

## Mitigasi Risiko Sistem Informasi Perpustakaan Perguruan Tinggi Swasta XYZ Menggunakan Management of Risk (MOR)

Yulhendri Yulhendri<sup>1</sup>, Setianingsih<sup>2</sup>, Hannah Patricia<sup>3</sup>, Syifa Maulida Akmalia<sup>4</sup>, Arif Apriansah<sup>5</sup>, Ariansah<sup>6</sup>

<sup>1-6</sup>Program Studi Sistem Informasi, Universitas Esa Unggul

**Alamat:**Jl. Harapan Indah Boulevard No. 2, Pusaka Rakyat, Kec. Tarumajaya, Kabupaten Bekasi, Jawa Barat 17214

**Email :**[yulhendri@esaunggul.ac.id](mailto:yulhendri@esaunggul.ac.id)<sup>1\*</sup>, [setngsh@gmail.com](mailto:setngsh@gmail.com)<sup>2</sup>, [hannahptrcia@gmail.com](mailto:hannahptrcia@gmail.com)<sup>3</sup>, [syifamaulidaakm@gmail.com](mailto:syifamaulidaakm@gmail.com)<sup>4</sup>, [arifapriansah924@gmail.com](mailto:arifapriansah924@gmail.com)<sup>5</sup>, [ansaha741@gmail.com](mailto:ansaha741@gmail.com)<sup>6</sup>

**Abstract.** *One of the libraries in XYZ private university provides an information system to support library services such as borrowing books, extending the loan period, and returning books. This information system is inseparable from the risks and impacts that threaten its use. The purpose of this research is to analyze the risks contained in the information system using the ITIL framework. The ITIL framework is used as a guide in developing operational steps so that the continuity of library information system services can run well. Based on the research that has been done, the results show that there are 5 risks consisting of 2 risks with low risk levels, 1 risk with medium risk levels, and 2 risks with high risk levels*

**Keywords:** *library, information system, risk management, ITIL*

**Abstrak.** Salah satu perpustakaan di universitas swasta XYZ menyediakan sistem informasi untuk mendukung layanan perpustakaan seperti peminjaman buku, perpanjangan masa peminjaman, dan pengembalian buku. Sistem informasi ini tidak terlepas dari risiko dan dampak yang mengancam penggunaannya. Tujuan dari penelitian ini adalah untuk menganalisis risiko yang terdapat pada sistem informasi tersebut dengan menggunakan kerangka kerja ITIL. Kerangka kerja ITIL digunakan sebagai panduan dalam menyusun langkah-langkah operasional agar keberlangsungan layanan sistem informasi perpustakaan dapat berjalan dengan baik. Berdasarkan penelitian yang telah dilakukan, didapatkan hasil bahwa terdapat 5 risiko yang terdiri dari 2 risiko dengan tingkat risiko rendah, 1 risiko dengan tingkat risiko sedang, dan 2 risiko dengan tingkat risiko tinggi.

**Kata kunci:** perpustakaan, sistem informasi, manajemen risiko, ITIL

### PENDAHULUAN

Kebutuhan akan layanan pendidikan semakin meningkat seiring dengan perkembangan teknologi informasi. Perguruan tinggi harus bekerja sama dengan teknologi untuk menyediakan layanan terbaik. Menurut Supriyanto (2008), jaringan informasi modern memungkinkan seseorang untuk memenuhi kebutuhan informasi kapan saja dan di mana saja tanpa batas ruang dan waktu. Dengan demikian, semua tugas dapat diselesaikan tanpa harus berada di lokasi tertentu.

Sistem informasi perpustakaan adalah hubungan antara teknologi informasi yang terdiri dari hardware (perangkat keras), software (perangkat lunak), dan koleksi informasi perpustakaan. Sistem informasi ini berfungsi sebagai alat atau media untuk mengkomunikasikan koleksi perpustakaan dengan pengguna, sehingga mereka dapat

*Revised Desember 31, 2023, Revised Januari 18, 2024; Accepted Februari 29, 2024*

\* Yulhendri Yulhendri, [yulhendri@esaunggul.ac.id](mailto:yulhendri@esaunggul.ac.id)

mengakses informasi dengan mudah, cepat, dan tepat. Salah satu lembaga pendidikan yang menerapkan sistem informasi dalam keberlangsungan layanan perpustakaan adalah universitas swasta XYZ. Tujuan dari sistem ini adalah untuk memberikan layanan yang berkualitas tinggi bagi pemustaka Universitas XYZ.

Sangat penting untuk memahami dan mengelola risiko yang terkait dengan sistem informasi perpustakaan perguruan tinggi swasta XYZ. Setiap lembaga diharapkan dapat membuat rencana yang komprehensif untuk memastikan bahwa layanan terus beroperasi dengan baik, terutama ketika menggunakan layanan TI. Sistem informasi perpustakaan perguruan tinggi swasta XYZ dapat menghadapi banyak bahaya yang mengancam keamanan data dan efektivitas layanan.

ITIL (*Information Technology Infrastructure Library*) dapat menjadi kerangka kerja yang sangat berguna untuk mengelola risiko tersebut karena memungkinkan perguruan tinggi swasta XYZ untuk memiliki proses yang terstruktur dalam mengelola sistem informasi perpustakaan berfokus di ruang lingkup tata kelola layanan TI. Dibantu dengan metode MoR (*Management of Risk*) kami dapat mengidentifikasi risiko potensial dan merekomendasikan tindakan untuk meminimalkan dampak risiko yang mengancam layanan perpustakaan universitas XYZ.

## **TINJAUAN PUSTAKA**

### **1. Kerangka Kerja Manajemen Risiko TI (MOR)**

Terdapat kerangka kerja melakukan aktivitas manajemen resiko SI, yaitu serangkaian proses yang standar untuk menata/mengelola dan memberikan informasi untuk aktivitas manajemen risiko yang proses tersebut dilakukan secara berkala. ITIL memunculkan pedoman panduan manajemen risiko untuk sistem teknologi informasi dengan perantara publikasi kerangka kerja ITIL.

Kerangka Kerja Manajemen Risiko adalah suatu kerangka kerja yang digunakan untuk mengelola risiko dalam bidang teknologi informasi. Kerangka kerja ini dapat membantu organisasi dalam mengidentifikasi, mengevaluasi, dan mengelola risiko TI secara efektif. Management of Risk (MoR) adalah metode standar yang digunakan manajemen risiko TI serta menilai risiko di organisasi. Berikut adalah kerangka kerja MoR:



Gambar 1 Management of Risk

MoR memiliki prinsip yaitu intisari pengembangan penerapan manajemen resiko yang benar juga diturunkan prinsip dari tata kelola dari perusahaan / corporate governance. Mor digunakan sebagai pendekatan kepada organisasi untuk mewujudkan prinsip dan dibutuhkan untuk mengartikan dalam persetujuan pada dokumen:

1. Strategi manajemen risiko
2. Petunjuk proses
3. Penstrategian
4. Permasalahan log

Mor memiliki 4 proses aktivitas untuk manajemen risiko yaitu:

#### 1. Identifikasi

Dalam mencapai tujuan risiko dan kesempatan dapat mempengaruhi dalam aktivitas

#### 2. Menilai

Net effect dalam identifikasi ancaman adalah peluang kegiatan.

#### 3. Perencanaan

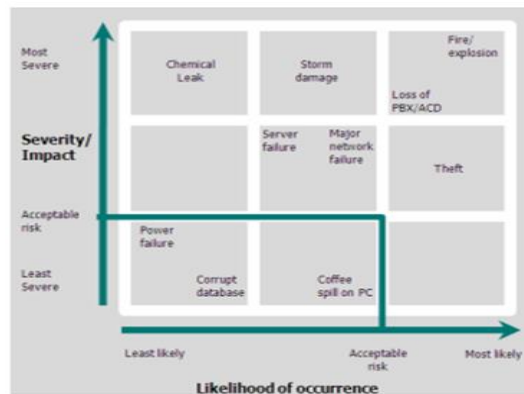
Menyiapkan secara detail ulasan manajemen untuk mengurangi ancaman dan mengembangkan kesempatan.

#### 4. Implementasi

Pengaplikasian perencanaan manajemen risiko, pemantauan efisiensi dalam pengambilan langkah yang dibutuhkan untuk menjaga hasil yang tidak sesuai.

**MOR Embedding and reviewing** dibutuhkan pengecekan secara berkala untuk meningkatkan komunikasi dibutuhkan kegiatan yang tepat yang menjanjikan masyarakat akan tetap up to date dalam memajukan perubahan dalam gertakan, kesempatan dalam semua aspek manajemen risiko.

## Profil risiko layanan TI



## 2. Information Technology Service Continuity Management (ITSCM)

IT Service Continuity Management (ITSCM) merupakan elemen krusial dalam manajemen TI yang bertujuan memastikan kelangsungan operasional organisasi dalam situasi darurat atau bencana. Ini mencakup proses perencanaan, pengujian, dan pemulihan sistem serta layanan TI jika terjadi gangguan atau keadaan darurat.

Menurut Forum Manajemen Layanan Teknologi Informasi (itSMF) pada tahun 2008, teknologi merupakan elemen inti dalam operasi bisnis. Untuk kelangsungan dan ketersediaan bisnis secara keseluruhan, penting bagi bisnis untuk memperhatikan pengurangan risiko dan strategi pemulihan. Menjaga kemampuan pemulihan menjadi krusial agar proses bisnis berjalan secara efisien.

Tujuan dari Manajemen Kelangsungan Layanan TI (ITSCM), menurut itSMF pada tahun 2007, adalah menjaga kemampuan pemulihan layanan TI agar sesuai dengan kebutuhan, persyaratan, dan jadwal bisnis yang telah disetujui. ITSCM, menurut Institute Governance Teknologi Informasi (ITGI) pada tahun 2007, merupakan kelanjutan dari semua aktivitas siklus hidup layanan yang harus dijamin. Setelah rencana kelangsungan dan pemulihan layanan dibuat, penting agar keduanya sejalan dengan rencana bisnis dan prioritasnya. Menyusun kebijakan strategis ITSCM yang tepat dan mengintegrasikannya dengan rencana bisnis adalah kunci kesuksesan proses ITSCM. Ini dapat dicapai dengan melakukan evaluasi dampak bisnis secara teratur dan latihan manajemen risiko.

## 3. Elemen kunci dari Manajemen Kelangsungan Layanan TI (ITSCM):

Identifikasi Layanan Vital: ITSCM dimulai dengan mengenali layanan TI yang krusial bagi kelangsungan operasional bisnis. Langkah ini memerlukan pemahaman mendalam akan layanan mana yang harus dipulihkan dengan prioritas tertinggi ketika terjadi situasi darurat.

Evaluasi Risiko: Melibatkan penilaian terhadap risiko yang mungkin memengaruhi layanan vital tersebut. Ini termasuk mengidentifikasi ancaman potensial dan dampaknya

terhadap layanan TI, membantu dalam mengevaluasi seberapa rentan sistem terhadap bencana. Rencana Pemulihan: Membuat strategi dan rencana pemulihan yang terstruktur untuk memastikan layanan TI bisa kembali berjalan secepat mungkin setelah terjadinya gangguan. Ini mencakup langkah-langkah spesifik, peran tim, dan sumber daya yang diperlukan.

Pengujian dan Perbaikan: Proses pengujian berkala terhadap rencana pemulihan untuk menjamin efektivitas dan keandalannya saat dibutuhkan. Evaluasi hasil pengujian dan terus-menerus melakukan perbaikan pada rencana tersebut juga penting dalam ITSCM.

Keterlibatan Pihak Terkait: Melibatkan semua stakeholder dalam proses ITSCM, termasuk manajemen, staf TI, dan pengguna akhir layanan tersebut.

Dokumentasi dan Pelaporan: Pentingnya mendokumentasikan setiap aspek dari proses ITSCM, mulai dari analisis risiko, rencana pemulihan, laporan pengujian, hingga evaluasi. Hal ini mendukung transparansi, auditabilitas, dan kemampuan untuk belajar dari pengalaman sebelumnya.

#### 4. ITSCM dalam Konteks Perpustakaan Perguruan Tinggi XYZ menggunakan Framework ITIL

Identifikasi Kebutuhan Bisnis:	Mengidentifikasi layanan kunci dan kebutuhan bisnis dari sistem informasi perpustakaan untuk merencanakan pemulihan darurat yang efektif.
Penilaian Risiko:	Melakukan penilaian risiko yang komprehensif untuk mengidentifikasi potensi gangguan atau bencana yang mungkin mempengaruhi layanan perpustakaan.
Perencanaan Pemulihan:	Membuat rencana pemulihan yang terperinci yang mencakup langkah-langkah pemulihan, tindakan darurat, sumber daya yang dibutuhkan, dan prioritas pemulihan.
Pengujian dan Peningkatan Berkelanjutan:	Melakukan pengujian secara berkala terhadap rencana pemulihan untuk memastikan keefektifannya, serta melakukan perbaikan terus-menerus berdasarkan hasil pengujian.
Komitmen dan Keterlibatan Stakeholder:	Melibatkan semua pihak terkait seperti staf perpustakaan, pengguna, dan pihak terkait lainnya dalam proses perencanaan, pengujian, dan pemulihan.
Dokumentasi dan Pelaporan:	Mendokumentasikan semua proses, rencana, dan hasil pengujian untuk memastikan transparansi dan ketersediaan informasi yang diperlukan saat terjadi bencana atau gangguan.
Pelatihan dan Kesadaran:	Menyelenggarakan pelatihan secara berkala untuk staf perpustakaan mengenai rencana pemulihan darurat dan tindakan yang harus diambil saat terjadi gangguan.
Koordinasi dengan Pihak Eksternal:	Membangun kerjasama dengan entitas eksternal seperti layanan pemulihan bencana, penyedia layanan cloud (jika digunakan), atau lembaga terkait lainnya untuk memperluas upaya pemulihan.

Table 1 Elemen Kunci ITSCM

## METODE PENELITIAN

Dalam proses pengumpulan data di penelitian ini, penulis menggunakan metode wawancara kepada staf perpustakaan perguruan tinggi XYZ dan observasi yaitu dengan mengamati proses bisnis yang terjadi secara langsung maupun pada sistem informasi yang disediakan oleh pihak perpustakaan.

## HASIL DAN PEMBAHASAN

### 1. Perencanaan Manajemen Risiko

Risiko	Ancaman
Listrik padam	Terhentinya proses bisnis dalam sistem terkait sirkulasi dan pemantauan data peminjaman dan pengembalian buku
Jaringan down	Keterlambatan dalam mengakses sistem informasi perpustakaan di web repository
Kurangnya kontrol keamanan	Hilangnya buku oleh mahasiswa maupun ketidak sengajaan staf perpustakaan.
Kurangnya kontrol keamanan	Kerusakan hardware akibat kelalaian pengunjung perpustakaan.
Software versi lama	Menyebabkan proses booting yang berulang sehingga menghambat staf perpustakaan untuk mengoperasikan komputer dan mengakses sistemnya.

Table 2 Perencanaan Manajemen Risiko

### 2. Implementasi

#### a. Tahap Inisialisasi

Perlu dilakukan aktivitas-aktivitas sebagai berikut.

##### 1. Pemilihan kebijakan

Dibutuhkannya kerja sama dan komunikasi yang baik dalam organisasi agar terjalannya kerja sama yang baik dalam keterlibatan di organisasi tersebut. Kebijakan ini dapat dilihat tujuan serta keseriusan dari manajemen dan peran pemimpin sangat berpeluang besar dalam penentuan keberhasilan aktivitas tersebut.

##### 2. Lingkup

Pada tahap ini menentukan skala dan tanggung jawab tim dengan kesesuaian keahlian dan keterampilan yang dimiliki hal tersebut akan berpengaruh di setiap aktivitas yang dilakukan.

### 3. Alokasi sumberdaya

Kesinambungan bisnis memerlukan sumber daya manusia. Kejadian ini sangat dibutuhkan untuk mendukung kesinambungan pada proses. Hasil penyediaan sumberdaya dengan akurat dapat efektivitas pada performa yang dilakukan.

### 4. Struktur pengendalian dan organisasi proyek

Aktivitas yang dilakukan membutuhkan arahan dan bimbingan yang baik, dikarenakan aktivitas tersebut bersifat rumit sehingga membutuhkan proses yang sistematis dan tertanggunglangi

### 5. Perencanaan dan Proyek yang berkualitas

Persiapan dan rencana yang baik dapat kemungkinan keberhasilan yang lebih besar dalam pencapaian yang unggul. Setiap proses aktivitas harus dipersiapkan secara matang meminimalisir resiko terjadinya kegagalan.

## b.Tahap Kebutuhan dan Strategi

Sumber Risiko	Risiko	Likelihood	Impact	Level Risiko
Human disaster	Buku hilang	Low	Low	Low
Human disaster	Kerusakan hardware	Low	Low	Low
Technology disaster	Listrik padam	Low	High	Medium
Technology disaster	Jaringan down	High	Medium	High
Technology disaster	Software versi lama	High	Medium	High

Table 3 Analisis Risiko

## c. Analisis Risiko

Sumber Risiko	Risiko	Strategi keberlangsungan layanan TI
Human disaster	Buku hilang	Pertimbangkan untuk menyediakan layanan pengecekan atau screening kepada pengunjung sebelum keluar dari area perpustakaan
Human disaster	Kerusakan hardware	Pertimbangkan untuk menyediakan layanan pengecekan atau screening kepada pengunjung sebelum memasuki area perpustakaan
Technology disaster	Jaringan down	a. Memeriksa kondisi router wifi b. Perbarui firmware router secara teratur untuk membantu meningkatkan kinerja router wifi c. Gunakan repeater atau extender wifi d. Gunakan kabel ethernet langsung ke router
Technology disaster	Software versi lama	Melakukan update software secara berkala

Table 4 Strategi Keberlangsungan Layanan TI

## KESIMPULAN

Berdasarkan hasil penelitian yang telah dilaksanakan maka diperoleh simpulan sebagai berikut: Proses penilaian risiko menggambarkan profil risiko yang mengancam sistem informasi perpustakaan. Proses ini didasarkan pada tingkat risiko yang terkait dengan sumber daya. Sumber ancaman dapat diidentifikasi berdasarkan dua jenis sumber risiko yakni dari human disaster dan technology disaster. Berdasarkan hasil analisis, didapatkan hasil bahwa terdapat 2 risiko dengan level rendah, 1 risiko dengan level menengah, dan 2 risiko dengan level tinggi. Rekomendasi penanganan sudah ditentukan untuk membantu mengatasi risiko-risiko tersebut.

## DAFTAR PUSTAKA

- AlArabi, M. M. U., Santosa, I., & Nurtrisha, W. A. (2023). Asesmen dan Peningkatan Manajemen Layanan Teknologi Informasi Pada Practice Supplier Management dan Service Level Management Menggunakan ITIL 4. *EProceedings of Engineering*, 10(2).
- Ayuh, J. A., & Chernovita, H. P. (2021). Analisis Incident Management E-Court Pada Pengadilan Negeri Salatiga Menggunakan Framework ITIL V4. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 8(2), 585–598.
- Herlinudinkhaji, D., & Ramadhani, L. K. (2023). Tata Kelola Layanan Teknologi Informasi dengan ITIL V4 untuk Estimasi Layanan. *REMIK: Riset Dan E-Jurnal Manajemen Informatika Komputer*, 7(1), 452–457.
- Maliki, I. (2010). Manajemen Resiko Teknologi Informasi I Untuk Keberlangsungan Layanan Publik Menggunakan Framework Information Technology Infrastructure Library (Itil Versi 3). Seminar Nasional Aplikasi Teknologi Informasi (SNATI).