ANALISIS DAN PENERAPAN MANAJEMEN RISIKO APLIKASI PEMANTAUAN SERTA SISTEM MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN

SNI ISO/IEC 27001:2013

(Studi Kasus: KPID Jawa Barat)

Topan Nurdiansyah, M. Hendayun
Program Studi Magister Teknik Informatika
Pascasarjana Universitas Langlangbuana
jurnalpascaunla@gmail.com

ABSTRACT

In the success of the Electronic-Based Government System and Information Security Management System (SMKI), the West Java KPID must participate in it. West Java KPID has a monitoring application that functions to process recorded data and produce findings of violations of broadcast content in television broadcasts. In the monitoring application, there are national TV broadcasts that have networked main stations and local TV broadcasts. The monitoring application can only monitor television because there is a TV tuner that can make a computer capable of processing television signals and then recording them into and into the database and recording 24 hours of television viewing. Given the importance of information and the high risk of interference, the West Java KPID needs to carry out information security governance activities in the environment, especially in monitoring applications because there is data recording the contents of television broadcasts. There are frequent bugs and crashes in monitoring applications due to loss of voltage and not having a temporary power supply. The need for LAN network security to minimize the threat of attacks on monitoring applications. Risk assessment is needed to maintain the aspects of Confidentiality, Integrity, and availability and develop controls to minimize threats. This study carries out risk management monitoring applications using SNI ISO/IEC 27005: 2013 and carries out risk assessment controls based on SNI ISO/IEC 27001: 2013.

The steps taken are identification of information assets, threats, vulnerabilities, risks, impacts and clause mapping based on risk assessment. Then do a maturity level analysis, gap analysis, recommendation of control objectives and information security. So that this study resulted in a risk assessment, proposed mapping of control and control objectives based on SNI ISO/IEC 27001: 2013, the level of maturity of information security, findings and recommendations.

ABSTRAK

Didalam menyukseskan Sistem Pemerintah Berbasis Elektronik dan Sistem Manajemen Keamanan Informasi (SMKI), KPID Jabar harus ikut serta didalamnya. KPID Jabar memiliki aplikasi pemantauan yang berfungsi untuk mengolah data hasil rekaman dan menghasilkan temuan pelanggaran isi siaran didalam siaran televisi. Didalam aplikasi pemantauan terdapat siaran TV nasional yang memiliki induk stasiun berjaringan dan siaran TV lokal. Aplikasi pemantauan hanya bisa memantau televisi karena adanya alat bantu (TV tunner) yang bisa membuat komputer mampu memproses sinyal televisi lalu direkam kedalam dan masuk kedalam database serta proses merekam

selama 24 jam tayangan televisi. Mengingat pentingnya informasi dan tingginya kemungkinan risiko terjadi gangguan, KPID Jawa Barat perlu untuk melakukan kegiatan tata kelola keamanan informasi dilingkungan terutama pada aplikasi pemantauan karena terdapat data rekaman isi siaran televisi. Sering terjadi bugs dan crash pada aplikasi pemantauan yang disebabkan hilangnya voltase listrik dan belum memiliki penampung daya listrik sementara. Perlunya pengamanan jaringan LAN untuk meminimalisir ancaman terjadinya serangan pada aplikasi pemantauan. Dibutuhkan penilaian risiko untuk menjaga aspek Kerahasiaan (confidentiality), keutuhan (Integrity), dan ketersediaan (availability) serta menyusun kendali untuk meminimalisir terjadinya ancaman. Penelitian ini melakukan manajemen risiko aplikasi pemantauan menggunakan SNI ISO/IEC 27005: 2013 dan melakukan pengendalian penilaian risiko berdasarkan SNI ISO/IEC 27001: 2013.

Langkah yang dilakukan adalah identifikasi aset informasi, ancaman, kerentanan, risiko, dampak dan pemetaan klausul berdasarkan penilaian risiko. Lalu melakukan analisis maturity level, gap analisis, rekomendasi objektif kontrol dan keamanan informasi. Sehingga penelitian ini menghasilkan penilaian risiko, usulan pemetaan objektif kontrol dan kontrol berdasarkan SNI ISO/IEC 27001: 2013, tingkat kematangan kemanan informasi, temuan dan rekomendasi.

Kata Kunci : Aplikasi Pemantauan, Manajemen Risiko, SMKI, SNI ISO/IEC 27005: 2013, ISO/IEC 27001: 2013.

I. PENDAHULUAN

Komisi Penyiaran Indonesia (disingkat KPI) adalah sebuah lembaga independen di Indonesia yang kedudukannya setingkat dengan lembaga negara lainnya yang berfungsi sebagai regulator penyelenggaraan penyiaran di Indonesia. Komisi ini lahir atas amanat Undang-undang Nomor 32 Tahun 2002, terdiri atas KPI Pusat dan KPI Daerah (tingkat Provinsi). Anggota KPI Pusat (9 orang) dipilih oleh Dewan Perwakilan Rakyat dan KPI Daerah (7 orang) dipilih oleh Dewan Perwakilan Rakyat Daerah. Selain itu, anggaran program kerja KPI Pusat dibiayai oleh APBN (Anggaran Pendapatan Belanja Nasional) dan KPI Daerah dibiayai oleh APBD (Anggaran Pendapatan Belanja Daerah).

KPI dan KPID merupakan wujud peran serta masyarakat berfungsi mewadahi aspirasi serta mewakili kepentingan masyarakat akan penyiaran harus mengembangkan program-program kerja hingga akhir kerja dengan selalu memperhatikan tujuan yang diamanatkan Undang-undang nomor 32 tahun 2002 Pasal 3:

"Penyiaran diselenggarakan dengan tujuan untuk memperkukuh integritas nasional, terbinanya watak dan jati diri bangsa yang beriman dan bertaqwa, mencerdaskan kehidupan bangsa, memajukan kesejahteraan umum, dalam rangka membangun masyarakat yang mandiri, demokratis, adil dan sejahtera, serta menumbuhkan industri penyiaran Indonesia"

KPID Jawa Barat sendiri mulai berdiri pada bulan Oktober 2004. Keberadaannya diharapkan dapat mewadahi aspirasi dan mewakili kepentingan masyarakat di Jawa Barat di bidang penyiaran. Fungsi ini sejalan dengan azas pokok KPID sebagai lembaga yang bersifat independen, yang memastikan masyarakat untuk dapat menerima konten siaran yang sehat dan positif.

Gambar 1 Jumlah Lembaga Penyiaran di Jawa Barat Tahun 2021

Kemajuan teknologi informasi dan komunikasi yang ada saat ini menyadarkan banyak orang betapa besar manfaatnya bila diterapkan dalam hal peningkatan kualitas dan kuantitas pelayanan publik. Berkembangnya teknologi informasi dalam masa saat ini begitu cepat, sehingga tidak terelakan akan membawa dampak perubahan. Tidak terkecuali sektor pemerintahan yang akan terkena dampaknya dalam menjalankan roda pemerintahan dan kepentingan masyarakat dengan menerapkan teknologi informasi. Pengembangan teknologi informasi membutuhkan perencanaan yang baik. Berdasarkan Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *e-Government*, penyelenggaran pemerintahan didorong untuk menggunakan sistem elektronik dalam setiap layanan dan kegiatan. Selain itu, adanya Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, ditujukan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya. Tata kelola dan manajemen sistem pemerintahan berbasis elektronik secara nasional juga diperlukan untuk meningkatkan keterpaduan dan efisiensi sistem pemerintahan berbasis elektronik.

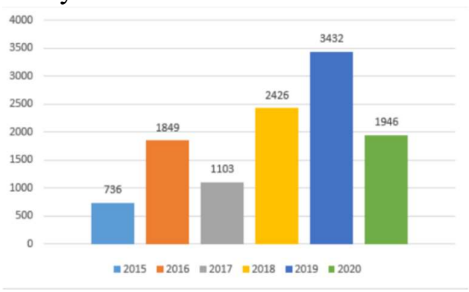
Pemerintah menyadari pentingnya peran SPBE untuk mendukung semua sektor pembangunan. Upaya untuk mendorong penerapan SPBE telah dilakukan oleh pemerintah dengan menerbitkan peraturan perundang-undangan sektoral yang mengamanatkan perlunya penyelenggaraan sistem informasi atau SPBE. Sejauh ini kementerian, lembaga, dan pemerintah daerah telah melaksanakan SPBE secara sendiri-sendiri sesuai dengan kapasitasnya, dan mencapai tingkat kemajuan SPBE yang sangat bervariasi secara nasional. Untuk membangun sinergi penerapan SPBE yang berkekuatan hukum antara kementerian, lembaga, dan pemerintah daerah, diperlukan Rencana Induk SPBE Nasional yang digunakan sebagai pedoman bagi Instansi Pusat dan Pemerintah Daerah untuk mencapai SPBE yang terpadu.

Tidak dipungkiri, seiring nya perkembangan teknologi informasi semakin rentannya celah kejahatan maka perlunya keamanan sistem informasi. Pemerintah Indonesia telah mengeluarkan kebijakan terkait dengan *system* manajemen keamanan informasi melalui Peraturan Menteri Kominfo No. 4 Tahun 2016 yang mengatur tentang Sistem Manajemen Pengamanan Informasi bagi penyelenggara sistem elektronik yang terdiri dari Institusi penyelenggara negara, korporasi, lembaga independen dan badan hukum lain yang bergerak dalam ranah pelayanan publik berdasarkan asas risiko. Peraturan ini juga mengatur penyelenggara sistem elektronik yang menyelenggarakan sistem elektronik strategis, harus segera tersertifikasi SNI ISO/IEC 27001. Begitu pula dengan penyelenggara yang menyelenggarakan sistem elektronik tinggi, juga harus segera menerapkan standar SNI ISO/IEC 27001. Peraturan lainnya terdapat pada Permen Kominfo No 4 tahun 2016 pasal 3 (c), Peraturan Pemerintah Republik Indonesia No 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik pasal 24 ayat (2), serta ayat (4), menyambung pasal tersebut, peraturan Badan Siber dan Sandi Negara tentang Sistem Pengamanan dalam

Penyelenggaraan Sistem Elektronik pada pasal 9 ayat 1, 2 dan 3.

Dengan adanya peraturan tersebut, Komisi Penyiaran Indonesia Daerah (KPID) Jawa Barat dituntut untuk melakukan penerapan Sistem Manajemen Pengamanan Informasi. Salah satu standar yang dapat digunakan untuk menganalisa tingkat keamanan informasi di KPID Jawa Barat adalah standar ISO/IEC 27001 sesuai dengan insiden yang banyak terjadi.

Didalam menyukseskan Sistem Pemerintah Berbasis Elektronik dan Sistem Manajemen Pengamanan Informasi, KPID Jawa Barat harus ikut serta didalamnya. KPID Jawa Barat memiliki aplikasi pemantauan yang berfungsi untuk mengolah data hasil rekaman dan menghasilkan temuan pelanggaran isi siaran didalam siaran televisi. Didalam aplikasi pemantauan terdapat siaran TV nasional yang memiliki stasiun induk berjaringan serta siaran TV lokal. Aplikasi pemantauan hanya bisa memantau televisi karena adanya alat bantu (TV *tunner*) yang bisa membuat komputer mampu memproses sinyal televisi lalu direkam kedalam dan masuk kedalam *database* serta proses merekam selama 24 jam tayangan televisi. Sedangkan untuk memantau radio masih dilakukan secara manual karena belum adanya alat seperti alat bantu (seperti tv *tunner*) dan belum terekam kedalam *database* serta dilakukan secara *realtime* untuk memantau. Didalam memantau radio, masih didalam area Bandung Raya saja karena frekuensi yang dapat ditangkap dengan alat radio dan belum adanya infrastruktur untuk menangkap frekuensi radio se Jawa Barat. Oleh karena itu, KPID Jawa Barat melakukan penertiban siaran kepada lembaga siaran meminta hasil rekaman selama sebulan dan mengirimkan rekaman siaran kepada KPID Jawa Barat. KPID Jawa Barat dibantu 4 tenaga pemantau dan 2 asisten dalam memantau isi siaran televisi dan radio se Jawa Barat. Selain memantau, KPID Jawa Barat menerima aduan masyarakat terhadap isi siaran melalui media sosial dan website KPID Jawa Barat.



Gambar 2 Data Jumlah Temuan Pelanggaran Tahun 2015 – 2020

Mengingat pentingnya informasi dan tingginya kemungkinan risiko terjadi gangguan, KPID Jawa Barat perlu untuk melakukan kegiatan tata kelola keamanan informasi dilingkungan terutama pada aplikasi pemantauan karena terdapat data rekaman isi siaran televisi. Sering terjadi *bugs* dan *crash* pada aplikasi pemantauan yang disebabkan hilangnya voltase listrik dan belum memiliki penampung daya listrik sementara. Belum adanya pelatihan keamanan informasi dan pegawai khusus untuk merawat server. Selain itu, adanya temuan perangkat fisik yang tidak terawat sehingga bisa terjadi kerusakan pada peralatan. Perlunya pengamanan jaringan LAN untuk meminimalisir ancaman terjadinya serangan pada aplikasi pemantauan. Dibutuhkan penilaian risiko untuk menjaga aspek Kerahasiaan *(confidentiality),* keutuhan *(Integrity),* dan ketersediaan *(availability)* serta menyusun kendali untuk meminimalisir terjadinya ancaman. Peneliti melakukan manajemen risiko aplikasi pemantauan menggunakan SNI ISO/IEC 27005: 2013 dan melakukan pengendalian penilaian risiko berdasarkan SNI ISO/IEC 27001: 2013. Diharapkan dapat mengamankan aset-aset yang terdapat di lingkungan aplikasi pemanataun KPID Jawa Barat. Kondisi saat ini KPID Jawa Barat belum melaksanakan

kegiatan Sistem Manajemen Keamanan Informasi.

II. PENELITIAN TERKAIT

Pada bagian ini, berisi literatur penelitian sebelumnya yang terkait dengan peneliti ini, diantaranya adalah sebagai berikut:

A. Sitta Rif'atul Musyaroh, Rahardian Bisma (2021) dalam penelitian ini menggunakan ISO/IEC 27001:2013 dan melakukan gap analisis. Penelitian ini bertujuan untuk mengetahui kondisi sistem keamanan informasi terkini dan bagaiamana kesiapan Diskominfo Kota Madiun untuk mencapai sertifikasi ISO/IEC 27001:2013. Kuesioner yang digunakan peneliti yaitu berupa *checklist* berdasarkan toolkit ISO/IEC 27001 dari CertiKit. hasil analisis kesenjangan yang dilakukan secara menyeluruh terhadap persyaratan-persyaratan ISO/IEC 27001:2013, yaitu Diskominfo Pemerintah Kota Madiun memiliki kesiapan untuk melakukan sertifikasi ISO/IEC 27001:2013 sebesar 71%.

B. Ito Setiawan, Aldistya Riesta Sekarini, Retno Waluyo, Fiby Nur Afiana (2021), Penelitian ini menggunakan ISO 3100:2018 dan standar pengendalian menggunakan ISO 27001:2013. Tujuan penelitian adalah mengetahui risiko dan juga dampak dari penggunaan sistem informasi di Tripio Purwokerto. Melakukan Kegiatan monitoring dan review dengan mengadakan pertemuan dengan topik bahasan penerapan teknologi informasi untuk membahas kendala-kendala atau kemungkinan risiko yang akan mengganggu proses bisnis organisasi dan membahas pencegahan agar dapat meminimalisir risiko yang akan terjadi dikemudian hari. Dari hasil penelitian yang telah dilakukan dapat ditarik kesimpulan bahwa terdapat 15 risiko yang terdiri dari 6 risiko dengan tingkat risiko *high*, 7 risiko dengan tingkat risiko medium, dan 2 risiko dengan tingkat risiko *low*. Rekomendasi kontrol yang digunakan mengacu pada ISO 27001:2013.

C. Dadan Rahmat (2019) dalam penelitian ini menggunakan siklus *Plan-Do-Check-Act* pada SNI ISO/IEC 27001 dan manajemen risiko menggunakan SNI ISO/IEC 27005. Penelitian ini bertujuan untuk mengetahui Perencanaan Sistem Manajemen Keamanan Informasi (SMKI) menggunakan Standar SNI ISO/IEC 27001:2013 di Universitas Muhammadiyah Sukabumi. Hasil dari penelitian ini adalah Universitas Muhammadiyah telah melakukan dokumentasi terhadap kebijakan dan keamanan informasi untuk menanggulangi insiden pihak luar, tetapi pencatatan tersebut belum mencakup penerapan Kontrol Keamanan Informasi organisasi. Pembuatan SMKI menghasilkan 2 (dua) dokumen, yaitu dokumen yang meliputi kebijakan, penilaian risiko, ruang lingkup, dan *Statement Of Applicability* (SOA) serta dokumen 2 (dua) yang berisi prosedur keamanan informasi.

D. Hikam Haikal Radya Hans Ananza, Irfan Darmawan, Rahmat Mulyana (2019) berfokus pada evaluasi kondisi tata kelola keamanan informasi pada saat ini dan merekomendasikan pengelolaan tata kelola keamanan informasi agar dapat menjadi lebih baik. Alat yang digunakan untuk mengevaluasi dan merekomendasikan adalah standar ISO 27001:2013. Penelitian ini bertujuan untuk membantu Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat dalam menghadapi regulasi yang perlu dipatuhi terutama dalam bidang pengelolaan keamanan informasi serta untuk

mengetahui dan meminimalkan risiko-risiko keamanan informasi yang ada pada dinas tersebut, dilakukan penggunaan standar ISO 27001:2013. Proses yang dilakukan adalah menganalisis kesenjangan terhadap ISO 27001:2013, memetakan kesenjangan tersebut kepada risiko, menganalisis risiko tersebut, memprioritaskan risiko, dan memberikan rekomendasi sesuai dengan risiko terkait. Rekomendasi yang dihasilkan berupa kontrol personel, kontrol proses, dan kontrol teknologi. Kontrol personel akan menghasilkan pembagian tugas, fungsi, dan kompetensi. Kontrol proses menghasilkan kebijakan keamanan informasi dan *Standard Operating Procedure* (SOP). Kontrol teknologi menghasilkan penggunaan aplikasi untuk mempermudah pekerjaan yang sudah ada. Ketiga control tersebut disusun untuk menangani risiko keamanan informasi dan meningkatkan kualitas tata kelola keamanan informasi.

E. Darma Yanto Putra , Theresia Wati, I Wayan Widi P (2020) dalam penelitian ini menggunakan ISO/IEC 27001:2013 dan menggunakan pengukuran tingkat kematangan *System Security Engineering Maturity Level* (SSE–CMM). Penelitian bertujuan untuk memberikan rekomendasi dan melakukan audit untuk memberikan hasil yang menggambarkan seberapa besar penilaian yang didapat oleh organisasi, kemudian akan memberikan rekomendasi yang tentu saja di analisis terlebih dahulu dari berbagai sumber. Hasil penelitian ini adalah tingkat kematangan ISO 27001 dengan rata – rata berada di level dua, diharapkan penelitian ini sangat membantu memberikan rekomendasi terhadap kontrol keamanan informasi sebagai pedoman dan prosedur untuk menerapkan kebijakan keamanan informasi.

Pada penelitian ini, peneliti membuat peringkat urutan ancaman hasil dari ukuran risiko, melakukan penilaian risiko menggunakan kerangka kerja SNI ISO/IEC 27005:2013 selanjutnya melakukan rencana pemetaan kontrol dengan kerangka kerja SNI ISO/IEC 27001:2013, melakukan *maturity level* menggunakan metode SSE – CMM, melakukan analisis gap serta menghasilkan Rekomendasi Objektif Kontrol dan Keamanan Informasi SNI ISO/IEC 27001.

III. METODE PENELITIAN

A. Keamanan Informasi

Sebelum Definisi Keamanan Informasi menurut (ISO 27001) dalam (Sarno dan Iffano, 2009: 27) adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis

Definisi lain keamanan informasi menurut (SMKI dalam Sarno dan iffano, 2009:45) adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Maka keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, mengoftimalkan pengembalian investasi (*return on investment*).

Bahwa ini berarti Kemanan informasi berkaitan upaya perlindungan atau mengamankan aset yang berharga terhadap kehilangan, pengungkapan penyalahgunaan, atau kerusakan yang mungkin terjadi upaya dalam menjamin kelangsungan bisnis (*business continuity*), meminimalkan risiko bisnis (*reduce business risk*) dan

memaksimalkan pengembalian investasi dan peluang.

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dari seoluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimasi risiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis dalam sebuah organisasi. Jenis-jenis keamanan informasi dapat dibagi menjadi beberapa bagian sebagai berikut :

1. Keamanan Fisik (*Physical Security*) Merupakan strategi untuk mengamankan individu atau anggota organisasi, aset fisik dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi dan bencana alam yang terjadi.
2. Keamanan Pribadi (*Personal Security*) Merupakan bagian dari keamanan fisik yang berhubungana dengan melindungi personil/SDM pada organisasi yang memiliki akses terhadap informasi yang biasanya saling berhubungan dengan ruang lingkup *Phisical security*.
3. Keamanan Operasional (*Operation Security*) Keamanan Informasi Fokus yang membahas bagaimana strategi untuk mengamankan kemampuan organisasi untuk beroperasi tanpa ada gangguan.
4. Keamanan Komunikasi (*Communication Security*) Bertujuan mengamankan media komunikasi, teknologi komunikasi beserta isinya, serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. Keamanan Jaringan (*Network Security*) Fokus pada pengamatan peralatan jaringan data organisasi, jaringan beserta isinya, serta kemampuan untuk menggunakan jaringan dalam memenuhi fungsi komunikasi data organisasi.

B. Karakteristik Keamanan Informasi

Keamanan informasi juga memiliki 3 karakteristik penting yang disebut dengan singkatan CIA yaitu :

1. *Confidentiality*/ kerahasiaan: merupakan landasan utama dalam setiap kebijakan keamanan sistem informasi, yaitu seperangkat aturan yang diberikan, menentukan apakah suatu subjek tertentu dapat mendapatkan akses ke objek tertentu. Memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.
2. *Integrity*/ kepercayaan: merupakan kepercayaan terhadap sebuah informasi yang ada. Keaslian informasi dapat terwujud jika informasi belum dirubah perubahan perubahan terjadi karena kesalahan secara sengaja maupun tidak.
3. *Availability*/ ketersediaan: merupakan ketersediaan sumber informasi ketika dibutuhkan. Ketersediaan ini dapat terpengaruh oleh faktor teknis, faktor alam, dan faktor manusia.

Ketiga karakteristik diatas saling berkaitan dan harus dipenuhi untuk menjaga keamanan informasi. Salah satu dukungan keamanan informasi adalah dengan adanya tata kelola keamanan informasi agar risiko keamanan informasi dapat dikurangi atau dihindari.

C. Sistem Manajemen Keamanan Informasi

Pengertian Sistem manajemen keamanan informasi (SMKI) atau information security management system (ISMS). (SMKI dalam sarno dan iffano, 2009:46) 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 keamnan informasi perusahaan. Keamanan Informasi ditujukan untuk menjaga aspek kerahasiaan, keutuhan, dan ketersediaan dari informasi

Sistem manajemen keamanan informasi yang diterapkan perusahaan atau instansi adalah dalam upaya mengamankan aset informasi terhadap ancaman yang mungkin terjadi. Oleh sebab itu, kemanan informasi secara tidak langsung menjamin kelangsungan bisnis perusahaan.

Sistem manajemen keamanan informasi menjadi penting diterapkan agar informasi yang beredar di perusahaan dapat dikelola dengan benar sehingga perusahaan dapat mengambil keputusan berdasarkan informasi yang ada dengan benar pula dalam rangka memberikan layanan yang terbaik kepada pelanggan. Tujuan dari SMKI sendiri adalah untuk meminimalisir risiko dan menjamin kelangsungan bisnis secara proaktif untuk membatasi dampak dari pelanggaran keamanan, dan keamanan informasi ditujukan yaitu untuk menjaga aspek Kerahasiaan (confidentiality), keutuhan (Integrity), dan ketersediaan (availability) dari informasi.

Sistem Manajemen Keamanan Informasi juga harus mengacu pada standar nasional atau internasional yang ada agar kualitas pengamanan yang diberikan tinggi dan mampu menanggulangi adanya masalah. Standar internasional yang telah direkomendasikan untuk penerapan SMKI adalah SNI ISO/IEC 27001:2013. Standar berjalan berbasis risiko sehingga mampu mengurangi ancaman dan menanggulangi masalah dengan cepat dan tepat. Dimana Implementasi dari SMKI ini meliputi kebijakan, proses, prosedur, struktur organisasi, serta fungsi dari software dan hardware.

Indonesia sendiri melalui BSN (Badan Standar Nasioanal) kenapa mengadopsi pada standar ISO karena indonesia merupakan satu anggota bahkan menjadi anggota Dewan sehingga memiliki peran aktif dan penting dalam organisasi internasional tersebut, sehingga dengan demikian indonesia harus menjalankan kebijakan dan standar yang diterbitkan oleh ISO.

D. SNI ISO/IEC 27001 : 2013

ISO (*International Organization for Standardization*) adalah pengembang terbesar di dunia standar international secara sukarela. Standar international memberikan keamanan yang lebih spesifik, layanan yang baik, membantu industri lebih efisien dan efektif. ISO/IEC 27001 merupakan standar keamanan informasi yang diterbitkan pada bulan Oktober 2005 oleh ISO dan IEC (*The International Electrotechnical Commission*). implementasi ISO/IEC 27001 mencakup pada semua organisasi seperti perusahaan swasta, lembaga, pemerintahan dan lembaga nirlaba. ISO/IEC 27001 adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi atau *Information Security Management System*, biasa disebut ISMS, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahan dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi diperusahan berdasarkan "*best practise*" dalam pengamanan informasi. Standar ini menjelaskan syarat untuk membuat, menerapkan, memonitor, menganalisa dan memelihara serta mendokumentasikan SMKI dalam kontek risiko keamanan informasi organisasi keseluruhan. Standar ini menjelaskan pula bagaimana mendidkripsikan menetapkan, mengimplementasikan, mengoprasikan,

mengamati, meninjau memelihara dan mengembangkan sistem.

ISO/IEC 27001 mendefinisikan pula keperluan untuk SMKI, sehingga SMKI yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari risiko dan kegagalan pengamanan sistem informasi, serta memberikan jaminan pemulihan operasi bisnis akibat kerugian yang timbulkan. ISO/IEC 27001 diterapkan tidak selalu harus digunakan dari keseluruhan kontrol melainkan disesuaikan dengan kebutuhan kontrol dari organisasi masing-masing.

E. SNI ISO/IEC 27005 : 2013

Standar ini memberikan pedoman untuk Manajemen Risiko Keamanan Informasi dalam suatu organisasi, mendukung khususnya persyaratan Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan ISO/lEC 27001. untuk membantu pelaksanaan yang memuaskan dari keamanan informasi berdasarkan pendekatan manajemen risiko. Standar ini berlaku pada semua jenis organisasi (misalnya perusahaan komersial, instansi pemerintah, organisasi non-profit) yang berniat untuk mengelola risiko yang dapat membahayakan keamanan informasi organisasi.

F. Manajemen Risiko

Adalah proses untuk mengidentifikasi risiko, menganalisa risiko, dan melakukan penanganan untuk mengurangi risiko sampai dampaknya terhadap prosesbisnis di organisasi pada level yang diterima atau diperbolehkan.

Pengelolaan risiko adalah suatu aktivitas organisasi yang terkoordinasi yang mengarahkan dan mengontrol organisasi untuk menghadapi suatu risiko yang berhubungan dengan proses bisnisnya. Secara garis besarnya organisasi harus memahami: risiko apa yang dihadapi yang hubunganya dengan keamanan informasi, kelemahan dan ancaman terhadap informasi, cara terbaik untuk menghadapi risiko, dan menentukan kontrolkontrol keamanan yeng berhubungan dengan risiko yang timbul.

Hubungan dengan membangun SMKI adalah pelaksanaan manajemen risiko meliputi langkah-langkah:

- Melakukan inventarisasi aset
- Melakukan penilain risiko
- Cara penanganan risiko

G. Penilaian Risiko

Penilaian risiko mengukur atau menggambarkan secara kualitatif suatu risiko dan memungkinkan manajer untuk memprioritaskan risiko sesuai dengan keseriusan yang mereka rasakan atau kriteria lain yang telah ditetapkan. Penilaian risiko memuat kegiatan-kegiatan berikut:

1. Analisis risiko yang terdiri dari:
   - Identifikasi risiko
   - Estimasi risiko
2. Evaluasi risiko

Penilaian risiko menentukan nilai aset informasi, mengidentifikasi ancaman-ancaman yang berlaku dan kerentanan yang ada (atau bisa ada), mengidentifikasi kontrol yang ada dan efeknya pada risiko yang teridentifikasi, menentukan konsekuensi potensial dan akhirnya memprioritaskan risiko yang diperoleh dan menggolongkan terhadap kriteria evaluasi risiko yang diatur dalam penetapan konteks.Menentukan Nilai Risiko

H. Menentukan Nilai Risiko

Adalah gambaran dari seberapa besar akibat yang akan diterima organisasi jika ancaman yang menyebabkan kegagalan keamanan Informasi terjadi. Adapun nilai risiko ditentukan oleh metode Metode Kualitatif

Membuat perkiraan terhadap biaya yang ditanggung oleh organisasi akibat dari risiko yang diterima. Nilai risiko ditentukan dengan range :

- Low Risk (risiko Kecil = 0-2)
- Medium Risk (risiko sedang = 3-5)
- High Risk (risiko Tinggi= 6-8)

Banyak cara untuk menghubungkan faktor-faktor tersebut, seperti contoh, nilai diberikan kepada aset, kerentanan, dan ancaman digabungkan untuk mendapatkan nilai risiko yang diukur, seperti metode yang menggunakan tabel seperti tabel dibawah ini.

TABEL I
MATRIKS NILAI ASET, KEMUNGKINAN TERJADI, DAN KEMUDAHAN

Kemungkinan terjadi – Ancaman		Rendah (R)			Sedang (S)			Tinggi (T)		
Kemudahan eksploitasi		R	S	T	R	S	T	R	S	T
Nilai Aset	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Sebagai contoh untuk menentukan peringkat nilai risiko yang ditangani, jika sebuah aset mempunyai nilai 3, ancamannya "*high*" dan kerentanannya "*low*", maka nilai dari risikonya adalah 5. Ukuran matriks, dalam hal jumlah kategori keparahan ancaman, kategori keparahan kerentanan, dan jumlah kategori penilaian aset, dapat disesuaikan dengan kebutuhan organisasi. Tabel dibawah memetakan kemungkinan ini terhadap dampak bisnis yang terkait dengan skenario insiden. Risiko yang timbul diukur pada skala 0 sampai 8 yang dapat dievaluasi terhadap kriteria penerimaan risiko.

I. Evaluasi Risiko

Sebuah daftar risiko dengan tingkat nilai yang diberikan dan kriteria evaluasi risiko sifat dari keputusan yang berkaitan dengan evaluasi risiko dan kriteria evaluasi risiko yang akan digunakan untuk membuat keputusan telah diputuskan ketika menentukan konteks. Keputusan dan konteks ini harus ditinjau kembali secara lebih rinci pada tahap ini ketika telah mengetahui lebih dalam tentang risiko tertentu yang teridentifikasi. Hasilnya adalah Sebuah daftar risiko yang diprioritaskan menurut kriteria evaluasi risiko dalam kaitannya dengan skenario insiden yang mengarah ke risiko tersebut.

Sebuah daftar risiko yang diprioritaskan menurut risiko kriteria evaluasi dalam kaitannya dengan skenario insiden yang mengarah ke risiko tersebut. Adapun Tindakan yang dilakukan adalah Kontrol untuk mengurangi, mempertahankan, menghindari, atau mentransfer risiko harus dipilih dan rencana penanganan ditetapkan dan langkah-langkah pelaksanaan yaitu Ada empat pilihan yang tersedia untuk penanganan risiko yaitu mengurangi risiko mempertahankan risiko, menghindari risiko dan mentransfer risiko.

J. Maturity Level

Model perhitungan yang digunakan untuk mengukur tingkat kematangan menggunakan SSE-CMM. SSE-CMM adalah *Capability Maturity Model* (CMM) untuk *System Security Engineering* (SSE).

CMM adalah kerangka untuk mengembangkan proses, seperti proses teknis baik formal maupun informal. SSE-CMM terdiri dari dua bagian, yaitu:

a. Model untuk teknik keamanan proses, proyek dan organisasi, dan

b. Metode penilaian untuk mengetahui kematangan proses.

SSE-CMM menjelaskan karakteristik penting dari suatu proses rekayasa keamanan organisasi yang harus ada untuk memastikan

teknik keamanan yang baik dengan tidak menganjurkan proses tertentu atau berurutan, namun mengambil praktek secara umum yang diamati dalam industri. Model ini merupakan standar untuk mempraktekkan rekayasa keamanan yang meliputi:

a. Siklus hidup, secara keseluruhan termasuk pengembangan, pengoperasian dan,kegiatan pemulihan kembali.

b. Organisasi, keseluruhan termasuk pengelolaan, pengorganiasian dan kegiatan rekayasa.

c. Prilaku, berinteraksi dengan disiplin lain, seperti sistem, perangkat lunak, perangkat keras, faktor manusia, rekayasa pengujian, pengelolaan sistem, operasi dan pemeliharaan.

d. Berinteraksi dengan organisasi lain termasuk pengambil alihan, pengelolaan manajemen, sertifikasi, akreditasi dan evaluasi.

Model SSE-CMM memberikan gambaran menyeluruh tentang prinsip-prinsip dan arsitektur yang didasarkan SSE-CMM, gambaran eksekutif dari model, saran untuk pengggunaan model yang tepat, praktek-praktek yang termasuk dalam model, dan deskripsi atribut dari model. Metode penilaian SSE-CMM menjelaskan proses dan alat untuk mengevaluasi kemampuan teknik keamanan informasi. Ruang lingkup SSE-CMM meliputi beberapa hal yaitu:

a. SSE-CMM ditujukan untuk kegiatan rekayasa keamanan yang meliputi produk yang terpercaya atau siklus hidup keamanan sistem, termasuk definisi konsep, analisa kebutuhan, perancangan, pengembangan, integrasi, instalasi, operasi, perawatan dan pengawasan.
b. SSE-CMM diterapkan untuk mengamankan pengembang produk, keamanan pengembang sistem dan integrator dan organisasi yang menyediakan jasa keamanan dan rekayasa keamanan.
c. SSE-CMM diterapkan untuk semua jenis dan ukuran rekayasa keamanan organisasi, seperti komersial, pemerintahan dan akademisi.

Untuk mengidentifikasi sejauh mana perusahaan/organisasi telah memenuhi standard keamanan informasi yang baik, dapat menggunakan kerangka identifikasi yang direpresentasikan dalam sebuah tingkat kematangan yang memiliki tingkat pengelompokkan kapabilitas perusahaan.

TABEL III
KRITERIA INDEX PENILAIAN PADA TINGKAT KEMATANGAN

Range	Keterangan
0 – 0.50	*Non - Exisiten*
0.51 – 1.50	*Initial / Ad Hoc*
1.51 – 2.50	*Repeatable But Invinitve*
2.51 – 3.50	*Define Process*
3.51 – 4.50	*Managed and Measurable*
4.51 – 5.00	*Optimized*

Sebagaimana dijelaskan dalam tabel diatas, bahwa SSE-CMM mempunyai lima tingkat kemampuan untuk menunjukkan tingkat kematangan proses, berikut penjelasannya:

a. Tingkat 0 tidak semua praktek dasar dilakukan.
b. Tingkat 1 semua praktek dasar dilakukan namun secara informal, yang artinya tidak ada dokumentasi, tidak ada standar dan dilakukan secara terpisah.
c. Tingkat 2 *planned and tracked* yang menandakan komitmen merencanakan proses standar.
d. Tingkat 3 well defined yang berarti proses standar telah berjalan sesuai dengan definisi.
e. Tingkat 4 dikendalikan secara kuantitatif, yang berarti peningkatan kualitas melalui monitoring setiap proses.

f. Tingkat 5 ditingkatkan terus-menerus yang menandakan standar telah sempurna dan fokus untuk beradaptasi terhadap perubahan.

Metode SSE-CMM digunakan dengan memberikan skor pada setiap area proses yang dipilih antara 0 sampai 5 untuk setiap area proses.

IV. HASIL DAN PEMBAHASAN

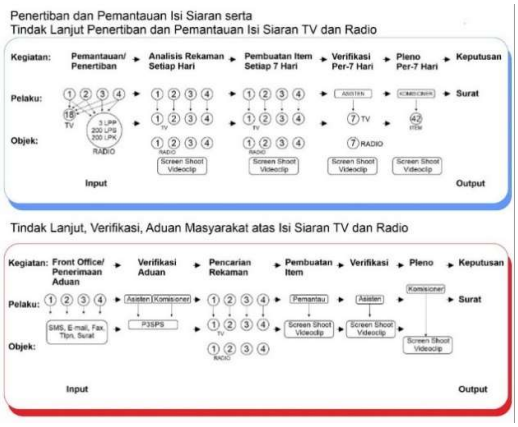
Pengumpulan data dilakukan dengan melakukan wawancara terhadap Ketua KPID Jawa Barat dan Staff yang berhubungan dengan proses bisnis yang ada di KPID Jawa Barat. Data mengenai visi dan misi serta produk-produk yang ada di KPID Jawa Barat telah terangkum dalam bentuk *company profile* KPID Jawa Barat.

A. Identifikasi Proses Bisnis dan IT

Tahap ini meliputi pendefinisian struktur organisasi KPID Jawa Barat, lalu fungsi dan proses bisnis yang dikerjakan.

- Proses Bisnis

Berdasarkan hasil observasi, wawancara dan analisa yang dilakukan terhadap proses bisnis aplikasi pemantauan di KPID Jawa Barat, maka diperoleh gambaran



permasalahan yang dialami oleh perusahaan. Di bawah ini merupakan alur proses pemantauan dan aduan.

Gambar 3 Alur Proses Pemantauan dan AduanDari alur proses

Dari alur proses pemantauan dan aduan di atas, terdapat 3 entitas yaitu Pemantau, Asisten dan Komisioner. Pemantau terdiri dari 4 dan 2 Asisten yang saling bekerjasama dalam proses penemuan item temuan pelanggan. Temuan item di validasi berdasarka P3SPS. Lalu di buatkan laporan item pelanggaran dan di berikan kepada asisten untuk di di buat rekap data dan di serahkan kepada Komisioner untuk memutuskan temuan tersebut melanggar atau tidak. Hasil dari keputusan itu berupa surat teguran apabila tayangan tersebut melanggar dan di serahkan kepada Lembaga Penyiaran yang melanggar.

- Aplikasi Pemantauan

Kondisi saat ini, Aplikasi pemantauan berfungsi untuk mengolah data hasil rekaman. KPID Jawa Barat memiliki 2 versi aplikasi pemantauan,

a. Aplikasi pemantauan versi 1.0 merupakan aplikasi untuk mengolah hasil rekaman siaran televisi dan untuk pembuatan laporan menggunakan aplikasi lain.
b. Aplikasi pemantauan versi 2.0. merupakan sistem informasi dan merekam siaran televisi.

Dari 2 versi aplikasi diatas secara efisien versi 2.0 karena membantu dalam segi waktu pengolahan data dan menghasilkan suatu keputusan. Versi 2.0 memiliki kelemahan dalam segi pengambilan hasil rekaman yang harus di download berdasarkan tanggal rekaman oleh pemantau, dengan kapasitas download melebih 1 Gb. Untuk versi 1.0, tidak adanya proses download karena sudah ada fitur untuk menampilkan hasil rekaman berdasarkan tanggal rekaman. Dari kedua versi tersebut hanya bisa merekam

siaran televisi karena adanya alat bantu TV *tunner* sebagai konversi frekuensi ke dalam komputer/server. Proses perekaman siaran televisi dilakukan selama 24/7.

Kondisi saat ini, aplikasi menggunakan aplikasi pemantauan versi 1.0 untuk memantau siaran Televisi. Karena aplikasi pemantauan versi 2.0 tidak sesuai dengan kebutuhan (proses download hasil rekaman yang memakan waktu lama) dan terjadinya aliran listrik mati serta belum adanya alat penampung listrik sementara mengakibatkan aplikasi *crash* dan *error*. Selain itu, setelah habisnya kontrak *maintance* dari pihak ketiga, dan kurangnya SDM mengakibatkan tidak terawatnya aplikasi pemantau versi 2.0. Maka dalam penelitian ini, peneliti melakukan identifikasi risiko pada aplikasi yang sedang berjalan. Terdapat jaringan LAN yang menghubungkan komputer *user* dengan *server* serta terhubung dengan internet.

Berikut adalah spesifikasi infrastruktur dalam aplikasi pemantauan di KPID Jawa Barat, yaitu:

a. Server Media *Monitoring Center* (Televisi)
   - TV *Recording Server*
   - Processor Dual Xeon 2609 V3
   - RAM DDR4 1 x 8 GB
   - Hardisk HDD x 10 TB
   - PSU 600 watt
b. TV *Tunner* PAL/NTSC *Analogue*
c. Rak *Server* ukuran 19”
d. Monitor
e. *Set Top Box*
f. Antena dan Jaringan Antena
g. KVM *Switch* 8 port
h. LAN
i. *Operating System* (Windows Server 2016 12 core)

B. *Hasil Analisis Identifikasi Aset*

Setelah melakukan penelitian, maka ada 5 kategori aset yang berhasil diidentifikasi, ditunjukan dalam tabel III sebagai berikut:

TABEL IIIII
IDENTIFIKASI ASET

No	Kategori Aset	Nama Aset
1	Informasi	Data Rekaman Televisi
2	Perangkat Keras dan Jaringan	• Server • Komputer Desktop • Jaringan LAN • Internet • Switch • Printer • Mesin Penghacur Kertas • Monitor • TV *Tunner* PAL/NTSC Analogue • Jaringan Antena • Antena • *Set Top Box*
3	Perangkat Lunak	• Sistem Operasi (Linux, Windows) • Aplikasi *Office* • PostgreSQL
4	Sumber Daya Manusia	• Komisioner • Asisten • Pemantau • Tenaga Teknis
5	Fasilitas Pendukung	• Ruang Penyimpanan *Server* • Rak Server • Lemari Arsip • Ruangan Pemantau • Genset • AC

C. *Penilaian Aset*

Langkah selanjutnya setelah identifikasi aset adalah untuk menyepakati skala yang akan digunakan dan kriteria untuk menetapkan lokasi tertentu pada skala untuk setiap aset, berdasarkan penilaian. Kriteria yang digunakan sebagai dasar untuk menetapkan nilai untuk setiap aset adalah biaya yang timbul akibat hilangnya

kerahasiaan, integritas dan ketersediaan karena suatu insiden

Setelah menetapkan kriteria untuk dipertimbangkan, organisasi harus menyepakati suatu skala untuk digunakan di seluruh organisasi. Memakai jumlah tingkatan antara 3 (seperti rendah, sedang, tinggi) untuk skala penilaian aset.

TABEL VI
PENILAIAN ASET

No	Kategori Aset	Nama Aset	Nilai Aset
1	Informasi	Data Rekaman Televisi	3
2	Perangkat Keras dan Jaringan	• Server • Komputer Desktop • Jaringan LAN • Internet • Switch • Printer • Mesin Penghacur Kertas • Monitor • TV *Tuner* PAL/NTSC Analogue • Jaringan Antena • Antena • *Set Top Box*	• 3 • 3 • 3 • 2 • 2 • 2 • 2 • 2 • 2 • 2 • 2 • 2
3	Perangkat Lunak	• Sistem Operasi (Linux, Windows) • Aplikasi *Office* • PostgreSQL	• 2 • 2 • 3 • 3
4	Sumber Daya Manusia	• Komisioner • Asisten • Pemantau • Tenaga Teknis	• 2 • 3 • 3 • 3
5	Fasilitas Pendukung	• Ruang Penyimpanan *Server* • Rak *Server* • Lemari Arsip • Ruangan Pemantau • Genset • AC	• 3 • 2 • 1 • 2 • 3 • 2

D. Analisis Kemungkinan (Kecendrungan), Dampak, Penilaian Risiko dan Pengendalian

Setelah dilakukannya tahapan identifikasi risiko berdasarkan kritikalitas pada aset dengan selanjutnya dilakukan analisa risiko aset berdasarkan kriteria kerahasian (*Confidentiality*), integritas (*Integrity*) dan ketersediaan (*Availability*). Selanjutnya dilakukan penilaian risiko dan pengendalian berdasarkan hasil dari nilai risiko di tunjukkan pada Lampiran 1.

TABEL V
PENILAIAN RISIKO DAN PENGENDALIAN

Nama Aset	Data Rekaman TV									
Kerentanan	Tidak ada petugas khusus yang merawat dan mengelola									
Ancaman	Kehilangan data									
Dampak	Data menjadi rusak dan tidak akurat									
Pengendalian	Penambahan pegawai melakukan pelatihan kepada pegawai									
Nilai Aset	3									
Nilai Dampak	3									
Nilai Kemungkinan	3									
Nilai Risiko	7									
Kriteria Risiko	Tidak diterima									
										Dan Seterusnya

E. Peringkat Ancaman Dengan Pengukuran Risiko

Selanjutnya dilakukan pengurutan ancaman dalam rangka mengukur risiko.

Langkah ini memungkinkan ancaman yang berbeda dengan konsekuensi dan kemungkinan terjadinya yang berbeda harus dibandingkan dan diperingkat dalam urutan prioritas.
Ukuran risiko = (nilai aset x kemunkinan terjadi ancaman)

TABEL VI
PERINGKAT ANCAMAN

Nama Aset	Ancaman	Nilai Aset	Nilai Kemungkinan Terjadi	Ukuran Risiko	Urutan Ancaman
Data Rekaman	Kehilangan Data	5	4	20	1
Dan seterusnya					

F. Pemetaan Objektif Kontrol dan Keamanan Kontrol

Setelah dilakukan penilaian risiko, maka selanjutnya melakukan rencana pemetaan kontrol dengan kerangka kerja SNI ISO/IEC 27001:2013 yaitu terdapat pada Lampiran 1. Hasil dari 5 kategori aset dari peringkat risiko keseluruhan memiliki penilaian risiko 3 termasuk pada risiko rendah dan penilaian risiko 7 termasuk pada risiko tinggi.

Hasil dari pemetaan kontrol dengan kerangka kerja SNI ISO/IEC 27001:2013 maka yang perlu dirancang SMKI berdasarkan penelitian yang dilakukan pemetaan tersebut terdapat 16 kontrol didalam Klausul SNI ISO/IEC 27001:2013 dari yang digunakan yaitu sebagai berikut :

TABEL VII
PEMETAAN KONTROL SNI ISO/IEC 27001:2013

No	Klausul SNI ISO/IEC 27001:2013	Kontrol
1	Kebijakan untuk keamanan informasi	A.5.1.1
2	Penyaringan	A.7.1.1
3	Kepedulian, pendidikan dan pelatihan keamanan informasi	A.7.2.2
4	Kepemilikan aset	A.8.1.2
5	Penghapusan atau penyesuaian hak akses	A.9.2.6
6	Prosedur log-on yang aman	A.9.4.1
7	Mengamankan kantor, ruangan dan fasilitas	A.11.1.3
8	Melindungi terhadap ancaman eksternal dan lingkungan	A.11.1.4
9	Penempatan dan perlindungan peralatan	A.11.2.1
10	Utilitas pendukung	A.11.2.2
11	Keamanan kabel	A.11.2.3
12	Pemeliharaan peralatan	A.11.2.4
13	Peralatan pengguna yang tidak diawasi	A.11.2.8
14	Cadangan informasi	A.12.3.1
15	Pecatatan kejadian	A.12.4.1
16	Kendali jaringan	A.13.1.1
17	Hak kekayaan intelektual	A.18.1.2

G. Analisis Maturity Level

Peneliti melakukan penilaian *maturity level* menggunakan SSE-CMM (*System Security Engineering - Capability Maturity Model*) dengan menyebarkan kuisioner berdasarkan hasil pemetaan kontrol dengan kerangka kerja SNI ISO/IEC 27001:2013 pada aplikasi pemantauan di KPID Jawa Barat. Adapun pihak-pihak yang menilai yaitu Komisioner, Asisten, Pemantau dan Tenaga Teknis IT.

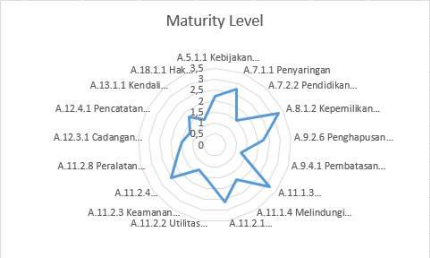
TABEL VIII
PERHITUNGAN *MATURITY LEVEL*

Klausul	Skor	Level
A.5 Kebijakan keamanan informasi	2.125	2
A.7 Keamanan sumber daya	2.125	2
A.8 Manajemen aset	3.25	3
A.9 Kendali aset	1.75	1
A.11 Kamanan fisik dan lingkungan	2.1	2
A.12 Keamanan operasi	1.375	1
A.13 Keamanan komunikasi	1.75	2
A.18 Kesesuaian	1.25	1
Rata-rata *Maturity Level*	1.96	2

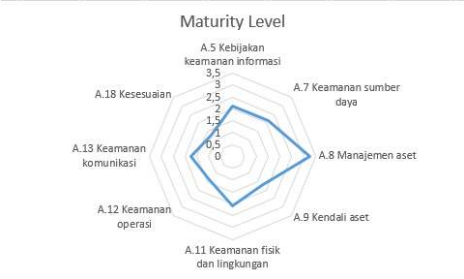
Berikut adalah hasil dari tingkat kematangan berdasarkan hasil analisis

berdasarkan Klausul SNI ISO/IEC 27001 menggunakan SSE dan CMM, pada penelitian ini menggunakan *Spider Chart* menjadi acuan peneliti untuk menggunakan diagram tersebut selain itu diagram dapat lebih mudah dipahami secara visual.

Gambar 4 Grafik berdasarkan kontrol SNI ISO/IEC 27001



Gambar 5 Grafik berdasarkan klausul SNI ISO/IEC 27001



Berdasarkan hasil penilian di atas, nilai dan tingkat tertinggi pada Klausul Manajemen aset dengan skor 3,25 pada level 3 dan nilai terendah pada Klausul Kesesuaian dengan skor 1,25 pada *level* 1. Terdapat nilai yang sama antara Klausul Kebijakan keamanan informasi dengan Klausul Keamanan sumber daya dengan skor 2,125 pada *level* 2 dan Klausul Manajemen aset dengan Klausul Keamanan komunikasi dengan skor 1,75 pada *level* 2. Hasil perhitungan untuk mendapatkan nilai rata-rata pengendalian keamanan informasi pada aplikasi pemantauan sebesar 1,96. Dari nilai tersebut, dapat disimpulkan bahwa informasi keamanan berada pada *level* 2, yang di definisikan *planned and tracked* yang menandakan komitmen merencanakan proses standar

H. Analisis Kesenjangan (Gap Analysis)

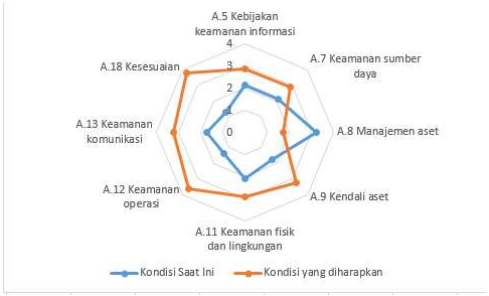
Tahap berikutnya melakukan penilian kesenjangan konxaxscscadisi saat ini dan kondisi yang diharapakan serta merekomendasikan hasil dari penilaian kesenjangan tersebut.

TABEL IX
PERHITUNGAN ANALISIS KESENJANGAN

Klausul	Kondisi Saat Ini	Kondisi yang diharapkan	Gap
A.5 Kebijakan keamanan informasi	2.125	5	2.875
A.7 Keamanan sumber daya	2.125	5	2.875
A.8 Manajemen aset	3.25	5	1.75
A.9 Kendali aset	1.75	5	3.25
A.11 Kamanan fisik dan lingkungan	2.1	5	2.9
A.12 Keamanan operasi	1.375	5	3.625
A.13 Keamanan komunikasi	1.75	5	3.25
A.18 Kesesuaian	1.25	5	3.75
Rata-rata			3.03

Dari hasil tersebut, kemudian dirata-rata untuk mendapatkan nilai gap atau kesenjangan maka nilai yang dihasilkan adalah 3.03 berarti nilai kesenjangan antara kondisi saat ini dengan kondisi yang diharapkan memiliki celah yang cukup besar, maka diperlukan penyesuaian masing-masing kontrol. Rekomendasi akan diberikan kepada masing-masing kontrol. Rasio nilai tingkat kematangan saat ini dan nilai tingkat kematangan yang diharapkan digambarkan pada Gambar, berikut:

Gambar 6 Pengukuran Grafik pada Gap Analisis



Seperti yang ditunjukkan pada Gambar, bahwa kondisi saat ini pada maturiry level diwakili oleh garis biru sementara pada garis merah adalah kondisi yang diharapkan. Dari gambar tersebut diatas terlihat bahwa *maturity level* pada kondisi yang diharapkan meningkat terus menerus yang menandakan standarnya telah sempurna dan fokus untuk beradaptasi terhadap perubahan.

Dengan demikian semakin tinggi nilai gap pada suatu klausul, semakin besar kemungkinan untuk terjadi pelanggaran keamanan dan semakin rendahnya nilai gap pada klausul maka semakin kecil kemungkinan terjadinya masalah keamanan. Di jelaskan tingkat nilai gap terendah pada klausul Kesesuaian yaitu 3.75 dan nilai gap tertinggi pada klausul Manajemen aset yaitu 1.75.

I. Rekomendasi Objektif Kontrol dan Keamanan Informasi SNI ISO/IEC 27001

Setelah dilakukan penilaian *maturity level* dan analisis gap selanjutnya adalah menentukan kondisi pada aplikasi pemantauan, apakah sudah sesuai dengan standar SNI ISO/IEC 27001:2013 serta pemberian rekomendasi. Rekomendasi dapat digunakan untuk perbaikan pada aplikasi pemantauan di KPID Jawa Barat. Berikut ini adalah kondisi sekaligus rekomendasi yang diberikan:

TABEL X
HASIL KONDISI SAAT INI DAN REKOMENDASI KLAUSUL KEBIJAKAN KEAMANAN INFORMASI

A.5 Kebijakan keamanan informasi		
A.5.1 Arahan manajemen untuk keamanan informasi		
Kontrol	**Kondisi Saat Ini**	**GAP**
A.5.1.1 Kebijakan untuk keamanan informasi	Belum adanya SOP untuk keamanan informasi terhadap fisik dan lingkungan	Berdasarkan kontrol A.5.1.1, Pihak manajemen seharusnya membuat SOP untuk keamanan informasi terhadap fisik dan lingkungan
Sudah ada kebijakan informasi mendukung hak akses, prinsip kontrol aset dan pembatasan untuk peran pengguna tertentu	Sudah sesuai kontrol A.5.1.1	Sudah ada kebijakan informasi mendukung hak akses, prinsip kontrol aset dan pembatasan untuk peran pengguna tertentu
Rekomendasi		
Pihak manajemen perlu membuat SOP untuk keamanan informasi fisik dan lingkungan		
Dan Seterusnya		

V. KESIMPULAN

Kesimpulan dari hasil penelitian ini adalah perencanaan Sistem Manajemen Keamanan Informasi pada aplikasi Pemantauan di KPID Jawa Barat berdasarkan pemetaan kontrol dengan kerangka kerja SNI ISO/IEC 27001: 2013, yaitu:

1. Setelah dilakukannya tahapan identifikasi risiko berdasarkan kritikalitas pada aset dengan selanjutnya dilakukan analisa risiko aset berdasarkan kriteria kerahasian *(Confidentiality)*, integritas *(Integrity)* dan ketersediaan *(Availability)*, lalu dilakukan penilaian risiko, terdapat 5 kategori aset dari peringkat risiko keseluruhan memiliki penilaian risiko 3 termasuk pada risiko rendah dan penilaian risiko 7 termasuk pada risiko tinggi.
2. Terdapat 17 kontrol hasil dari pemetaan Obejktif kontrol dan kontrol berdasarkan SNI ISO/IEC 27001:2013 adalah A.5.1.1 Kebijakan untuk keamanan informasi, A.7.1.1 Penyaringan, A.7.2.2 Kepedulian,

pendidikan dan pelatihan keamanan informasi, A.8.1.2 Kepemilikan aset, A.9.2.6 Penghapusan atau penyesuaian hak akses, A.9.4.1 Prosedur *log-on* yang aman, A.11.1.3 Mengamankan kantor, ruangan dan fasilitas, A.11.1.4 Melindungi terhadap ancaman eksternal dan lingkungan, A.11.2.1 Penempatan dan perlindungan peralatan, A.11.2.2 Utilitas pendukung, A.11.2.3 Keamanan kabel, A.11.2.4 Pemeliharaan peralatan, A.11.2.8 Peralatan pengguna yang tidak diawasi, A.12.3.1 Cadangan informasi, A.12.4.1 Pencatatan kejadian, dan A.13.1.1 Kendali jaringan

3. Tingkat kematangan keamanan informasi pada aplikasi pemantauan terdapat tingkat tertinggi pada Klausul Manajemen aset dengan skor 3,25 pada level 3 dan nilai terendah pada Klausul Kesesuaian dengan skor 1,25 pada level 1. Hasil nilai rata-rata kontrol keamanan informasi pada aplikasi pemantauan sebesar 1,96. Dari nilai tersebut, dapat disimpulkan bahwa informasi keamanan berada pada *level* 2, yang di definisikan *planned and tracked*.
4. Berdasarkan hasil pemeriksaan keamanan informasi aplikasi pemantauan berdasarkan SNI ISO/IEC 27001 terdapat kebijakan dan prosedur yang belum terdokumentasi, bahkan ada beberapa tindakan dalam organisasi yang dilakukan berdasarkan spontanitas dan tanpa ada aturan baku yang bersifat formal. Ada beberapa kontrol yang sudah dilakukan sesuai dengan SNI ISO/IEC 27001.

DAFTAR PUSTAKA

[1] Titus Kristanto, Mohammad Sholik, Dewi Rahmawati, Muhammad Nasrullah (2019). Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ. JISA (Jurnal Informatika dan Sains).

[2] Reynaldo Adi Putra Pratama Gala, Rizal Sengkey, Charles Punusingon (2020). Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI. Jurnal Teknik Informatika.

[3] Muhammad Bakri, Nia Irmayana (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001. Jurnal TEKNOKOMPAK.

[4] Ito Setiawan, Aldistya Riesta Sekarini, Retno Waluyo, Fiby Nur Afiana (2021). Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto. Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer.

[5] Yuni Cintia Yuze, Yudi Priyadi, Candiwan (2016). Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001: 2013 Serta Rekomendasi Model Sistem Menggunakan Data Flow Diagram pada Direktorat Sistem Informasi Perguruan Tinggi. Jurnal Sistem Informasi Bisnis.

[6] Sitta Rif'atul Musyarofah, Rahadian Bisma (2020). Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun. Journal of Emerging Information Systems and Business Intelligence.

[7] Siti Alvi Sholikhatin, Dr. Arief Setyanto, S.Si., M.T, Emha Taufiq Luthfi, S.T.,M.Kom (2018). Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik

Universitas Muhammadiyah Purwokerto). Jurnal IT CIDA.

[8] Winda Apriandari, Ashwin Sasongko (2018). Analisis Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Di DISKOMINFO Kota Sukabumi). Jurnal Ilmiah SANTIKA.

[9] Bramantiyo Eko Putro (2016). Analisa Control Self Assessment Audit Pada Klausul A.5 Security Policy Hingga Klausul A.9 Physical And Environmental Security Telkom Flexi Kebon Sirih Jakarta Pusat Menggunakan ISO/IEC 27001. Media Jurnal informatika Vol.8 No.1.

[10] Marinda Yunella, Admaja Dwi Herlambang, Widhy Hayuhardhika Nugraha Putra (2019). Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer Vol. 3, No. 10.

[11] Anggi Anugraha Pura, Oky Dwi Nuhayati, Ike Pertiwi Windasari (2016). Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 27001. Jurnal Teknologi dan Sistem Komputer, Vol.4, No.1.

[12] Periyadi (2015). Analisis Risiko Teknologi Informasi Sistem Terintegrasi iGracias Berbasis Risk Assesment Menggunakan SNI ISO-IEC 27001-2009. Jurnal Teknologi Informasi Vol. 2, No. 3.

[13] Fajar Ilham Satria Yudha, Rd. Erwin Gunadhi (2016). Risk Assesment Pada Manajemen Risiko Keamanan Informasi Mengcau Pada British Standart ISO/IEC 27005 Risk Management. Jurnal Algoritma Sekolah Tinggi Teknologi Garut.

[14] Erny Nursetyawati, Rokhman Fauzi, Ryan Adhitya Nugraha (2020). Manajemen Keamanan Informasi Mengunakan Metode Analisi Risiko ISO 27005:2008 Pada Diskominfo Jawa Barat. *e-Proceeding of Engineering* : Vol.7, No.2.

[15] Dadan Rahmat, ST., MT (2019). Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar SNI ISO/IEC 27001: 2013. Jurnal Informatika – COMPUTING Volume 06 Nomor 02.

[16] Furqon Mauladani, Daniel Oranova Siahaan (2018). Perancangan SMKI Berdasarkan SNI ISO/IEC27001:2013 dan SNI ISO/IEC27005:2013. CSRID Journal, Vol. 10 No. 1

[17] Saepudin, M. Hendayun, Arief Zulianto (2019). Audit Keamanan Sistem Informasi Akademik Perguruan Tinggi XYZ Menggunakan SNI ISO/IEC 27001:2013. Jurnal Produktif Vol.3 No.2

[18] Fuad Nasher (2018). Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa secara Elektronik (LPSE) di Dinas Komunikasi dan Informatika Kabupaten Cianjur dengan Menggunakan SNI ISO/IEC 27001:2013. Media Jurnal Informatika Vol. 10, no.1

[19] Hikam Haikal Radya Hans Ananza, Irfan Darmawan, Rahmat Mulyana (2019). Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Menggunakan Standart ISO 27001:2013 (Studi Kasus: DISKOMINFOTIK Kabupaten Bandung Barat. *e-Proceeding of Engineering* : Vol.6, No.2

[20] Ino Anugrah, R.Hengki Rahmanto (2017). Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-

Militarized Zone. Jurnal Penelitian Ilmu Komputer, Sistem Embedded & Logic

[21] Haries Anom Suseyto Aji Nugroho, Wing Wahyu Winarno, Sudarmawan (2018). Metode *Silogisme And* Untuk Validitas Jawaban Dari Responde Dalam Analisis Maturity Level Keamanan Informasi Berbasis SNI ISO 27001:2013 Pada Dinas Kependudukan dan Pencatatan Sipil Kota XYZ. Jurnal TRANSFORMASI, Vol. 14, No. 2

[22] Darma Yanto Putra, Theresia Wati, I Wayan Widi P (2020). Audit Keamanan Sistem Informasi Berdasarkan SNI – ISO 27001 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional "Veteran" Jakarta. Seminar Nasional Pengaplikasian Telematika (SINAPTIKA 2020)

[23] SNI ISO/IEC 27001: 2013

[24] SNI ISO/IEC 27005: 2013