BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terdahulu merupakan pengamatan terhadap fakta-fakta dari penelitian-penelitian sebelumnya yang muncul dari suatu masalah sebagai dasar perbandingan penelitian saat ini. Berikut tabel tinjauan terdahulu akan disajikan pada Tabel 2.1.

Tabel 2.1 Tinjauan Penelitian Terdahulu

No	Sumber penelitian, Judul dan Tahun	Isi Penelitian
1	V. Agrawal[1], *framework for the information classification in ISO* 27005 *standard*. 2017	Penelitian ini membahas dimana sebuah klinik kesehatan disajikan dengan kerangka kerja ISO 27005 untuk menguji, kemudian mengidentifikasi informasi penting yang akan terlibat di dalam bidang kesehatan. Tahap-tahapan yang dilakukan pada penelitian: a. Melakukan penilaian risiko. b. Melakukan pemeliharaan risiko. c. Melakukan pemantauan risiko. Kesimpulan: penelitian ini bertujuan untuk mengusulkan kerangka kerja di dalam bidang kesehatan *klinik* untuk menunjukkan berbagai objek informasi yang terlibat dalam standar manajemen risiko ISO27005 dan mengklasifikasikan informasi berdasarkan pedoman yang disediakan oleh skema UNINETT.

Tabel 2.1 Tinjauan Penelitian Terdahulu Lanjutan

NO	Sumber penelitian, Judul dan Tahun	Isi Penelitian
1	Sri Aryani, Made Sudarma[2], Implementation Of The ISO / IEC 27005 In Risk Security Analysis Of Management Information System, 2016	Penelitian ini membahas tentang hasil analisis Sistem Informasi Manajemen Keamanan (SMKI) di PT UPT SAMSAT Denpasar. Kerangka kerja yang akan digunakan dalam proses analisis ini adalah ISO / IEC 27005. Tahapan-tahapan yang dilakukan pada penelitian: a. Melakukan identifikasi aset. b. Melakukan penilaian aset. c. Melakukan penilaian dampak risiko. Kesimpulan: Hasil analisis ini menentukan tingkatan level aset yang terdaftar memiliki tingkat risiko tertinggi dan daftar aset mana yang memiliki tingkat ancaman tertinggi.
2	Fajar Ilham Satria Yudha, Erwin Gunardhi[3], *risk assessment* pada manajemen risiko kemanan informasi mengacu pada *british standard iso/iec 27005 risk management.* 2013	Penelitian ini membahas tentang tujuan untuk mengetahui kondisi kemanan dan memberikan hasil *risk assessment* berdasarkan *assessment*, objek penelitian pada *assessment* yaitu sebuah infrastruktur aliran data *digital* data-data pertahanan dan database *OLTP* serta *OLAP* kelemahan pada Badan Pertahanan Nasional(BPN). Tahapan-tahapan yang dilakukan pada penelitian: a. Melakukan identifikasi risiko. b. Melakukan estimasi risiko. c. Melakukan evaluasi risiko. Kesimpulan: Risiko yang telah teridentifikasi di prioritaskan berdasarkan penilaian yang di tentukan menurut standar ISO dari prioritas risiko mana yang paling berpengaruh ke tingkat risiko yang paling kecil.

Tabel 2.1 Tinjauan Penelitian Terdahulu Lanjutan

NO	Sumber penelitian, Judul dan Tahun	Isi Penelitian
1	Ega Lestaria Sukma[4], dengan judul evaluasi manajemen risiko keamanan informasi sistem *provisioning getway* telkom flexi. 2013	Penelitian ini membahas tentang dimana kondisi manajemen risiko keamanan informasi untuk mendapatkan nilai kematangannya, kemudian dilakukan perancangan melalui *risk assessment* sehingga di dapatkan rekomondasi control yang perlu di terapkan untuk sistem tersebut. Tahapan-tahapan yang dilakukan pada penelitian: a. Melakukan perencanaan. b. Melakukan pengumpulan data. c. Melakukan anlisis. d. Melakukan evaluasi. Kesimpulan: keluaran yang di hasilkan adalah evaluasi tingkat kematangan manajemen risiko keamanan informasi sistem *provisioning getway* telkom flexi.

Dari pengamatan penelitian terdahulu dapat disimpulkan bahwa kerangka kerja ISO 27005 terdapat sedikit kesamaan dalam melakukan tahapan untuk menghasilkan manajemen risiko yang pantas bagi sebuah perusahaan atau organisasi. Sedangkan yang dilakukan pada penelitian ini terdapat juga perbedaan dari tahapan-tahapan untuk manajemen risiko di PT. Sunrise Steel seperti dalam melakukan identifikasi aset, penilaian aset, dan evaluasi. Namun, perusahaan tersebut belum seluruhnya menggunakan manajemen risiko dengan tepat.

2.2 Teori Dasar

Dalam teori dasar meliputi penjelasan dan definisi dari beberapa kajian-kajian teori dasar yang terkait dengan penelitian yang dilakukan.

2.2.1 Prinsip Manajemen Risiko

Prinsip manajemen risiko dapat dikatakan efektif apabila memliki tujuan untuk menerapkan prinsip-prinsip seperti berikut:

a. Manajemen risiko harus mempunyai nilai tambah.

b. Manajemen risiko adalah bagian dari proses organisasi.

c. Manajemen risiko merupakan proses pengambilan keputusan.

d. Manajemen risiko bersifat sistematik, dinamis, terstruktur dan tepat waktu.

e. Manajemen risiko mempunyai fasilitas akan terjadinya perbaikan dan peningkatan organisasi secara berkelanjutan[5].

2.2.2 Manajemen Risiko

Risk Management (Manajemen Risiko) merupakan suatu proses yang logis dan sistematis dalam menganalisa, mengidentifikasi, mengevaluasi, dan mengendalikan risiko yang berhubungan dengan segala aktivitas, fungsi, gambar atau suatu proses dengan tujuan sebuah perusahaan yang mampu meminimalisir kerugian dan memaksimumkan kesempatan. Implementasi dari manajemen risiko ini membantu perusahaan dalam melaksanakan penilaian risiko, implementasi strategi mitigasi risiko, dan penggunaan teknik dan prosedur untuk pemantauan keadaan keamanan sistem informasi[6].

2.2.3 Risiko

Risk (Risiko) mempunyai tingkat dampak pada sebuah organisasi yang termasuk misi, fungsi, gambar, reputasi. Selain itu risiko ini juga berdampak pada aset organisasi dan individu yang nantinya akan menghasilkan potensi dampak ancaman dan kemungkinan ancaman itu terjadi[6].

Risiko merupakan kombinasi dari dampak yang akan terjadi apabila suatu peristiwa yang tidak diinginkan dan berkemungkinan terjadi pada peristiwa tersebut. Untuk mengukur tingkatan atau menggambarkan penilaian terhadap suatu risiko kemungkinan seorang manajer mampu untuk memprioritaskan risiko dengan keseriusan yang dirasakan atau kriteria lain yang telah di tetapkankan secara pendekatan kualitatif[7].

Dari penjelasan definisi diatas, maksud dari definisi risiko adalah ketidak pastian dalam peluang, kerugian, dan tujuan organisasi. Maka risiko dapat diartikan sebagai peluang atau kemungkinan yang akan berpengaruh terhadap suatu tujuan dan dapat menghasilkan kerugian secara finansial apabila peluang kerugian tersebut belum dikelola dengan baik[8].

Risiko dapat dibedakan dalam bebeerapa kategori yang dapat dilihat pada apa risiko akan berdampak, diantaranya:

a) *Strategic Risk*, suatu risiko yang berhubungan dengan sebuah organisasi secara keseluruhan, seterusnya akan berada pada level tertinggi disebuah organisasi dan dapat menyebabkan timbul berbagai jenis-jenis risiko lainnya[9].

b) *Complaince Risk*, suatu risiko *financial loss* atau rusaknya reputasi sebuah organisasi yang mun gkin akan terjadi sebagai akibat ketidak patuhan terhadap organisasi tersebut, terdapat hokum, regulasi, peraturan, standar regulasi organisasi yang ada di setiap aktivitas organisasi[10].

c) *Reputational risk*, suatu risiko yang biasanya berpotensi terhadap citra perusahaan. Risiko ini berkaitan dengan praktek bisnis organisasi yang dapat menyebabkan turunnya jumlah pelanggan, juga turunya pendapatan. *Reputational risk* bisa terjadi dari akibat kegagakan sebuah organisasi dalam mengelola jenis-jenis risiko yang ada dengan secara belum efektif[11].

d) *Operatiomal Risk*, suatu risiko munculnya sebuah akibat dari tidak kesesuaian sistem yang berjalan, baik dari proses internal sistem teknologinya maupun orang-orang yang terkait didalamnya[12].

2.2.4 Penilaian Risiko

Penilaian risiko menentukan nilai aset informasi, mengidentifikasi ancaman-ancaman yang berlaku terhadap kerentanan yang ada dan mengidentifikasi kontrol yang dirasakan pada risiko identifikasi, menentukan konsekuensi potensial kemudian memperioritaskan risiko yang diperoleh dan membagikan kriteria evaluasi risiko yang diatur dalam konteks[13]. Dalam penilaian risiko terdapat beberapa langkah utama yaitu:

a) *System Characterization,* suatu ruang lingkup dari sistem yang akan dinilai risikonya. Tahap ini membuat identifikasi batasan-batasan dari sistem tersebut berserta sumber daya dan informasi yang berkaitan dengan sistem.

b) *Threat Identification,* suatu proses identifikasi sumber ancaman yang ada pada sebuah organisasi. Ancaman disini dapat diakibatkan oleh adanya tidak terdapat kontrol dengan baik, sehingga terjadi adanya kelemahan internal maupun internal[14].

c) *Vulnerability Identification,* suatu proses identifikasi dari sumber kerentanan pada sebuah oraganisasi. Kerentanan adalah kelemahan dalam prosedur dari keamanan sistem, perancangan, implementasi, atau kontrol iternal yang dapat diekploitasi.

d) *Control Analysis,* suatu proses analisa kontrol yang ada untuk meminimalisir dari terjadinya ancaman[15].

e) *Likelihood Determination,* suatu penentuan level dari kemungkinan terjadinya ancaman. Level kemungkinan tersebut dikategorikan *High*, *Medium*, dan *Low*[16].

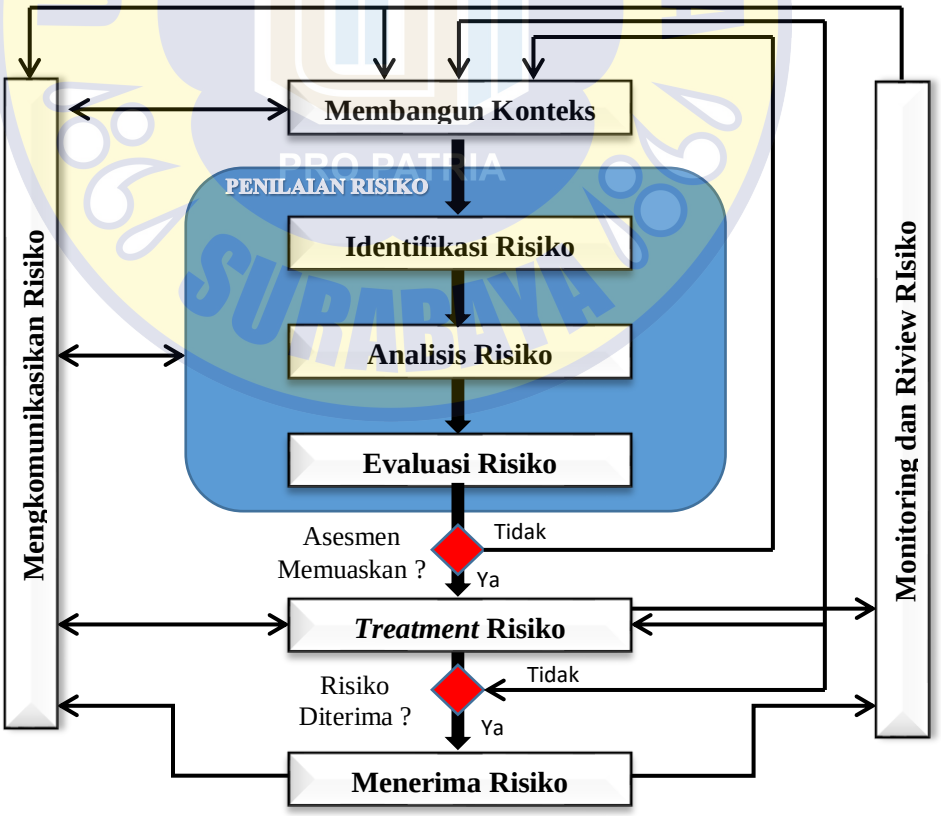
f) *Impact Analysis,* suatu analisis dampak dari kelemahan yang telah dieksploitasi dengan tujuan tingkat kepentingan sistem dan data. Hasil dari analisi ini adlah level dari dampak yang dikategorikan *Hight, medium*, dan *Low.*

g) *Control recommendation,* suatu penentuan rekomendasi dari berbagai kontrol-kontrol yang dapat memitigasi ataupun mengeliminasi risiko yang

telah diidentifikasi, yang dimana kontrol tersebut sesuai dengan oprasional organisasi[17].

2.2.5 *Framework* ISO 27005

Kerangka kerja ISO 27005 merupakan bagian standar dari 27000 yang membahas sistem manajemen keamanan informasi risiko keamanan *(*SMKI*)*. Standar ini menyediakan pedoman untuk manajemen risiko keamanan informasi dalam sebuah organisasi dan individu[18]. *Framework* ini mempunyai ruang lingkup yang besar, misalnya perusahaan komersial, intansi pemerintah, dan organisasi yang berniat mengelola risiko yang dapat mengancam keamanan informasi organisasi[19]. Berikut penjelasan berdasarkan ISO/IEC 27005 manajemen risiko yang disusun seperti pada Gambar 2.1.



Gambar 2.1 Proses Manajemen Risiko Keamanan ISO 27005 [11]

Seperti hasil yang pada Gambar 2.1, proses manajemen risiko kemanan informasi dapat dilakukan secara berulang sebagai penilaian risiko atau perlakuan risiko. Dalam hal ini Konteks harus ditetapkan dahulu, kemudian penilaian risiko dilakukan, setelah semua diperlakukan dan memberikan informasi yang cukup, selanjutnya dilakukan memodifikasi risiko ke tingkat yang dapat diterima, setelah selesai memodifikasi risiko selanjutnya menentukan perlakuan risiko. Jika informasi masih belum cukup, cara lain dari penilaian risiko bisa dilanjutkan dengan evaluasi risiko, kriteria penerimaan risiko atau kriteria dampak yang akan dilakukan dari ruang lingkup sebuah organisasi[20]. Dalam SMKI, menetapkan konteks, penilaian risiko, mengembangkan rencana penanganan dan penerimaan risiko adalah bagian dari rencana yang akan dilakukan dalam SMKI pada kontrol yang pierlukan untuk mengurangi risiko ke tingkat yang dapar diterima dan dilaksanakan sesuai dengan rencana penanganan[7]. Berikut adalah beberapa definisi proses ISO 27005 yang terdiri dari:

a. Proses komunikasikan risiko yang memberikan pertimbangan dan penilaian terhadap risiko yang ada saat ini, hal ini dijadikan pertimbangan dalam proses untuk pengambilan keputusan dari segi nilai, konsep, maupun kebutuhan. Maka, dalam rencana mengkomunikasikan risiko untuk dapat dijadikan pertimbangan, seperti cara untuk pesan penyampaian harus secara jujur, mudah dimengerti, terakurat, dan fakta yang ada[21].
b. Membangun konteks pada dasarnya menentukan batasan dari internal dan eksternal yang akan dijadikan pertimbangan dalam pengelolaan risiko. Menentukan konteks eksternal dimana sebuah organisasi harus memahami

konteks eksternal yang akan dilakukan untuk memastikan siapa saja yang terdapat kepentingan dan sasaran sampai mendapat pertimbangan dalam menenetukan kriteria risiko. Maka penentukan konteks internal merupakan suatu didalam organisasi yang dapat mempengaruhi sebuah organisasi dalam pengelolaan risiko, jadi konteks internal dapat dijadikan berupa struktur organisasi, proses bisnis[22].

c. Dalam proses analisis mempunyai sebuah identifikasi dan penilaian yang didalamnya berupa identifikasi risiko, estimasi risiko, dan evaluasi risiko sebagai analisis di sebuah organisasi. Identifikasi risiko dapat di definisikan sebagai dengan membuat daftar risiko yang dapat membahayakan dan merugikan dalam sebuah organisasi. Estimasi risiko bisa diartikan sebagai perkiraan risiko yang akan terjadi, bisa berupa ancaman dan dampak yang dapat merugikan sebuah organisasi untuk menggagalkan pencapaian sasaran. Evaluasi risiko dapat didefinisikan sebagai pembantu proses pengambilan keputusan berdasarkan hasil identifikasi risiko dan peniliannya. Proses evaluasi risiko akan menjadi sebuah recomendasi dan masukan bagi proses perlakuan risiko bagi perusahaan[23].

d. Proses penanganan (*treatment*) risiko mempunyai bagian sebagai untuk menghindari datangnya risiko, mitigasi risiko, dan kontrol risiko.

e. Proses penerimaan risiko harus memastikan risiko secara jujur dan akurat untuk dapat diterima oleh para pengelola organisasi. Hal ini penting terutama dalam situasi di mana pelaksanaan kontrol diabaikan atau ditunda, misalnya karena biaya yang belum cukup[5].

2.2.6 Profil Studi Kasus

PT Sunrise Steel salah satu perusahaan perseroan yang ada di Indonesia yang mempunyai inovasi yang baik sebagai kebutuhan konsumen terhadap Material Baja Lapis Alumunium Seng (BjLAS). Melalui langkah inovasi yang memanfaatkan teknologi, produk BjLAS menjadi salah satu produk yang memenuhi prinsip *longer usage term* diantara produk lainnya. Pada masa mendatang akan menyentuh seluruh aspek kehidupan manusia dengan adanya kegunaan aplikasi produk BjLAS yang nantinya bermanfaat bagi kehidupan sehari-hari mulai dari bangunan, komponen elektronik, peralatan rumah tangga. PT Sunrise Steel yang juga mempunyai Visi, Misi, dan Sasaran pada Tabel 2.2.

Tabel 2.2 Visi Misi dan Sasaran

VISI	MISI	SASARAN
Menjadi perusahaan baja lapis multinasianal.	1. Menguasai pangsa pasar baja lapis nasional. 2. Meningkatkan produktifitas sumber daya manusia, kualitas produk, layanan dan daya saing. 3. Secara proaktif melakukan pengembangan produk	Meningkatkan efektifitas sistem manajemen mutu secara berkesinambungan untuk meningkatkan kepuasan pelanggan.

(Sumber: hasil penelitian PT. Sunrise Steel)

2.2.7 Job Deskripsi Organisasi

1. Ka. IT Teknis :
    a. Menangani masalah teknis Teknologi Informasi dan Komunikasi.
    b. Menangani *maintenance.*
    c. Memelihara *aplikasi* maupun *software.*
    d. Mengadakan pengecekan secara berkala.
2. Ka. IT Support :
    a. Melakukan pengecekan aset TI berjalan seperti seharusnya.
    b. Memastikan komputer yang digunakan terhubung ke jaringan.
    c. Mengecek update setiap pembaharuan *software* maupun *aplikasi.*
    d. Memelihara aset pendukung seperti printer, proyektor, dan lain-lain.
3. Ka. IT Teknis *Network Enginering* :
    a. Memasang dan memelihara *server hardware* dan infrastruktur *software* baru.
    b. Memastikan semua peralatan IT memenuhi standar industri.
    c. Memonitor penggunaan *web* oleh semua pekerja.
    d. Memonitor penggunaan jaringan.
    e. Mengatur anti *spam*, dan *virus protection*.
4. Ka. IT Teknis *Aplikasi Development* :
    a. Memperbaiki masalah terhadap aplikasi.
    b. Mengadakan *user acceptance testing* untuk memastikan program mudah digunakan, cepat, dan akurat.
    c. Membuat solusi jika terdapat maslah pada *aplikasi*.