Implementasi Manajemen Risiko pada Aplikasi XYZ dengan Pendekatan SNI ISO/IEC 27005:2018

1st Rahmat Rambe
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
rahmatrambe@student.telkomuniversity.ac.id

2nd Arfive Gandhi
Fakultas Informatika
Universitas Telkom
andung, Indonesia
arfivegandhi@telkomuniversity.ac.id

3rd Mira Kania Sabariah
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
mirakania@telkomuniversity.ac.id

Abstrak—*Risk manager* atau manager risiko adalah suatu proses yang pengelolaan risikonya dilakukan terhadap suatu ketidakpastian yang berkaitan dengan ancaman yang terjadi pada suatu website atau aplikasi sehingga menyebabkan tumbuhnya risiko. Metodologi risk manager sendiri sering digunakan dalam manajemen proyek yang terbaru untuk pengelolaan risiko, Proses sistem Aplikasi XYZ sendiri berisi mengenai informasi data pribadi calon mahasiswa dan data administrasi yang berhubungan dengan universitas. Semua pengisian data dilakukan oleh calon mahasiswa secara online melalui aplikasi yang disediakan. Pada sistem PMB yang sedang berlangsung saat ini ditemukan banyak permasalahan yang dialami oleh calon mahasiswa terutama pada saat penguksesan aplikasi. Oleh karena itu, data yang masuk kedalam sistem database universitas ada double, tidak ke upload dan gagal proses penginputan. Masing-masing risiko ditangani secara accept, avoid. Hasil akhir penelitiain ini digunakan untuk melihat daftar risiko, ancaman, dan yang lainnya yang berkaitan serta mengeluarkan solusi dan pemberian keputusan yang akan dipertimbangkan kembali oleh pihak Universitas ABC dalam pengembangan, pengelolaan dan pemeliharan Aplikasi XYZ kedepannya. Solusi yang yang dikeluarkan pada penelitian terdapat pada bagian rekomendasi kontrol yang di buat berdasarkun rekomendasi dari ISO 27005.

Kata kunci— *risk manager*, SNI ISO/IEC 27005:2018, universitas XYZ, sistem penerimaan mahasiswa baru (PMB), aplikasi XYZ.

I. PENDAHULUAN

Perkembangan teknologi yang semakin maju dan luas dimanfaatkan oleh Universitas ABC sebagai salah satu peluang perkembangan kemajuan IPTEK dan melihat indeks kemajuan penggunaan teknologi di kalangan siswa, dosen, dan masyarakat sekitar universitas. Setiap aplikasi yang digunakan dan dimplementasikan dengan sesuai alur, proses bisnis, dan kebutuhan akan memiliki risiko, Risiko bisa terjadi dari segi mana saja, dari segi software maupun hardware. Timbulnya risiko juga dapat diperoleh dari penggunaan aplikasi.dari developer sebagai pembuat aplikasi dan, dari biaya yang dapat merugikan perusahaan jika risiko yang ditimbulkan aplikasi sangat banyak dan harus terus dilakukan perbaikan dan pemeliharan. Salah satu contoh dari studi kasus yang diangkat dalam penelitian ini dan telah digunakan oleh hampir semua universitas di indonesia dan merupakan salah satu bagian dari perkembangan teknologi era kemajuan saat ini adalah Aplikasi XYZ.

Proses penerimaan mahasiswa baru dilakukan oleh pihak universitas dengan beberapa tahapan dan untuk sekarang sudah dapat dilakukan secara online melalui aplikasi. Alur dari proses sistem penerimaan mahasiswa baru melalui Aplikasi XYZ bertujuan memudahkan calon-calon mahasiswa. Proses diawali dengan calon-calon mahasiswa membuat akun pribadi, mengisi identitas diri, melakukan pembayaran administrasi pendaftaran, dan lainnya yang disesuaikan dengan kebutuhan dan alur penerimaan mahasiswa baru. Sebagai tanda bukti pendaftaran calon-calon mahasiswa baru yang telah berhasil. Penerapan Aplikasi XYZ ini memiliki dampak positif dan negatif, pada penyedia aplikasi. Pada saat pandemi ini dan kondisi teknologi yang semakin berkembang dampak positifnya adalah proses pendaftaran lebih efisien dan memperluas jangkauan pendaftaran. Dengan adanya aplikasi ini, pengetahuan orang- orang mengenai teknologi semakin update dan semakin maju. Untuk dampak negatif terdapat biaya atau pengeluaran dalam pembuatan, pemeliharan, dan perbaikan aplikasi. Semua hal tersebut yang merupakan dampak terhadap aplikasi dari segi kerugian bisa disebabkan karena aplikasi yang mengalami kerusakan ataupun timbulnya suatu risiko yang menyebabkan penggunaan dan proses berjalannya aplikasi mengalami kehambatan.

Aplikasii XYZ sendiri dari pengamatan terhadap pengembangan yang dilakukan belum mengimplementasikan manajemen risiko yang baik, sehingga pengembang merespon risiko yang terjadi pada aplikasi secara sporadic dan reaktif, bukan berdasarkan apa yang telah direncanakan dari awal sebelum pembuatan

aplikasi. Risiko sendiri adalah sebuah kejadian yang sangat merugikan bagi saatu perusahaan atau penyedia aplikasi dan bersifat sangat tidak pasti dalam jangka waktu tertentu [1]. Risiko yang timbul ini harus dikendalikan terlebih dahulu dengan upaya untuk tidak terjadinya gangguan atau timbulnya risiko lain yang lebih besar terhadap penyedia aplikasi dan aplikasi itu sendiri. Pada aplikasi yang dijadikan sebagai objektif dalam penelitian ini umumnya yang timbul adalah risiko dari segi teknologi, keuangan, dan sistem operasional.

Dengan timbulnya risiko pada Aplikasi XYZ diperlukannya suatu Teknik untuk mengendalikan risiko tersebut. Teknik ini disebut risk management atau manajemen risiko. Manajemen risiko adalah suatu proses yang dimana pengelolaan risiko sendiri dilakukan terhadap suatu ketidakpastian yang berkaitan dengan ancaman yang terjadi pada suatu aplikasi [2]. Manajemen risiko sendiri disini adalah suatu konsep horu yang digunakan dalam upaya bisnis bidang e-commerce ataupun lainnya termasuk salah satunya hidang pendidikan [2]. Metodologi manajemen risiko sendiri sering digunakan dalam tahap manajemen proyek yang terbaru akan pengelolaan risiko. Hal tersebut dilakukan karena konsep ini memiliki adaptabilitas yang tinggi terhadap setiap perubahan yang terjadi. Salah satu metode yang digunakan dalam konsep manajemen risiko adalah dengan menggunakan pendekatan standar SNI ISO/IEC 27005:2018. Pendekatan ini adalah suatu indeks yang ditentukan dan diterapkan untuk memantau, menerapkan, mengkaji, memelihara, dan perbaikan terhadap sistem manajemen keamanan sistem informasi terutama dalam mengatasi tumbuhnya suatu risiko terhadap suatu aplikasi [3].

Alasan penggunaan pendekatan ini adalah karena mende pendekatan ini sangat sesuai dengan sasaran kebutuhan perusahaan dalam penerapan dan proses manajemen risiko yang terjadi pada suatu aplikasi. Alasan lain menggunakan pendekatan ISO 27005-2018 adalah karena ISO 27005:2018 adalah bagian dari keluarga ISO 27005 yang memiliki beberapa kelebihan seperti, mengurangi vulnerability, mengurangi threat, mengurangi impact dan lainnya. Pendekatan ini juga digunakan dalam konsep manajemen risiko adalah untuk menilai kesesuaian terhadap suatu pihak baik secara internal maupun eksternal dan dapat melihat hasil akhir daftar risiko, daftar ancaman dan daftar keterkaitan antara risiko yang terjadi dengan ancamannya dan bagaimana solusi yang tepat untuk mengatasi risiko tersebut dengan mengacu pada nilai risiko yang telah di peroleh sebelumnya. Oleh karena itu dalam penelitian ini peneliti memanfaatkan kelebihan dan manfaat dari ISO 27005 sendiri terutama dalam proses sistem keamanan informasi dan manajemen informasi yang baik pada Aplikasi XYZ sebagai upaya dalam pengurangan tingkat risiko.

Penelitian ini bertujuan untuk mengetahui apa saja risiko yang ditimbulkan pada setiap aset yang dimiliki oleh Aplikas iXYZ termasuk ancaman apa saja yang berpotensi mempengaruhi aplikasi tersebut. Serta untuk mengetahui bagaimana penerapan manajamen risiko pada Aplikasi XYZ setelah dilakukannya unalisis risiko dan mengetahui solusi apa saja yang direkomendasikan untuk memperbaiki peningkatan timbulnya risiko berdasarkan data risiko dan ancaman yang sebelumnya. Serta untuk mengetahui apakah rekomendasi tersebut sudah sesuai dengan yang ingin dicapai oleh pihak Universitas ABC.

II. KAJIAN TEORI

A. Risk/Risiko

Risiko adalah suatu akibat yang kurang menyenangkan dan dimana disini maksudnya bisa merugikan atau membahayakan dari suatu perbuatan atau tindakan. Dengan kata lain risiko adalah suatu kemungkinan yang ditimbulkan karena adanya ketidakpastian sehingga mengakibatkan suatu kerugian yang disebabkan karena kehilangan Sebagian atau keseluruhan modal. Risiko juga dapat diartikan sebagai suatu peluang terjadinya ancaman [1].

B. Risk Manager/Manajemen Risiko

Manajemen risiko adalah suatu proses pendekatan atau pengelolaan terhadap saatu metodologi yang mengelola suatu ketidakpastian risiko yang berkaitan dengan ancaman, Dengan kata lain, manajemen risiko adalah suatu pendekatan terstruktur yang bertugas untuk mengelola ketidakpastian yang berkaitan dengan ancaman sehingga menyebabkan tumbuhnya suatu risiko. Tugas manajemen risiko sendiri adalah untuk menetapkan risiko dan meng-kategorikan risiko tersebut. Di dalam proses manajemen risiko terdapat penilaian risiko yang bertujuan untuk menilai di tingkat atau level mana serta di prioritas manakah risiko yang telah diidentifikasi sebelumnya. Salah satu cara untuk mengelola risiko yang terjadi atau sebuah ancaman yaitu dibutuhkan sebuah strategi seperti memindahkan risiko kepada pihak lain (transfer risk). Menghindari risiko (avoid risk),mengurangi efek negative risiko (mitigate risk) dan menampung Sebagian risiko tertentu (accept risk) [2].

GAMBAR 1
ELEMENT MANAJEMEN RISIKO

C. Keamanan Informasi

Keamanan informasi adalah suatu mekanisme atau kegiatan untuk penjagaan suatu informasi tersebut aman dari seluruh ancaman yang mungkin terjadi sebagaimana hal ini adalah suatu upaya dalam memastikan dan menjamin kelangsungan proses bisnis,meminimalkan risiko bisnis dan memaksimalkan peluang bisnis. Sistem keamanan dilihat dari proses penyimpanan, pemprosesan,dan transmisi yang dimana ketiganya harus aman secara integritas, available dan confidentially dalam upaya transmisi mekanisme penerapan sistem keamanan informasi [3]. Menurut Lawrie Brown dalam upaya menjaga suatu informasi beliau menyarankan menggunakan “Risk Management Model” untuk menghadapi ancaman yang akan terjadi pada suatu

sistem. Ada 3 komponen yang memberikan kontribusi besar terhadap suatu risiko, yaitu asset,vulnerabilities,dan threats [4].

D. Standar Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) atau lebih sering dikenal dengan sebutan ISMS (Information Security Management System) adalah suatu rencana atau strategi manajemen yang menspesifikasikan kebutuhan-kebutuhan yang diperlukan untuk implementasi kontrol keamanan yang telah disesuaikan dengan kebutuhan organisasi. ISMS juga dapat dikatakan sebagai suatu pendekatan yang sistematis dalam menetapkan,mengimplementasikan,mengoperasional.memantau meninjau dan memelihara serta meningkatkan keamanan suatu informasi pada suatu organisasi dalam upaya mencapai suatu tujuan bisnis. Sistem keamanan informasi sendiri tidak hanya berhubungan pada perangkat lunak tetapi secara keseluruhan seperti dari sisi orang, proses dan teknologi yang digunakan. Pengelolaan kemanan sistem informasi yang baik dibutuhkan untuk mengantipasi ancaman-ancaman yang kemungkinan akan terjadi [1].

E. Teknik Manajemen Risiko

Teknik manajemen risiko sendiri memiliki beberapa komponen yang akan digunakan sebagai komponen pada penentuan faktor risiko yang termasuk didalamnya yaitu pemeliharaan dan pengembangan suatu perangkat lunak. Oleh karena itu dibutuhkannya suatu analisis dengan cara membuat kuisioner yang disebar kepada beberapa responden. Setiap komponen yang ada memiliki tahapan-tahapan tersendiri dalam upaya pengelolaan perangkat lunak seperti dari segi komponen penentuan requirements.penjadwalan kerja,interaksi dengan pengguna.pengerjaan.pelatihan hingga tahap akhir dari segi evaluasi [2].

F. ISO/IEC 27005:2018

SNI ISO/IEC 27005:2018 adalah suatu standarisasi indeks yang dibuat dalam pengukuran, pemantauan, penerapan, pengkajian, pemeliharaan, dan perbaikan model Sistem Manajemen Keamanan Informasi (SMKI). Desain penerapan SMKI dari suatu perusahaan sendiri dipengaruhi oleh kebutuhan dan sasaran dari perusahaan tersebut. Standarisasi ini dibuat dengan sistem pendukungnya dapat diperkirakan akan berubah dari waktu ke waktu. Penerapan SMKI disesuaikan dengan kebutuhan yang di inginkan oleh perusahaan. Standar yang digunakan disini ditujukan untuk menilai kesesuaian sistem oleh pihak terkait haik secara internal maupun kebutuhan eksternal [5]

III. METODE

Penelitian ini menggunakan pendekatan secara kualitatif dan pengolahan data secura observasi dan wawancara. Pendekatan kualitatif adalah suatu pendekatan yang dilakukan oleh peneliti secara utuh terhadap subjek penelitian yang dilakukan [6]. Dalam pendekatan kualitatif peneliti harus mampu melihat dan menemukan letak suatu peristiwa dari suatu fenomena yang terjadi secara langsung untuk dipahami dan diumati. Fenomena yang dapat diamati secara langsung seperti tingkah perilaku, persepsi, motivasi ataupun tindakan lain yang dilakukan secara holistic.

Teknik Pengumpulan data dalam penelitian ini menggunakan teknik triangulasi. Teknik triangulasi adalah teknik pengumpulan data yang dimana menggabungkan pengambilan data melalui observasi. Wawancara, dokumentasi dan survey menjadi suatu kesatuan dalam proses yang terpadu. Teknik triangulasi sendiri dalam sebuah penelitian bertujuan untuk mencari ketidaksamaan antara data yang diperoleh dari satu sumber dengan sumber lainnya. Hal ini dimaksudkan untuk menyatukan perbedaan yang ada supaya kesimpulan yang diambil lebih akurat dan tepat. Dalam penelitian ini pengumpulan data dispesifikkan kembali dengan menggunakan pengumpulan data dari hasil observasi dan wawancara. Observasi dilakukan langsung pada objek penelitian dan wawancara dilakukan pada staff analisis dan pengelola pengembangan Aplikasi XYZ. Proses observasi dilakukan pada aplikasi secara langsung untuk mengamati secara langsung fakta-fakta yang akan di jadikan dasar dalam penelitian ini sesuai keadaan dan perilaku objek penelitian. Secara umum hasil penelitian ini dengan menggunakan teknik observasi dan pendekatan kualitatif lebih menekankan makna daripada generalisasi

Wawancara dilakukan untuk memberikan dan menanyakan mengenai kesimpulan yang dibuat oleh peneliti dan hasil penelitian mengenai tingkat risiko yang terjadi pada aplikasi sertu bagaimana sistem manajemen dalam menangani risiko yang muncul dengan baik dan benar, Wawancara dilakukan pada orang yang memiliki tanggung jawab besar pada Aplikasi XYZ, terutama aset yang dimiliki. Penelitian ini juga di tinjau berdasarkan waktu dan data yang diperoleh.dimana pelaksanaan penelitian ini menggunakan sistem cross sectionall. Sistem cross sectionall adalah suatu sistem dimana penelitian yang dilakukan hanya satu kali dan titik fokusnya berpusat pada analisis data berdasarkan variabel yang ditentukan serta hasil observasi yang diamati [6]. Semua yang diperoleh dikumpulkan pada satu waktu dan pada sampe data yang sama dan telah ditetapkan sebelumnya.

IV. HASIL DAN PEMBAHASAN

Proses manajemen risiko sendiri disini menggunakan teknik pendekatan SNI ISO 27005:2018. Pada bab ini juga akan dijelaskan mengenai data-data yang dibutuhkan dimulai dari teknik pengumpulan data, penetapan konteks, penilaian risiko, manajemen risiko dan kesimpulan atau pengambilan sebuah keputusan. Universitas ABC mempunyai banyak aset yang berhubungan dengan Aplikasi XYZ tersebut sehingga aset ini dapat dijadikan sebuah data untuk di identifikasi dan dilakukan manajemen risiko serta melihat daftar risiko beserta dampak ancamannya.

A. Context establishment

Context establishment atau penetapan ruang lingkup atau penetapan konteks adalah tahapan awal dalam penyusunan manajemen risiko dalam teknik manajemen risiko menggunakan teknik iso 27005 [2]. Context establishment disini bertujuan sebagai landasan awal sebelum melakukan risk assesment. Penentuan ruang lingkup dilakukan pada Aplikasi XYZ. Ruang lingkup

yang akan dibahas pada penelitian ini berdasarkan data atau aset yang dimiliki Universitas ABC terutama yang berkaitan dengan Aplikasi XYZ tersebut seperti *hardware*, *software* dan data lainnya.

Kriteria kemungkinan terjadi atau likelihood adalah suatu ketetapan untuk mengukur tingkat kemungkinan terjadinya suatu risiko [3]. Berikut Kriteria Kemungkinan Terjadi Llikelihood dapat dilihat pada tabel 1 sebagai berikut :

TABLE 1
KRITERIA KEMUNGKINAN TERJADI LLIKELIHOOD)

Level	Kemungkinan	Keterangan
q	Sangat Rendah (SR)	Kemungkinan terjadinya kecil yaitu 1 kali dalam setahun pada beberapa kondisi yang tidak normal atau tidak pernah terjadi sama sekali pada beberapa kondisi.Presentasi kemungkinan terjadinya adalah ≤10%.
2	Rendah (R)	Kemungkinan terjadinya kecil yaitu 1 – 2 kali dalam setahun pada banyak keadaan dengan tingkat presentasi kemungkinan terjadinya adalah 13% > x ≤ 25% dalam setahun.
3	Sedang (SD)	Pada setiap kondisi atau keadaan kemungkinan terjadi yaitu 4-8 kali dengan tingkat presentasi kemungkinan terjadinya adalah 25% > x ≤ 35% dalam setahun.
4	Tinggi (T)	Akan ada kemungkinan terjadi dalam 1 tahun sebanyak >15 kali pada setiap kondisi atau banyak keadaan.Persentasi kemungkinan terjadinya adalah 35% > x ≤ 65%.
5	Sangat Tinggi (ST)	Kemungkinan terjadi dapat berturut-turut pada banyak keadaan atau kondisi.Persentasi kemungkinan terjadi dalam 1 tahun >65%.

Kriteria impact atau dampak adalah suatu ketetapan untuk mengukur tingkat kemungkinan dampak yang terjadi terhadap suatu risiko [3]

TABLE 2
KRITERIA DAMPAK (IMPACT)

Level	Kategori Dampak	Keterangan
1	Sangat Rendah (Tidak Signifikan)	Tidak ada pengaruh yang signifikan terhadap proses kegiatan operasional serta tidak mengancam atau mengganggu proses bisnis.Dampak operasional serta biaya yang ditimbulkan pada skala ini sangat kecil sehingga pengaruh terhadap keamanan aset sangat tidak berpengaruh sama sekali.
2	Rendah	Dampak yang ditimbulkan pada sistem operasional tidak terlalu serius dan sangat kecil atau hanya berpengaruh pada jaringan tidak secara menyeluruh.Pada skala ini pengaruh dampak yang ditimbulkan pada sistem operasional hanya sekitaer 5-10% dan hal ini dapat ditangani langsung dengan cara di maintanance.
3	Sedang	Dampak yang ditimbulkan pada skala ini dari segi proses kegiatan operasional sudah cukup besar yaitu sekitar 10-15%. Kegiatan operasional sudah mengalami kelumpuhan dan data atau informasi yang terdapat didalamnya mengalami error.Untuk akses hanya dapat dilakukan oleh satu pihak yaitu admin atau pihak yang diizinkan untuk memegang akses terhadap sistem.Pada skala ini sama dengan skala rendah untuk mengenai data atau aset akan ada yang hilang,rusak atau tidak dapat digunakan atau diakses sehingga diperlukan data backup dan membutuhkan waktu yang cukup lama untuk mengembalikan/memulihkannya.
4	Tinggi (signifikan)	Pada skala ini kemampuan kegiatan operasional sudah dapat dikatakan kehilangan kontrol yang sangat besar yaitu sekitar 1520% tetapi belum hampir secara menyeluruh dan untuk pengaksesan masih sama dengan skala sedang yaitu hanya pihak admin atau pihak yang diberikan memegang kendali akses terhadap sistem.Untuk mengenai data atau aset pada skala ini sama seperti pada skala sedang tetapi untuk pemulihan butuh waktu yang sangat cukup lama atau tidak dapat sama sekali dipulihkan.Hal ini juga berdampak pada kerahasiaan dan kejaminan data yang terdapat didalamnya.
5	Sangat Tinggi (Sangat Signifikan)	Skala ini adalah skala yang sangat sangat besar yaitu sistem mengalami kegagalan atau kelumpuhan total pada kegiatan operasional dan tingkat kegalalan ini sebesar >20%. Hal ini mengakibatkan kegiatan operasional sistem tidak dapat dilanjutkan atau dengan kata lain terhenti total.Untuk data atau aset sama seperti pada skala signifikan yaitu data atau aset tidak dapat dipulihkan atau dikembalikan sama sekali. Data atau aset informasi dicuri oleh pihak tertentu sehingga kerahasiaan dan kejaminan data sama sekali tidak terjaga dengan baik. Hal ini mengakibatkan kepercayaan terhadap instansi menurun akibat dari dampak yang ditimbulkan.

B. Analisis Risk

Analisis risiko dilakukan dengan meneliti risiko yang ada berdasarkan nilai tingkat kemungkinan terjadi,nilai tingkat ancaman yang terjadi pada aset tersebut dan nilai dampak nya. Sehingga diperoleh daftar risiko yang terjadi pada aset yang dimiliki dan tingkat risiko tersebut.

TABLE 3
DATA HASIL PENELITIAN RISIKO

No	Kode Aset	Kode Resiko	Ancaman	Likehood	Dampak	Nilai	Tingkat Resiko
1	AS1	R1	AC1. Akses data oleh pihak yang tidak berhak (sniffing).	4	5	20	High
		R2	AC8. Kerusakan Hardware.	3	3	16	Medium
		R3	AC11. Gangguan upgrade system.	3	4	12	Medium
		R4	AC12. Adware,Malware, Spyware.	4	5	20	High
		R5	AC13. Perangkat error saat digunakan/ngebug.	2	3	6	Low
		R6	AC14. Kesalahan penggunaan perangkat IT.	2	2	4	Low
2	AS2 AS3 AS4 AS5	R7	AC1. Akses data oleh pihak yang tidak berhak (sniffing).	4	5	20	High
		R8	AC2. Duplicate data.	2	2	4	Low

Berdasarkan paparan analisis risiko diatas,secara keseluruhan dinyatakan bahwa keseluruhan aset yang dimiliki Universitas ABC pada Aplikasi XYZ tersebut memiliki hasil yaitu teridentifikasinya 41 risiko dengan 3 kategori yaitu : High dengan nilai 17-25, Medium dengan nilai 10-16 dan Low dengan nilai 1-9. Dengan adanya data ini dapat dikatakan bahwa semua aset yang dimiliki memiliki peran yang sangat penting bagi proses bisnis dan keberlangsungan aktivitas.

Mengacu pada Tabel 4 penelitian ini mengambil 3 data hasil analisis risiko, yaitu pada risiko R40 yang berskala Low (sangat rendah), risiko R38 yang berskala Medium (sedang) dan risiko 36 yang berskala High (tinggi). Risiko R40 merupakan risiko yang terjadi pada data aset ke 15 dan ancaman ke 13 pada Aplikasi XYZ. Risiko ini berhasil di identifikasi dan di analisis dengan melihat nilai dampak nya yaitu sebesar 3 dan nilai likehoodnya adalah sebesar 2. Hasil perolehan nilai tersebut disesuaikan berdasarkan kriteria kemungkinan terjadinya risiko dan kriteria kemungkinan dampak yang terjadi yang dibahas pada tabel 4 dan 5. Nilai likehood dan nilai dampak akan dimasukkan kedalam matriks risiko sehingga hasil perkalian kedua nilai tersebut memperoleh nilai tingkat risiko. Hal ini sudah dilakukan dan ditanyakan melalui wawancara langsung pada staff pengembangan Aplikasi XYZ mengenai hasil dan nilai yang diperoleh.

TABLE 4
ESTIMASI RISIKO

Nilai Jangkauan	Tingkat Risiko		Estimasi Penanganan Risiko
1-9	Sangat Rendah, Rendah	Low	≤ 3 Hari
10-16	Sedang	Medium	5 – 8 Hari
17-25	Sangat Tinggi, Tinggi	Hight	≥ 10 Hari

C. Risk Evalution

Berdasarkan hasil analisis risiko yang telah dilakukan dan dipaparkan pada tabel data hasil penelian risiko, risiko yang telah berhasil di identifikasi dan dilakukan perbandingan sesuai ancaman yang terjadi pada tiap aset serta diberi keterangan tingkat risikonya maka selanjutnya adalah paparan hasil evaluasi risiko berdasarkan data pada tabel 15 dan kriteria evaluasi risiko,maka pada tabel 18 ini dapat diketahui prioritas risiko dalam proses manajemen risiko yang dilakukan.

TABLE 5
HASIL REKAP EVALUASI PENILAIAN RISIKO

No	Kode Risiko	Nilai Risiko	Penerimaan Risiko	Prioritas
1	R1	20	Tidak Diterima	1
2	R4	20	Tidak Diterima	2
3	R7	20	Tidak Diterima	3
4	R11	20	Tidak Diterima	4
5	R13	20	Tidak Diterima	5
6	R16	20	Tidak Diterima	6
7	R17	20	Tidak Diterima	7
8	R19	20	Tidak Diterima	8
9	R21	20	Tidak Diterima	9
10	R26	20	Tidak Diterima	10
11	R29	20	Tidak Diterima	11
12	R31	20	Tidak Diterima	12
13	R36	20	Tidak Diterima	13
14	R2	9	Tidak Diterima	14
15	R3	12	Tidak Diterima	15
16	R9	12	Tidak Diterima	16
17	R20	12	Tidak Diterima	17
18	R27	12	Tidak Diterima	18
19	R28	12	Tidak Diterima	19
20	R30	12	Tidak Diterima	20
21	R32	12	Tidak Diterima	21
22	R33	12	Tidak Diterima	22
23	R35	12	Tidak Diterima	23
24	R38	12	Tidak Diterima	24
25	R39	12	Tidak Diterima	25
26	R10	9	Diterima	26
27	R15	9	Diterima	27
28	R18	9	Diterima	28
29	R23	9	Diterima	29
30	R25	9	Diterima	30
31	R37	9	Diterima	31
32	R5	6	Diterima	32

33	R12	6	Diterima	33
34	R22	6	Diterima	34
35	R40	6	Diterima	35
36	R6	4	Diterima	36
37	R8	4	Diterima	37
38	R14	4	Diterima	38
39	R24	4	Diterima	39
40	R41	4	Diterima	40
41	R34	3	Diterima	41

D. Prototype

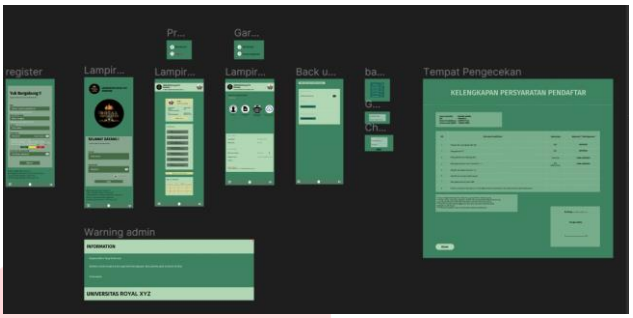
Desain prototype yang dibuat menggunakan desain model handphone karena pada saat ini kebanyakan masyarakat setiap harinya menggunakan handphone serta lebih praktis dan simpel. Pembuatan prototype dengan handphone sebagian model desain juga dapat mempermudah calon mahasiswa baru mengakses dengan mudah aplikasi tersebut terutama pada fitur-fitur nya. Pembuatan prototype selain dari sisi pengguna (calon mahasiswa baru) juga dibuat dari sisi pengguna (admin), karena ada beberapa fitur tambahan atau perbaikan dari segi sisi admin terhadap aplikasi tersebut [7].

Rancangan prototype dengan mendesain ulang aplikasi pada fitur login dengan studi kasus gambaran desain ditujukan pada pengguna aplikasi khususnya calon mahasiswa baru di Universitas ABC. Desain protoype dilakukan sesuai rekomendasi kontrol nomor 9, kode A.9.4.3 tentang sistem pengaturan password dan A.11.2.2 mengenai utilitas pendukung yang merujuk pada risiko nomor 24 dan 41 dengan skala rendah tetapi tetap menjadi masalah ditiap aplikasi.

Desain yang dibuat yaitu dengan menambahkan satu fitur atau satu utilitas pendukung pada bagian sub menu register. Yang dimasuk penambahan utilitas pendukungnya disini adalah menambahkan skala pada saat pembuatan password aplikasi. Password tersebut harus memenuhi skala yang dibuat agar akun bisa terdaftar dan bisa login dikemudian waktu. Penambahan skala disini sudah sesuai dengan proses manajemen risiko pengenai pengaturan password yang baik dan terlindungi. Penambahan fitur warning/reminder serta pengecekan data pada aplikasi oleh admin adalah kreativitas pengembangan aplikasi yang disesuaikan dengan kebutuhan pengguna serta manajemen keamanan data dan informasi. Hal ini merujuk rekomendasi kontrol nomor 8, kode A.12.1.3 tentang pemeliharaan peralatan dan rekomendasi kontrol nomor 9, kode A.9.4.3 tentang utilitas pendukung. Berdasarkan penelitian yang dilakukan,risiko yang terjadi berada pada skala kecil hingga sedang.

Pada aplikasi juga akan ditampilkan status pencadangan yang telah dilakukan seperti jumlah kapasitas data yang dicadangkan,waktu pencadangan terakhir, opsi pencadangan apakah dilakukan setiap hari,minggu atau bulan. Serta ada juga fitur delete backup untuk menghapus file atau data yang telah dicadangkan sebelumnya dan pengaturan mengenai akun yang dijadikan tempat pencadangan seluruh file.

Berikut adalah tampilan desain prototype secara keseluruhan yang terdiri dari desain protoype pada menu login,tampilan depan proses pendaftaran,tampilan desain backup, manajemen password hingga desain prototype tampilan warning untuk admin dan pengecekan data pendaftaran calon mahasiswa baru sudah sesuai atau tidak.



GAMBAR 2
TAMPILAN RANCANGAN PROTOTYPE

V. KESIMPULAN

Berdasarkan penelitian yang dilakukan pada Aplikasi XYZ dengan pendekatan ISO/IEC 27005:2018 dan dilakukannya implementasi manajemen risiko pada aplikasi tersebut maka diperoleh kesimpulan bahwa Diperoleh hasil identifikasi jenis ancaman dan risiko berdasarkan kriteria kemungkinan dan dampak, muka secara keseluruhan terdapat 15 jenis ancaman dari 16 data aset yang dimiliki dan diperoleh dan Aplikasi XYZ tersebut. Terdapat 41 risiko yang diperoleh berdasarkan data aset, kemungkinan ancaman dan dampak yang terjadi. Jenis ancaman dan risiko yang diperoleh dibagi kedalam 3 kategori dari 5 kriteria kemungkinan, yaitu low (rendah), medium (sedang) dan hight (tinggi).nSehingga dimana setiap 1 aset dapat memiliki lebih dari 1 ancaman yang terjadi baik yang sama jenisnya maupun beda. Dan setiap ancaman memiliki dampak yang berbeda-beda. Olehbkarena itu dari hasil identifikasi diperoleh data 13 jenis ancaman yang berkategori high (tinggi), 12 jenis ancaman yang berkategori medium (sedang) dan 16 jenis ancaman yang berkategori low (rendah). Dalam hal ini dapat disimpulkan juga bahwa aset yang diperoleh dari Aplikasi XYZ mayoritas atau kebanyakan memiliki tingkat kemungkinan terjadinya ancaman yang berskala rendah (low).

Hasil penelitian dan analisis risiko yang dilakukan pada aset yang dimiliki Aplikasi XYZ tersebut terdapat 6 risiko yang dapat ditangani secara accept, 13 risiko secara avoid. 12 risiko secara mitigate dan 10 risiko yang ditangani secara transfer. Selanjutnya dilakukan implementasi manajemen risiko dengan pendekatan ISO/IEC 27005:2018 pada Aplikasi XYZ dan diperlukan 16 rekomendasi kontrol terhadap 41 risiko yang sesuai dengan ketetapan dan referensi dari ISO/IEC 27005:2018. Rekomendasi kontrol tersebut meliputi pembatasan akses informasi, pemeliharaan, pencadangan, teknisi ulasan aplikasi dan kontrol terhadap malware. Hal tersebut sudah disesuaikan dengan kebutuhan dari Universitas ABC sendiri.

REFERENSI

[1] S. Sahira, R. Fauzi, I. Santosa and e. al. "Analisis Manajemen Risiko Pada Aplikasi E-Office Yang Dikelola oleh Pt. Telkom Indonesia Menggunakan Standar ISO/IEC 27005: 2018." Analisis Manajemen Risiko Pada Aplikasi E-Office Yang Dikelola Oleh Pt. Telkom Indonesia Menggunakan Standar ISO/IEC 27005: 2018, vol. 7, no. 2, pp. 6897-6909. 2020.

[2] E. Nursetyawati, R. Fauzi and ….. "Perancangan Manajemen Keamanan Informasi Menggunakan Metode Analisis Risiko ISO 27005:2018 pada Dinas Komunikasi dan Informatika Jawa Barat," eProceedings…… vol. 7, no. 2, pp. 7338-7347, 2020.

[3] A. Anang. A. Gandhi and Y. G. Sucahyo, "The Design of Information Security Risk Management: A Case Study Human Resources Information System at XYZ University," Proceedings-2021 4th International Conference on Computer and Informatics Engineering: IT-Based Digital Industrial Innovation for the Welfare of Society, IC21E 2021. Pp. 198-203, 2021.

[4] R. G. Fajar Ilham Satria Yudha, "RISK ASSESSMENT PADA MANAJEMEN RESIKO KEAMANAN INFORMASI MENGACU PADA BRITISH STANDARD ISO/IEC 27005 RISK MANAGEMENT." Jurnal stt garut.ac.id, vol. 13, no. 1. P. 8. 2016.

[5] W. Yustanti, A. Qoiriah, R. Bisma and A. Prihanto, "Strategi Identifikasi Resiko Keamanan Informasi Dengan Kerangka Kerja ISO 27005:2018," Journal of Information Engineering and Educational Technology, vol. 3, no. 2, pp. 51-56, 2019.

[6] D. Sugiyono, Metode Penelitian Kuantitatif, Kualitatif.dan Tindakan, 2013.

[7] L. S. Musianto, "Perbedaan Pendekatan Kuantitatif Dengan Pendekatan Kualitatif Dalam Metode Penelitian." Jurnal Manajemen dan Wirausaha, vol. 4, no. 2, pp. 123-136, 2002.

[8] B. Hendrik and B. R. Suteja, "Identifikasi Risiko Program Maintenance dalam Pengelolaan Proyek Berbasis Agile Menggunakan Pohon Klasifikasi." Jurnal Teknik Informatika dan Sistem Informasi, vol. 7. No. 1, pp. 296-306, 2021.

[9] J. Jonny. A. Ambarwati and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas Dan Aset Menggunakan ISO 27005," Sistemasi, vol. 10, no. 1, p. 1, 2021.

[10] e. a. Inge S. "Risk Assesment Pada Manajemen Resiko Keamanan Informasi Mengacu Pada British Standard ISO/IEC 27005 Risk Management," Occupational Medicine, vol. 53, no. 4, p. 130, 2013,

[11] S. Salahuddin, A. Ambarwati and M. N. A. Azam, "Identifikasi Risiko Keamanan Informasi Menggunakan ISO 27005 Pada Sebuah Perguruan Tinggi Swasta Di Surabaya." Seminar Nasioanl Sistem Informasi (SENASIF), pp. 990-996, 2018.

[12] R. Puspita, "Analisis Manajemen Resiko Teknologi Informasi Dan Pemetaan Maturity Level Pada Pt. Xyz Menggunakan Framework Cobit 4.1." Jurnal Manajemen Informatika (JAMIKA), vol. 7, no. 2, pp. 43-54, 2017.

[13] M. Cobit and A. Pambudi, "Audit Keamanan Informasi Berdasarkan Triangle CIA," Information Technology Journal (INTECHNO Journal), vol. 1, no. 4, pp. 47-56, 2019.

[14] F. Mubarok, H. Harliana and I. Hadijah, "Perbandingan Antara Metode RUP dan Prototype Dalam Aplikasi Penerimaan Siswa Baru Berbasis Web." Creative Information Technology Journal, vol. 2, no. 2. P. 114.

[15] C. Chazar, "Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001:2005." Jurnal Informasi. Vol. 7, no. 2, pp. 48-57, 2017.

[16] A. Widya, Suripto and D. Adistya, "Identifikasi Risiko Penerapan E-Ticketing (Pada Perum Damri Cabang Lampung)," Jurnal Kompetitif Bisnis, vol. 1, no. 5, pp. 251-257, 2021.

[17] F. Nasher, "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, pp. 1-16, 2020.

[18] D. Rahmat, "Perancangan Sistem Manajemen Keamanan Informasi Menggunakan Standar SNI ISO/IEC 27001:2013," Jurnal Informatika-COMPUTING Volume 06 Nomor 02, Desember 2019: 37-41 ISSN:2656-3861, vol. 06, pp. 37-41, 2019. [19] L. S. O. I.J.T.C.IJ.T.IS. S. 2.IS. ISO, "Iso/lec 27005:2008," vol. 3, p. 61, 2008.

[20] S. S. E. F. Y. S. G. A. R. Patino, "ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005." 2018 5th International Conference on eDemocracy and eGovernment, ICEDEG 2018, no. 2021, pp. 75-82, 2018.

[21] I. M. M. M. K. Putra. "Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005," 3rd 2021 East Indonesia Conference on Computer and Information Technology, EIConCIT 2021, pp. 14-19, 2021.