**PROPOSAL SKRIPSI**

**EVALUASI KEAMANAN JARINGAN MENGGUNAKAN STANDAR ISO/IEC 27001 DI KANTOR KOMUNIKASI DAN INFORMATIKA KABUPATEN MUARA ENIM**

1. **Pendahuluan**
	1. **Latar belakang**

Seiring dengan perkembangan teknologi, penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini menjadi kebutuhan dan tuntutan di setiap lembaga penyelenggara pelayanan publik. Mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik. Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan, keutuhan, ketersediaan.

Kantor Komunikasi dan Informatika Kabupaten Muara Enim merupakan suatu lembaga pemerintah yang memiliki tugas menyelenggarakan urusan di bidang komunikasi dan informatika dalam pemerintahan untuk membantu dalam tata kelola Teknologi Informasi dan Komunikasi di Kabupaten Muara Enim. Keamanan informasi pada kantor Kominfo Muara Enim sangat diperlukan karena menyangkut tentang keamanan informasi sebuah intansi pemerintahan yang sangat rahasia. Informasi itu bisa berbentuk dalam *hard copy*, penyimpanan secara digital, *visual* (video, diagram), ditampilkan di *website*, verbal (percakapan, panggilan telpon), dan sebagainya. Apapun bentuk informasi yang disajikan, informasi tersebut harus selalu aman. Mengingat pentinggnya keamanan informasi, maka kebijakan tentang kamanan informasi harus baik dan setidaknya harus mencakup beberapa prosedur seperti prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik dan lingkungan, prosedur pengamannan *logical security*, proseredur pengamanan operasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi. Untuk itu diperlukan evaluasi keamanan sistem manajemen informasi untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur. Standar yang digunakan dalam manajemen keamanan informasi adalah ISO/IEC 27001. ISO/IEC 27001 dipilih karena standar ini sangat fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dan ukuran struktur organisasi.

ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi pada sebuah organisasi.

Berdasarkan uraian-uraian di atas maka penulis bermaksud untuk mengangkat permasalahan tersebut sebagai bahan penelitian ini. Adapun judul yang dipilih yaitu ”Evaluasi Keamanan Jaringan Menggunakan Standar ISO/IEC 27001 Di Kantor Komunikasi dan Informatika Kabupaten Muara Enim”.

* 1. **Rumusan Masalah**

Berdasarkan latar belakang yang ada, maka penulis ingin merumuskan permasalahan yang ada yaitu “Seberapa baik manajemen keamanan informasi pada Kantor Komunikasi dan Informatika Kabupaten Muara Enim menggunakan standar ISO/IEC 27001?”

* 1. **Batasan Masalah**

Untuk lebih mengarahkan masalah yang ada serta tidak menyimpang dari permasalahan yang akan dilakukan dalam penelitian maka penulis hanya membatasi beberapa klausul yang digunakan dalam evaluasi ini yaitu:

1. Manajemen Aset
2. Manajemen SDM
3. Keamanan Fisik dan Lingkungan
4. Kontrol Akses
5. Akuisisi Sistem Informasi Pengembangan Dan Pemeliharaan
	1. **Tujuan dan Manfaat Penelitian**
		1. **Tujuan**

Berdasarkan dari latar belakang dan masalah yang diteliti maka tujuan dari penelitian ini adalah :

1. Mampu menerapkan tatakelola keamanan informasi secara efektif, efisien,dan konsisten.
2. Membuat evaluasi terhadap sistem yang diterapkan sehingga dapat memberikan solusi terbaik terhadap sistem tersebut.

**1.4.2. Manfaat**

Manfaat yang bisa didapatkan dari penelitian ini adalah :

1. Meningkatkan efektifitas dari kinerja jaringan di Kantor Komunikasi dan Informatika Kabupaten Muara Enim.
2. Sebagai usaha dalam meningkatkan sistem keamanan informasi di Kantor Komunikasi dan Informatika Kabupaten Muara Enim.

**II.** **TINJAUAN PUSTAKA**

**2.1. Landasan Teori**

**2.1.1. IT Audit**

IT Audit merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien (Weber, 2000)

**2.1.2. 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 dalam peluang bisnis. (ISO/IEC 27001, 2005).

Keamanan informasi terdiri dari perlindungan terhadap beberapa aspek. Aspek-aspek yang dimaksud adalah sebagai berikut :

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 izin dari pihak yang berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk mnjamin aspek integritas ini.
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).

Pengamanan informasi tersebut dapat dicapai dengan melakukan suatu kontrol yang terdiri dari kebijakan, proses, prosedur, struktur organisasi, serta fungsi-fungsi infrastruktur TI. Sedangkan *Information Security Management System* (ISMS) adalah suatu cara untuk melindungi dan mengelola informasi berdasarkan pendekatan yang sistematis terhadap risiko bisnis, untuk mempersiapkan, mengimplementasikan, mengoperasikan, mengawasi, meninjau kembali, memelihara, serta meningkatkan pengamanan informasi. ISMS merupakan suatu pendekatan secara organisasi untuk pengamanan informasi.

**2.1.3. ISO/IEC 27001**

ISO (*International Organization for Standarzitation*) adalah pengembang terbesar di dunia standar international secara sukarela. Standar international memberikan keamanan yang lebih spesifik, layanan yang baik, membantu industry lebih efisien dan efktif. Dikembangkan melalui kesepakatan global, mereka membantu untuk mengatasi hambatan perdagangan internasional.

ISO/IEC 27001 adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. Standar ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi atau *Information Security Management Syestem*, biasadisebut *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.

Adapun 11 klausul dari ISO/IEC 27001 yaitu :

1. *Security policy* (kebijakan keamanan informasi)

Untuk memberikan arahan dan dukungan manajemen keamanan informasi. Manajemen harus menetapkan arah kebijakan yang jelas dan menunjukan dukungan, serta komitmen terhadap keamanan informasi melalui penerapan dan pemeliharaan suatu kebijakan keamanan informasi di seluruh jajaran organisasi.

1. *Organization of information security* (Organisasi keamanan informasi)

Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggung jawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah.

1. *Asset management* (Manajemen aset)

Manajemen Aset didefinisikan menjadi sebuah proses pengelolaan aset (kekayaan) baik berwujud dan tidak berwujud yang memiliki nilai ekonomis,nilai komersial, dan nilai tukar, mampu mendorong tercapainya tujuan dari individu dan organisasi. Melalui proses manajemen *planning*, *organizing*, *leading* dan *controling*. bertujuan mendapat keuntungan dan mengurangi biaya (*cost*) secara effisien dan effektif.

1. *Human resources security* (Keamanan sumber daya manusia)

Organisasi harus menetapkan dan menyediakan sumberdaya manusia yang dibutuhkan untuk menerapkan, mengoprasikan, memantau, meningkatkan dan memelihara keamanan informasi.

1. *Physical and environmental security* (Keamanan fisik dan Lingkungan)

Untuk mencegah akses tanpa otoritas, kerusakan, dan gangguan terhadap tempat dan informasi bisnis. Fasilitas pemrosesan informasi bisnis harus berada di wilayah yang aman, terlindungi secara aman dengan sistem pengamanan dan kontrol masuk yang memadai. Fasilitas tersebut harus dilindungi secara fisik dari akses tanpa ijin, kerusakan dan gangguan. Prlindungan harus disesuaikan dengan identifikasi resiko.

1. *Communications and operations management* (Manajemen Komunikasi dan Operasi)

Untuk menjamin bahwa fasilitas pemrosesan informasi berjalan dengan benar dan aman harus ditetapkan tanggung jawab dan prosedur untuk manajemen dan operasi seluruh fasilitas pemrosesan informasi. Hal ini mencakup pengembangan operasi yang tepat dan prosedur penanganan insiden. Dimana harus ditetapkan pemisah tugas untuk mengurangi penyalahgunaan system karena kecerobohan atau kesenjangan.

1. *Access control* ( Akses kontrol)

Untuk mencegah akses tanpa ijin terhadap sistem informasi. Akses kontrol adalah bagaimana hanya administrator yang mempunyai akses control saja yang dapat mengakses tempat pemrosesan informasi.

1. *Information system acquisition, development, and maintenance* (Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi)

Untuk memastikan bahwa keamanan dibangun dalam system informasi. Persyaratan keamanan system mencakup infrastruktur, aplikasi bisnis dan aplikasi yang dikembangkan pengguna.

1. *Information security incident management* (Manajemen insiden keamanan informasi)

Manajeman insiden keamanan informasi adalah bagaimana memanajemen agar satu atau serangkaian kejadian keamanan informasi yang tidak diinginkan atau tidak diharapkan yang mempunyai kemungkinan secara signifikan dapat mengganggu operasi bisnis dan mengancam keamanan informasi.

1. *Business continuity management* (Manajemen kelangsungan usaha)

Untuk menghadapi kemungkinan penghentian kegiatan usaha dan melindungi proses usaha dari kegagalan atau bencana. Proses manajemen kelangsungan usaha harus diterapkan untuk mengurangi kerusakan akibat bencana atau kegagalan sistem keamanan yang mungkin terjadi seperti bencana alam, kecelakaan, kegagalan alat dan keterlambatan sampai ke tingkat yang dapat ditolerir melalui kombinasi pencegahan dan pemulihan kontrol. Rencana darurat harus disiapkan dan ditrapkan untuk memastikan proses usaha dapat disimpan ulang dalam skala waktu yang dibutuhkan. Manajemen kelangsungan bisnis harus mencakup control untuk mengidentifikasi dan mengurangi resiko, membatasi konsekuensi kesalahan yang merusak, dan memastikan penyimpulan terhadap operasional yang penting.

1. *Compliance* ( Kesesuaian)

Untuk menghindari pelanggaran terhadap hukum pidana maupun hukum perdata, perundangan, atau kewajiban kontrol serta ketentuan keamanan lainnya.

* 1. **Penelitian Sebelumnya**

Penelitian sebelumnya dilakukan oleh Nur Hariawan Bulu, 2013 dengan judul Analisis Keamanan Jaringan STMIK Amikom Yogyakarta berdasarkan ISO/IEC 2001:2005 Standar A.11.4.4. Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa control A.11.4.4 ISO/IEC 27001:2005 membahas tentang pengamanan dari dalam, khususnya bagaimana mengamankan perangkat-perangkat jaringan yang terdapat dari sistem dari segi akses fisik ataupun logical dari orang-orang yang tidak berwenang mengaksesnya.

Penelitian selanjutnya dilakukan oleh Moch. Rhasid Ridho, 2012 dengan judul Evaluasi Keamanan Informasi Mengunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009. Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa dengan adanya audit independen dengan menggunakan aplikasi KAMI dapat memberikan solusi yang tepat bagi peningkatan kelengkapan dan kematangan keamanan informasi bagi penyelenggara pelayanan publik.

Dari dua penelitian tersebut dapat disimpulkan bahwa ISO/IEC 27001 merupakan sebuah standar yang dapat diterapkan sebagai acuan dalam mengamankan suatu informasi yang aman dan handal pada lembaga/instansi tersebut.

**III.** **METODOLOGI PENELITIAN**

* 1. **Waktu dan Tempat**

Penelitian dilakukan di Kantor Kominfo Muara Enim, akan dimulai pada bulan November 2013 sampai dengan bulan Februari 2014 jam 07.30 sampai dengan 16.00 WIB.

* 1. **Alat dan Bahan**

Adapun alat dan bahan yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Perangkat Keras (*Hardware*)
	1. Laptop Axioo
	2. *Mouse*

2. Perangkat Lunak (*Software*)

a. Sistem Operasi *Windows 7*

b. *Mozila Firefox* digunakan untuk mencari literature dari intrnet

c. *Microsoft Office* sebagai aplikasi pengolahan data untuk penulisan laporan

* 1. **Metode Penelitian**
		1. **Penelitian *Action Research* (Penelitian Tindakan)**

Penelitian tindakan merupakan penelitian yang bertujuan mengembangkan metode kerja yang paling efisien, sehingga biaya produksi dapat ditekan dan prokdutivitas lembaga dapat meningkat. (Sugiyono,2007:9)

Adapun tahapan dalam melakukan penelitian *Action Research* yaitu sebagai berikut :

1. Melakukan Diagnosa (diagnosing)

Melakukan identifikasi masalah-masalah yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan. Pada penelitian ini penulis melakukan diaknosa terhadap sistem keamanan informasi pada Kantor Komunikasi dan Informatika Kabupaten Muara Enim.

1. Membuat Rencana Tindakan (action planning)

Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Pada tahap ini peneliti melakukan rencana tindakan dengan melakukan survei berkenaan masalah yang akan dianalisis tersebut apakah penelitian tersebut dapat dilaksanakan atau tidak di Satuan Kerja Teknologi Informasi. Dalam hal ini penulis tertarik pada sistem keamanan informasi pada Kantor Komunikasi dan Informatika Kabupaten Muara Enim.

1. Melakukan Tindakan (action taking)

Pada *action taking* peneliti melakukan menganalisis manajemen kemananan informasi menggunakan standar yang sudah ditetapkan oleh badan standarrisasi keamanan jaringan yaitu ISO/IEC 27001 dengan jaringan yang ada di kantor Kominfo Muara Enim.

1. Melakukan Evaluasi (evaluating)

Setelah masa tahap *action taking* dianggap cukup, kemudian peneliti melakukan evaluasi hasil dari analisis yang telah dilakukan tadi, pada tahap ini dilihat apakah sistem kemanan informasi di Kantor Komunikasi dan Informatika Kabupaten Muara Enim sudah sesuai dengan standar yang ada.

1. Pembelajaran (learning)

Tahap ini merupakan bagian akhir yang telah dilalui dengan melaksanakan *review* tahap demi tahapan dan dapat memahami prinsip kerja dari hasil analisis.

* 1. **Metode Pengumpulan Data**

Dalam penelitian ini metode pengumpulan data yang digunakan adalah sebagai berikut :

* + 1. **Data Primer**
1. Observasi

Penulis mengadakan peninjauan langsung ke Kantor Komunikasi dan Informatika Kabupaten Muara Enim yang merupakan pusat sistem informasi di instansi tersebut dengan mengamati, mencatat dan menganalisis keamanan informasi yang ada di Kantor tersebut dan bagaimana mengamankan sistem keamanan informasi menggunakan standarISO/IEC 27001 pada Kantor Komunikasi dan Informatika Kabupaten Muara Enim.

1. Wawancara (*Interview*)

Untuk mendapatkan data secara langsung dari sumber yang mengerti sehubungan dengan pengamatan yang penulis lakukan. Dalam hal ini penulis mengajukan pertanyaan-pertanyaan kepada karyawan yang berada di Kantor Komunikasi dan Informatika Kabupaten Muara Enim yang bertugas sebagai *administrator* pada instansi tersebut.

* + 1. **Data Sekunder**

Data sekunder yang sifatnya informasi diperoleh penulis dengan melakukan *Study* *literature* yang *relevan*, yaitu dengan cara mempelajari buku dan jurnal yang berkaitan dengan penulisan penelitian.

* 1. **Metode Analisis Data**

Metode analisis data yang digunakan adalah metode kuantitatif. Menurut Tuban (2001) metode kuantitatif adalah ilmu seni yang berkaitan dengan tata cara (metode) pengumpulan data, analisa data, dan interpretasi hasil analisis untuk mendapatkan informasi guna penarikan kesimpulan dan pengambilan keputusan.