliputi teknologi, kebijakan, dan organisasi. Sehingga lebih proaktif dapat melakukan upaya deteksi, pencegahan, merespon, mengontrol, dan mengevaluasi dari dari suatu ancaman terhadap keamanan informasi.

Tata kelola pemerintahan berbasis SPBE (Sistem Pemerintahan Berbasis Elektronik) khususnya penyedia sistem elektronik harus menjamin sistem elektronik yang handal dan aman. Untuk memastikan hal tersebut, diperlukan suatu kebijakan sebagai landasan hukum terkait dengan sistem manajemen keamanan informasi. Kebijakan dan regulasi keamanan informasi tersebut juga diperlukan untuk mendukung arah dari kegiatan-kegiatan sesuai dengan tugas pokok dan fungsi Polri agar senantiasa sesuai dengan dinamika perkembangan teknologi informasi. Pada tingkatan operasional kebijakan regulasi berbentuk pedoman, petunjuk pelaksanaan, petunjuk teknis yang menjadi acuan utama bagi keamanan informasi. Tata cara perumusan penetapan dan penerapan kebijakan keamanan informasi mengikuti tata cara berdasarkan peraturan perundangan dan dilakukan dengan mempertimbangkan kebutuhan nasional, perkembangan situasi dan kondisi keamanan informasi serta perkembangan teknologi.

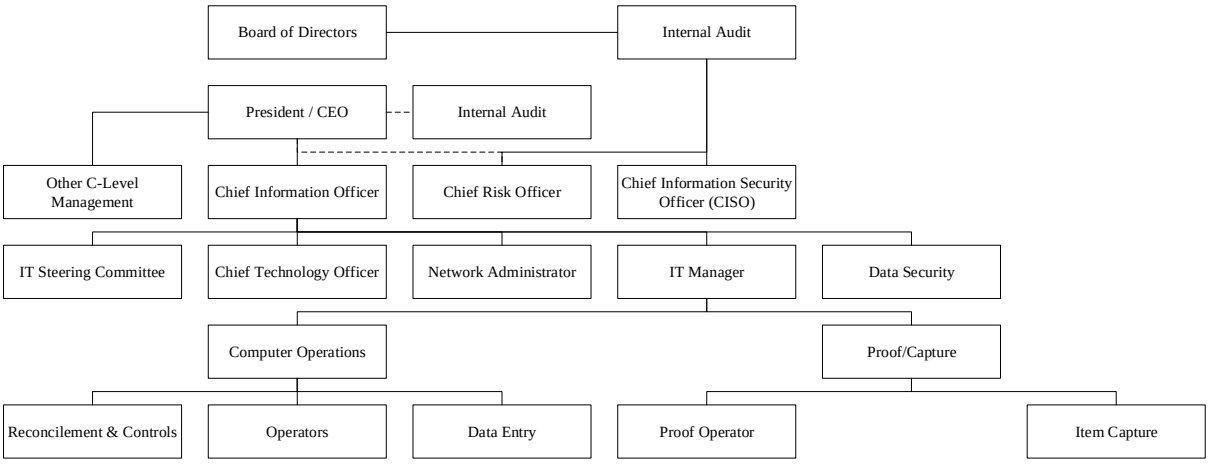
Perumusan kebijakan tersebut disusun dan diselaraskan dengan menggunakan beberapa kerangka kerja diantaranya SNI ISO 27001:2013 tentang SMKI, Octave Allegro, dan COBIT 2019. Penyelarasan kerangka kerja ini digunakan dengan mempertimbangkan proses utama dari setiap Satuan Kerja pada Polri sehingga dapat di selaraskan sesuai dengan tugas pokok, fungsi dan kebutuhan. Pengembangan kerangka kerja SNI ISO 27001:2013 tentang SMKI, Octave Allegro, dan COBIT 2019 merupakan bagian dari sistem manajemen keamanan informasi yang secara keseluruhan meliputi deteksi, pencegahan, merespon, mengontrol, dan mengevaluasi keamanan informasi berdasarkan pendekatan risiko sebagaimana ditunjukan pada Gambar 8 dimana sistem manajemen kcceamanan informasi mencakup struktur,

kebijakan, kegiatan perencanaan, tanggung jawab, praktek, prosedur, proses dan sumber daya organisasi.



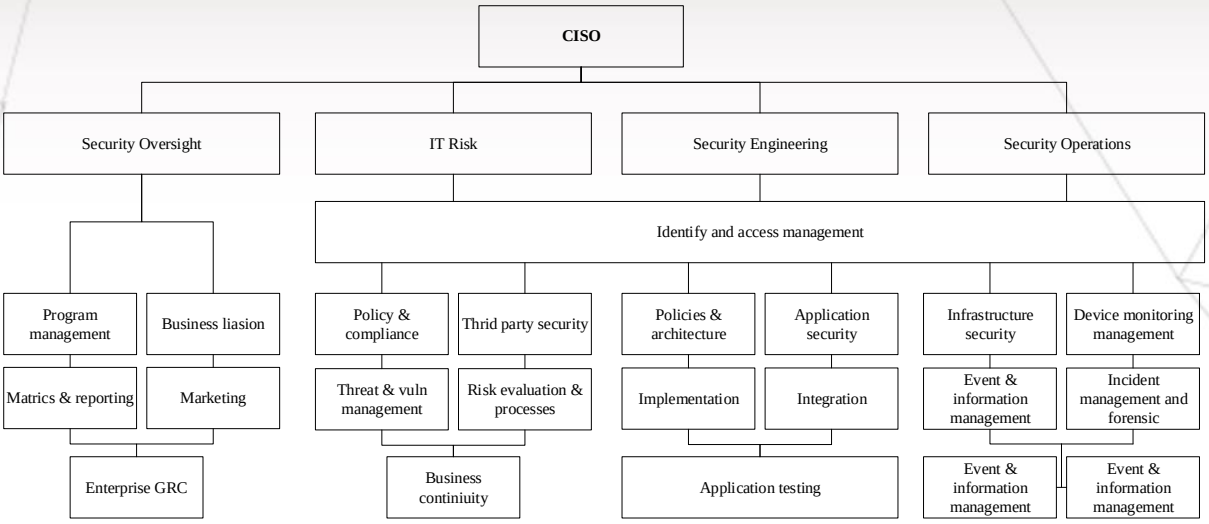
Gambar 8 Kerangka Kerja SMKI

Selain kebijakan organisasi merupakan hal penting terkait dengan keamanan informasi. Organisasi harus dibangun, dikembangkan, dan disesuaikan dengan penyelenggaraan sistem keamanan informasi. Organisasi keamanan informasi ditujukan untuk memastikan pihak-pihak terkait dapat melaksanakan tugas sesuai dengan tujuan dan komitmen organisasi dalam mengimplementasikan keamanan informasi. Pada lampiran A naskah akademik ini menjelaskan nama dan fungsi dari posisi dari struktur organisasi tata kelola keamanan informasi berdasarkan COBIT 2019 sebagaimana ditunjukan pada Gambar 9.



Gambar 9 Struktur Organisasi Tata Kelola Keamanan Informasi

Secara konseptual, Gambar 9 menggambarkan tata kelola keamanan informasi secara keseluruhan. Namun dalam pelaksanaanya, implementasi struktur organsisasi tata kelola keamanan informasi tersebut dapat diselaraskan dengan kondisi struktur organisasi yang telah ada saat ini. Hal ini dikarenakan, struktur organisasi dalam instansi pemerintah khususnya Polri bersifat ad hoc sehingga membutuhkan waktu untuk mengubah struktur organisasi yang ada. Beberapa penyelarasan dapat dilakukan dengan mengimplementasikan struktur organisasi tata kelola keamanan informasi kedalam organisasi yang ada saat ini dengan mengedepankan fungsi dan peran CISO (*Chief Information Security Officer*) sebagaimana ditunjukkan pada Gambar 10.



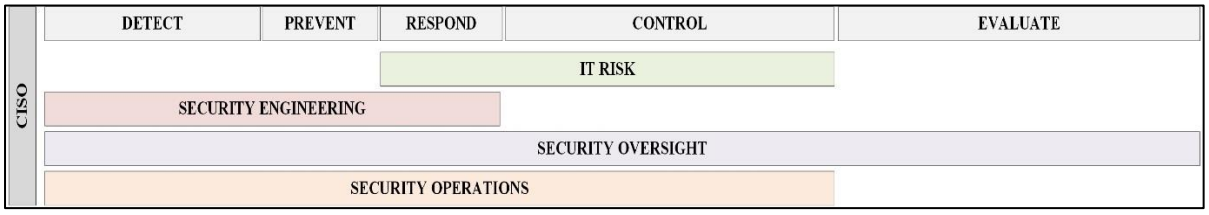
Gambar 10 Struktur organisasi CISO

CISO merupakan pejabat paling senior bertanggung jawab atas semua aspek manajemen keamanan di seluruh perusahaan. Tugas dan fungsi CISO dapat diselaraskan dengan pejabat dalam organisasi Polri saat ini khususnya yang menyediakan dan mengelola pelayanan sistem elektronik. CISO dapat diselaraskan dengan jabatan pada posisi Kabag, Kasubdit, ataupun Kanit dengan sebelumnya menambahkan tugas sebagai seorang CISO yang diantaranya:

1. Mengembangkan, menerapkan, dan memantau program keamanan informasi perusahaan dan manajemen risiko TI yang strategis dan komprehensif;
2. Bekerja secara langsung dengan unit kerja untuk memfasilitasi penilaian risiko dan proses manajemen risiko;
3. Kembangkan dan tingkatkan kerangka kerja manajemen keamanan informasi;
4. Memahami dan berinteraksi dengan disiplin ilmu terkait melalui komite untuk memastikan penerapan kebijakan dan standar yang konsisten di semua proyek, sistem, dan layanan teknologi;
5. Memberikan kepemimpinan bagi organisasi keamanan informasi perusahaan;
6. Bermitra dengan pemangku kepentingan bisnis di seluruh organisasi untuk meningkatkan kesadaran akan masalah manajemen risiko; dan
7. Membantu perencanaan teknologi bisnis secara keseluruhan, memberikan pengetahuan saat ini dan visi masa depan dari teknologi dan sistem yang digunakan saat ini.

Penambahan tugas dalam struktur organisasi Bagian, Sub Direktorat, ataupun Unit juga membutuhkan penambahan personil. Hal ini dengan tujuan untuk menjaga efektifitas pekerjaan dan mengelola tingkat stress kerja setiap personil sesuai dengan analisis beban kerja yang telah ditentukan.

Dalam mengelola manajemen keamanan informasi, CISO juga dibantu oleh beberapa bagian dibawahnya diantaranya *IT Risk*, *Security Engineering*, *Security Oversight*, dan *Security Operation* sebagaimana ditunjukan pada Gambar 11. *IT Risk* bertugas dalam ruang lingkup *respond* dan *control* pada kerangka kerja. *Security Engineering* bertugas dalam ruang lingkup *detect* dan *prevent* pada kerangka kerja. *Security Oversight* bertugas dalam ruang lingkup *detect, prevent, respond, control*, dan *evaluate* pada kerangka kerja. Terakhir *Security Operation* bertugas dalam ruang lingkup *detect* dan *control* pada kerangka kerja.



Gambar 11 Perangkat CISO

Untuk memastikan kebijakan dan struktur organisasi berjalan sesuai dengan tujuan dan komitmen organisasi terkait dengan keamanan informasi diperlukan suatu mekanisme pemeriksaan dan pengawasan baik internal maupun eksternal yang dikenal dengan istilah audit. Audit bertujuan untuk mengevaluasi serta memastikan apakah semua kegiatan atau proses yang selama ini dilakukan telah memenuhi *key performance indeks* (KPI) dan memastikan jika semua tujuan organisasi terpenuhi. Dalam organisasi Polri, fungsi audit dilaksanakan oleh ITWASUM Polri terhadap aspek perencanaan, pengorganisasian, pelaksanaan, pengendalian, keuangan, dan pengadaan barang serta jasa. Namun ITWASUM Polri belum mengemban fungsi khusus terkait dengan perkembangan era Police 4.0 yaitu terkait dengan Audit Keamanan Informasi.

Pelaksanaan audit keamanan informasi, dapat dilakukan berdasarkan risiko yang telah diidentifikasi dari masing-masing penyedia dan pengelola layanan sistem elektronik. Saat ini telah banyak kerangka kerja yang dapat digunakan untuk melakukan audit terhadap keamanan informasi maupun tata kelola keamanan informasi. Pada naskah akademik ini, audit tata kelola keamanan informasi dapat dilakukan dengan menggunakan Indeks KAMI 4.0. Indeks KAMI 4.0 merupakan tools audit yang paling mudah dan mendukung berbagai macam kerangka kerja keamanan informasi. Ruang lingkup pelaksanaan audit tata kelola keamanan informasi dapat dilakukan terhadap semua aplikasi yang menyediakan dan mengelola layanan sistem elektronik dengan CISO, pengguna, operator, dan pihak terkait (vendor) sebagai sasaran auditnya. Hasil audit ini digunakan untuk menentukan apakah saat ini peyedia dan mengelola layanan sistem

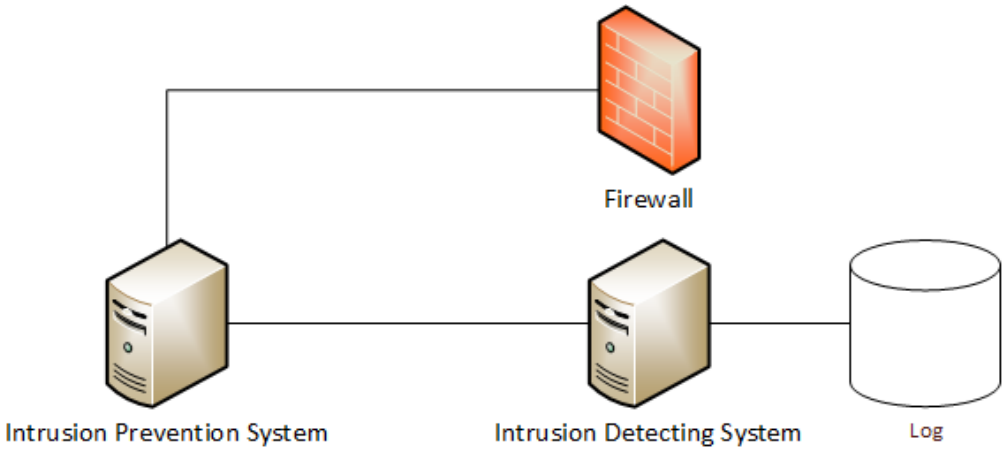
elektronik telah memastikan *confidentiality*, *integrity*, dan *availability* pada layanan yang diberikan dengan standar penilaian tingkat 3 berdasarkan penilaian tingkat kematangan dalam pengelolaan keamanan informasi.

B. Pengembangan dan Pengujian Distro Linux Presisi Sebagai Metode Keamanan Server

Pada naskah ini, diusulkan suatu sistem operasi Linux baru yang dinamakan Linux Presisi. Linux Presisi merupakan sistem operasi turunan dari Ubuntu, yang dapat digunakan untuk membuat server yang aman. Hal ini dikarenakan Linux Presisi memiliki metode keamanan yang menggabungkan IPS (*Intrusion Prevention System*) dan *Honeypot* berbasis *open source*.

B.1 Perancangan IPS (Intrusion Prevention System)

IPS merupakan kombinasi antara fasilitas *blocking capabilities* dari *Firewall* dan kedalaman inspeksi paket data dari *Intrusion Detection System* (IDS). Pada saat bekerja, IPS akan membuat akses kontrol dengan cara melihat konten aplikasi sehingga IPS mampu mencegah serangan yang datang dengan bantuan administrator dan akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori (Pradipta, 2017). Pada naskah ini, *firewall* yang diterapkan merupakan firewall software dengan menggunakan iptables, Kemudian, pada IDS menggunakan tools *snort*.

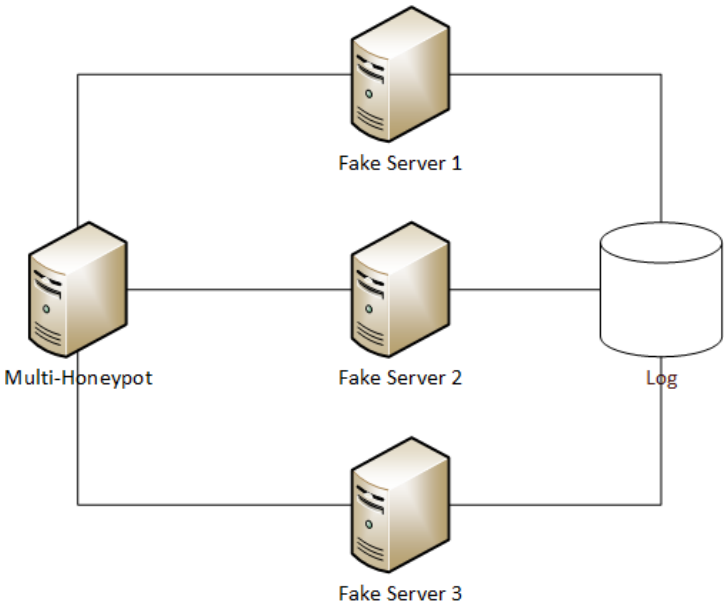


Gambar 11 *Intrusion Prevention System*

B.2 Perancangan *Honeypot*

Honeypot merupakan sumber sistem informasi data yang bersifat terbuka, dan dibuat seolah-olah mirip dengan sistem sebenarnya untuk dikorbankan, karena memiliki sumber informasi data palsu untuk menjebak penyerang. Dengan adanya *honeypot*, segala aktivitas ilegal yang

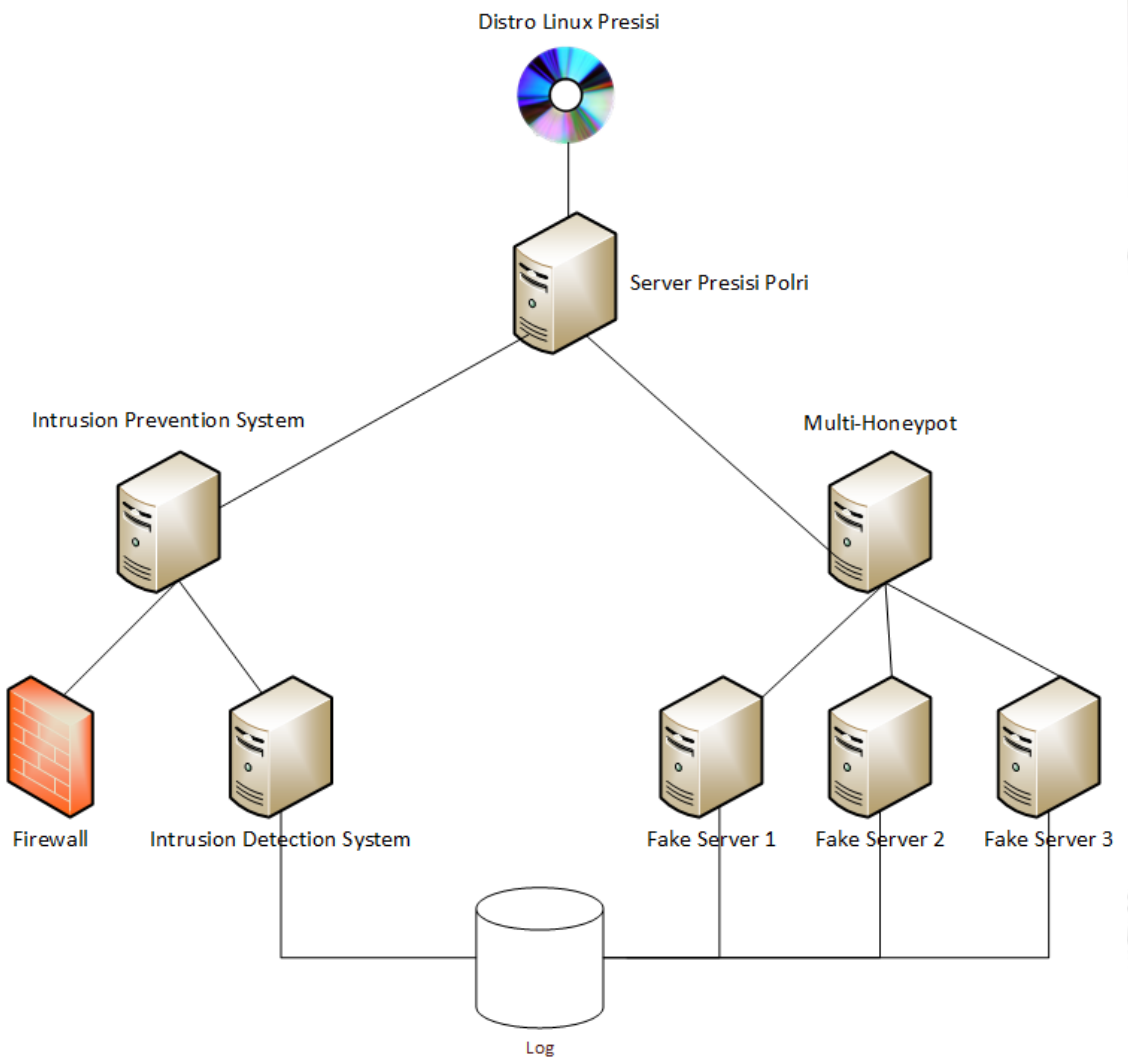
dilakukan oleh penyerang dapat digunakan administrator sebagai informasi tentang penyerang untuk menganalisis, serta mempelajari aktivitas-aktivitas yang cenderung membahayakan sistem (Husnan, 2013). Pada naskah ini, honeypot yang diterapkan yaitu dengan menggunakan *tools honeyd*. Dengan membuat 3 server palsu (*multiple honeypot*).



Gambar 12 *Multi-Honeypot*

B.3 Distro Linux Presisi

Setelah tahap perancangan serta implementasi metode keamanan IPS dan *Honeypot*. Selanjutnya dilakukan tahapan *Remastering* agar IPS dan *Honeypot* terkompilasi menjadi suatu Distro Linux baru yang dinamakan Linux Presisi. Linux Presisi tersebut akan menjadi suatu sistem operasi yang dapat memberikan perlindungan keamanan di layer *application.* Penggunaan Linux presisi cukup mudah untuk diterapkan, karena cukup hanya diinstal di suatu komputer maka komputer tersebut telah memiliki sistem operasi yang aman.



Gambar 13 Distro Linux Presisi

C. Pengembangan Tata Kelola Keamanan Informasi Berbasis COBIT, SNI ISO 27001:2013 dan Octave Allegro

C.1 Rancangan Integrasi SNI ISO 27001 dan OCTAVE Allegro

Pada bagian ini akan membahas mengenai analisa lanjutan dan desain model SMKI SNI ISO 27001:2013 berdasarkan integrasi dengan penilaian risiko dari OCTAVE Allegro dengan megumpulkan data berdasarkan kajian literatur dan melaksanakan elaborasi beberapa kerangka kerja SMKI dan MRKI. Dari hasil analisis tersebut telah ditetapkan pengembangan ini menggunakan kerja kerja SNI ISO 27001:2013 yang dipadukan dengan kerangka kerja manajemen risiko keamanan informasi OCTAVE Allegro.

C.1.1 Tahapan Kerangka SNI ISO 27001:2013

Inti dari kerangka kerja SNI ISO 27001:2013 terdapat pada klausul 4 hingga 10. Klausul tersebut berisi ketentuan, proses dan aktifitas yang menjadi prasyarat yang harus dipatuhi dalam proses sertifikasi. Keseluruhan ketentuan yang ada dalam klausul 4 - 10 harus dipenuhi oleh organisasi yang menyatakan diri sesuai dengan standar ini. Tahapan-tahapan kegiatan manajemen keamanan informasi SNI ISO 27001:2013 yang diuraikan berdasarkan langkah umum proses manajemen keamanan informasi, ditampilkan pada tabel berikut:

Tabel 3 Tahapan SNI ISO 27001:2013

No.	Tahapan	Kegiatan
1	Ruang Lingkup	
2	Acuan Normatif	
3	Istilah dan Definisi	
4	Konteks Organisasi	Memahami organisasi dan konteksnya
		Memahami kebutuhan dan harapan dari pihak yang bekepentingan
		Penentuan ruang lingkup SMKI
		Sistem manajemen keamanan informasi
5	Kepimpinan	Kepemimpinan dan komitmen
		Kebijakan
		Peran organisasi, tanggung jawab, dan wewenang
6	Perencanaan	Tindakan untuk menangani risiko dan peluang
		Sasaran keamanan informasi dan perencanaan untuk mencapainya
7	Dukungan	Sumber daya
		Kompetensi
		Kepedulian
		Komunikasi
		Informasi terdokumentasi
8	Operasi	Perencanaan dan pengendalian operasional
		Penilaian risiko keamanan informasi
		Penanganan risiko keamanan informasi
9	Evaluasi Kinerja	Pemantauan, pengukuran, analisis dan evaluasi

No.	Tahapan	Kegiatan
		Audit Internal
		Reviu Manajemen
10	Perbaikan	Ketidaksesuaian dan tindakan korektif
		Perbaikan berkelanjutan

C.1.2 Tahapan Kerangka OCTAVE Allegro

Tahapan-tahapan MRKI pada metode OCTAVE Allegro diuraikan berdasarkan langkah kegiatan yang ditampilkan pada tabel IV.2, berikut:

Tabel 4 Tahapan Metode OCTAVE Allegro

Fase	Proses
Fase 1: Menetapkan *Drivers*	P1: Menetapkan *Risk Measurement Criteria*
Fase 2: Profil Aset	P2: Mengembangkan *Information Asset Profile*
	P3: Mengidentifikasi *Information Asset Containers*
Fase 3: Mengindentifikasi *Threat*	P4: Mengindentifikasi *area of concern*
	P5: Mengidentifikasi *threats scenarios*
Fase 4: Mengidentifikasi dan Mitigasi Risiko	P6: Mengidentifikasi risiko
	P7: Menganalisis risiko
	P8: Memilih pendekatan mitigasi

C.1.3 Integrasi SNI ISO 27001:2013 – OCTAVE Allegro

Hasil analisis sistem manajemen keamanan informasi SNI ISO 27001:2013 berdasarkan manajemen risiko OCTAVE Allegro yang disesuaikan dengan organisasi SSDM Polri menghasilkan integrase antara keduanya dengan cara memetakan kegiatan berdasarkan kesesuaian. Hasilnya dapat dilihat pada tabel 5, berikut:

Tabel 5 Pemetaan Metode OCTAVE Allegro pada SNI ISO 27001:2013

No.	Tahapan	Kegiatan	OCTAVE Allegro
1	Ruang Lingkup		
2	Acuan Normatif		
3	Istilah dan Definisi		

No.	Tahapan	Kegiatan	OCTAVE Allegro
4	Konteks Organisasi	Memahami organisasi dan konteksnya	
		Memahami kebutuhan dan harapan dari pihak yang bekepentingan	
		Penentuan ruang lingkup SMKI	
		Sistem manajemen keamanan informasi	
5	Kepimpinan	Kepemimpinan dan komitmen	
		Kebijakan	
		Peran organisasi, tanggung jawab, dan wewenang	
6	Perencanaan	Tindakan untuk menangani risiko dan peluang	P1, P2, P3, P4, P5, P6, P7
		Sasaran keamanan informasi dan perencanaan untuk mencapainya	P8
7	Dukungan	Sumber daya	
		Kompetensi	
		Kepedulian	
		Komunikasi	
		Informasi terdokumentasi	
8	Operasi	Perencanaan dan pengendalian operasional	
		Penilaian risiko keamanan informasi	
		Penanganan risiko keamanan informasi	
9	Evaluasi Kinerja	Pemantauan, pengukuran, analisis dan evaluasi	
		Audit Internal	
		Reviu Manajemen	
10	Perbaikan	Ketidaksesuaian dan tindakan korektif	
		Perbaikan berkelanjutan	

Berdasarkan tabel 5, semua proses OCTAVE Allegro (P1-P8) telah tercakup dalam kerangka SNI ISO 27001:2013 khususnya pada klausul 6 yaitu perencanaan bagian 6.1 mengenai tindakan untuk menangani risiko yang dijabarkan pada 6.1.2 tentang penilaian risiko keamanan informasi dan 6.1.3 yaitu penanganan risiko keamanan informasi. Penjabaran integrase klausul 6 SNI ISO 2700:2013 dan OCTAVE Allegro dapat dilihat pada tabel 6, berikut:

Tabel 6 Pemetaan Metode OCTAVE Allegro pada Klausul 6.1 SNI ISO 27001:2013

No.	Klausul 6.1 SNI ISO 27001:2013	Kegiatan	Octave Allegro
1	6.1.1 Umum		
2	6.1.2 Penilaian risiko keamanan informasi	Menetapkan dan memelihara kriteria risiko keamanan informasi	P1
		Memastikan bahwa penilaian risiko keamanan informasi yang diulang akan memberikan hasil yang konsisten, valid dan sebanding	P2, P3
		Mengidentifikasi risiko keamanan informasi	P4, P5, P6
		Menganalisis risiko keamanan informasi:	P7
		Mengevaluasi risiko keamanan informasi	P7
3	6.1.3 Penanganan risiko keamanan informasi	Memilih opsi penanganan risiko keamanan informasi yang tepat, dengan mempertimbangkan hasil penilaian risiko	P8
		Menentukan semua kendali yang diperlukan untuk menerapkan opsi penanganan risiko keamanan informasi yang dipilih	P8

Sesuai dengan tujuan pengembangan agar diperoleh proses SMKI yang sesuai dengan kebutuhan organisasi, proses penilaian risiko hanya akan meggunakan metode dari OCTAVE Allegro yang dijelaskan lebih rinci menggunakan *worksheet* (lembar kerja) berdasarkan framework tersebut pada Lampiran B dari pengembangan ini.

Selanjutnya, pada tahap pengembangan model tata kelola keamanan informasi dilakukan dengan memetakan ISO/IEC 27001 terhadap domain dalam model ini COBIT 2019. Pada ISO/IEC 27001 terdiri dari 10 klausul, 14 area, 35 sasaran pengendalian dan 114 kontrol, yang kemudian dipetakan kedalam 40 domain dalam model inti COBIT 2019 yang terpilih.

Pemetaan ini dimaksudkan untuk mendapatkan model tata kelola keamanan informasi yang bukan hanya memiliki kematangan secara tata kelola keamanan informasi, tetapi juga memiliki kematangan pada aktivitas kendali secara teknis. Proses pemetaan Pada ISO/IEC 27001:2013 ke dalam domain dalam model inti COBIT 2019 dilakukan berdasarkan sasaran kendali dalam domain COBIT 2019. Karena COBIT 2019 pada prinsipnya dapat diselaraskan dengan berbagai macam *framework*. Hasil pemetaan ISO/IEC 27001:2013 ke dalam domain dalam model inti COBIT 2019 ditunjukkan dalam Tabel II.1 Pemetaan ISO/IEC 27001 ke dalam Domain COBIT 27001:2013.

Tabel 7 Pemetaan ISO/IEC 27001:2013 ke COBIT 2019.

Area		**Sasaran Pengendalian**		**Domain COBIT 2019**
1.	Kebijakan keamanan informasi.	1.	Arahan manajemen untuk keamanan informasi.	EDM
2.	Organisasi keamanan informasi.	2.	Organisasi internal.	EDM
		3.	Perangkat bergerak (*mobile device*) dan *teleworking*.	EDM
3.	Keamanan sumber daya manusia.	4.	Sebelum dipekerjakan.	APO 07
		5.	Selama bekerja.	APO 07
		6.	Penghentian dan perubahan kepegawaian.	APO 07
4.	Manajemen asset.	7.	Tanggung jawab terhadap asset.	BAI 09
		8.	Klasifikasi informasi.	BAI 09
		9.	Penanganan media.	BAI 09
5.	Kendali akses.	10.	Persyaratan bisnis untuk kendali akses.	DSS 05
		11.	Manajemen akses pengguna.	DSS 05
		12.	Tanggung jawab pengguna.	DSS 05
		13.	Kendali akses sistem dan aplikasi.	DSS 05
6.	Kriptografi.	14.	Kendali kriptografi.	DSS 05
7.	Keamanan fisik dan lingkungan.	15.	Daerah aman.	DSS 05
		16.	Peralatan	DSS 05

Area		Sasaran Pengendalian		Domain COBIT 2019
8.	Keamanan operasi	17.	Prosedur dan tanggung jawab operasional.	DSS 01
		18.	Perlindungan dari malware.	DSS 05
		19.	Cadangan (*Backup*).	APO 14
		20.	Pencatatan (*logging*) dan pemantauan.	DSS 05
		21.	Kendali perangkat lunak operasional.	DSS 05
		22.	Manajemen kerentanan teknis.	DSS 05
		23.	Pertimbangan audit sistem informasi.	MEA 04
9.	Keamanan komunikasi.	24.	Manajemen keamanan jaringan.	DSS 05
		25.	Perpindahan informasi.	DSS 05
10.	Akuisisi, pengembangan dan perawatan system.	26.	Persyaratan keamanan sistem informasi.	APO 13
		27.	Keamanan dalam proses pengembangan dan dukungan.	APO 04
		28.	Data uji.	APO 14
11.	Hubungan pemasok	29.	Keamanan informasi dalam hubungan pemasok.	APO 10
		30.	Manajemen penyampaian layanan pemasok.	APO 10
12.	Manajemen insiden keamanan informasi	31.	Manajemen insiden keamanan informasi dan perbaikan.	DSS 05
13.	Aspek keamanan informasi dari manajemen keberlangsungan bisnis.	32.	Keberlangsungan keamanan informasi.	DSS 04
		33.	Redundansi.	DSS 04
14.	Kesesuaian.	34.	Kesesuaian dengan persyaratan hukum dan kontraktual.	MEA 03
		35.	Reviu keamanan informasi.	APO 13

Berdasarkan hasil pemetaan ISO/IEC 27001:2013 ke dalam domain model inti COBIT 2019, selanjutnya akan digunakan untuk memetakan *Goals Cascade* COBIT 2019. Kemudian hasil pemetaan akan dibandingkan dengan pemetaan berdasarkan *desain factor* dalam COBIT 2019 dengan area fokus pada keamanan informasi. Faktor desain merupakan faktor yang dapat mempengaruhi desain sistem tata kelola perusahaan dan memposisikannya untuk kesuksesan dalam penggunaan informasi dan teknologi. Visi, misi, dan sasaran strategis yang dimasukan kedalam 11 faktor desain dalam COBIT 2019.

Untuk mendapatkan desain tata kelola keamanan informasi yang ideal berdasarkan ISO/IEC 27001:2013 dan COBIT 2019. Sebelumnya telah dilakukan pemetaan ISO/IEC 27001:2013 kedalam domain model inti COBIT yang dilanjutkan dengan pemilihan domain model inti COBIT 2019 dengan menggunakan COBIT 2019 *goals cascade* dan COBIT 2019 *design factor*. Selanjutnya, akan dilakukan pemilahan terhadap domain model inti COBIT 2019 terpilih berdasarkan perbandingan antara pemetaan ISO/IEC 27001:2013 kedalam COBIT 2019, pemilihan domain model inti COBIT 2019 dengan menggunakan *goals cascade*, dan pemilihan domain model inti COBIT 2019 dengan menggunakan *design factor* sebagaimana ditunjukkan didalam Tabel IV.2 Pemilahan domain model inti COBIT 2019.

Tabel 8 Pemilihan domain model inti COBIT 2019

Area		Sasaran Pengendalian		Domain COBIT 2019	Domain COBIT 2019 (*Goals Cascade*)	Domain COBIT 2019 (*Design Factor*)	Domain COBIT 2019 Terpilih
1.	Kebijakan keamanan informasi.	1.	Arahan manajemen untuk keamanan informasi.	EDM	EDM 01, EDM 03, EDM 04, EDM 05	EDM 01, EDM 03, EDM 05	EDM 01, EDM 03, EDM 05
2.	Organisasi keamanan informasi.	2.	Organisasi internal.	EDM			
		3.	Perangkat bergerak (*mobile device*) dan teleworking.	EDM			
3.	Keamanan sumber daya manusia.	4.	Sebelum dipekerjakan.	APO 07	Seluruh Domain Model Inti APO	APO 01, APO 03, APO 07, APO 08, APO 09, APO 10, APO 11, APO 12, APO 13, APO 14	APO 01, APO 03, APO 04, APO 07, APO 08, APO 09, APO 10, APO 11, APO 12, APO 13, APO 14
		5.	Selama bekerja.	APO 07			
		6.	Penghentian dan perubahan kepegawaian.	APO 07			

Area		Sasaran Pengendalian		Domain COBIT 2019	Domain COBIT 2019 (*Goals Cascade*)	Domain COBIT 2019 (*Design Factor*)	Domain COBIT 2019 Terpilih
4.	Manajemen asset.	7.	Tanggung jawab terhadap asset.	BAI 09	Seluruh Domain Model Inti BAI	BAI 06, BAI 07, BAI 08, BAI 10	BAI 06, BAI 07, BAI 08, BAI 09, BAI 10
		8.	Klasifikasi informasi.	BAI 09			
		9.	Penanganan media.	BAI 09			
5.	Kendali akses.	10.	Persyaratan bisnis untuk kendali akses.	DSS 05	Seluruh Domain Model Inti DSS	Seluruh Domain Model Inti DSS	Seluruh Domain Model Inti DSS
		11.	Manajemen akses pengguna.	DSS 05			
		12.	Tanggung jawab pengguna.	DSS 05			
		13.	Kendali akses sistem dan aplikasi.	DSS 05			
6.	Kriptografi.	14.	Kendali kriptografi.	DSS 05			
7.	Keamanan fisik dan lingkungan.	15.	Daerah aman.	DSS 05			
		16.	Peralatan	DSS 05			
8.	Keamanan operasi	17.	Prosedur dan tang-gung jawab opera-sional.	DSS 01			

Area		Sasaran Pengendalian		Domain COBIT 2019	Domain COBIT 2019 (*Goals Cascade*)	Domain COBIT 2019 (*Design Factor*)	Domain COBIT 2019 Terpilih
		18.	Perlindungan dari *malware*.	DSS 05			
		19.	Cadangan (*Backup*).	APO 14	Seluruh Domain Model Inti APO	APO 01, APO 03, APO 07, APO 08, APO 09, APO 10, APO 11, APO 12, APO 13, APO 14	APO 01, APO 03, APO 04, APO 07, APO 08, APO 09, APO 10, APO 11, APO 12, APO 13, APO 14
		20.	Pencatatan (*logging*) dan pemantauan.	DSS 05	Seluruh Domain Model Inti DSS	Seluruh Domain Model Inti DSS	Seluruh Domain Model Inti DSS
		21.	Kendali perangkat lunak operasional.	DSS 05			
		22.	Manajemen kerentanan teknis.	DSS 05			

Area		Sasaran Pengendalian		Domain COBIT 2019	Domain COBIT 2019 (*Goals Cascade*)	Domain COBIT 2019 (*Design Factor*)	Domain COBIT 2019 Terpilih
		23.	Pertimbangan audit sistem informasi.	MEA 04	Seluruh Domain Model Inti MEA	Seluruh Domain Model Inti MEA	Seluruh Domain Model Inti MEA
9.	Keamanan komunikasi.	24.	Manajemen keamanan jaringan.	DSS 05	Seluruh Domain Model Inti DSS	Seluruh Domain Model Inti DSS	Seluruh Domain Model Inti DSS
		25.	Perpindahan informasi.	DSS 05			
10.	Akuisisi, pengembangan dan perawatan system.	26.	Persyaratan keama-nan sistem informasi.	APO 13	Seluruh Domain Model Inti APO	APO 01, APO 03, APO 07, APO 08, APO 09, APO 10, APO 11, APO 12, APO 13, APO 14	APO 01, APO 03, APO 04, APO 07, APO 08, APO 09, APO 10, APO 11, APO 12, APO 13, APO 14
		27.	Keamanan dalam proses pengembang-an dan dukungan.	APO 04			
		28.	Data uji.	APO 14			
11.	Hubungan pemasok	29.	Keamanan informasi dalam hubungan pe-masok.	APO 10			
		30.	Manajemen penyam-paian layanan pema-sok.	APO 10			

Area		Sasaran Pengendalian		Domain COBIT 2019	Domain COBIT 2019 (*Goals Cascade*)	Domain COBIT 2019 (*Design Factor*)	Domain COBIT 2019 Terpilih
12.	Manajemen insiden keamanan informasi	31.	Manajemen insiden keamanan informasi dan perbaikan.	DSS 05	Seluruh Domain Model Inti DSS	Seluruh Domain Model Inti DSS	Seluruh Domain Model Inti DSS
13.	Aspek keamanan informasi dari manajemen keberlangsungan bisnis.	32.	Keberlangsungan keamanan informasi.	DSS 04			
		33.	Redundansi.	DSS 04			
14.	Kesesuaian.	34.	Kesesuaian dengan persyaratan hukum dan kontraktual.	MEA 03	Seluruh Domain Model Inti MEA	Seluruh Domain Model Inti MEA	Seluruh Domain Model Inti MEA
		35.	Reviu keamanan informasi.	APO 13	Seluruh Domain Model Inti APO	APO 01, APO 03, APO 07, APO 08, APO 09, APO 10, APO 11, APO	APO 01, APO 03, APO 04, APO 07, APO 08, APO 09,

Area		Sasaran Pengendalian		Domain COBIT 2019	Domain COBIT 2019 (*Goals Cascade*)	Domain COBIT 2019 (*Design Factor*)	Domain COBIT 2019 Terpilih
						12, APO 13, APO 14	APO 10, APO 11, APO 12, APO 13, APO 14

Table IV.2 Pemilihan domain model inti COBIT 2019, membandingkan domain model inti COBIT 2019 terpilih berdasarkan klausul ISO/IEC 27001:2013, *goal cascade* COBT 2019, dan *design factor* COBIT 2019. Pada tahap ini sudah dapat ditentukan domain model inti COBIT 2019 EDM yang sebelumnya belum dapat terpetakan berdasarkan klausul ISO/IEC 27001:2013. Berdasarkan hasil perbandingan pada Table IV.2 dihasilkan domain model inti COBIT 2019 sebagai berikut:

1. Pemetaan berdasarkan klausul dan Annex A ISO/IEC 27001:2013 diperoleh 10 domain model inti COBIT 2019 yaitu APO 07 *Managed Human Resources*, APO 10 *Managed Vendors*, APO 13 *Managed Security*, APO 14 *Managed Data*, BAI 09 *Managed Assets*, DSS 01 Manag*ed Operations*, DSS 04 *Managed Continuity*, DSS 05 *Managed Security Services*, MEA 03 *Managed Compliance With External* Requirements dan MEA 04 *Managed Assurance*. Sedangkan domain model inti COBIT 2019 EDM pada tahap ini belum dapat terpetakan secara spesifik, karena pada area kebijakan keamanan informasi dan organisasi keamanan informasi menyebar pada seluruh bagian domain model inti COBIT 2019 EDM;
2. Pemetaan berdasarkan *goals cascade* COBIT 2019 diperoleh 39 domain model inti COBIT 2019, kecuali EDM 02 *Ensure Benefit Delivery*; dan
3. Pemetaan berdasarkan COBIT 2019 *design factor* berdasarkan toolkit COBIT 2019 diperoleh 27 domain model inti COBIT 2019 yaitu EDM 01 *Ensured Governance Framework Setting and Maintenance*, EDM 03 *Ensured Risk Optimization*, EDM 05 *Ensured Stakeholder Engagement*. APO 01 *Managed I&T Management Framework*, APO 03 *Managed Enterprise Architecture*, APO 07 *Managed Human Resources*, APO 08 *Managed Relationships*, APO 09 *Managed Service Agreements*, APO 10 *Managed Vendors*, APO 11 *Managed Quality*, APO 12 *Managed Risk*, APO 13 *Managed Security*, APO 14 *Managed Data*. BAI 07 *Managed IT Change Acceptance and Transitioning*. BAI 08 *Managed Knowledge*, BAI 10 *Managed Configuration*. Semua domain model inti DSS, dan semua domain model inti MEA.

Table IV.2 Pemilihan domain model inti COBIT 2019, juga menunjukan jika terdapat 2 Domain yaitu DSS 04 *Managed Innovation* dan BAI 09 *Managed Assets* yang tidak terpetakan berdasarkan *goal cascade* dan *design factor* COBIT 2019. Sementara DSS 04 dan BAI 09 telah terpetakan secara spesifik dari ISO/IEC 27001:2013 sehingga dengan memperhatikan hal tersebut, pemetaan model inti yang akan dipilih untuk membuat model tata kelola dan manajemen keamanan informasi pada tesis ini dengan menggabungkan domain model inti

COBIT 2019 terpilih berdasarkan pemetaan ISO/IEC 27001:2013 dan pemetaan berdasarkan COBIT 2019 *design factor* yang menghasilka sebanyak 29 dari 40 domain model inti COBIT 2019 yang diantaranya:

1. EDM 01 *Ensured* Governance *Framework Setting and Maintenance*;
2. EDM 03 *Ensured Risk Optimization*;
3. EDM 05 *Ensured Stakeholder Engagement*;
4. APO 01 *Managed I&T Management Framework*;
5. APO 03 *Managed Enterprise Architecture*;
6. APO 04 *Managed Innovation*;
7. APO 07 *Managed Human Resources*;
8. APO 08 *Managed Relationships*;
9. APO 09 *Managed Service Agreements*;
10. APO 10 *Managed Vendors*;
11. APO 11 *Managed Quality*;
12. APO 12 *Managed Risk*;
13. APO 13 *Managed Security*;
14. APO 14 *Managed Data*;
15. BAI 06 *Managed IT Changes*;
16. BAI 07 *Managed IT Change Acceptance and Transitioning*;
17. BAI 08 *Managed Knowledge*;
18. BAI 09 *Managed Assets*;
19. BAI 10 *Managed Configuration*;
20. DSS 01 Manag*ed Operations*;
21. DSS 02 *Managed Service Requests and Incidents*;
22. DSS 03 *Managed Problems*;
23. DSS 04 *Managed Continuity*;
24. DSS 05 *Managed Security Services*;
25. DSS 06 *Managed Business Process Controls*;
26. MEA 01 *Managed Performance and Conformance Monitoring*;
27. MEA 02 *Managed System of Internal Control*;
28. MEA 03 *Managed Compliance with External Requirements*; dan
29. MEA 04 *Managed Assurance*.

Pada Tabel IV.2, telah ditentukan domain model inti COBIT 2019 terpilih. Selanjutnya domain model inti COBIT 2019 terpilih tersebut akan digunakan untuk menilai tata kelola keamanan informasi. Penilaian dilakukan dengan menggunakan tingkat 0-3 berdasarkan tingkat kemampuan COBIT 2019. Dengan taget capaian tingkat ideal suatu tata kelola keamanan informasi berdasarkan Indeks KAMI (Keamanan Informasi) dan COBIT 2019 yaitu pada tingkat 3 dengan definisi proses atau aktifitas mencapai tujuannya dengan cara yang jauh lebih terorganisir dengan menggunakan aset organisasi dan didefinisikan dengan baik.

Penilaian dilakukan dengan mengevaluasi aktifitas yang selama ini dilakukan sesuai dengan domain model inti COBIT 2019 terpilih. Penilaian Tata Kelola Keamanan Informasi dengan tingkat kemampuan 0 yang memiliki definisi kurangnya kemampuan dasar, pendekatan yang tidak lengkap untuk menangani tujuan tata kelola dan manajemen, dan atau mungkin tidak memenuhi maksud dari praktik proses apa pun. Tingkat kemampuan 1 dengan definisi proses atau aktivitas kurang lebih mencapai tujuannya melalui penerapan serangkaian aktivitas yang tidak lengkap yang dapat dicirikan sebagai awal atau intuitif dan tidak terlalu terorganisir. Tingkat kemampuan 2 dengan definisi proses atau aktivitas mencapai tujuannya melalui penerapan serangkaian aktivitas dasar dan sebagian diterapkan. Tingkat kemampuan 3 dengan definisi proses atau aktifitas mencapai tujuannya dengan cara yang jauh lebih terorganisir dengan menggunakan aset organisasi dan didefinisikan dengan baik.

Untuk dapat mencapai tingkat kemampuan 3 pada tata kelola keamanan informasi Polri, bukan hanya dinilai dari struktur organisasi dan sumber daya manusia, tetapi juga kebijakan yang mengatur terkait dengan tata kelola keamanan informasi. Pada setiap proses tata kelola keamanan informasi yang dilakukan pada Polri selanjutnya akan dituangkan dalam bentuk kebijakan yang mencakup pengelolaan proses T&I beserta keamanannya, pengelolaan administrasi pendukung keamanan T&I, serta penentuan dan implementasi standar untuk setiap proses T&I beserta keamanannya. Kebijakan tata kelola keamanan T&I disusun berdasarkan domain model inti COBIT 2019 tepilih yang sebelumnya telah dilakukan penilaian terhadapnya. Kebijakan tersebut meliputi:

1. Kebijakan area tata kelola T&I.
    a. Kebijakan pengaturan dan pemeliharaan kerangka tata kelola T&I;
    b. Kebijakan optimasi risiko yang terkelola; dan
    c. Kebijakan keterlibatan pemangku kepentingan.
2. Kebijakan penyelarasan, perencanaan, dan pengorganisasian T&I.

a. Kebijakan pengelolaan kerangka kerja manajemen T&I;
b. Kebijakan pengelolaan arsitektur perusahaan;
c. Kebijakan pengelolaan inovasi;
d. Kebijakan pengelolaan sumber daya manusia;
e. Kebijakan pengelolaan hubungan;
f. Kebijakan pengelolaan maklumat pelayanan;
g. Kebijakan pengelolaan kualitas layanan;
h. Kebijakan pengelolaan pengadaan T&I;
i. Kebijakan pengelolaan resiko;
j. Kebijakan pengelolaan keamanan informasi; dan
k. Kebijakan pengelolaan data.

3. Kebijakan membangun dan mengimplementasikan T&I.
   a. Kebijakan pengelolaan perubahan T&I;
   b. Kebijakan pengelolaan penerimaan dan transisi perubahan T&I;
   c. Kebijakan pengelolaan informasi dan klasifikasinya;
   d. Kebijakan pengelolaan asset; dan
   e. Kebijakan pengelolaan konfigurasi antar sumber daya.
4. Kebijakan penyampaian, layanan, dan dukungan T&I.
   a. Kebijakan pengelolaan operasional;
   b. Kebijakan pengelolaan permintaan layanan dan insiden;
   c. Kebijakan pengelolaan permasalahan;
   d. Kebijakan pengelolaan keberlanjutan bisnis;
   e. Kebijakan pengelolaan keamanan layanan; dan
   f. Kebijakan pengelolaan pengendalian proses bisnis.
5. Kebijakan pengawasan, evaluasi dan penilaian T&I.
   a. Kebijakan kinerja dan pemantauan kesesuaian;
   b. Kebijakan pengelolaan sistem pengendalian internal;
   c. Kebijakan pengelolaan kepatuhan dengan persyaratan eksternal; dan
   d. Kebijakan pengelolaan jaminan.

Secara umum, cakupan dari setiap kebijakan teknologi dan informasi berdasarkan domain model inti COBIT 2019 terpilih terdiri atas:

1. Pengelolaan kinerja proses teknologi dan informasi, yang mencakup:
   a. Identifikasi sasaran kinerja setiap proses;

b. Perencanaan dan pemantauan kinerja proses;
c. Penyesuaian kinerja proses berdasarkan rencana pengelolaan T&I;
d. Pendefinisian, penunjukan, dan komunikasi tanggung jawab dan autoritas pelaksanaan proses;
e. Identifikasi, alokasi, dan penggunaan resources dan informasi yang dibutuhkan untuk pelaksanaan proses; dan
f. Pengelolaan antarmuka untuk memastikan berjalannya komunikasi dan kejelasan tanggung jawab dari setiap pihak yang ditunjuk dan terlibat dalam pelaksanaan proses.

2. Pengelolaan *work products* (dokumen yang dihasilkan oleh suatu proses dalam domain model inti COBIT 2019 terpilih), yang mencakup:
   a. Pendefinisian dokumen hasil suatu proses T&I.
   b. Pendefinisian kebutuhan dokumentasi dan pengendalian untuk setiap dokumen hasil proses T&I;
   c. Pelaksanaan identifikasi, pendokumentasian, dan pengendalian dokumen hasil proses T&I; dan
   d. Peninjauan ulang dan penyesuaian dokumen hasil proses T&I berdasarkan rencana dan kebutuhan.
3. Pendefinisian standar proses T&I, yang mencakup:
   a. Pendefinisian proses standar, termasuk panduan khusus yang menjelaskan elemen-elemen dasar yang harus digunakan kedalam proses tersebut;
   b. Penentuan urutan dan interaksi proses standar dengan proses lainnya;
   c. Identifikasi kompetensi dan peran yang dibutuhkan untuk pelaksanaan suatu proses T&I sebagai bagian dari proses standar;
   d. Identifikasi infrastruktur dan lingkungan kerja yang dibutuhkan untuk melaksanakan suatu proses T&I sebagai bagian dari proses standar; dan
   e. Menentukan metode monitoring efektivitas dan kesesuaian suatu proses standar.
4. Pelaksanaan standar proses T&I, yang mencakup:
   a. Penetapan dan pelaksanaan standar dari proses T&I;
   b. Penunjukkan dan komunikasi kebutuhan peran, tanggung jawab, dan autoritas untuk pelaksanaan proses standar tersebut;
   c. Personel yang memiliki jenjang karir kepangkatan sesuai, kompetensi, baik pendidikan, pelatihan, maupun pengalaman, dalam pelaksanaan proses standar tersebut;

d. Pengadaan, alokasi, dan penggunaan sumber daya, informasi, infrastruktur, dan lingkungan kerja yang dibutuhkan untuk pelaksanaan proses standar tersebut; dan
e. Pengumpulan dan analisis data sebagai dasar untuk memahami efektivitas dan kesesuaian suatu proses serta sebagai bahan evaluasi dan perbaikan dari suatu proses standar.

Berdasarkan cakupan Kebijakan teknologi dan informasi tersebut, dapat dibuat suatu panduan komponen kebijakan berisi konten minimal yang harus dicantumkan dalam suatu dokumen kebijakan sebagaimana ditunjukkan pada Tabel V.2 Isi Komponen Kebijakan.

Tabel 9 Isi Komponen Kebijakan.

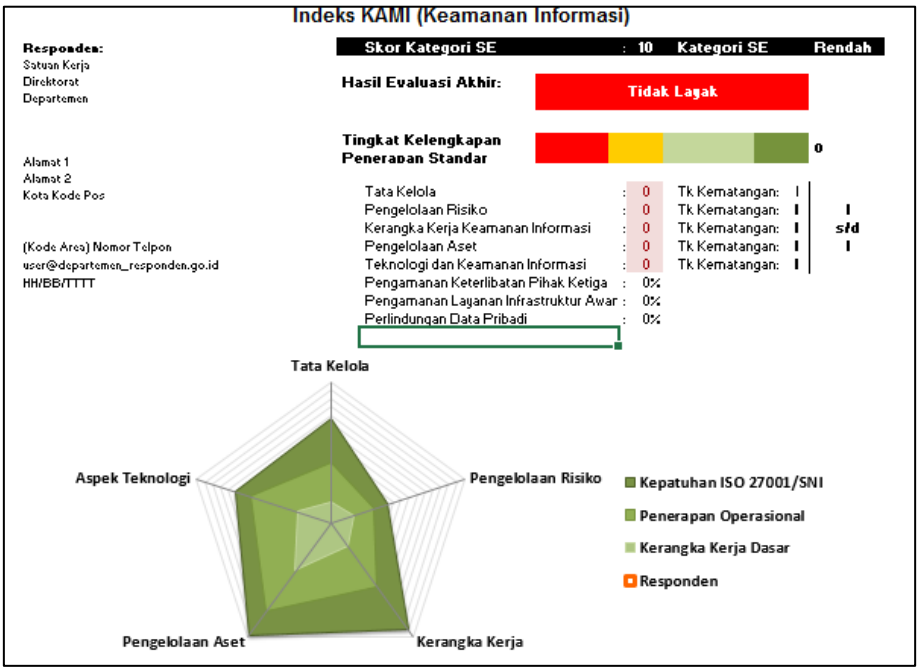
No	Komponen	Konten minimal
1.	Dokumen Proses.	a. Mencantumkan garis besar dari lingkup suatu proses. b. Mencantumkan diagram RACI (*responsible*, *accountable*, *consulted*, *informed*) pada penilitian ini menggunakan R (*responsible*) dan A (*accountable*) yang menyatakan tanggung jawab dan otoritas dari pihak yang terlibat. c. Mencantumkan informasi detail pemilik proses dan pihak-pihak yang terlibat berdasarkan diagram RACI. d. Mencantumkan detail dokumentasi dan pengendalian atas *work products*. e. Mencantumkan kebutuhan kompetensi dan training.
2.	Perencanaan proses	a. Mencantumkan detail dari sasaran kinerja proses T&I b. Mencantumkan detail dari rencana. c. Mencantumkan detail dari rencana training. dan pengadaan sumber daya terkait untuk suatu proses. d. Mencantunkan siapa, berbuat apa, dan bertanggung jawab kepada siapa.
3.	Rencana Kualitas *Work Products*	a. Mencantumkan detail kriteria kualitas serta konten dan struktur dari suatu *work product*. b. Mencantumkan detail kebutuhan dokumentasi dan pengendalian perubahan dari suatu *work product*.

No	Komponen	Konten minimal
4.	Record Kualitas *Work Products*	a. Mencantumkan detail dari tindakan-tindakan yang diambil apabila sasaran kinerja suatu proses tidak tercapai. b. Mencantumkan rekam jejak pelaksanaan review atas suatu *work product* atau standar proses. c. Mencantumkan bukti-bukti pelaksanaan review atas suatu *work product* atau standar proses.
5.	Prosedur dan Standar	a. Mencantumkan detail sasaran-saaran organisasional dari proses. b. Mencantumkan standar kerja minimum. c. Mencantumkan standar dari suatu prosedur d. Mencantumkan standar pelaporan dan kebutuhan monitoring e. Mencantumkan pemetaan proses ke prosedur standar f. Mencantumkan detail dari tanggung jawab dan otoritas dari pihak-pihak yang terkait dalam suatu standar proses. g. Mencantumkan detail pengendalian untuk memastikan keamanan informasi diantaranya: 1) Dokumen. 2) Rekaman. 3) Audit internal. 4) Tindakan perbaikan dan pencegahan. 5) Pelabelan, pengamanan, pertukaran & disposal informasi. 6) Pengelolaan *removable media* & *disposal media*. 7) Pemantauan penggunaan fasilitas t&i serta komunikasi. 8) *User access management*. 9) *Teleworking*. 10) Pengendalian instalasi software& hak kekayaan intelektual. 11) Pengelolaan perubahan t&i serta komunikasi. 12) Pengelolaan & pelaporan insiden keamanan informasi.

D. Penggunaan Indeks KAMI 4.1 Sebagai Tools Audit Keamanan Informasi

Pada naskah akademik, mengedepankan tata kelola keamanan informasi dengan mengembangkan kerangka kerja SNI ISO 27001:2013, Octave Allegro, dan COBIT 2019. Untuk mengukur tata kelola keamanan informasi tersebut, dibutuhkan suatu alat yang dapat mendukung kerangka kerja yang telah disusulkan dan diakui proses dan hasil pengukurannya secara legalitas yaitu Indeks KAMI. Indeks KAMI merupakan tools yang dapat digunakan untuk mengevaluasi tingkat kematangan dari suatu instansi dalam melakukan tata kelola keamanan informasi.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya memberikan gambaran indeks kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya sebagaimana ditunjukan pada Gambar 14. Penggunaan hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penyedia dan pengelola sistem elektronik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di instansi pemerintah.



Gambar 14 Indeks KAMI

Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2013, yang disusun kembali menjadi 5 (lima) area diantaranya:

1. Tata Kelola Keamanan Informasi. Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
2. Pengelolaan Risiko Keamanan Informasi. Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
3. Kerangka Kerja Keamanan Informasi. Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
4. Pengelolaan Aset Informasi. Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut; dan
5. Teknologi dan Keamanan Informasi. Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Penyusunan kembali menjadi 5 (lima) komponen ini dilakukan untuk mendapatkan bentuk evaluasi mandiri yang mudah untuk ditanggapi dimana hasil evaluasinya sendiri nanti akan dapat digunakan sebagai panduan pembenahan atau peningkatan kinerja tata kelola keamanan informasi.

Dalam setiap area, proses evaluasi akan membahas sejumlah aspek yang dibutuhkan untuk mencapai tujuan utama dari pengamanan di area tersebut. Setiap aspek tersebut memiliki karakteristik tersendiri terkait dengan pentahapan penerapan pengamanan sesuai dengan standar SNI ISO/IEC 27001:2013. Aspek yang dibahas (disampaikan dalam konteks pertanyaan) terdiri dari bentuk kerangka kerja dasar keamanan informasi, efektivitas dan konsistensi penerapannya, sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi.Bentuk pengamanan terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar SNI ISO/IEC 27001:2013.

Proses penilaian dilakukan melalui 2 (dua) metode yaitu jumlah (kelengkapan) bentuk pengamanan dan tingkat kematangan proses pengelolaan pengamanan informasi. Metode pertama mengevaluasi sejauh mana instansi responden sudah menerapkan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar SNI ISO/IEC 27001:2013, dalam hal

ini kontrol tersebut sudah dikembangkan dengan menggunakan kerangka kerja lain yaitu Octave Allegro dan COBIT 2019. Untuk area evaluasi tersebut diantaranya:

1. Tata Kelola 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 dalam area ini juga adalah adanya program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.
2. Pengelolaan Risiko Keamanan Informasi.

   Bentuk tata kelola yang diperlukan 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 efektifitasnya.
3. Kerangka Kerja Keamanan Informasi.

   Kelengkapan kontrol di area ini memerlukan sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektifitas kontrol dan langkah perbaikan.
4. Pengelolaan Aset Informasi.

   Kontrol yang diperlukan dalam area ini adalah bentuk pengamanan terkait keberadaan aset informasi, termasuk keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut.
5. Teknologi dan Keamanan Informasi.

   Untuk kepentingan Indeks KAMI, aspek pengamanan di area teknologi mensyaratkan adanya strategi yang terkait dengan tingkatan risiko, dan tidak secara eksplisit menyebutkan teknologi atau merk pabrikan tertentu.

Metode yang kedua merupakan perluasan dari evaluasi kelengkapan dan digunakan untuk mengidentifikasi tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT (Control *Objective for Information and related Technology*) yang sebelumnya telah dijabarkan pada Bagian II Naskah Akademik ini. Tingkat kematangan ini nantinya digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di suatu penyelenggara dan pengelolaan sistem elektronik.

Penilaian dengan menggunakan Indeks KAMI berbasis *checklist* sesuai dengan proses kegiatan yang dilakukan suatu instansi dalam melakukan sistem manajemen keamanan informasi. Nilai yang dihasikan menggambarkan kondisi sistem keamanan informasi saat ini. Selanjutnya nilai tersebut akan dibandingan dengan nilai sistem keamanan informasi yang diharapkan atau tingkat kematangan 3. Dengan membandingkan nilai tersebut, akan menghasilkan nilai *gap*. Nilai *gap* ini kemudian digunakan untuk memperbaiki sistem keamanan informasi pada area yang memiliki nilai dibawah nilai ideal berdasarkan tata kelola keamanan informasi yang telah dikembangkan.

BAB V
KESIMPULAN DAN SARAN

A. Kesimpulan

Teknologi informasi (TI) turut berkembang sejalan dengan perkembangan peradaban manusia. Perkembangan teknologi informasi meliputi perkembangan infrastruktur TI, seperti *hardware*, *software*, teknologi penyimpanan data (*storage*), dan teknologi komunikasi. Banyaknya sistem dan teknologi baru yang muncul menuntut Polri mengikuti perkembangan teknologi yang ada. Salah satunya adalah pemanfaatan big data untuk mendukung data yang diperlukan dalam sistem pemerintahan, organisasi maupun perusahaan. Big data adalah aset informasi bervolume tinggi, berkecepatan tinggi, dan beragam yang menuntut bentuk pemrosesan informasi inovatif yang hemat biaya yang memungkinkan peningkatan wawasan, pengambilan keputusan, dan otomatisasi proses. Salah satu implementasi big data pada Kepolisian Negara Republik Indonesia (Polri), yaitu penggunaan data personel Polri melalui Sistem Informasi Personel Polri (SIPP) sebagai rangka penyelenggaraan pembinaan sumber daya manusia Polri yang bersih, transparan, akuntabel dan humanis sebagai sarana pendukung berupa data personel yang akurat, tepat, dan tersedia setiap saat.

Penggunaan data yang memanfaatkan big data memerlukan keamanan informasi dari serangan siber agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab, mengingat pentingnya informasi SIPP yang menjadi rujukan utama mengenai informasi personel Polri. Untuk menjamin kelangsungan keamanan informasi ini, pemerintah telah menetapkan beberapa aturan, salah satunya adalah Peraturan Kementerian Komunikasi No. 4 Tahun 2016 yang mewajibkan sistem elektronik yang bersifat strategis menerapkan keamanan informasi. Pada peraturan ini disebutkan bahwa negara mewajibkan penyelenggara sistem elektronik strategis dan tinggi menerapkan SNI ISO 27001:2013 tentang sistem manajemen keamanan informasi. SSDM Polri saat ini belum menerapkan sistem manajemen keamanan informasi (SMKI) secara komprehensif sehingga ancaman bagi aset-aset informasi organisasi masih memungkinkan untuk terjadi dan dapat mengancam operasional dari institusi. Menindaklanjuti peraturan tersebut, pengembangan ini menghasilkan kerangka kerja tata kelola keamanan informasi berdasarkan SNI ISO 27001:2013, OCTAVE Allegro, dan COBIT 2019 yang khusus dibuat untuk data center pada tiga komponen penting, yaitu sumber daya manusia, proses, dan teknologi. Keluaran penelitian selanjutnya yaitu sistem pendeteksi serangan siber yang

aplikatif melalui sistem keamanan jaringan Honeypots guna mendukung keamanan informasi dan tata kelola keamanan informasi.

Pengembangan, pembangunan, dan implementasi keamanan informasi memerlukan kerangka kerja yang akan menjadi acuan agar implementasi dapat terjadi secara berkesinambungan dan terukur. Tata kelola pemerintahan berbasis SPBE khususnya penyedia sistem elektronik harus menjamin sistem elektronik yang handal dan aman. Pengembangan kerangka kerja SNI ISO 27001:2013 tentang SMKI, Octave Allegro, dan COBIT 2019 merupakan bagian dari sistem manajemen keamanan informasi secara keseluruhan meliputi deteksi, pencegahan, merespon, mengontrol, dan mengevaluasi keamanan informasi berdasarkan pendekatan risiko. Sistem manajemen keamanan informasi mencakup struktur, kebijakan, kegiatan perencanaan, tanggung jawab, praktek, prosedur, proses dan sumber daya organisasi.

Dalam membuat kebijakan keamanan informasi melalui kerangka kerja keamanan informasi dan tata kelola, dibuat suatu sistem memanfaatkan implementasi metode keamanan IPS dan Honeypot. Selanjutnya dilakukan Remastering agar IPS dan Honeypot terkompilasi menjadi suatu Distro Linux baru yang dinamakan Linux Presisi. Linux Presisi merupakan sistem operasi turunan dari Ubuntu, yang dapat digunakan untuk membuat server yang aman. Hal ini dikarenakan Linux Presisi memiliki metode keamanan yang menggabungkan IPS (*Intrusion Prevention System)* dan Honeypot berbasis open source. IPS merupakan kombinasi antara fasilitas *blocking capabilities* dari *Firewall* dan kedalaman inspeksi paket data dari Intrusion Detection System (IDS). Pada saat bekerja, IPS akan membuat akses kontrol dengan cara melihat konten aplikasi sehingga IPS mampu mencegah serangan yang datang dengan bantuan administrator dan akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori. Pada pengembangan ini, *firewall* yang diterapkan merupakan *firewall software* dengan menggunakan iptables, Kemudian, pada IDS menggunakan tools snort.

B. Saran

Berdasarkan analisa atas kondisi yang ada serta mengantisipasi kebutuhan saat ini dan masa mendatang, maka disarankan untuk melakukan implementasi pengembangan sistem keamanan Linux Presisi dan tata kelola keamanan informasi pada SSDM Polri mengingat organisasi belum memiliki dan menerapkan manajemen keamanan informasi secara komprehensif. Selanjutnya organisasi perlu melakukan evaluasi, monitoring, dan koordinasi terhadap rencana pengembangan yang telah ditetapkan. Hal ini sebagai tindakan korektif dari kontrol yang dibuat

apakah dapat meminimalisir risiko dan serangan yang dapat terjadi pada Big Data Polri yang mengancam operasional dari organisasi.

DAFTAR PUSTAKA

Andrianti, Ari dan Lola Yorita Astri. 2020. Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses DSS05 (Studi Pada RS Bhayangkara Jambi). *Indonesian Journal of Computer Science* ISSN 2302-4364 Vol. 9, No. 2, Edisi Oktober 2020.

Arman, N., Putra, W., & Rachmadi, A. Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 3, no. 6, p. 5750-5755, juli 2019. ISSN 2548-964X.

B. Kelley, M. (21 November 2013): *Stuxnet Was Far More Dangerous Than Previous Thought*, Available on https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?r=US&IR=T. Accessed on May 1, 2021.

Baykara, Muhammet & Das, Resul. (2018). A novel honeypot based security approach for real-time intrusion detection and prevention systems. Journal of Information Security and Applications. 41. 103-116. 10.1016/j.jisa.2018.06.004.

C. Moore, "Detecting Ransomware with Honeypot Techniques," 2016 Cybersecurity and Cyberforensics Conference (CCC), 2016, pp. 77-81, doi: 10.1109/CCC.2016.14.

Cannon, D., Bergmann, T., & Pamplin, B. 2006. Certified Information System Auditor Study Guide. Indianapolis: Wiley Publishing.

Caralli, R. A., Stevens, J. F., Young, L. R., dan Wilson, W. R. (2007): Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process: Defense Technical Information Center, Fort Belvoir, VA. https://doi.org/10.21236/ADA470450.

Chazar, C., dan Ramdhani, M. A. (2016): Model Perencanaan Keamanan Sistem Informasi Menggunakan Pendekatan Metode Octave dan ISO 27001:2005, 6.

Disterer, G. (2013): ISO/IEC 27000, 27001 and 27002 *for Information Security Management, Journal of Information Security*, 04(02), 92–100. https://doi.org/10.4236/jis.2013.42011.

Elky, S. (2007): An Introduction to Information System Risk Management, 18.

Glossary, G. (2007): Definition of Big Data - Gartner Information Technology Glossary. Available on https://www.gartner.com/en/information-technology/glossary/big-data. Accessed on 27 April 2021.

Gunawan, C.; Fenando, F. Pengukuran Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Studi Kasus Di PUSTIPD UIN Raden Fatah Palembang. JUSIFO (Jurnal Sistem Informasi) 2018, 4, 121-132.

Hafiz, Aliy. 2020. 14 Perangkat Keamanan Teknologi Informasi. Available on https://aliyhafiz.com/perangkat-keamanan-komputer-teknologi-informasi/. Accessed on April 25, 2021.

Haryatmoko (2020): Jalan Baru Kepemimpinan & Pendidikan: Jawaban atas Tantangan Disrupsi-Inovatif, PT. Gramedia Pustaka Utama, Jakarta.

Humaira (2012): *Comparison of Information Security Risk Evaluation Methodology of Octave-S and Octave Allegro*, Seminar Nasional Inovasi dan Teknologi (SNIT) 2012, Available on http://seminar.bsi.ac.id/snit/index.php/snit-2012/article/view/273/269, Hal. A-116.

Husnan, S. (2013): Implementasi Honeypot Untuk Meningkatkan Sistem Keamanan Server Dari Aktivitas Serangan.

International Telecommunication Union (ITU) (2017): Guide To Developing A National Cybersecurity Strategy.

Iwan. 2012: Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber, Tesis Universitas Pertahanan Indonesia, Jakarta.

ISACA. 2018. COBIT 2019: COBIT 2019 *Framework Introduction and Methodology*.

Kasma V. S, S. Sutikno and K. Surendro, "*Design of e-Government Security Governance System Using* COBIT 2019 : (*Trial Implementation* in Badan XYZ)," *2019 International Conference on ICT for Smart Society (ICISS)*, 2019, pp. 1-6, doi: 10.1109/ICISS48059.2019.8969808.

Keputusan Kepala Kepolisian Negara Republik Indonesia Nomor: Kep/88/I/2016, tentang Master Plan Teknologi Informasi Polri Tahun 2015-2019.

Lestari, R. (2013): Pengaruh Manajemen Risiko Terhadap Kinerja Organisasi, 13, 19.

Laudon, K. C., dan Laudon, J. P. (2012): *Management information systems: managing the digital firm* (12th), Prentice Hall, Boston.

Nasution, R. D. (2021): Pengaruh Modernisasi dan Globalisasi Terhadap Perubahan Sosial Budaya di Indonesia, 14.

Nachrowi, E., Yani Nurhadryani, & Heru Sukoco. (2020). *Evaluation of Governance and Management of Information Technology Services Using* Cobit 2019 and ITIL 4 . Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(4), 764 - 774.

Nugroho, F. P., Abdullah, R. W., dan Wulandari, S. (2019): Keamanan Big Data Di Era Digital Di Indonesia, 5, 7.

Nugroho, Haries Anom Suseyto Aji dan Wing Wahyu Winarno Sudarmawan. 2018. Jurnal Transformasi Informasi dan Pengembangan IPTEK Vol 14 No 2. ISSN 1978-5569.

Pradipta, Y. W. (2017): Implementasi *Intrusion Prevention System* (IPS) Menggunakan Snort dan IP Tables Berbasis Linux, 7, 8.

Prananda, Eriestu Rizqi, Kusprasapta Mutjiarsa. 2021. Perancangan Rekomendasi Kontrol Keamanan Informasi Berbasis Manajemen Risiko Keamanan Informasi Menggunakan Octave Allegro Dan SNI ISO 27001:2013 (Studi Kasus: Organisasi Staf Sumber Daya Manusia Polri). Thesis ITB. Bandung.

Rahayu, Intan. 2020. Regulasi Keamanan Informasi Dan Sosialisasi Indeks Keamanan Informasi (Indeks KAMI). Webinar BSSN. BSSN.

Rahmat, D. (2019). Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar SNI ISO/IEC 27001: 2013. COMPUTING Jurnal Informatika, 6(2), 37-41.

Rahmawati, I. (2017): Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense, 16.

Ritzkal, Ritzkal, et al. 2016. Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) Pada Fakultas Teknik Uika-Bogor. Prosiding Seminar Nasional Sains dan Teknologi. ISSN 2407-1846.

Riyantarno Sarno. 2009. Audit Sistem & Teknologi Informasi. Surabaya: ITS Press, 2009. 215.

Sarno, R. 2009. Sistem Manajemen Keamanan Informasi Berbasis ISO 27001. Surabaya ITS Press.

SNI ISO/IEC 27001:2013. Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan. Badan Standardisasi Nasional.

Shameli-Sendi, A., Aghababaei-Barzegar, R., dan Cheriet, M. (2016): *Taxonomy Of Information Security Risk Assessment* (ISRA), Computers & Security, 57, 14–30. https://doi.org/10.1016/j.cose.2015.11.001.

Sumarno, I. (2015): Solusi Network Security Dari Ancaman SQL Injection Dan Denial Of Service (DOS), 5, 12.

Sumarno, Sumarno. 2017. Solusi Network Security Dari Ancaman Sql Injection Dan Denial Of Service (Dos). TEKNOLOJIA, 5 (1). pp. 19-30. ISSN 1907-0802.

Suroso, Jarot S, Muhammad A. Fakhrozi. 2018. *Assessment of Information System Risk Management with Octave Allegro at Education Institution*, *Procedia Computer Science*, Volume 135, 2018, Pages 202-213, ISSN 1877-0509.

Susanto, H., Almunawar, M. N., dan Tuan, Y. C. (2011): *Information Security Management System Standards: A Comparative Study of the Big Five*, 11(05), 8.

Spitzner, L. (2003): *Honeypots: Simple, Cost-Effective Detection*, Available on https://community.broadcom.com/symantecenterprise/communities/communityhome/librarydocuments/viewdocument?DocumentKey=187c8f0570934ec1bf1bade562a2068b

&CommunityKey=1ecf5f55-9545-44d6-b0f44e4a7f5f5e68&tab=librarydocuments. Accessed on 1 Mei 2021

Spiztner, L. (2003): *Definitions and Value of Honeypots* | EE Times, diperoleh 27 April 2021, melalui situs internet: https://www.eetimes.com/definitions-and-value-of-honeypots/.

Wagiu, E. B., Siregar, R., & Maulany, R. 2019. Information System Security Risk Management Analysis in Universitas Advent Indonesia Using Octave Allegro Method. Abstract Proceedings International Scholars Conference, 7(1), 1741-1750.

Whitman, M. E., dan Mattord, H. J. (2012): P*rinciples of information security (4th ed), Course Technology, Boston,* MA, 617.

Whitman, M. E., dan Mattord, H. J. (2013): *Management of Information Security*, 594.

Wijatmoko, Taufiq Effendy. Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Kementerian Hukum dan HAM DIY. Cyber Security Dan Forensik Digital 3, No. 1 (July 23, 2020): 1–6.