p-ISSN 2088-5407
e-ISSN 2621-9001

PENGEMBANGAN APLIKASI PENILAIAN RISIKO KEAMANAN INFORMASI BERBASIS ISO 27005 MENGGUNAKAN METODE *PROTOTYPING*

Asriyanik[1], Prajoko[2]

[12]*Program Studi Teknik Informatika Universitas Muhammadiyah Sukabumi*

[12]*Asriyanik263@ummi.ac.id, prajoko@ummi.ac.id*

ABSTRAK

Penggunaan teknologi informasi pada suatu universitas terutama yang berbasis website atau mobile memiliki risiko yang cukup tinggi karena sistem yang bersifat global. Setiap risiko keamanan memiliki nilai dan level yang berbeda, begitu pula dampak dan biaya untuk penanganannya. Untuk dapat melakukan penanganan risiko yang sesuai maka harus dilakukan penilaian risiko keamanan informasi terlebih dahulu. Proses penilaian risiko salah satunya dapat menggunakan standar ISO 27005 yaitu tentang manajemen risiko keamanan informasi. Namun yang menjadi kendala, proses penilaian risiko ini masih menggunakan formulir manual sehingga tidak setiap orang dapat menggunakannya. Untuk mempermudahnya maka akan dibangun sebuah aplikasi berbasis web. Aplikasi penilaian risiko ini dibangun dengan menggunakan metode pengembangan prototyping sehingga waktu yang digunakan lebih cepat. Pengguna dari aplikasi ini adalah operator dan kepala bagian Sistem Informasi Akademik di Universitas Muhammadiyah Sukabumi sebagai tempat penelitian. Proses pengembangan system dimulai dari tahap analisis, perancangan dan implementasi. Hasil dari penellitian ini adalah menghasilkan sebuah aplikasi penilaiain risiko berbasis web yang dapat mudah digunakan oleh berbagai tipe pengguna.

Kata Kunci: *penilaian risiko, keamanan informasi, model prototyping*

PENDAHULUAN

Latar Belakang

Teknologi informasi telah menjadi bagian penting dalam membantu proses pengelolaan di suatu universitas. Terutama dengan adanya teknologi website dan mobile, maka setiap proses bisnis pada universitas menjadi berbasis website dan mobile. Pengembangan sistem berbasis website atau mobile lebih memudahkan pengguna dalam mengakses informasi karena sistem bersifat global. Namun, selain itu memunculkan kemungkinan terjadinya serangan oleh pihak yang tidak bertanggung jawab. Celah serangan untuk sistem berbasis website dapat dilakukan terhadap data, aplikasi ataupun jaringan. Jika hal ini terjadi maka akan menimbulkan dampak yang mungkin merugikan terhadap kelangsungan proses bisnis suatu universitas.

Untuk menangani hal tersebut, maka perlu dilakukan penilaian risiko keamanan informasi, agar tindakan penanganan risiko sesuai dengan prioritas. Beberapa standar untuk proses penanganan risiko keamanan informasi adalah dengan menggunakan OCTAVE, FAIR, NIST 300-80 dan ISO 27005. Setiap standar memiliki kelebihan dan kelemahan masing-masing. Namun menurut Peraturan Menteri

Komunikasi dan Informatika RI No. 4 Tahun 2016 tentang Sistem Manajemen Keamanan Informasi bahwa untuk proses pengelolaan keamanan informasi untuk organisasi publik menggunakan seri ISO 27000.

Proses penilaian risiko keamanan informasi dengan menggunakan ISO 27005 dapat dilakukan melalui beberapa tahapan Identifikasi risiko, analisis risiko dan evaluasi risiko. Pada saat ini proses penilaian risiko dengan menggunakan ISO 27005 masih menggunakan formulir manual atau dibantu dengan menggunakan Microsoft Excel. Proses penilaian risiko keamanan informasi adalah hal yang harus dilakukan oleh bidang teknologi informasi pada suatu organisasi, namun mungkin tidak setiap orang memahaminya. Untuk itu, maka perlu adanya sebuah aplikasi yang dapat memudahkan dalam proses penilaian risiko keamanan informasi. Adapun sistem yang akan dibangun adalah sistem berbasis web dengan metode pengembangan aplikasi menggunakan metode *Prototyping*.

Rumusan masalah

Rumusan masalah dari penelitian ini adalah bagaimana membangun aplikasi penilaian risiko keamanan informasi berbasis ISO 27005 menggunakan metode *Prototyping*?

Tujuan Penelitian

Tujuan penelitian yaitu menguraikan proses pengembangan aplikasi penilaian risiko keamanan informasi berbasis ISO 27005 dengan metode *Prototyping*.

STUDI PUSTAKA

Penilaian Risiko Berbasis ISO 27005

Penilaian risiko keamanan informasi adalah proses menentukan nilai risiko sehingga didapat prioritas risiko. Penilaian risiko keamanan informasi ditujukan untuk menghasilkan daftar level risiko sesuai dengan nilai risiko. Proses ini terbagi menjadi beberapa proses lagi yaitu:

a. Identifikasi Risiko, bertujuan untuk menentukan kemungkinan kerugian yang akan terjadi , kapan dan dimana kerugian yang akan muncul. Ada beberapa proses pada identifikasi risiko yaitu:
   1) Identifikasi aset, hasil yang diharapkan dari proses identifikasi aset adalah didapatkannya daftar aset untuk dikelola dengan risiko dan daftar proses bisnis yang terkait dengan aset.
   2) Identifikasi ancaman, Identifikasi ancaman dapat diperoleh dari lingkungan dalam dan luar. Dari lingkungan dalam dapat diidentifikasi dari insiden yang pernah terjadi, pengguna sistem, pemilik aset, dan juga sumber luar yang memungkinkan munculnya gangguan pada sistem. Hasil akhir dari proses ini adalah didapatkannya daftar ancaman yang dapat diidentifikasi tipe dan sumbernya.
   3) Identifikasi kendali keamanan yang telah ada. Proses ini dilakukan dengan cara mempelajari dokumen kendali yang telah dilakukan pada sistem. Hasil dari proses ini adalah didapatkannya daftar kendali keamanan yang berupa

rencana ataupun telah diterapkan dan statusnya.

4) Identifikasi kerentanan .Tujuan dari identifikasi kerentanan adalah mengetahui kelemahan yang ada pada sistem yang memungkinkan terjadinya ancaman. Kerentanan dapat berkaitan dengan aset, kontrol keamanan ataupun yang lainnya.
5) Identifikasi dampak ancaman atau insiden yang mungkin terjadi. Hasil akhir dari proses ini adalah didapatkannya daftar skenario insiden (ancaman) dan konsekuensinya yang terkait dengan proses bisnis dan aset.

b. Analisis Risiko

Analisis risiko merupakan kegiatan untuk melakukan penilaian terhadap ancaman, dampak dan risiko. Ada dua metode dalam proses analisis risiko yaitu metode kualitatif dan metode kuantitatif. Metode kuantitatif menentukan skala angka untuk menentukan kemungkinan dan dampak terjadinya risiko. Analisis kualitatif mengggunakan skala kualitatif. Proses analisis risiko terdiri dari tiga proses yaitu:

1) Penilaian dampak insiden atau ancaman Berdasarkan standar ISO 27005:2011 ada lima kriteria nilai dampak insiden yaitu very low (sangat rendah), low (rendah), medium (sedang), high (tinggi) dan very high (sangat tinggi). Penjelasan dari masing-masing kriteria dapat ditentukan oleh penanggung jawab sistem atau organisasi.
2) Penilaian kemungkinan terjadinya (likelyhood) insiden atau ancaman Kriteria kemungkinan terjadinya risiko menurut ISO 27005:2011 terdiri dari lima jenis yaitu very unlikely (sangat jarang), unlikely (jarang), possible (mungkin terjadi), likely (sering) dan frequent (sangat sering). Penamaan dan penjelasan kriteria dapat dibuat dan disesuaikan dengan kebutuhan organisasi.
3) Menentukan nilai risiko. Nilai risiko secara umum dihitung berdasarkan hasil kali nilai dampak dan nilai kemungkinan terjadinya risiko.

c. Evaluasi Risiko. Evaluasi risiko adalah proses untuk mengevaluasi level risiko yang telah didapatkan sebelumnya apakah telah sesuai atau belum dengan kondisi yang ada di lapangan dan juga referensi.

Pengembangan Perangkat Lunak

Secara umum, langkah kerja dalam pengembangan perangkat lunak meliputi tahapan berikut:

a. Analisis Kebutuhan Perangkat Lunak

Proses analisis ini adalah kegiatan dalam pengembangan perangkat lunak untuk mendapatkan kebutuhan pengguna. Hasil analisis dapat dimodelkan dengan menggunakan berbagai diagram, seperti *flowchart*, *workflow, Use Case*, *Data Flow Diagram, Flow Map* dan lainnya.

b. Perancangan Perangkat Lunak

Model perancangan perangkat lunak terbagi dua yaitu terstruktur dan berorientasi objek.

p-ISSN 2088-5407
e-ISSN 2621-9001

Setiap model memiliki diagram yang berbeda dalam menggambarkan hasil perancangannya. Selain itu juga, pada proses perancangan dilakukan perancangan basis data dan perancangan tampilan.

c. Implementasi/ Pengkodean

Implementasi adalah proses pengimplementasian hasil perancangan yang meliputi pengkodean dengan menggunakan bahasa pemrograman, pembuatan basis data dengan menggunakan Data Base Management System dan pembuatan tampilan dengan bantuan aplikasi untuk editor tampilan.

d. Pengujian Perangkat Lunak

Pengujian perangkat lunak dilakukan untuk menguji kesesuaian perangkat lunak yang telah dibuat dengan kebutuhan. Terdapat berbagai model pengujian perangkat lunak. Model pengujian yang paling sering digunakan yaitu pengujian *black box* dan pengujian *white box.*

e. Implementasi pada Lingkungan Kerja

Proses ini adalah mengimplementasikan perangkat lunak yang telah dibuat dalam lingkungan kerja. Pada tahapan ini biasanya muncul berbagai *feedback* dari pengguna untuk proses perbaikan pada masa mendatang.

Metode *Prototyping*

Pengembangan perangkat lunak dengan menggunakan metode *Prototyping* muncul saat pengembang perangkat lunak hanya memiliki sumber daya yang sedikit. Konsep pengembangan dengan model *Prototyping* dapat dilihat pada Gambar 1 berikut.

Gambar 1. Model Pengembangan *Prototyping*

a. Komunikasi

Mengkomunikasikan kebutuhan antara pembuat sistem dengan client, yaitu melalui diskusi tentang permasalahan, harapan dan solusi yang akan dibutuhkan.

b. Perencanaan Secara Cepat

Membuat perencanaan perangkat lunak dengan menggunakan diagram analisis kebutuhan sederhana sehingga dapat menentukan kebutuhan perangkat lunak yang akan dibangun secara ringkas.

c. Pemodelan Perancangan Secara Cepat

Membuat pemodelan perancangan perangkat lunak dengan ringkas yang meliputi rancangan proses, basis data dan tampilan.

d. Pembentukan Prototipe

Melalukan pengkodean sesuai dengan analisis dan rancangan awal yang telah ditentukan untuk membuat prototipe aplikasi.

e. Penyerahan sistem dan pengiriman umpan balik.

Memberikan aplikasi yang telah dibuat kepada client untuk diuji coba dan menunggu umpan balik tentang kekurangan sistem untuk diperbaiki kembali.

Kelima proses tersebut berulang sampai didapatkan aplikasi yang benar-benar sesuai dengan kebutuhan.

METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah metode *Prototyping* dalam pengembangan aplikasinya. Adapun data yang digunakan adalah data kualitatif dan proses penguraian penelitian secara deksriptif. Pengumpulan data dilakukan dengan cara wawancara, studi pustaka dan observasi terhadap lingkungan kerja di Universitas Muhammadiyah Sukabumi. Dalam proses implementasinya penelitian bertempat di Universitas Muhammadiyah Sukabumi dengan analisis kasus pada penilaian risiko Sistem Informasi Akademik.

PEMBAHASAN

a. Analisis Kebutuhan

Berdasarkan hasil pengumpulan data, maka didapatkan kebutuhan pengguna untuk aplikasi penilaian risiko keamanan informasi adalah sebagai berikut.

1) Pengguna Aplikasi

Pengguna aplikasi penilaian risiko keamanan informasi di Universitas Muhammadiyah Sukabumi adalah:

a) Operator SIM
b) Kepala Bagian SIM

2) Kebutuhan fungsional

Kebutuhan fungsional dari aplikasi penilaian risiko keamanan informasi adalah:

a) Pengguna dapat melakukan login
b) Administrator dapat melakukan menambah data pengguna
c) Pengguna dapat mengubah password
d) Pengguna dapat mengubah profil
e) Pengguna dapat memasukkan data umum tentang UMMI
f) Pengguna dapat memasukkan data identifikasi risiko yang meliputi data aset, ancaman, kontrol keamanan dan kerentanan
g) Pengguna dapat melihat mencetak data aset, ancaman, kontrol keamanan dan kerentanan
h) Pengguna dapat memasukkan data kategori dampak dan kemungkinan terjadinya risiko
i) Sistem secara otomatis dapat melakukan penilaian dan menentukan level risiko
j) Pengguna dapat melihat dan mencetak data dampak risiko, tingkat risiko, daftar skenario, dan daftar level risiko.

3) Kebutuhan non fungsional

Kebutuhan non fungsional untuk aplikasi penilaian risiko keamanan informasi ini adalah:

a) Data pengguna

p-ISSN 2088-5407
e-ISSN 2621-9001

b) Data aset
c) Data ancaman
d) Data kontrol keamanan
e) Data kerentanan
f) Data kategori dampak
g) Data kategori risiko
h) Data kategori kemungkinan
i) Data nilai risiko

b. Perancangan Proses

Rancangan aplikasi penilaian risiko keamanan informasi berbasis web adalah sebagai berikut.

Gambar 2. Workflow Aplikasi

c. Perancangan Basis Data

Aplikasi ini memiliki 12 tabel yaitu: tabel asal ancaman, tabel dokumen, tabel identifikasi ancaman, tabel identifikasi aset, tabel identifikasi kerentanan, tabel identifikasi kontrol, tabel kategori aset, tabel kategori dampak, tabel kategori kemungkinan, tabel kategori pemulihan, tabel penetapan konteks, dan tabel user.

Struktur tabel dari masing-masing tabel tersebut adalah:

1) Tabel asal ancaman

Tabel 1. Struktur Tabel Asal Ancaman

Nama Field	Tipe Data
Id	Int (11)
Kode	Varchar (25)
Asal	Varchar (25)

2) Tabel Dokumen

Tabel 2. Struktur Tabel Dokumen

Nama Field	Tipe Data
Id	Int (11)
Jenis_dok	Varchar
Nama_dok	Varchar
Nama	Varchar
Type	Varchar
Size	Varchar

3) Tabel Identifikasi Ancaman

Tabel 3. Struktur Tabel Identifikasi Ancaman

Nama Field	Tipe Data
Id	Int (11)
Kode_ancaman	Varchar
Tipe_ancaman	Varchar
Nama_ancaman	Varchar
Asal_ancaman	Varchar

4) Tabel Identifikasi Aset

Tabel 4. Struktur Tabel Identifikasi Aset

Nama Field	Tipe Data
Id	Int (11)
Kategori_aset	Varchar
Kode_aset	Varchar
Nama_aset	Varchar
Jumlah_aset	Int
Nilai_aset	Int
Deksripsi	Long text

p-ISSN 2088-5407
e-ISSN 2621-9001

5) Tabel Identifikasi Kerentanan

Tabel 5. Struktur Tabel Identifikasi Kerentanan

Nama Field	Tipe Data
Id	Int (11)
No_skenario	Int
Kode_aset	Varchar
Nama_aset	Varchar
Kategori_aset	Varchar
Kode_ancaman	Varchar
Nama_ancaman	Varchar
Nama_kerentanan	Varchar
Kontrolyangada	Varchar
keterangan	Varchar
Kemungkinanterjadi	Int
Nilai_dampak	Int

6) Tabel Identifikasi Kontrol Keamanan

Tabel 6. Struktur Tabel Kontrol Keamanan

Nama Field	Tipe Data
Id	Int (11)
Kode_aset	Varchar
Nama_aset	Varchar
Kategori_aset	Varchar
Nama_kontrol	Varchar
Penjelasan	Long text

7) Tabel Kategori Aset

Tabel 7. Struktur Tabel Kategori Aset

Nama Field	Tipe Data
Id	Int (11)
Kategori_aset	Varchar

8) Tabel Kategori Dampak

Tabel 8. Struktur Tabel Kategori Dampak

Nama Field	Tipe Data
Id	Int (11)
Kategori_dampak	Varchar
Nilai	Int
Penjelasan	Long text

9) Tabel Kategori Kemungkinan

Tabel 9. Struktur Tabel Kategori Kemungkinan

Nama Field	Tipe Data
Id	Int (11)
Kategori_kemungkinan	Varchar
Nilai	Int
Penjelasan	Long text

10) Tabel Kategori Pemulihan

Tabel 10. Struktur Tabel Kategori Pemulihan

Nama Field	Tipe Data
Id	Int (11)
Pemulihan	Varchar

11) Tabel Penetapan Konteks

Tabel 11. Struktur Tabel Penetapan Konteks

Nama Field	Tipe Data
Id	Int (11)
Nama_universitas	Varchar
Visi	Long text
Misi	Long text
Tujuan	Long text

p-ISSN 2088-5407
e-ISSN 2621-9001

Nama Field	Tipe Data
Ruang_lingkup	Long text
Kebijakan_KI	Long text

12) Tabel user

Tabel 12. Struktur Tabel Penetapan Konteks

Nama Field	Tipe Data
Id	Int (11)
Nip	Varchar
nama	Varchar
jabatan	Varchar
password	Varchar
status	Varchar

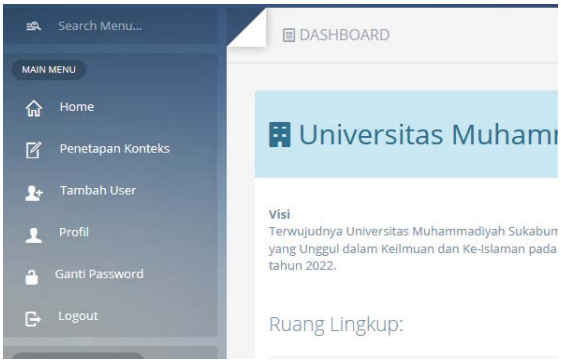
d. Implementasi

Hasil dari perancangan diimplementasikan dengan menggunakan bahasa pemrograman PHP dan basis data MySQL. Adapun hasil dari implementasi adalah sebagai berikut.

1) Tampilan halaman login

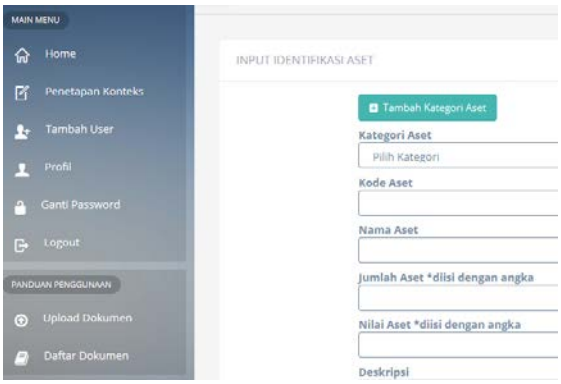
Gambar 3. Tampilan halaman login

2) Tampilan Halaman Utama



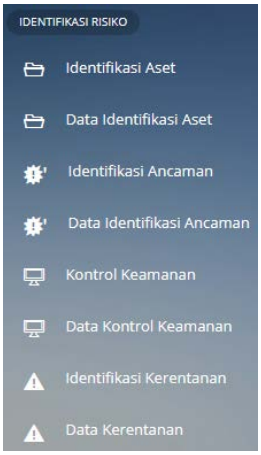
Gambar 4. Tampilan halaman utama

3) Tampilan halaman penilaian risiko



Gambar 5. Tampilan halaman identifikasi Aset

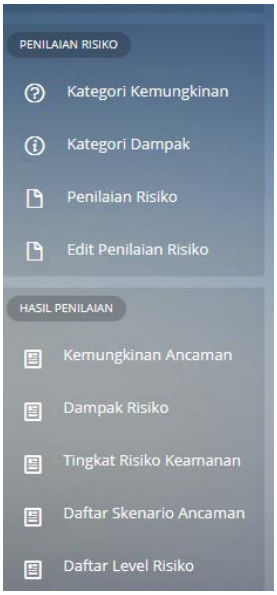
4) Tampilan Menu Identifikasi Risiko



Gambar 6. Tampilan Menu Identifikasi Risiko

p-ISSN 2088-5407
e-ISSN 2621-9001

5) Tampilan Menu Penilaian Risiko



Gambar 7. Tampilan Menu Penilaian Risiko

6) Tampilan Halaman Level Risiko

Gambar 8. Tampilan Hasil Penilaian Risiko

KESIMPULAN

Berdasar pada uraian di atas, maka untuk membuat aplikasi penilaian risiko keamanan informasi berbasis ISO 27005 dapat digunakan model prototyping karena model aplikasi yang sederhana disesuaikan dengan kebutuhan user serta dapat dilakukan dengan lebih cepat dalam proses pengembangannya.

UCAPAN TERIMA KASIH

Pada kesempatan ini kami ingin mengucapkan terima kasih kepada kementertian riset dan teknologi RI atas hibah yang telah diberikan kepada kami untuk SKIM PDP pada tahun 2018 dengan nomor kontrak 136/IV.I/K/2018. Juga kepada LPPM Universitas Muhammadiyah Sukabumi.

DAFTAR PUSTAKA

[1] Asriyanik, & Hendayun, M. (2017). Tata Kelola Teknologi Informasi Menggunakan COBIT 5. Jurnal Teknik Informatika dan Sistem Informasi (JuTISI), Vol. 3 No. 1 Hal. 206-216.

[2] Chazar, C. (2015). Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005. Jurnal Informasi, VII(2), Vol 7 No. 2 Hal: 48-57.

[3] Dewi, N. A., & Yudana, I. G. (2016). Analisa Manajemen Risiko pada Sistem Akademik di STMIK STIKOM Bali. Seminar Nasional Teknologi Informasi dan Multimedia 2016 (pp. 7-12). Yogyakarta: STIMIK AMIKOM.

[4] Djaelangkara, R. T., Sengkey, R., & Lantang, O. A. (2015). Perancangan Sistem Informasi Akademik Sekolah Berbasis Web Studi Kasus Sekolah Menengah Atas Kristen 1 Tomohon. Jurnal Teknik Elektro dan Komputer, Hal. 86-94.

[5] Indrayani, E. (2011). Pengelolaan Sistem Informasi Akademik Perguruan Tinggi Berbasis Teknologi Informasi dan

Komunikasi (TIK). Jurnal Penelitian Pendidikan, Vol.12 No. 1 Hal: 51-67.

[6] Iskandar, K. (2012). Perancangan Sistem Informasi Akademik Perguruan Tinggi Menggunakan Use Case dan Rich Picture. ComTech, Vol. 3 No. 1 Hal: 654-662.

[7] ISO. (2011). ISO 27005: Information Security Risk Management. Switzerland: ISO.

[8] Kementrian Komunikasi dan Informatika RI. (2016). *Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Jakarta: Kemkominfo RI.*

[9] Pressman, Roger. (2012). *Rekayasa Perangkat Lunak – Pendekatan Praktisi.* Yogyakarta: Andi.

[10] Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). Jurnal CorelIT, 2(2), Vol.2 No.2 Hal: 8-13.