BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terdahulu merupakan pengamatan awal dari kegiatan sebuah penelitian yang nantinya dapat menjadi dasar perbandingan dengan penelitian saat ini. Pada Tabel 2.1 penelitian terdahulu ini akan menjelaskan bagaiman cara mengamankan aset – aset atau sistem keamanan dengan menggunakan metode NIST SP 800 – 30.

Tabel 2.1 Penelitian Terdahulu

No	Penelitian, Judul dan tahun	Isi Penelitian
1.	A. Elanda dan D. Tjahjadi 2018 [1] Analisis Manajemen Risiko Sistem Keamanan Ids (*Intrusion Detection System*) dengan Framework (*National Institute Of Standards And* Technology) Sp 800-30. (Studi Kasus : Disinfolahtaau Mabes Tni Au)	Permasalahan yang terjadi : Aset TI IDS (*Intrusion Detection System*) adalah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi penyusupan. sistem komputer (bisa merupakan kombinasi software dan hardware) kurangnya keamanan pada sistem tersebut sehingga rawannya terjadi serangan *hacker*. Langkah-langkah untuk melakukan penelitian : 1. Metode pengumpulan data : a. observasi b. wawancara c. idenfikasi masalah Kesimpulan : Pihak peneliti merekomendasikan keamanan IDS (*Intrusion Detection System*) agar tidak mudah menjadi serangan *hacker* pada lawan tersebut .

Pada Tabel 2.2.Penelitian terdahu ini akan menjelaskan bagaimana cara mengamankan sistem keamanan aplikasi tersebut dan juga menganilasa proses tata cara penilaian yang ada aplikasi pembelajaran yang ada di *pada UPN "Veteran" Jakarta* menggunakan metode *Oktave Allegro.*

Tabel 2.2 Penelitian Terdahulu

No	Penelitian, Judul dan tahun	Isi Penelitian
2.	Henki Bayu Seta, Theresiawati,Tri Rahayu 2017 [2] Manajamen Risiko Aplikasi Pembelajaran Berbasis Online Pada Universitas Dengan Menggunakan Metode Oktave Allegro	Permasalahan yang terjadi : UPN "Veteran" Jakarta belum pernah melakukan penilaian manajemen risiko pada aplikasi pembelajaran berbasis online (*e-learning*) untuk melindungi aset dan menjaga keberlangsungan proses bisnis pada UPN "Veteran" Jakarta. Kesimpulan : penelitain ini berupa rekomendasi pendekatan mitigasi untuk perlindungan sistem informasi diantaranya mengadakan training secara regular terhadap staff mengenai tanggung jawab dalam melindungi informasi aset dan dilakukan penyuluhan mengenai pentingnya keamanan

Pada Tabel 2.3 Penelitian Terdahulu ini akan menjelaskan bagaiman cara mengatasi permasalahan-permasalahan sistem yang sering terjadinya gangguan pada sistem tersebut dengan menggunakan metode NIST SP 800-30 Revisi 1 dengan hasil akhir melakukan rekomendasi berdasarkan penilaian-penilaian pada permasalahan tersebut.

Tabel 2.3 Penelitian Terdahulu

No	Penelitian, Judul dan tahun	Isi Penelitian
3.	Fathoni Mahardika 2017 [3] Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800 – 30 Revisi 1	Permasalahan yang terjadi : STMIK Sumedang memiliki permasalahan dalam penggunaan TI antara lain : 1. Masih sering terjadinya insiden keamanan informasi yang menyebabkan terganggunya proses bisnis perusahaan, 2. Belum adanya pengawasan dan perencanaan yang tepat dalam pengelolaan keamanan informasi di STMIK Sumedang. Kesimpulan : Merekomendasi melindungi proses bisnis organisasi yang penting dari ancaman keamanan, meminimalisir risiko kerugian serta menghindari kegagalan serius terhadap informasi yang ada di STMIK Sumedang.

Pada Tabel 2.4 Penelitian Terdahulu ini akan menjelaskan bagaimana cara menganalisa permasalahan-permasalahan yang terjadi pada *E-Learning* dengan melakukan pendekatan ORM (Object Relational Mapping) yang terkait permasalahan tersebut.

Tabel 2.4 Penetiain Terdahulu

No	Penelitian, Judul dan tahun	Isi Penelitian
4.	S. Patomviriyavong, B. Samphanwattanachai 2006 [4] eLearning Operational Risk Assessment and Management: A Case Study of the M.Sc. in Management Program	Permasalahan yang terjadi : Paper ini menganalisis bagaimana administrator universitas dapat mengidentifikasi faktor risiko operasional yang terlibat dengan operasi *e-Learning.* Empat jenis risiko operasional utama yang terlibat dengan eLearning dinilai sebagai : 1. Risiko konten, 2. Risiko teknologi, 3. Risiko orang, 4. Risiko proses. Kesimpulan : Penelitian ini menyarankan pendekatan ORM yang terkait dengan risiko operasional eLearning. Misalnya, harus ada alokasi sumber daya yang efisien dan pemisahan fungsi administrasi dalam program akademik.

Hasil kesimpulan dari Daftar Pustaka bahwa metode NIST SP 800 – 30 Revisi 1 merupakan metode yang berfokus pada sistem keamanan pada suatu sistem dan memiliki hasil berupa rekomendasi sebagai meminimalisir permasalahan sistem yang di kelompokan dengan penilaian dilakukan berdasarkan kondisi masalah organisasi tersebut. Persamaan dari Penelitian Terdahulu ini penelitian dilakukan menggunakan metode NIST SP 800-30 Revisi 1 yang membahas tentang keamanan sistem. Sedangkan perbedaan yang terdapat pada penelitian ini dengan Penelitian Terdahulu yang di atas membahas tentang sistem keamanan *web* pembelajaran *online* yang ada di Universitas Narotama

2.2 Teori Dasar yang Digunakan

Deskripsi dan definisi dari beberapa kajian teori dasar yang terkait dengan penelitian yang dilakukan .

2.3 eLINA (*e-learning*)

Aplikasi sistem pembelajaran eLINA Universitas Narotama merupakan aplikasi yang sangat penting bagi mahasiswa maupun dosen karena memiliki banyak manfaat bagi mahasiswa yaitu sebagai pengganti tatap muka, memberikan materi tanpa harus bertemu dengan dosen, pelaksanaan capain pembelajaran bisa dilakukan secara *online*, form diskusi bagi dosen/mahasiswa dan segala materi bisa diakases kapan saja.

2.4 Manajemen Risiko

Manajemen risiko organisasi secara unum memliki arti sebagai sistem pengelolaan risiko yang dihadapi oleh organisasi secara komprehensif untuk tujuan meningkatkan nilai perusahaan. Meskipun demikian, masih ada banyak definisi dan pengertian manajemen risiko organisasi lainnya, berikut beberapa definisi manajemen risiko organisasi[5].

Manajemen risiko adalah suatu proses identifikasi, mengatur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Strategi yang dapat digunakan anatara lain: mentranfer risiko pada pihak lain, menghindari risiko, mengurangi efek buruk risiko, dan menerima sebagian maupun seluruh konsekuensinya dari risiko tertentu[6].

Risiko ada di mana-mana, bisa datang kapan saja, dan sulit dihindari. Jika risiko tersebut menimpa suatu organisasi, maka organisasi tersebut bisa mengalami kerugian yang signifikan. Dalam beberapa situasi, risiko tersebut bisa mengakibatkan kehancuran organisasi tersebut. Karena itu risiko penting untuk dikelola. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga kita bisa memperoleh hasil yang paling optimal. Dalam konteks organisasi, organisasi juga akan menghadapi banyak risiko[7].

2.4.1 Risiko dan Penilaian Risiko

Penilaian risiko membahas potensi dampak buruk terhadap operasi dan aset organisasi, individu, organisasi lain, dan kepentingan keamanan nasional, serta ekonomi Amerika Serikat. Hal tersebut timbul dari operasi dan pengunaan sistem informasi dan informasi yang telah diproses, disimpan, dan dikirim oleh sistem. Organisasi melakukan penilaian risiko untuk menentukan risiko umum bagi misi inti/fungsi bisnis organisasi, misi/proses bisnis, misi/segmen bisnis, infrastruktur umum/layanan pendukung, serta sistem informasi. Penilaian risiko dapat mendukung berbagai keputusan juga aktivitas berbasis risiko[8].

2.5 Keamanan Infrormasi

Keamanan informasi memiliki peran yang sangat penting dan menarik bagi dunia teknologi saat ini. Bagi pengguna ponsel maupun pengguna komputer pribadi, inilah mengapa keamanan informasi merupakan suatu hal yang paling penting dalam kehidupan sehari-hari serta di bidang teknologi IT. Studi keamanan informasi memiliki begitu banyak konsep dan juga topik yang harus dikuasai oleh setiap profesional IT. Dalam pengetahuan dan keterampilan keamanan informasi hanya

beberapa yang terlibat dalam sektor teknologi IT, misalnya analis keamanan dunia maya, analis forensik, administrator jaringan, administrator sistem, pengembang aplikasi, dan lainnya. Kurangnya pengetahuan dalam bidang keamanan informasi ini akan mengembangkan aplikasi yang tidak aman atau membangun jaringan yang tidak aman dan lebih mudah bagi penyerang untuk menembus. Oleh karena itu inilah alasan mengapa pengetahuan keamanan informasi sangat penting dalam kehidupan kita sehari-hari. Terlepas dari karir yang dipilih[9].

2.6 *E–Learning*

E–Learning adalah alat atau sistem pendidikan berbasis komputer yang memungkinkan untuk pembelajaran dimana saja, kapan saja, dan disampaikan melalui internet. Sistem ini memberikan kemampuan peserta didik untuk menyesuaikan pembelajaran, secara efektif bahkan memungkinkan orang yang sibuk untuk melanjutkan karir dan mendapatkan kualifikasi baru. Beberapa perkembangan penting dalam pendidikan telah terjadi sejak peluncuran internet. Belakangan ini para pelajar cukup berpengalaman dalam menggunakan *smartphone*, seperti pengiriman pesan teks dan penggunaan internet bukan lagi menjadi masalah yang rumit. Papan pesan, media sosal, dan berbagai cara komunikasi *online* lainnya memungkinkan para pelajar untuk tetap belajar dalam membahas hal–hal yang terkait dengan kursus. Sembari memberikan rasa kebersamaan dalam dunia *e–learning* yang serba cepat, teknologi yang tersedia juga selalu berubah dan konten kursus harus segera diperbarui untuk memberi informasi pada mahasiswa[10].

Mengembangkan *e – learning* lebih mahal dari pada menyiapkan bahan – bahan kelas dan melatih para pelatih terutama jika multimedia atau metode yang sangat interaktif digunakan. Namu, biaya pengiriman untuk *e-learning* (termasuk server *web* dan dukungan teknis) jauh lebih rendah daripada biaya untuk fasilitas kelas, waktu instruktur, peserta dan waktu kerja hilang untuk menghadiri sesi kelas[11]

2.7 Metode NIST SP 800–30 *Revisi 1*

NIST (*National Institute of Standard and Technology*) merupakan organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, serta standar dan teknologi untuk meningkatkan fasilitas dan kualitas kehidupan. Kegunaan utamanya adalah meneliti berbagai ilmu untuk mempromosikan dan meningkatkan infrastruktur teknologi. NIST mengeluarkan rekomendasi melalui publikasi khusus 800-30 *Revisi 1* tentang *Guide for Conducting Risk Assessments*[12].

Metode ini terutama dirancanag untuk menjadi suatu perhitungan kualitatif. Proses ini sangat komprehensif, meliputi segala sesuatu dari sumber ancaman identifikasi untuk evaluasi berkelanjutan dan penilaian[13].

2.7.1 Proses Metode NIST SP 800 – 30 *Revisi 1*

Keamanan informasi yang dapat dijelaskan sebagai berikut :

a. mempersiapkan penilaian

   Mengidentifikasi tujuan penilaian risiko dalam hal informasi yang dihasilkan oleh penilaian dan keputusan yang akan didukung oleh penilaian.

b. melakukan penilaian

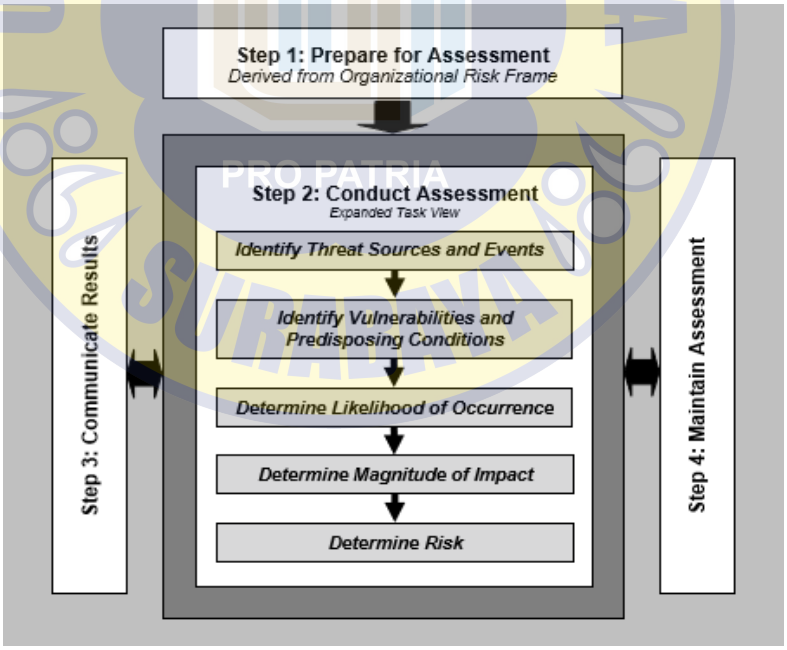
Mengidentifikasi dan menggambarkan sumber ancaman yang menjadi perhatian termasuk kapabilitas, niat, dan karakteristik penargetan untuk ancaman permusuhan serta berbagai efek untuk ancaman non-permusuhan.

c. mengkomunikasikan hasil penilaian

Mengkomunikasikan hasil penilaian risiko kepada pembuat keputusan organisasi untuk mendukung respons risiko.

d. menjaga penilaian

Melakukan pemantauan berkelanjutan terhadap faktor-faktor risiko yang berkontribusi terhadap perubahan risiko pada operasi dan aset organisasi, individu, organisasi lain atau bangsa.



Gambar 2.1 Proses Penilaian Risiko[12]

Setiap langkah dibagi ke dalam serangkaian tugas. Untuk setiap tugas, panduan memberikan informasi tambahan untuk organisasi yang melakukan penilaian risiko, tabel risiko, dan skala penilaian contoh yang dicantumkan dalam tugas, kemudian direferensikan silang ke informasi tambahan yang lebih rinci dalam lampiran pendukung, memberikan langkah-langkah dasar dalam proses penilaian risiko serta menyoroti tugas-tugas khusus untuk melakukan penilaian.

2.7.2 Tahapan Metode NIST SP 800 – 30 *Revisi 1*

Pada tahapan ini akan menjelaskan beberapa langkah - langkah untuk menganalisa suatu permasalahan pada penelitian ini :

1. Mempersiapkan Penilaian
   a. Idenfikasi tujuan

      Identifikasi tujuan penilaian risiko dalam hal informasi yang dimaksudkan untuk dihasilkan oleh penilaian dan keputusan penilaian yang dimaksudkan untuk mendukung.

   b. Identifikasi Ruang Lingkup

      Identifikasi ruang lingkup penilaian risiko dalam hal penerapan organisasi, kerangka waktu yang didukung, dan pertimbangan arsitektur/teknologi.

   c. Idenfikasi asumsi dan kendala

      Identifikasi asumsi dan kendala spesifik tempat penilaian risiko dilakukan.

   d. Identifikasi sumber informasi

      Identifikasi sumber-sumber informasi deskriptif, ancaman, kerentanan, dan dampak yang akan digunakan dalam penilaian risiko.

e. Identifikasi model risiko dan pendekatan analisis

   Identifikasi model risiko dan pendekatan analitik yang akan digunakan dalam penilaian risiko.

2. Melakukan penilaian

   a. Identifikasi sumber ancaman

      Identifikasi dan gambarkan sumber ancaman yang menjadi perhatian, termasuk kapabilitas, niat, dan karakteristik penargetan untuk ancaman permusuhan dan berbagai efek untuk ancaman non-permusuhan.

   b. Identifikasi peristiwa ancaman

      Identifikasi potensi peristiwa ancaman, relevansi peristiwa, dan sumber ancaman yang dapat memulai peristiwa tersebut

   c. Identifikasi kerentanan

      Identifikasi kerentanan dan kondisi predisposisi yang memengaruhi kemungkinan kejadian ancaman yang menimbulkan dampak negatif.

   d. Penentuan kemungkinan

      Menentukan kemungkinan bahwa peristiwa ancaman menimbulkan dampak yang merugikan, dengan mempertimbangkan:

      i. karakteristik sumber ancaman yang dapat memulai peristiwa tersebut.

      ii. kerentanan/kondisi predisposisi yang diidentifikasi.

      iii. kerentanan organisasi yang mencerminkan upaya perlindungan/ penanggulangan yang direncanakan atau diimplementasikan untuk menghambat peristiwa tersebut.

e. Identifikasi Dampak

Menentukan dampak buruk dari peristiwa ancaman yang menjadi perhatian, dengan mempertimbangkan:

i. karakteristik sumber ancaman yang dapat memulai peristiwa tersebut.

ii. kerentanan/kondisi predisposisi yang diidentifikasi.

iii. kerentanan organisasi yang mencerminkan upaya perlindungan/ penanggulangan yang direncanakan atau diimplementasikan untuk menghambat peristiwa tersebut.

f. Menentukan risiko

menentukan risiko bagi organisasi dari peristiwa ancaman yang menjadi pertimbangan dengan mempertimbangkan:

i. dampak yang akan dihasilkan dari peristiwa tersebut

ii. kemungkinan terjadinya peristiwa.

3. Mengkomunikasikan hasil penilaian

a. Komunikasi hasil penilaian risiko

Mengkomunikasikan hasil penilaian risiko kepada pembuat keputusan organisasi untuk mendukung respons risiko.

b. Informasi terkait dengan risiko

Bagikan informasi terkait risiko yang dihasilkan selama penilaian risiko dengan personil organisasi yang tepat.

4. Menjaga penilaian

   a. Faktor risiko monitor

      Melakukan pemantauan berkelanjutan terhadap faktor-faktor risiko yang berkontribusi terhadap perubahan risiko pada operasi dan aset organisasi, individu, organisasi lain, atau Bangsa.

   b. Penilaian risiko yang baru

      memperbarui penilaian risiko yang ada menggunakan hasil dari pemantauan berkelanjutan faktor-faktor risiko.