LAPORAN TEKNIS

Analisis Manajemen Risiko Teknologi Informasi

Perpustakaan UIN Sulthan Thaha Saifuddin Jambi

1.0 Pendahuluan

Teknologi Informasi (TI) telah menjadi tulang punggung operasional perpustakaan modern, mengubahnya dari sekadar gudang buku menjadi pusat pengetahuan digital yang dinamis. Di Perpustakaan UIN Sulthan Thaha Saifuddin Jambi, TI memfasilitasi layanan esensial mulai dari katalogisasi digital, akses ke jurnal ilmiah internasional, hingga manajemen sirkulasi dan keanggotaan. Ketergantungan yang mendalam ini memunculkan spektrum risiko yang dapat mengancam integritas data, ketersediaan layanan, dan reputasi institusi. Oleh karena itu, manajemen risiko TI yang proaktif dan terstruktur bukan lagi pilihan, melainkan keharusan strategis untuk melindungi aset informasi, menjamin kelangsungan layanan, dan mendukung pencapaian tujuan akademik universitas.

1.1 Latar Belakang

Bagi institusi pendidikan tinggi seperti UIN Sulthan Thaha Saifuddin Jambi, perpustakaan adalah jantung kegiatan akademik. Ketergantungan pada sistem digital seperti Online Public Access Catalog (OPAC), repositori institusional, dan database langganan membuat operasional perpustakaan rentan terhadap ancaman TI. Gangguan pada sistem ini, baik disebabkan oleh faktor alam, kesalahan manusia, maupun kegagalan sistem, dapat menghambat proses belajar-mengajar dan penelitian. Memahami dan mengelola risiko-risiko ini secara sistematis adalah langkah fundamental untuk memastikan bahwa investasi teknologi memberikan manfaat maksimal dan tidak menjadi sumber kerentanan baru.

1.2 Tujuan dan Ruang Lingkup

Tujuan umum: Memberikan analisis komprehensif mengenai risiko TI di Perpustakaan UIN Sulthan Thaha Saifuddin Jambi.

Tujuan khusus: 1. Mengidentifikasi potensi risiko TI yang relevan dengan operasional, infrastruktur, dan layanan perpustakaan. 2. Menganalisis dan mengevaluasi tingkat setiap risiko berdasarkan kemungkinan (likelihood) dan dampak (impact). 3. Memberikan rekomendasi tindakan penanganan yang praktis dan dapat ditindaklanjuti untuk risiko prioritas.

Ruang lingkup: 1. Fokus pada 20 risiko TI yang teridentifikasi dalam konteks infrastruktur dan layanan perpustakaan. 2. Analisis mengikuti kerangka kerja ISO 31000:2018.

1.3 Metodologi

Pendekatan kualitatif mengikuti alur proses manajemen risiko dalam ISO 31000:2018. Langkah metodologis: 1. Identifikasi kebutuhan analisis risiko TI. 2. Studi pustaka (ISO 31000:2018). 3.

Pengumpulan dan identifikasi daftar 20 risiko, dikelompokkan menurut penyebab (Alam, Manusia, Sistem). 4. Analisis dan evaluasi menggunakan kriteria likelihood dan impact; pemetaan ke matriks risiko. 5. Perumusan rekomendasi penanganan untuk risiko prioritas.

2.0 Kerangka Kerja Manajemen Risiko ISO 31000:2018

Penggunaan ISO 31000:2018 memastikan proses manajemen risiko terstruktur, komprehensif, dan konsisten. Kerangka ini menyediakan prinsip, panduan, dan proses yang dapat diadaptasi organisasi, termasuk perpustakaan.

Komponen utama proses manajemen risiko menurut ISO 31000: - Komunikasi dan Konsultasi Berjalan paralel pada semua tahapan; melibatkan kepala perpustakaan, staf TI, dan perwakilan pengguna. - Penetapan Cakupan, Konteks, dan Kriteria Menetapkan batas analisis, konteks internal/eksternal, dan kriteria penilaian. - Penilaian Risiko (Risk Assessment) Terdiri dari identifikasi, analisis, dan evaluasi risiko. - Penanganan Risiko (Risk Treatment) Memilih dan menerapkan opsi mitigasi, transfer, penerimaan, atau penghindaran. - Pemantauan dan Peninjauan Menjamin kontrol efektif dan memperbarui informasi risiko secara berkala.

3.0 Penetapan Konteks dan Kriteria Risiko

Sebelum penilaian, ditetapkan kriteria dan alat (matriks) untuk menilai risiko secara konsisten.

3.1 Kriteria Risiko

Tabel 1 Kriteria Likelihood

Kriteria	Keterangan	Frekuensi	Nilai
Rare	Risiko sangat jarang terjadi	> 3 tahun	1
Unlikely	Risiko jarang terjadi	2–3 tahun	2
Possible	Risiko kadang terjadi	1–2 tahun	3
Likely	Risiko sering terjadi	7–12 bulan	4
Certain	Risiko pasti terjadi	< 7 bulan	5

Tabel 2 Kriteria Impact

Kriteria	Keterangan	Nilai
Insignificant	Risiko tidak mengganggu aktivitas operasional perpustakaan.	1
Minor	Menghambat sebagian kecil aktivitas, namun tidak mengganggu layanan utama.	2
Moderate	Mengganggu proses bisnis dan sebagian besar layanan perpustakaan.	3
Major	Menyebabkan hambatan hampir seluruh aktivitas utama perpustakaan.	4
Catastrophic	Menyebabkan seluruh aktivitas perpustakaan berhenti total.	5

3.2 Matriks Evaluasi Risiko

Risiko dihitung sebagai: **Nilai Risiko = Likelihood × Impact**.

Tabel 3 Matriks Evaluasi Risiko

Likelihood Impact	1 (Insignificant)	2 (Minor)	3 (Moderate)	4 (Major)	5 (Catastrophic)
5 Certain	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

Tabel 4 Keterangan Warna Risiko

Warna	Jenis Risiko	Rentang Nilai	Keterangan singkat
Hijau	Low Risk	1–4	Risiko kecil, diatasi dengan kebijakan operasional.
Kuning	Medium Risk	5–8	Perlu kebijakan dan pengawasan.
Oranye	Medium High Risk	9–12	Memerlukan perhatian dan penanganan khusus.
Merah	High Risk	15–25	Harus segera ditangani; prioritas utama.

4.0 Penilaian Risiko

Bagian ini memaparkan identifikasi, analisis, dan evaluasi 20 risiko TI yang relevan.

4.1 Identifikasi Risiko

Tabel 5 Daftar Risiko (ID, Faktor, Kemungkinan Risiko)

ID	Faktor	Kemungkinan Risiko
R01	Alam	Gempa bumi
R02	Alam	Banjir
R03	Alam	Petir
R04	Alam	Kebakaran
R05	Alam	Listrik padam
R06	Manusia	Penyalahgunaan hak akses
R07	Manusia	Hacking
R08	Manusia	Human error
R09	Manusia	Kurangnya pelatihan

ID	Faktor	Kemungkinan Risiko
R10	Sistem	Server down
R11	Sistem	Kapasitas penuh
R12	Sistem	Overheating
R13	Sistem	Kehilangan data
R14	Sistem	Data korup
R15	Sistem	Versi perangkat lunak yang sudah lama
R16	Sistem	Web server bermasalah
R17	Sistem	Backup failure
R18	Sistem	Koneksi internet terganggu
R19	Sistem	Kerusakan perangkat
R20	Sistem	CCTV tidak berfungsi

4.2 Analisis Risiko

Setiap risiko dinilai berdasarkan Likelihood dan Impact; berikut ringkasan penilaian dan nilai risiko (Likelihood × Impact).

Tabel 6 Analisis Risiko

ID	Risiko	Likelihood (Nilai & Justifikasi)	Impact (Nilai & Justifikasi)	Nilai Risiko
R01	Gempa bumi	1 (Rare) Gempa besar jarang terjadi di Jambi	5 (Catastrophic) Dapat merusak struktur gedung dan server	5
R02	Banjir	2 (Unlikely) Tergantung lokasi; potensi pada musim hujan	4 (Major) Merusak koleksi fisik dan infrastruktur TI	8
R03	Petir	3 (Possible) Badai petir cukup umum di iklim tropis	3 (Moderate) Lonjakan listrik dapat merusak perangkat tanpa proteksi	9
R04	Kebakaran	1 (Rare) Pencegahan modern mengurangi kemungkinan	5 (Catastrophic) Potensi kehilangan total aset fisik dan digital	5
R05	Listrik padam	4 (Likely) Pemadaman dari penyedia cukup sering	3 (Moderate) Mengganggu layanan jika UPS tidak mencukupi	12
R06	Penyalahgunaan hak akses	3 (Possible) Banyak staf dengan tingkat kesadaran keamanan bervariasi	4 (Major) Modifikasi/hilangnya data katalog atau kebocoran data anggota	12
R07	Hacking	2 (Unlikely) Target relatif,	4 (Major) Pencurian data, defacement, pengambilalihan	8

ID	Risiko	Likelihood (Nilai & Justifikasi)	Impact (Nilai & Justifikasi)	Nilai Risiko
		namun ada ancaman	sistem	
R08	Human error	4 (Likely) Kesalahan entri dan penghapusan tidak sengaja umum	3 (Moderate) Menyebabkan inkonsistensi data katalog	12
R09	Kurangnya pelatihan	4 (Likely) Staf mungkin jarang mendapat pelatihan terkini	3 (Moderate) Meningkatkan human error dan kerentanan terhadap social engineering	12
R10	Server down	3 (Possible) Kegagalan hardware/software dapat terjadi	4 (Major) Layanan inti (OPAC, e-resources) lumpuh	12
R11	Kapasitas penuh	3 (Possible) Pertumbuhan data digital cepat	3 (Moderate) Sistem melambat, tidak dapat menambah data baru	9
R12	Overheating	2 (Unlikely) Kegagalan AC bisa terjadi	3 (Moderate) Penurunan kinerja atau shutdown darurat server	6
R13	Kehilangan data	2 (Unlikely) Backup tersedia, kehilangan total jarang	5 (Catastrophic) Kehilangan data katalog/repositori melumpuhkan layanan	10
R14	Data korup	3 (Possible) Akibat kegagalan hardware atau listrik tiba-tiba	4 (Major) Database OPAC tidak dapat digunakan	12
R15	Versi perangkat lunak yang sudah lama	4 (Likely) Anggaran terbatas menunda pembaruan	4 (Major) Celah keamanan dapat dieksploitasi	16
R16	Web server bermasalah	3 (Possible) Kesalahan konfigurasi atau lonjakan trafik	3 (Moderate) Website dan OPAC tidak dapat diakses	9
R17	Backup failure	3 (Possible) Backup bisa gagal tanpa pemantauan	4 (Major) Meningkatkan dampak kehilangan/kerusakan data	12
R18	Koneksi internet terganggu	4 (Likely) Ketergantungan pada ISP dan beban jaringan kampus	4 (Major) Akses jurnal online dan layanan eksternal terhenti	16
R19	Kerusakan perangkat	4 (Likely) Perangkat staf rentan rusak	2 (Minor) Mengganggu staf, tetapi tidak menghentikan layanan utama	8
R20	CCTV tidak berfungsi	3 (Possible) Perangkat dapat rusak atau salah konfigurasi	2 (Minor) Melemahkan keamanan fisik dan investigasi	6

4.3 Evaluasi Risiko

Ringkasan pengelompokan risiko (berdasarkan nilai):

1. **High Risk (Nilai 15–25):**
    a. R15 Versi perangkat lunak yang sudah lama (16)
    b. R18 Koneksi internet terganggu (16)
2. **Medium High Risk (Nilai 9–12):**
    a. R05, R06, R08, R09, R10, R14, R17 (nilai 12)
    b. R13 (10)
    c. R03, R11, R16 (nilai 9)
3. **Medium Risk (Nilai 6–8):**
    a. R02, R07, R19 (nilai 8)
    b. R12, R20 (nilai 6)
4. **Low Risk (Nilai 1–5):**
    a. R01, R04 (nilai 5)

Matriks (penempatan berdasarkan Likelihood × Impact):

Likelihood Impact	1	2	3	4	5
Certain (5)					
Likely (4)		R19	R05,R08,R09	R15,R18	
Possible (3)		R20	R03,R11,R16	R06,R10,R14,R17	
Unlikely (2)			R12	R02,R07	R13
Rare (1)					R01,R04

5.0 Rencana Penanganan Risiko

Rekomendasi difokuskan pada risiko High dan Medium High. Setiap rekomendasi disajikan sebagai langkah tindakan yang dapat diimplementasikan.

Tabel 7 Rencana Penanganan (Ringkas)

ID	Risiko	Tingkat Risiko	Rekomendasi Tindakan Penanganan
R15	Versi perangkat lunak yang sudah lama	High	1. Audit perangkat lunak menyeluruh. 2. Jadwal patch rutin. 3. Alokasi anggaran upgrade/ lisensi.
R18	Koneksi internet terganggu	High	1. Koneksi sekunder (failover). 2. Bandwidth management. 3. Opsi akses offline untuk sumber penting.
R05	Listrik padam	Medium High	1. Pastikan UPS memadai. 2. Uji rutin UPS/Genset. 3. SOP pemadaman listrik.

ID	Risiko	Tingkat Risiko	Rekomendasi Tindakan Penanganan
R06	Penyalahgunaan hak akses	Medium High	1. Terapkan least privilege. 2. Review hak akses berkala. 3. Aktifkan logging aktivitas.
R08	Human error	Medium High	1. Dokumentasi & SOP. 2. Validasi sistem. 3. Pelatihan penyegaran.
R09	Kurangnya pelatihan	Medium High	1. Pelatihan keamanan & penggunaan sistem berkala. 2. Materi pelatihan mudah diakses.
R10	Server down	Medium High	1. Monitoring proaktif. 2. Strategi failover/virtualisasi. 3. Ketersediaan spare part.
R14	Data korup	Medium High	1. Gunakan UPS untuk server/storage. 2. Jadwalkan pengecekan integritas database.
R17	Backup failure	Medium High	1. Notifikasi otomatis kegagalan backup. 2. Penanggung jawab verifikasi backup.
R13	Kehilangan data	Medium High	1. Terapkan strategi backup 3-2-1. 2. Kembangkan dan uji DRP (Disaster Recovery Plan).
R03	Petir	Medium High	1. Pasang surge arrester. 2. Periksa grounding/petanahan gedung.
R11	Kapasitas penuh	Medium High	1. Monitoring kapasitas. 2. Kebijakan retensi & arsip. 3. Rencana penyimpanan scalable.
R16	Web server bermasalah	Medium High	1. Load balancing. 2. Web Application Firewall. 3. Monitoring kinerja real-time.

6.0 Kesimpulan dan Rekomendasi

Laporan ini menyajikan analisis risiko TI yang sistematis untuk Perpustakaan UIN Sulthan Thaha Saifuddin Jambi berdasarkan ISO 31000:2018. Terdapat 20 risiko yang diidentifikasi, dengan fokus mitigasi pada risiko-sistem yang dominan.

6.1 Kesimpulan

1. 20 risiko TI diidentifikasi (faktor Alam, Manusia, Sistem); faktor Sistem paling dominan.
2. Distribusi tingkat risiko: 2 risiko High (10%), 11 risiko Medium High (55%), 5 risiko Medium (25%), 2 risiko Low (10%).
3. Risiko prioritas: R15 (perangkat lunak lama) dan R18 (koneksi internet terganggu).