Jurnal Gema Pustakawan
Vol. 9, No. 2, Desember 2021, pp. 130~148
ISSN: 2338-2171

Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan Universitas Riau)

Endang Murniati[1],Evi Susanti[2], Nurhayati[3], dan Rusmadi Awza[4]

[1,2,3]Perpustakaan Universitas Riau
[4]Dosen Jurusan Ilmu Komunikasi Fisip Universitas Riau

Email: endang_murniati@yahoo.co.id

Diajukan: 15-11-2021; **Direview**: 05-12-2021; **Diterima**: 20-12-2021; **Direvisi**: 27-12-2021

Abstrak

Risiko teknologi informasi (TI) di Perpustakaan Universitas Riau, merupakan kejadian yang berpotensi mengganggu proses pelayanan. Risiko TI yang belum terpetakan, mengakibatkan ketidakseimbangan dalam proses identifikasi risiko, sehingga layanan kurang optimal. Untuk memperbaiki ketidakseimbangan ini, risiko TI harus diidentifikasi dan layanan TI harus ditingkatkan agar proses layanan perpustakaan tidak terhenti. Tujuan dari penelitian ini adalah untuk mendapatkan gambaran tentang penerapan framework NIST SP 800-30 oleh Perpustakaan Unri untuk evaluasi risiko sistem informasi perpustakaan. Metode yang digunakan dalam penelitian ini adalah dengan melakukan wawancara dengan orang-orang yang terlibat langsung dengan sistem aplikasi SLiMS Perpustakaan Unri. Temuan penelitian ini dapat digunakan untuk memetakan risiko dengan merinci bagaimana menilai risiko sistem informasi perpustakaan dan bagaimana mengelola bahaya sistem informasi perpustakaan Unri.

Kata Kunci: Management resiko, Metode NIST SP 800-30, Sistem Informasi

Abstract

In the Unri Library, the risk of information technology (IT) is an event that has the potential to disrupt the service process. IT risks that have not been mapped have resulted in an imbalance in the risk identification process in the Unri Library, so that services are less than optimal. To correct this imbalance, IT risks must be identified and IT services must be improved so that the library service process is not stalled. The purpose of this study was to obtain an overview of the application of the NIST SP 800-30 framework by the Unri Library for risk evaluation of library information systems. The method used in this research is to conduct interviews with people who are directly involved with the Unri Library SLiMS application system. The findings of this study can be used to map risks by detailing how to assess the risk of library information systems and how to manage the dangers of Unri's library information systems.

Keywords: Risk Management, NIST SP 800-30 Method, Information Systems

Pendahuluan

Perpustakaan Universitas Riau telah melaksanakan Sistem Manajemen Mutu (SMM) ISO 9001-2008 sejak tahun 2016 dan diupgrade menjadi ISO 9001-2015 pada tahun 2019, implementasi sistem manajemen mutu ini bertujuan untuk memberikan pelayanan yang bermutu kepada masyarakat pada umumnya dan pemustaka Universitas Riau pada khususnya. Pelayanan bermutu ini bertujuan untuk memberikan kepuasan kepada pemustaka. Berbicara masalah pelayanan bermutu adalah pelayanan yang dapat memberikan kepuasan kepada pemustaka yang artinya pemustaka mendapat pelayanan informasi secara cepat, mudah dan tepat, pelayanan tersebut dapat

diberikan apabila menggunakan sistem informasi dalam pengelolaan perpustakaan. Sistem informasi adalah perpadan antara teknologi informasi yang terdiri dari perangkat keras *(hardware)* dan perangkat lunak *(software)* dan informasi itu sendiri yang merupakan koleksi perpustakaan. Jadi teknologi informasi merupakan alat atau media untuk mengkomunikasikan koleksi perpustakaan kepada pengguna, sehingga pemustaka dapat dengan mudah, cepat dan tepat mendapatkan informasi yang dibutuhkan.

Kolaborasi informasi dengan menggunakan perangkat teknologi web memungkinkan kecepatan dan keakuratan informasi menjadi tujuan utama, oleh karena itu ketika ada ungkapan "siapa yang menguasai informasi" muncul di masyarakat, dapat dipastikan bahwa ia memiliki keunggulan posisi dalam persaingan global. Saat ini, karakteristik pengguna perguruan tinggi semakin bergantung pada informasi terkini. Hal ini menjadikan suatu tantangan dan sekaligus menjadi peluang untuk mengembangkan konsep perpustakaan berbasis digital.

Risiko sering didefinisikan sebagai beberapa jenis hambatan yang mengganggu sistem informasi. Risiko dapat didefinisikan sebagai setiap kejadian atau situasi yang berhubungan dengan sistem informasi perpustakaan yang berdampak negatif pada perpustakaan. Jika terjadi gangguan pada sistem informasi perpustakaan maka kegiatan pengelolaan perpustakaan dan layanan akan terhenti karena sistem informasi perpustakaan juga berperan sebagai sistem manajemen perpustakaan sehingga apabila salah satu unsur atau bagian bermasalah maka akan terganggu proses lainnya.

Perpustakaan Universitas Riau (UNRI) telah mengaplikasikan sistem informasi yang dilatarbelakangi oleh pengetahuan, perkembangan ilmu dan teknologi. Implikasi dari penerapan sistem informasi tersebut mengantarkan Perpustakaan Unri mendapatkan beberapa prestasi yaitu mendapatkan akreditasi dari Perpusnas dengan nilai maksimal "A" dan mendapat sertifikat ISO 9001 tahun 2008 dan 2015 sehingga pencapaian ini dapat mendukung akreditasi Universitas dan akreditasi prodi di lingkungan Unri. Perpustakaan Unri sudah menerapkan manajemen risiko yang merupakan salah satu persyaratan dari sistem manajemen mutu oleh ISO 9001-2015 sejak tahun 2019, namun pelaksanaannya sebatas perencanaan dan pelaksanaan yang dituangkan dalam bentuk *SOP (Standar Operasional Prosedur)* dan melaksanakan kegiatan berdasarkan permasalahan yang terjadi pada bidang informasi teknologi. Penilaian risiko secara lebih menyeluruh belum dilakukan dan hanya berjalan apa adanya.

Maulana (dalam Nurochman, 2014) menyatakan semakin banyak aset informasi yang tersedia bagi pengguna melalui teknologi web, semakin besar ancaman terhadap pengoperasian yang tepat dari sistem informasi perpustakaan. Penggunaan manajemen risiko sistem informasi dapat mengurangi dampak kerusakan yang dapat berupa konsekuensi finansial, penurunan reputasi, penghentian aktivitas perusahaan, kegagalan aset yang dapat dinilai, dan keterlambatan dalam pengambilan keputusan.

Teknik rencana kerja atau kerangka penilaian risiko NIST *(National Institute of Standart and Tecnology)* SP 800-30, yang dapat digunakan untuk memeriksa bahaya sistem informasi perpustakaan merupakan metode untuk menerapkan manajemen risiko sistem informasi yang komprehensif dan terorganisir. Kerangka kerja NIST SP 800-30 menganalisis manajemen risiko secara mendalam dalam kaitannya dengan model proses analitis pada tingkat praktik manajemen sejalan dengan siklus hidup pengembangan sistem, sehingga ideal untuk digunakan dalam menilai risiko dalam aktivitas manajemen risiko sistem informasi. Para peneliti berikut menawarkan berbagai studi sebelumnya yang mengeksplorasi tantangan manajemen risiko di perpustakaan dalam

kaitannya dengan rencana kerja NIST SP 800-30, yang digunakan untuk menganalisis risiko dalam sistem informasi perpustakaan.

Nurochman (2014) dengan judul penelitian "Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan UGM)" yang diteliti menggunakan metode kualitatif dengan pendekatan studi kasus, dengan studi utama yang akan diteliti adalah implementasi manajemen risiko sistem informasi perpustakaan menggunakan Publikasi Khusus NIST 800-30 kerangka kerja manajemen risiko, dengan hasil 1. Berdasarkan peringkat tingkat risiko, metode penilaian risiko menguraikan profil risiko yang mengancam sistem informasi perpustakaan, termasuk bentuk risiko teknologi dan bahaya manusia 2. Pengurangan risiko atau *risk reduction* adalah dilakukan dengan menggeser risiko 3. Kajian manajemen risiko tidak dilakukan sesuai prosedur 4. Struktur Kajian NIST SP 800-30 dapat menjelaskan profil ancaman risiko yang menghambat pengembangan perpustakaan berbasis web.

Selanjutnya Valena, dkk. (2019) melakukan penelitian dengan judul yang senada yaitu "Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode NIST SP 800-30, metode yang digunakan kualitatif, dengan hasil 1. Proses penilaian risiko mendeskripsikan profil resiko yang mengancam sistem informasi perpustakaan berdasarkan rangking level resiko meliputi keterlambatan pengembalian buku, buku hilang, tidak ada backup data sejarah buku rusak, ketidaksesuaian data, dan pinjam meminjam KTM orang lain. 2. Mitigasi risiko atau peringanan resiko dilaksanakan dengan mengimplementasikan sistem *early warning* dan monitoring. 3. Evaluasi manajemen resiko belum dilaksanakan sesuai prosedur. 4. Kerangka kerja NIST SP 800-30 mampu mendeskripsikan profil ancaman resiko yang mengancam keberlangsungan sistem informasi pada sebuah organisasi.

Sedangkan hasil penelitian dari Astuti (2018) dengan judul "Implementasi Manajemen Risiko Sistem Informasi Menggunakan Cobit 5", merupakan penelitian dengan tema yang sama namun dengan kerangka kerja yang berbeda. Cobit 5 adalah domain proses APO 12 (Align, Plan, Organize) yang merupakan kerangka kerja dengan urutan kerja sebagai berikut: mengumpulkan data, menganilisis resiko, menjaga profil resiko, mengartikulasi risiko, menentukan portofolio tindakan pengelolaan dan menanggapi risiko, dengan hasil mendapatkan gambaran profil resiko yang mengancam sistem informasi perpustakaan berdasarkan rangking level risiko.

Hasil penelitian dari Han, dkk. (2016) dengan judul "*Risk assessment of digital library information security: a case study*" penelitian ini mengadopsi *convenience sampling* untuk memilih responden. Penilaian aset dilakukan melalui analisis bisnis dan fungsi terkait perpustakaan digital melalui kuesioner yang mengumpulkan data untuk menentukan jenis aset dan pentingnya atribut aset. Metode kuesioner skala Likert lima poin digunakan untuk mengidentifikasi kemungkinan ancaman dan pengaruhnya terhadap aset.

Hasil penelitian dari Xie, dkk. (2019) dengan judul *"An IoT-based risk warning system for smart libraries"* bertujuan mengusulkan sistem peringatan risiko untuk pembangunan atau renovasi perpustakaan dalam aspek manajemen risiko. Sistem yang digunakan Sistem berbasis Internet of Things (IoT) yang diusulkan terdiri dari sensor yang secara otomatis memantau status material, peralatan, dan aktivitas konstruksi secara real time. Teknik AI termasuk penalaran berbasis kasus dan himpunan fuzzy diterapkan. Hasil temuannya adalah Sistem dapat dengan mudah melacak aliran material dan memvisualisasikan proses konstruksi. Percobaan menunjukkan bahwa sistem yang diusulkan dapat secara efektif mendeteksi, memantau dan mengelola risiko dalam proyek konstruksi termasuk pembangunan perpustakaan.(Xie, dkk., 2019).

Dari gambaran hasil penelitian sebelumnya, dan pentingnya kegiatan penilaian risiko sistem informasi perpustakaan sebagai layanan utama Perpustakaan Universitas Riau dalam mewujudkan pelayanan prima, maka peneliti memilih untuk melakukan penelitian dengan judul "Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan Universitas Riau)

Tinjauan Pustaka

A) Manajemen Resiko

Menurut Angreni (2018) manajemen risiko yang terintegrasi dikenal dengan istilah *Enterprise Risk Management* (ERM). Perkembangan ekonomi global dan ekonomi digital yang melanda sendi-sendi bisnis, penerapan ERM semakin penting dan dibutuhkan, baik di tingkat global maupun domestik. Manajemen risiko digambarkan sebagai suatu cara untuk mengenali, mengkualifikasi, memutuskan sikap, menemukan solusi, dan memantau serta melaporkan risiko yang terjadi dalam setiap tindakan atau proses secara logis dan metodis. (Nurochman, 2014).

Bagaimana sebuah organisasi dapat mengelola risiko yang dihadapinya tergantung dari bagaimana manajemen risiko digunakan dalam lingkungan organisasi. Manajemen risiko pada hakikatnya dilakukan melalui proses identifikasi risiko, penilaian dan pengukuran risiko, serta pengelolaan risiko, menurut Hanafi, sebagaimana dikemukakan oleh Nurochman (2014). Organisasi sering mengoptimalkan risiko karena mereka merasakan potensi imbalan dari risiko ini; namun, jika sebuah organisasi tidak dapat mengambil risiko, hampir dipastikan tidak akan berkembang.

Pendapat beberapa pakar tentang manajemen resiko yang telah dipaparkan, peneliti menarik kesimpulan bahwa manajemen risiko merupakan upaya dari suatu organisasi untuk meminimalkan dampak dari kerugian atau ketidakpastian dalam bentuk penerapan proses perbaikan secara terus menerus dalam proses pengambilan keputusan. Hal ini merupakan tantangan dan risiko yang harus dihadapi jangan dihindari bila ingin berkembang. Risiko dikelola sesuai dengan ketentuan atau kerangka kerja sehingga akan mendatangkan suatu peluang yang akan membesarkan organisasi tersebut.

B) Sistem Informasi

Menurut Tantra (dalam Nurochman, 2014), sistem informasi adalah metode sistematis untuk mengumpulkan, memasukkan, memproses, dan menyimpan data, serta mengelola, mengendalikan, dan melaporkannya untuk membantu perusahaan atau organisasi mencapai tujuannya.

SLIMS (Senayan Library Information Manajemen System)

Senayan Library Information Management System (SLIMS), menurut Ridho (dalam Murniati, 2019), merupakan perangkat lunak sistem manajemen perpustakaan *open source* berlisensi di bawah GPL v3. Perpustakaan Kemendiknas, Pusat Informasi dan Humas, Kemendiknas adalah yang pertama mengembangkan dan memanfaatkan aplikasi ini. Program ini akhirnya dibangun oleh komunitas pengguna dan penggiat SLiMS dari waktu ke waktu. Kontrol versi PHP, MySQL, dan Git digunakan untuk membuat aplikasi SLiMS. SLiMS berhasil meraih juara pertama kategori open source pada ajang INAICTA 2009.

Aplikasi Senayan Library Information Management System (SLIMS) merupakan program sistem informasi manajemen perpustakaan. Sebagian besar fitur sudah melayani kegiatan perpustakaan, seperti *Online Public Access Catalog* (OPAC), pencarian sederhana (*Simple Search*)

dan pencarian lanjutan (*Advanced Search*), manajemen keanggotaan, manajemen data bibliografi, manajemen sirkulasi (pinjaman, pengembalian, dan denda), laporan dan statistik, penghitung pengunjung, dan 2 fitur berguna lainnya untuk membantu mempermudah pengelolaan tugas perpustakaan.

C). Perpustakaan

Menurut Yusup (2012), perpustakaan dipandang tidak hanya sebagai ruang secara fisik, tetapi juga sebagai rangkaian kegiatan yang dihasilkan dari kontak dan komunikasi. Perpustakaan juga dilihat sebagai salah satu dari banyak struktur masyarakat, dan dalam beberapa hal, perpustakaan dianggap sebagai ilmu pengetahuan dan seni. Dalam hal perpustakaan sebagai suatu proses kegiatan, maka proses yang terjadi di lingkungan perpustakaan lebih diutamakan. Komunikasi antar komponen (manusia, media, suku cadang, alat, lingkungan, dan informasi) terjadi satu arah secara sinergis dan rumit.

Berikut ini akan dijelaskan pengertian khusus perpustakaan perguruan tinggi yang digunakan peneliti sebagai obyek penelitian. Perpustakaan menurut PNRI (2017) merupakan aspek penting dari kegiatan pendidikan, penelitian, dan pengabdian kepada masyarakat, serta berperan sebagai pusat sumber belajar untuk membantu perguruan tinggi memenuhi tujuan pendidikannya.

Jenis-jenis Ancaman Sistem Informasi Perpustakaan

Menurut Nurochman (2014) sumber ancaman yang memungkinkan mengganggu aktivitas layanan sistem informasi perpustakaan antara lain:

a. Ancaman Alam
   Bencana alam, seperti banjir, tsunami, kelembaban yang berlebihan, intrusi air laut, badai, dan bencana terkait air lainnya, diklasifikasikan sebagai risiko alam. Tanah longsor, gempa bumi, dan letusan gunung berapi adalah semua potensi risiko terhadap tanah. Kebakaran hutan, petir, dan angin kencang termasuk di antara bahaya alam lainnya.
b. Acaman lingkungan / teknis.
   Gangguan listrik, seperti pemadaman listrik, pengurangan tegangan, atau peningkatan cepat gangguan listrik dari waktu ke waktu, adalah contoh risiko lingkungan. Medan elektromagnetik, gangguan hewan pengerat (tikus), dampak insektisida, dan kebocoran AC adalah semua hal yang perlu dipertimbangkan.
c. Ancaman manusia
   Ancaman yang berasal dari manusia terbagi menjadi dua ancaman dari internal perpustakaan dan eksternal perpustakaan.

D) Kerangka Kerja Manajemen Risiko

Ada banyak kerangka kerja untuk melakukan aktivitas manajemen risiko sistem informasi, yang merupakan seperangkat proses standar untuk mengelola dan memberikan pengetahuan untuk aktivitas manajemen risiko yang dilakukan secara bertahap. NIST menerbitkan pedoman untuk Panduan Manajemen Risiko untuk Sistem Teknologi Informasi melalui publikasi khusus kerangka kerja NIST SP 800-30.

NIST *(National Institute of Standard and Technology) Special Publication (SP)* 800-30 merupakan panduan manajemen risiko untuk sistem teknologi informasi, menurut Erlanda (2018). Ini adalah teknik kualitatif yang digunakan untuk mempelajari keamanan untuk mengidentifikasi, mengevaluasi, dan mengelola risiko sistem TI. Pemerintah Pusat Amerika Serikat telah menetapkan

seperangkat standar. Prosedur ini cukup menyeluruh, termasuk mulai dari risiko hingga identifikasi sumber untuk melakukan tinjauan dan penilaian yang berkelanjutan.

NIST SP 800-300 merupakan framework yang digunakan dalam sistem informasi manajemen risiko, menurut Dini (2020), di mana NIST memberikan tiga langkah dalam proses manajemen risiko, yaitu penilaian risiko, mitigasi risiko, dan evaluasi risiko. Hasil akhir dari aktivitas tersebut adalah serangkaian saran untuk mengurangi bahaya yang akan muncul dalam sistem informasi.

NIST mengeluarkan rekomendasi melalui publikasi khusus 800-30 tentang *Risk Management Guide for Information Technology System*. Terdapat 9 proses dalam pengelolaan risiko. Berikut adalah penjelasan lebih rinci mengenai sembilan langkah pada metode NIST:

1. Karakteristik sistem (*System Characterization*)

Tahap pertama pada penilaian resiko pada sistem TI adalah menentukan ruang lingkup usaha. Batas-batas terhadap sistem harus diidentifikasi terlebih dahulu, bersama dengan sumber daya dan informasi yang merupakan bagian dari sistem tersebut pada tahap ini. Karakteristik sistem TI membentuk ruang lingkup dari penialaian risiko, yang menggambarkan batas-batas otorisasi operasional atau akreditasi, dan memberikan informasi (misalnya, perangkat keras, perangkat lunak, interface sistem, data dan informasi, divisi yang bertanggung jawab atau dukungan personil, dan data kritis.

2. Identifikasi Ancaman (*Threat Identification*)

Setiap kondisi atau kejadian yang berpotensi menyebabkan kerusakan pada sistem TI diklasifikasikan sebagai sumber ancaman. Manusia, alam, dan bahaya lingkungan adalah sumber risiko yang paling umum. Proses ini mendeteksi ancaman yang akan mengeksploitasi kelemahan sistem TI. Kelemahan atau kerentanan mungkin secara tidak sengaja disebabkan atau dieksploitasi secara aktif. Ketika tidak ada ancaman, sumber ancaman tidak menimbulkan risiko. Saat memeriksa kemungkinan ancaman risiko, penting untuk mengevaluasi sumber bahaya, potensi kerentanan, dan tindakan saat ini.

3. Identifikasi Kerentanan (*Vulnerability Identification*)

Proses ini terdiri dari pembuatan daftar kerentanan sistem teknis dan non-teknis (kekurangan atau kelemahan) yang mungkin sebabkan oleh kemungkinan sumber ancaman. Kerentanan dapat berkisar dari peraturan yang tidak memadai atau bertentangan yang mengendalikan penggunaan komputer organisasi untuk perlindungan yang tepat hingga berbagai perangkat lunak, perangkat keras, atau kesalahan lain yang membentuk jaringan komputer organisasi. Output - Kumpulan kerentanan sistem (pengamatan) yang dapat dieksploitasi oleh sumber ancaman yang mungkin.

4. Analisis Kontrol (*Control Analysis*)

Tujuan dari langkah ini adalah untuk melakukan analisa pengendalian yang telah diimplemantasikan atau direncanakan untuk meminimalkan atau menghilangkan kemungkinan-kemungkinan ancaman dari kelemahan dan kekurangan yang ada.

5. Penentuan Kemungkinan (*Likelihood Determination*)

Penilaian secara keseluruhan terhadap kemungkinan atau kecenderungan yang menunjukan adanya peluang kelemahan yang dapat dilakukan oleh lingkungan ancaman. Berikut ini faktor-faktor yang harus dipertimbangkan seperti motivasi dan sumber ancaman, sifat dari kerentanan, dan keberadaan dan efektifitas pengendalian saat ini dapat dilihat pada tabel 1.

Tabel 1. Defenisi Kemungkinan/Kecenderungan

Tingkat Kemungkinan Resiko	Defenisi Kemungkinan
Tinggi	Sumber ancaman bermotivasi tinggi yang dapat mempengaruhi perusahaan atau organisasi; ini terjadi ketika langkah-langkah untuk menghindari kerentanan tidak efektif.
Sedang	Sumber ancaman yang dapat memberikan dampak negatif kepada instansi, tetapi instansi tersebut masih dapat melakukan control di area yang dapat menghambat keberhasilan dari kerentanan.
Rendah	Kontrol digunakan untuk mencegah, secara drastis mengurangi, atau memblokir kerentanan yang akan muncul di dalam perusahaan dari sumber ancaman bermotivasi rendah.

Sumber: Manajemen Risiko It Pada Sistem Iraise Menggunakan Metode Nist SP 800-30 (Yuriska, 2021)

6 Analisis Dampak (Impact Analysis)

Tujuan dari fase ini adalah untuk mengetahui seberapa besar dampak negatif dari ancaman dari keberhasilan mengeksploitasi kerentanan. Relevansi misi organisasi, sensitivitas dan kekritisan (nilai atau kepentingan), biaya terkait, hilangnya kerahasiaan, integritas, dan ketersediaan sistem dan data adalah semua aspek yang perlu dipertimbangkan. Besaran *rating efek* ditentukan oleh klasifikasi SP NIST 800-30 rendah, sedang, dan tinggi, seperti terlihat pada tabel 2 di bawah ini:

Tabel 2. Defenisi besarnya Dampak

Besarnya Dampak	Defenisi Dampak
Tinggi	a. Dapat mengakibatkan kehilangan yang sangat tinggi dari aset atau sumber daya berwujud utama yang sangat mahal. b. Dapat secara signifikan melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. c. Dapat menyebabkan kematian manusia atau cedera serius.
Sedang	a. Dapat mengakibatkan kehilangan yang sangat tinggi dari aset atau sumber daya berwujud utama yang sangat mahal. b. Dapat melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. c. Dapat menyebabkan cedera pada manusia.
Rendah	a. Dapat mengakibatkan hilangnya beberapa asset atau sumber daya b. Secara nyata dapat mempengaruhi misi, reputasi, atau minat

	organisasi.

Sumber: Manajemen Risiko IT Pada Sistem Iraise Menggunakan Metode Nist SP 800-30 (Yuriska, 2021)

7. Penentuan Risiko (Risk Determination)

Pada tahap ini penilaian terhadap tingkat risiko bagi sistem TI dilakukan. Kemungkinan sumber ancaman menyerang kerentanan sistem TI, serta sejauh mana efek yang akan terjadi jika sumber ancaman berhasil menyerang kerentanan sistem TI, digunakan untuk menentukan kategori risiko ini. Untuk mengurangi dan menghilangkan bahaya, kebijakan pengendalian keamanan saat ini harus diikuti.

8. Rekomendasi Control (Control Recommendations)

Kontrol yang dapat meminimalkan atau menghilangkan risiko ditemukan di seluruh prosedur ini. Tujuan dari pedoman pengendalian adalah untuk menurunkan tingkat risiko sistem TI dan data ke tingkat yang dapat ditanggung oleh perusahaan. Pertimbangkan faktor-faktor berikut ketika merekomendasikan kontrol dan opsi alternatif untuk mengurangi atau menghilangkan risiko yang teridentifikasi: (a) Efektivitas dari pilihan yang disarankan, (b) Perundang-undangan dan peraturan, (c) Kebijakan organisasi, dan (d) Dampak Operasional .

9. Dokumentasi

Hasil penilaian risiko (sumber ancaman dan kerentanan yang teridentifikasi, penilaian risiko, dan saran pengendalian) harus didokumentasikan dalam laporan formal setelah selesai.

Metode penelitian

Penelitian ini menggunakan teknik kualitatif dan pendekatan studi kasus. Dengan melakukan wawancara mendalam dan observasi langsung (observasi) serta meringkas item-item yang terkait dengan sasaran penelitian, maka penelitian dilakukan secara cermat, menyeluruh, dan menyeluruh. Penerapan manajemen risiko sistem informasi perpustakaan yang memanfaatkan kerangka kerja manajemen risiko Publikasi Khusus NIST 800-30 adalah penelitian utama yang harus dieksplorasi.

Penelitian kualitatif mengacu pada konteks sosial, yang terdiri dari tiga elemen: tempat, pelaku, dan aktivitas yang berinteraksi secara sinergis. Dalam penelitian ini, situasi sosial merupakan aspek intrinsik dari organisasi perpustakaan yang berkaitan dengan penggunaan manajemen risiko sistem informasi. Pemilihan sumber data untuk orang yang diwawancarai dilakukan secara sengaja, dengan pertimbangan dan tujuan tertentu.

Informan penelitian adalah pegawai perpustakaan yang memiliki pengalaman dan berinteraksi dengan sistem informasi perpustakaan. Informan penelitian dapat dikatagorikan sebagai berikut: Koordinator IT, koordinator pengembangan koleksi, staf bagian pelayanan, staf bagian server dan programer, staf bagian jaringan dan hardware, staf bagian web.

Hasil dan Pembahasan

Proses Penilaian Risiko

Tahapan penilaian risiko menggunakan framework NIST SP 800-30 meliputi proses sebagai berikut:

Karakteristik Sistem *(System Characterization*)

Perangkat keras, perangkat lunak, data dan informasi, serta sumber daya manusia yang mendukung sistem informasi merupakan karakteristik dari sistem SLiMS. PC dengan perangkat lunak program aplikasi dan Windows 10 Professional 64 bit sebagai sistem operasi adalah salah satu sumber daya perangkat keras. Perangkat lunak server didasarkan pada sistem operasi Linux dan bahasa pemrograman PHP. Data infrastruktur, data perangkat, data server, dan data penyerang adalah contoh data dan informasi.

a. Spesifikikasi Perangkat keras

Tabel 3. Spesifikasi Perangkat Keras

NAMA HARDWARE	SPESIFIKASI	JUMLAH	SATUAN
Unifi Access Point U6-LR-US	Features: 1.3 GHz dual-core processor (now upgraded to support full-duplex 1 Gbps TCP/IP performance)	1	Unit
Unifi Access Point AC SHD UAP-AC-SHD.	Ubiquiti Unifi Access Point AC SHD UAP-AC-SHD. • Dimensions: 220 x 220 x 48.1 mm • Weight: 830 g	1	Unit
Unifi Access Point Nano HD	4x4 MU-MIMO on 5GHz (1733Mbps max PHY rate), 2x2 MIMO on 2.4GHz (300Mbps max PHY rate) 802.3af	2	Unit
Unifi Access Point AC M PRO	Overview Of Unifi UAP Nano HD UAP-nanoHD MU-MIMO Enterprise AP Compact 802.11ac Wave2 MU-MIMO Enterprise Access Point.	2	Unit
Unifi Switch 16 Port	Specifications: ~ Model: US-16-150W ~ 16x Gigabit ports ~ 1x Serial Console Port	2	Unit
Unifi Switch 8 Port	Deskripsi ubiquiti unifi switch 8port poe 60w / us-8-60w US-8-60W Dimensions 148.0 x 99.5 x 30.7 mm (5.83 x 3.92	1	Unit
LINKSYS Gigabit Switch	Accelerate your performance and productivity when you send large files to network servers, drives, and printers at Gigabit speeds. - Wired connection speed up to 1000 Mbps	6	Unit
PC All In One	ACER All-in-One Aspire S24-880 [DQ.BA8SN.002] - Black Processor: Intel Core i7-8550U RAM: 8GB DDR4	1	Unit
PC All In One	Desktop PC All In One ASUS [V222UBK-BA541D] DOS Prosesor Intel® Core™ i5-8250U Processor Sistem Operasi DOS	38	Unit
Mini PC	Deskripsi INTEL NUC 6CAYH 4GB SSD 120gb MINI PC CPU: Intel Celeron J3455 CPU, quad-core, 1.5 GHz (2.3 GHz burst), 10W TDP	5	Unit
PC All In One Pelayanan Mandiri	LENOVO All-in-One A340-22IWL [F0EB00HMID] - Black	4	Unit

b. Spesifikasi Perangkat lunak server

Software untuk Server: terdiri dari : PVE (Proxmox Virtual Environment), VPS (Virtual personal Server). Sedangkan setiap VPS sendiri memiliki perangkat sebagai berikut: [1] OS (Operating System); dalam mesin server virtual yang dibangun untuk sistem ini sistem operasi yang digunakan adalah sistem operasi Linux Ubuntu Server, [2] Web server; sebagai web server digunakan Apache2, [3] DBMS (Database Management System); sebagai DBMS dalam sistem ini adalah MySQL Server, versi menyesuaikan, program ini bisa didapatkan secara gratis dengan men-download dari internet, [4] Sistem Otomasi Perpustakaan; aplikasi ini merupakan aplikasi utama yang dijalankan di atas server yang telah disiapkan.

c. Spesifikasi Perangkat lunak server

Software untuk Server: terdiri dari : PVE (Proxmox Virtual Environment), VPS (Virtual personal Server). Sedangkan setiap VPS sendiri memiliki perangkat sebagai berikut: [1] OS (Operating System); dalam mesin server virtual yang dibangun untuk sistem ini sistem operasi yang digunakan adalah sistem operasi Linux Ubuntu Server, [2] Web server; sebagai web server digunakan Apache2, [3] DBMS (Database Management System); sebagai DBMS dalam sistem ini adalah MySQL Server, versi menyesuaikan, program ini bisa didapatkan secara gratis dengan men-download dari internet, [4] Sistem Otomasi Perpustakaan; aplikasi ini merupakan aplikasi utama yang dijalankan di atas server yang telah disiapkan.

d. Spesifikasi jaringan server

Spesifikasi infrastruktur untuk jaringan adalah sebagai berikut:

1. PC Router; 2 Core CPU, 2 Gb Ram, 500 Gb Hd, Rj45 Port x2
2. Network Switch 1 gbps x 8 port
3. Network Switch 100 mbps x 24 port x 2
4. Network Switch 100 mbps x 8 port x 12
5. UTP Cable Cat 6

e. PC Pengguna/Operator :

- OS Windows 10 Professional 64bit
- OS Kali Linux
- Browser Chromium/Google ChromeOperator

Operator terbagi menjadi dua yaitu operator untuk pustakawan dan operator untuk administrator sistem.

Identifikasi Ancaman *(Threat Ientification)*

Perpustakaan Universitas Riau telah menggunakan aplikasi SLiMS untuk pengelolaan otomasi perpustakaan. Aplikasi ini sangat memudahkan bagi pengelola perpustakaan untuk melakukan pengolahan bahan koleksi dan bagian layanan. Namun dalam pelaksanaannya masih ditemukan beberapa hal yang mengancam terhentinya proses berjalannya aplikasi.

Kerusakan hardware menjadi salah satu ancaman dalam proses pengelolaan sistem informasi perpustakaan. Selain itu pemeliharaan jaringan juga sangat perlu dilakukan mengingat jalur kabel LAN yang menggunakan UTP masih memakai teknologi lama. Sangat di perlukan pembaharuan atau peremajaan jaringan kabel lan dengan menggunakan teknologi UTP cat 6.

Hasil dari wawancara dan observasi di lapangan mendapatkan beberapa sumber ancaman yang teridentifiksi dapat menggangu sistem informasi *(SLIMS)* di Perpustakaan Universitas Riau sebagai berikut:

Tabel 3 Sumber Ancaman

JENIS RISIKO	DAMPAK
Petir	Terhentinya sistem operational
	Terjadinya kerusakan pada hardware
Pemadaman Listrik	Pemadaman Listrik yang mengakibatkan terhambatnya proses input data
Kesalahan Hak Akses	Terhentinya layanan informasi perpustakaan
	Penyalahgunaan Hak Akses oleh pengguna
Server Down	Loading sistem yang lama
	Sistem tidak dapat dijalankan
Hacker	Serangan terhadap server mengakibatkan sistem overload dan hang
Kesalahan Input Data	Kelalaian petugas dalam penginputan data
	Human Error
Kebakaran	Terhentinya sistem operational
	Tehambatnya proses penginputan data
Lupa Password	Kehilangan hak akses
Kerusakan Hardware	Sistem tidak berjalan
	Tidak bisa bekerja secara maksimal
Hilangnya Data-data Penting	Terjadi ketidak cocokan data
Sumber Daya Manusia	Kekurangan SDM untuk menangani

Sumber: Hasil wawancara, 2021

Identifikasi Kerentanan (*Vulnerability Identification)*

Hasil dari wawancara dan observasi di lapangan mendapatkan bebarapa kerentanan dari sistem informasi *SLIMS* di Perpustakaan Universitas Riau, terdapat pada tabel 4. berikut ini :

Tabel 4. Identifikasi Ancaman

No.	Kerentanan	Sumber Ancaman	Ancaman
	Penangkal Petir Belum ada	Sumber Daya Alam	Perangkat dan jaringan tersambar petir dapat mengalami kerusakkan.
	Listrik	Sumber Daya Listrik	1. Kabel Listrik belum diperbarui sesuai standar, akibatnya mempengaruhi jalannya arus dan keamanan kurang terjamin. 2. Listrik padam secara mendadak. Ketika hal ini terjadi berulang-ulang maka akan mengakibatkan rusaknya infrastruktur IT. 3. Ketika UPS padam server (data center) tidak dapat beroperasi.
	Server	Hardware & Newtwork	1. Data selalu bertambah sehingga server tak mencukupi 2. Server harus dijaga keamanannya, bila tidak aman akibatnya data hilang, sistem eror, dan akses menjadi lambat.
	Jaringan		3. Jaringan harus dipastikan aman dari ancaman petir dan kebakaran, bila tidak informasi tidak dapat diakses.
	PC (Personal Computer)		4. PC harus selalu di update, bila tidak akan menghambat kinerja.

(Keamanan Sistem)	Security System	1. Password secara berkala harus diganti untuk keamanan data, bila tidak data dapat diakses sesorang yang tak bertanggungjawab, atau kehilangan data
		2. Diserang Virus
Pemeliharaan Sistem	Software	1. Sistem harus selalu diupgrade, agar dapat mengikuti perkembangan.
		2. Menggunakan software tambahan yang tidak terbatas waktu, bila tidak sowftware diciptakan tidak dapat diopresikan lagi apabila batas waktunya telah habis.
Human Eror	Sumber Daya Manusia	1. Operator harus konsisten agar dalam entry data koleksi agar data terjaga validitasnya
		1. Menyiapkan backup SDM apabila yang bersangkutan berhalangan sementara atau tetap.
Kekurangan SDM		1. Menyiapkan backup SDM apabila yang bersangkutan berhalangan sementara atau tetap.
		2. Menyiapkan SDM yang bertanggung jawab menangani pencegahan bila terjadi kebakaran

Sumber: Hasil wawancara, 2021

Analisis control *(Control Analysis)*

Kegiatan Analisa control sudah dilaksanakan dan didokumentasikan sesuai dengan prosedur yang telah ditetapkan dalam dokumen ISO 9001-2015 dan dijadikan target kinerja bagian IT yang berupa sasaran mutu sebagai berikut:

1. Rerata keberhasilan backup database 90 % per bulan
2. Rerata update windows 90% seluruh computer dalam waktu sekali 3 bulan.

Beberapa kegiatan Analisa control sudah dilaksanakan namun belum terdokumentasi. Berikut hasil wawancara dan observasi di lapangan di dapatkan Analisa control yang digambarkan pada tabel 5 mengenai identifikasi pengendalian sebagai berikut:

Tabel 5. Identifikasi Pengendalian

No.	Ancaman	Pengendalian
1	Petir	Memasang penangkal petir untuk gedung dan grounding untuk jaringan
2	Listrik	1. Memasang UPS yang memadai untuk supply listrik cadangan dan memasang genset.
		2. Memperbarui kabel listrik sesuai standar
3	Server	1. Menerapkan software baru untuk dapat meringkas data sehingga data yang sebelumnya membutuhkan tempat yang besar menjadi kecil
		2. Menyimpan server secara virtual
		3. Melakukan backup data secara rutin dan berkala.

4	Jaringan	Menjaga keamanan jaringan untuk menghindaru petir dan kebakaran, dengan memasang grounding, detector dan racun api
5	PC/Komputer	Mengupgrade windows secara rutin dan berkala
6	Keamanan Sistem	1. Mengubah paswaord secara berkala 2. Memasang aplikasi tambahan untuk menjaga keamanan sistem dari serangan virus.
7	Pemeliharaan Sistem	1. Sistem harus selalu diupgrade, agar dapat mengikuti perkembangan teknologi. 2. Menggunakan software tambahan yang tidak terbatas waktu sehingga software tetap bisa diakses .
8	Sumber daya manusia	1. Membuat prosedur entry data koleksi 2. Melakukan pelatihan dan sosialisasi 3. Membuat prosedur untuk menangani staf IT Yang kompeten yang berhalangan sementara atau tetap.

Sumber: Hasil wawancara, 2021

Kemungkinan Yang Menentukan *(Likelihood Determination)*

Hasil kemungkinan risiko yang mengancam sistem informasi dapat dideskripsikan menggunakan kemungkinan ancaman risiko dengan menganalisa control yang dilaksanakan untuk mengantisipasi potensi ancaman risiko, apakah Analisa control dapat berjalan efektif atau bahkan Analisa control tidak dapat mencegah potensi ancaman risiko yang mengganggu sistem informasi.

Analisis Dampak *(Impact Analysis)*

Berdasarkan kemungkinan risiko yang mengancam maka dampak dari risiko tersebut adalah sebagai berikut:

Tabel 6. Dampak Risiko

No.	Jenis Risiko	Konsekuensi	Nilai Dampak
1	Petir	Terhentinya proses pengambilan keputusan dan hilangnya kemampuan menyediakan sistem informasi yang menunjang proses bisnis perpustakaan.	Tinggi
2	Listrik	Terhentinya proses pengambilan keputusan dan hilangnya kemampuan menyediakan sistem informasi yang menunjang proses bisnis perpustakaan. Terhentinya layanan informasi perpustakaan dan menurunya kemampuan sistem yang berakibat pada kegagalan informasi yang dilayankan	Tinggi
3	Server	Terhentinya proses pengambilan keputusan dan hilangnya kemampuan menyediakan sistem informasi yang menunjang proses bisnis perpustakaan.	Tinggi
4	Backup data	Hilangnya reputasi perpustakaan sebagai penyedia informasi Hilangnya kemampuan perlindungan terhadap asset informasi	Tinggi
5	Jaringan	Terhentinya proses pengambilan keputusan dan hilangnya kemampuan menyediakan sistem informasi yang menunjang proses bisnis perpustakaan. Terhentinya layanan informasi perpustakaan dan menurunya kemampuan sistem yang berakibat pada kegagalan informasi yang	Tinggi

		dilayankan	
6	PC	Kinerja kurang maksimal	Sedang
7	Keamanan Sistem	Kepuasan pengelola serta pemustaka tidak tercapai	Tinggi
8	Kebakaran	Hilangnya reputasi perpustakaan sebagai penyedia informasi Hilangnya kemampuan perlindungan terhadap asset informasi	Tinggi
9	Sumber Daya Manusia	Ketergantungan pada 1 staf	Tinggi
		Antisipasi ancaman yang tidak terdeteksi karena keterbatasan SDM	Tinggi
		Data koleksi perpustakaan kurang valid.	Sedang

Sumber: Hasil wawancara, 2021

Risiko yang menentukan *(Risk Determination)*

Berdasarkan hasil analisis diperoleh risiko yang menentukan yang digambarkan dalam tabel 7 sebagai berikut:

Tabel 7. Penentuan Risiko

Tipe Resiko	Predikat Kemungkinan Ancaman	Predikat Dampak	Predikat Risiko	Predikat Level Ranking
Petir	Tinggi	Tinggi	Tinggi	Tinggi
Listrik	Tinggi	Tinggi	Tinggi	Tinggi
Backup data/server	Tinggi	Tinggi	Tinggi	Tinggi
Jaringan	Tinggi	Tinggi	Tinggi	Tinggi
PC	Sedang	Sedang	Sedang	Sedang
Keamanan Sistem	Tinggi	Tinggi	Tinggi	Tinggi
Kebakaran	Tinggi	Tinggi	Tinggi	Tinggi
Sumber daya manusia	Sedang	Sedang	Sedang	Sedang

Sumber: Hasil wawancara, 2021

Dokumentasi Hasil *(Control Recommendation)*

Tujuan dari control ini adalah untuk mengurangi tingkat risiko terhadap sistem dan data ke tingkat yang dapat diterima. rekomendasi kontrol dapat dilihat pada tabel 8 sebagai berikut:

Tabel 8. Rekomendasi Kontrol

No	Tipe Risiko	Level Risiko	Rekomendasi
1.	Petir	Tinggi	Memasang penangkal petir untuk keamanan Gedung. Memasang grounding untuk keamanan infrastruktur IT
2.	Listrik	Tinggi	Memasang genset yang khusus di kelola Perpustakaan Unri. Menyediakan UPS dengan kapasitas yang memadai Mengganti kabel listrik dan memperbaiki aliran khusus jalur IT.
3.	Backup data/sever	Tinggi	Membackup database secara rutin. Menyimpan server secara virtual Meringkas data dengan menggunakan teknologi *Docker* agar server cukup untuk menyimpan data.

			Mengadakan tempat penyimpanan server NVme
4.	Jaringan	Tinggi	Menjaga jaringan supaya terhindar dari petir dan kebakaran.
3.	Keamanan Sistem	Tinggi	Pasword selalu diganti secara rutin dan berkala Menggunakan software untuk menangkal virus
4.	Kebakaran	Tinggi	Menyediakan tabung racun api untuk memadamkan api sebelum menjalar kemana-mana. Menyediakan detector untuk mengantisipasi sebelum terjadi kebakaran
6.	Sumber daya manusia	Tinggi Sedang Sedang	Menambah tenaga IT Membuat prosedur untuk tenaga IT yang keluar atau pensiun. Membuat Prosedur entry data koleksi harus dilaksanakan dengan cara sosialisasi, pelatihan dan validasi.
7.	PC	Sedang	Mengupgrade windows secara rutin dan berkala

Sumber: Hasil wawancara, 2021

Tabel 8 merupakan rekomendasi kontrol yang dapat digunakan sebagai Langkah mitigasi risiko pada tahap berikutnya dan disesuaikan dengan visi dan misi Perpustakaan Universitas Riau.

Proses Peringanan Risiko *(Risk Mitigation)*

Pada tahap ini melaksanakan mitigasi risiko yang berupa tindakan peringanan profil risiko yang sudah terdokumentasi. Setelah dianalisis pada tahap penilaian risiko maka didapatkan profil risiko dengan berbagai proses rekomendasi pemecahan yang sekiranya dapat digunakan dalam proses peringanan risiko yang sesuai dengan kebutuhan di Perpustakaan Universitas Riau. Dalam kegiatan mitigasi risiko diperlukan tahapan proses yang meliputi berbagai kegiatan secara bertahap dan berkelanjutan sebagai berikut:

1. Prioritas Aksi

   Kegiatan yang direncanakan untuk menindaklanjuti hasil rekomendasi kontrol dan untuk mengantisipasi ancaman risiko adalah berdasarkan level resiko dengan prioritas katagori tinggi karena apabila tidak segera ditindaklanjuti akan mengakibatkan fatal hilangnya asset institusi dan hilangnya kemampuan menyediakan sistem informasi yang menunjang proses bisnis perpustakaan.
2. Evaluasi Rekomendasi Kontrol

   Hasil dari Rekomendasi Kontrol yang telah dibahas sebelumnya dapat dievaluasi sebagai berikut: Beberapa rekomendasi kontrol yang mempunyai risiko tinggi menjadi prioritas utama untuk segera dilaksanakan dengan pertimbangan dana mencukupi, apabila tidak mencukupi memilih kegiatan yang terdapat dalam rekomendasi yang sesuai dengan dana yang ada.

   Beberapa kegiatan mitigasi risiko sudah dilaksanakan oleh tim IT karena tidak membutuhkan biaya yang tinggi namun membutuhkan pengalaman serta keahlian tinggi seperti menyimpan server secara virtual dan meringkas data. Rekomendasi untuk risiko sedang segera dilaksanakan karena tidak memerlukan anggaran yang tinggi.
3. Analisa Akibat dan Biaya

   Hasil dari rekomendasi kontrol tidak sepenuhnya dapat direalisasikan dalam waktu dekat serta bersamaan namun dianalisa berdasarkan ketersediaan dana dan mempertimbangkan akibat yang ditimbulkan apabila tidak segera direalisasikan. Hasil dari wawancara serta pengamatan dilapangan di dapatkan bahwa, pada tahun ini kegiatan untuk mitigasi risiko yang direncanakan agar segera dilaksanakan adalah pemasangan grounding yaitu alat untuk melindungi jaringan dari sambaran petir serta pemasangan kabel server untuk memperbarui kabel yang sudah ada. Kedua kegiatan tersebut penting untuk segera dilaksanakan,

disamping adanya biaya yang memadai juga bertujuan untuk melindungi server dan jaringan, karena kedua peralatan ini, ibarat manusia adalah jantungnya, apabila tidak berfungsi akan berhenti semuanya. Pembaharuan kabel secara keseluruhan akan dilaksanakan secara bertahap sesuai dengan anggaran yang ada.

4. Pemilihan Kontrol

   Perpustakaan Universitas Riau memilih penyimpanan server ada dua tempat, yang pertama server yang menyimpan aplikasi atau software yang sifatnya tetap atau baku disimpan atau dikelola oleh UPT. TIK sedangkan aplikasi yang sifatnya untuk dikembangkan maka diletakkan di Perpustakaan agar staf IT mudah mengelolanya.

5. Tugas dan Tanggung Jawab

   Mitigasi risiko merupakan proses kegiatan rutin dan berkelanjutan yang memerlukan peran dan personil yang bertangguang jawab. Perpustakaan Universitas Riau dalam struktur organisasi memiliki bidang IT yang bertanggung jawab mengelola sistem informasi beserta komplemen-komplemennya. Bidang IT terdiri dari coordinator IT yang membawahi 5 staf dengan tanggung jawab sebagai berikut : programmer dan server, jaringan dan PC, website, operator untuk penerimaan karya ilmiah.

   Tugas dan tanggungjawab untuk kegiatan mitigasi risiko sistem informasi dilaksanakan oleh koordinator IT merupakan pustakawan yang mempunyai kemampuan manajerial sebagai seorang penanggung jawab teknologi informasi dibantu oleh *IT support system.*

6. Pengembangan Rencana Perlindungan

   Pengembangan rencana perlindungan sesuai dengan rekomendasi kontrol pada tahap penilaian risiko. rekomendasi kontrol digunakan sebagai acuan rencana perlindungan asset informasi di Perpustakaan Universitas Riau.

7. Implementasi Kontrol

   Pada tahap ini Perpustakaan Universitas Riau telah mengimplementasikan proses mitigasi risiko dengan tidak membutuhkan biaya besar namun mempunyai resiko tinggi sebagai berikut:

1) Keamanan server , yang sudah dilakukan adalah meringkas data yang sebelumnya membutuhkan atau memakan tempat yang besar, namun pada tahun 2017 tim IT menemukan teknologi *Docker* yang merupakan teknologi server untuk menyatukan banyak data, setelah mempelajarinya dan melakukan beberapa kali uji coba dan akhirnya berhasil melakukan peringkasan atau penyatuan beberapa data. Perpustakaan Universitas Riau sebelumnya mempunyai 5 server yang sudah penuh, namun sekarang hanya 2 server yang terisi, masih ada 3 server untuk cadangan. Jadi pengembangan ini merupakan strategi agar semua data perpustakaan beberapa tahun kedepan masih dapat tersimpan dengan naman.
2) Melakukan backup data secara rutin dan berkala, kegiatan ini sudah lama dilaksanakan, sejak menerapkan ISO 9001 2008 tahun 2016 hingga sekarang telah mengupgrade ISO menjadi ISO 9001-2015, backup data dijadikan sasaran mutu atau target kinerja bagian IT, hasilnya menunjukkan target tercapai 100%.
3) Menurut ketentuan untuk menghindari rusaknya server akibat kebakaran atau bencana lainnya sebaiknya server disimpan terpisah dari Gedung Perpustakaan Universitas Riau dan hal ini sudah dilakukan dengan menyimpan server ke data center di Jakarta serta penyimpanan server secara virtual di Amerika.
4) Antisipasi apabila terjadi kebakaran, Perpustakaan juga sudah menyiapkan racun api sebanyak 5 tabung yang terpasang dibagian-bagian yang dianggap mempunyai risiko tinggi

seperti ruang server, ruang koleksi, ruang administrasi, ruang pengembangan koleksi dan ruang kerja staf.

5) Keamanan Sistem
Kegiatan untuk menangani keamanan Sistem Infomsi sudah dilaksanakan seperti menggunakan *software* tambahan untuk mengamankan dari serangan virus dan untuk penggantian *password* secara rutin dan berkala sedang dipersiapkan mekanismenya.

6) Sumber Daya Manusia
Pedoman kegiatan entry data koleksi sudah ada namun hasilnya masih terdapat ketidakkonsistenan yang mengakibatkan ketidakvalidan jumlah koleksi.

Evaluasi Risiko *(Risk Evaluation)*

Faktor-faktor yang Mempengaruhi Pelaksanaan Manajemen Risiko

1. Penerapan Sistem Manajemen Mutu ISO 9001-2015

Tahun 2017 Perpustakaan Universitas Riau mendapatkan sertifikat SMM ISO 9001-2008 dan tahun 2019 dapat mengupgarde SMM ISO 9001-2015, perbedaan ISO 9001-2008 dengan ISO 9001-2015 terdapat pada penerapan manajemen risiko perpustakaan dan sejak itu Perpustakaan merancang penerapan manajemen risiko. Manajemen risiko sangat penting diterapkan di sebuah insitusi demikian pula dengan Perpustakaan Universitas Riau juga menerapkan sistem manajemen risiko untuk melindungi asset dari peristiwa yang tak terduga dan dapat memberikan pelayanan yang bermutu.

2. Perencanaan Kegiatan Manajemen Risiko Sistem Informasi

Perpustakaan Universitas Riau telah menerapkan SLIMS (Senayan Library Information Manajemen Sistem sejak tahun 2012. SLIMS merupakan sistem informasi yang biasanya diterapkan pada perpustakaan sekolah dan perpustakaan perguruan tinggi yang berfungsi untuk pengelolaan sistem informasi dari mulai perencanaan bahan pustaka sampai koleksi terpajang di bagian pelayanan dan siap untuk dilayankan, pelaporan serta evaluasi secara digital atau menggunakan jaringan dan aplikasi yang juga berfungsi sebagai alat pengambilan keputusan. Begitu pentingnya sistem informasi bagi perpustakaan sehingga asset ini memerlukan perlindungan agar tetap dapat berjalan sesuai yang kita inginkan bersama, ibarat manusia nyawanya sistem informasi, apabila terjadi kendala maka perpustakaan akan berhenti tidak beroperasi. Untuk itu menerapkan manajemen risiko untuk sistem informasi sangat penting agar perpustakaan dapat berfungsi secara optimal dan kepuasan pemustaka dapat tercapai.

3. Menentukan sasaran mutu atau target untuk manajemen risiko Sistem Informasi.

Penerapan manajemen risiko sistem informasi di perpustakaan diawali dengan menentukan target atau sasaran mutu untuk melindungi sistem informasi seperti yang telah ditetapkannya sasaran mutu bagian IT yaitu sebagai berikut:

a. Keberhasilan backup data 100%
b. Rerata update windows 90% seluruh computer

Kedua target atau sasaran mutu tersebut di atas bertujuan untuk melindungi data dan meningkatkan kinerja, dan masih ada kegiatan-kegiatan lainnya untuk melindungi sistem informasi namun belum tercover dalam sasaran mutu dan belum terdokumentasi.

4. Menentukan skala prioritas

Penerapan rekomendasi yang terdapat pada tabel rekomendasi kontrol tidak dapat dilaksanakan semuanya secara bersamaan namun bertahap sesuai dengan predikat level risiko tinggi

dan mempunyai dampak yang tinggi juga serta biaya dapat terjangkau dan yang paling penting tersedia SDM yang mempunyai kompetensi untuk melaksanakan hasil rekomendasi tersebut.

Penutup

Berdasarkan hasil penelitian yang telah dilaksanakan maka diperoleh simpulan sebagai berikut: 1) Proses penilaian rsiko (risk *assessment*) mendeskripsikan profil risiko yang mengancam sistem informasi perpustakaan berdasarkan level rangking level risiko yang meliputi risiko sumber daya alam, risiko teknis dan risiko sumber daya manusia. Risiko alam yang diakibatkan oleh petir dengan level risiko tinggi, risiko teknis terdiri dari masalah listrik, server, jaringan, keamanan sistem, dan kebakaran dengan level risiko tinggi sedangkan risiko sumber daya manusia termasuk level risiko sedang dan risiko tinggi. Risiko tinggi terkait dengan kekurangan tenaga IT yang berkompeten sedangkan risiko sedang terkait dengan kurang validnya data koleksi akibat ketidakkonsistennya dalam entry data koleksi. 2) Mitigasi risiko atau peringanan risiko di Perpustakaan Universitas Riau dilaksanakan dengan cara kegiatan pengamanan server dengan cara: a) Membackup database secara rutin, b) Menyimpan server secara virtual, c) Meringkas data dengan menggunakan teknologi, d) *Docker* agar server cukup untuk menyimpan data, e) Mengadakan tempat penyimpanan server NVme. 3) Evaluasi kegiatan manajemen risiko. Kerangka kerja NIST Special Publication 800-30 mampu mendeskrepsikan profil ancaman risiko yang mengganggu pengembangan perpustakaan berbasis teknologi web dan memberikan solusi mitigasi risiko sebagai tindakan peringanan risiko, serta memiliki metode pengawasan secara menyeluruh melalui evaluasi pelaksanaan manajemen risiko sistem informasi perpustakaan dalam siklus pengembangan sistem informasi.

Daftar Pustaka

Angreni, Gayatri Rawit (2018). Manajemen Risiko Menjaga Stabilitas Makro dan Mikro. Jakarta: LPPI-Stabilitas.

Astuti, Rini. (2018). *Implementasi Manajemen Resiko Sistem Informasi Menggunakan Cobit 5*.. Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI. *Media Informatika* Vol. 17 (1).

Elanda, Anggi. (2018). *Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute Of Standards And Technology) Sp 800-30.* (Studi Kasus : Disinfolahtaau Mabes Tni Au). *Jurnal Ilmu-ilmu Informatika dan Manajemen* STMIK, Vol. 12 (1).

Fahmi, Irham (2016). Manajemen Risiko Teori, Kasus, dan Solusi edisi revisi. Bandung: Alfabeta.

Han, Z., Huang, S., Li, H. and Ren, N. (2016) "Risk assessment of digital library information security: a case study", *The Electronic Library.*. Vol. 34 (3), Hlm. 471-487. https://doi.org/10.1108/EL-09-2014-0158

Idzni, Izatri Dini et al. (2020) *Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30*. JURIKOM (Jurnal Riset Komputer), Vol. 7 (1).

Murniati, Endang.(2019) Pengaruh Slims (Senayan Library Information Management System) Terhadap Kinerja Pegawai di Perpustakaan Universitas Riau. *Tesis*, Program Pascasarjana Universitas Riau.

Nurochman, Arif. (2014) *Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan Universitas Gadjah Mada Yogyakarta*. Vol.10(2) https://jurnal.ugm.ac.id/bip/article/view/8830/6695.

PNRI. (2017) Standar Perpustakaan Perguruan Tinggi. Jakarta: PNRI.

Saepul, Ae dkk. (2017). Manajemen Risiko Teknologi Informasi Berbasis National of Standards ang Technology SP 800-30 di Universitas Jendral Achmad Yani. Seminar Nasional Informatikadan Aplikasinya. Cimahi

Valena, Danis Sela, Prabowo, Rizky, Irawati, Anie Rose, Aristoteles. (2019). Analisis Manajemen Risiko Sistim Informasi Perpustakaan Universitas Lampung Menggunakan Metode NIST SP 800-30. *Jurnal Komputasi.* Vol. 7 (1).

W. Syafitri. (2016) Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik UniversitasXYZ). J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.

Xie, Y., Liu, J., Zhu, S., Chong, D., Shi, H. and Chen, Y. (2019), "An IoT-based risk warning system for smart libraries", *Library Hi Tech*, Vol. 37 (4), Hlm. 918-932. https://doi.org/10.1108/LHT-11-2017-0254

Yusup, P. M. (2012) Perspektif Manajemen Pengetahuan Informasi, Komunikasi, Pendidikan, dan Perpustakaan. Jakarta: Rajawali Pers.

Yusrika, D. (2021) Manajemen Risiko IT Pada Sistem IraiseMenggunakan Metode Nist Sp 800-30. *Skripsi* Fakultas Sains Dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.