

# Analisis Manajemen Risiko Teknologi Informasi Pada Aplikasi LMS Sevima Edlink Menggunakan *Framework* ISO 31000 (Studi Kasus: Prodi Teknologi Informasi)

Bela Astuti<sup>1</sup>, Zidan<sup>2</sup>, Umar Faruq Vista<sup>3</sup>

Universitas Bangka Belitung<sup>1,2,3</sup>

belafauziastuti@gmail.com<sup>1</sup>, zidantiubb@gmail.com<sup>2</sup>, umar.vista@ubb.ac.id<sup>3</sup>

---

## Abstrak

Di era sekarang teknologi semakin berkembang dan canggih. Salah satunya teknologi informasi. Teknologi informasi berfungsi untuk membantu organisasi menemukan strategi bisnis baru untuk menghadapi persaingan dan juga meningkatkan produktivitas, agar teknologi informasi dapat dimanfaatkan sesuai dengan kepentingan strategi bisnis. Dengan begitu pentingnya melakukan analisis manajemen risiko terhadap risiko yang muncul di dalam Teknologi Informasi tersebut. Sehingga Universitas Bangka Belitung dapat melakukan pencegahan, penanganan dan perbaikan terhadap risiko tersebut sesuai tingkat prioritas risiko. Pengelolaan risiko dinilai sebagai sebuah tantangan untuk instansi di mana mereka akan menghadapi berbagai ancaman yang kompleks. Sehingga penelitian ini bertujuan untuk menganalisis risiko yang terjadi pada aplikasi LMS Sevima Edlink. Penerapan manajemen risiko pada penelitian ini menggunakan ISO 31000 yang terdiri dari tahapan identifikasi risiko, analisis risiko, evaluasi risiko, penanganan risiko serta monitoring dan *review*. Dari hasil penelitian ini, terdapat 1 kemungkinan risiko dengan tingkatan *high*, 11 kemungkinan risiko dengan tingkatan *medium*, dan 2 risiko tingkatan *low*. Sehingga dengan adanya penelitian ini diharapkan supaya dapat mengurangi kemungkinan risiko yang dapat disebabkan oleh berbagai faktor.

**Kata kunci:** Teknologi Informasi, Manajemen Risiko, ISO 31000

---

## PENDAHULUAN

Di era sekarang teknologi semakin berkembang dan canggih. Salah satunya teknologi informasi. Teknologi informasi berfungsi untuk membantu organisasi menemukan strategi bisnis baru untuk menghadapi persaingan, juga meningkatkan produktivitas (Desy Ria and Budiman 2021). Agar teknologi informasi dapat dimanfaatkan sesuai dengan kepentingan strategi bisnis (Sulistiani and Darwis 2020). Tata kelola teknologi informasi adalah bagian dari sebuah organisasi pada sistem dan teknologi informasi serta manajemen kinerja dan risiko. Salah satu standar yang digunakan dalam tata kelola teknologi informasi adalah ISO 31000. ISO 31000 merupakan kerangka kerja standar nasional yang sering digunakan untuk membantu mengelola risiko Teknologi Informasi (IT) dan berfungsi untuk memberikan panduan sistematis dalam proses pengidentifikasian, menganalisis, dan mengelola risiko guna meningkatkan efisiensi dan keberlangsungan operasional organisasi. Tujuan ISO 31000 ialah untuk membantu organisasi dalam mencapai sasaran dalam organisasi dan memastikan bahwa risiko yang sesuai dapat diidentifikasi, dinilai, dan dikelola secara efektif (Fachrezi, Dwika Cahyono, and Tanaem 2021).

Risiko merupakan potensi bahaya yang dapat mempengaruhi peluang organisasi dalam mencapai suatu tujuan (Bima Mahardika et al. 2019). Ketika sistem yang digunakan tidak berfungsi secara efektif, maka sebuah instansi yang bergantung pada sistem informasi dapat mengalami gangguan serius. Jika terdapat bahaya dalam perangkat lunak atau perangkat keras maka instansi tersebut harus siap mengambil tindakan yang tepat. Penanganan risiko tersebut akan ditujukan pada aset yang memiliki kemungkinan terjadinya risiko dengan mengidentifikasi penyebab dan mencari sebuah solusi dengan tepat (Fahlepi et al. 2023).

Universitas Bangka Belitung merupakan instansi yang bergerak di bidang pendidikan. Berdasarkan kuesioner yang telah dibagikan kepada Prodi Teknologi Informasi, instansi tersebut sudah menerapkan teknologi informasi dalam aktivitas pelayanan akademik

(SIAKAD), yang bertujuan untuk meningkatkan kinerja dan memberikan pelayanan akademik yang baik. Sistem Informasi Akademik (SIAKAD) merupakan sebuah sistem informasi yang digunakan dalam mengelola data dosen, data mahasiswa serta mengelola pelayanan administrasi akademik. Sistem informasi Akademik (SIAKAD) hadir sejak tahun 2020 yang dinilai sangat membantu dalam aktivitas yang dilakukan dosen, pegawai dan mahasiswa. Tetapi tidak dapat dipungkiri kemungkinan akan terjadinya ancaman risiko yang terjadi pada sistem, sehingga dapat mengganggu aktivitas proses bisnis sehingga kegiatan tidak bisa berjalan dengan baik. Adapun hasil dari kuesioner yang dibagikan peneliti lakukan dengan Prodi Teknologi Informasi mengenai Sistem Informasi Akademik (SIAKAD) dalam penerapannya Universitas Bangka Belitung belum pernah melakukan pengelolaan risiko terhadap Sistem Informasi Akademik (SIAKAD). (Fahlepi et al. 2023). Salah satu pendekatan untuk menguji manajemen risiko teknologi informasi ialah ISO 31000 (Bima Mahardika et al. 2019). Sistem manajemen risiko yang disiplin dan metodis dapat dibuat dengan menggunakan kerangka kerja sebagai panduan (Thenu et al. 2020).

Dalam peraturan presiden Nomor 5 Tahun 2018, Dalam lingkup manajemen SPBE manajemen risiko memiliki tujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam penerapan SPBE. Organisasi yang belum mempunyai memiliki panduan manajemen risiko SPBE dalam menyelenggarakan *e-government*. Maka akan mengakibatkan organisasi tersebut tidak akan melakukan identifikasi, analisis dan penanganan risiko SPBE yang berdampak pada pencapaian sasaran dan tujuan secara efektif jika risiko terjadi. Sehingga ISO 31000 dapat membantu organisasi dalam melakukan identifikasi, analisis dan penanganan (Aprianto et al. 2021).

Penelitian sebelumnya tentang ISO 31000 telah dipublikasikan di tahun 2017 yang berjudul “Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada program HRMS” yang dipublikasikan oleh Stefan Agustinus (Fahlepi et al. 2023). Fransisca Lady Nice pada tahun 2016 yang berjudul “Analisis Risiko Teknologi Informasi di Lembaga Penerbangan dan Antariksa Nasional (LAPAN).” ISO 31000 berfungsi untuk membantu mengidentifikasi manajemen risiko pada unit pelayanan organisasi. ISO 31000 tentang manajemen risiko telah dilakukan dalam penelitian (v) untuk melakukan prioritas risiko, perancangan *Standard Operational Procedure* (v), dan mengevaluasi sistem penjualan (v). Penerapan ISO 31000 pastinya bermanfaat bagi sebuah organisasi yang menerapkannya. Dengan penerapan tersebut dapat meningkatkan pengambilan risiko, melindungi nilai organisasi, dan meningkatkan kesadaran risiko dalam sebuah organisasi (Haryani 2024). ISO 31000 dapat memberikan kerangka kerja yang lebih fleksibel, sehingga dapat digunakan di berbagai organisasi, termasuk pendidikan. Dalam Manajemen risiko TI, ISO 31000 berguna untuk memberikan strategi pencegahan yang paling efektif setelah melakukan identifikasi risiko spesifik yang akan dihadapi (Nurhadi, Chumaidiyah, and Andrawina 2023). Hasil dari analisis manajemen risiko TI dapat berfungsi untuk mempermudah institusi dalam mengelola risiko yang terjadi dan dapat memastikan keberlangsungan operasional institusi (Aprikasari et al. 2024).

Melalui penelitian ini, analisis dilakukan terhadap penerapan I ISO 31000 di Prodi Teknologi Informasi dengan berfokus pada aplikasi LMS Sevima Edlink. Penelitian ini bertujuan untuk menganalisis risiko yang terjadi pada aplikasi LMS Sevima Edlink.

## TINJAUAN PUSTAKA

### Pengertian Risiko

Risiko adalah kemungkinan perubahan pada hal-hal yang terjadi secara alami atau kejadian tak terduga. Kejadian tersebut bisa menimbulkan ancaman terhadap properti dan keuntungan ekonomi karena terjadinya bahaya. Risiko muncul ketika terjadinya ketidakpastian yang memiliki efek samping yang potensial, seperti kemungkinan kerugian. Risiko dapat dijelaskan

sebagai suatu bentuk ketidakpastian tentang situasi suatu keadaan yang mengharuskan keputusan dibuat berdasarkan berbagai pertimbangan (Risnaeni, Rois, and Ramadhani 2019).

### **Pengertian Manajemen Risiko**

Manajemen risiko adalah penerapan fungsi manajemen terhadap pengelolaan dalam suatu risiko, termasuk risiko yang dialami oleh organisasi/perusahaan, rumah tangga, dan masyarakat. Proses ini mencakup beberapa tahap, seperti perencanaan, pengorganisasian, persiapan, kepemimpinan/koordinasi, dan evaluasi kegiatan manajemen risiko (Lionel et al. 2023).

Manajemen risiko dalam aplikasi teknologi informasi perusahaan adalah suatu proses yang memungkinkan manajer teknologi informasi untuk menyeimbangkan biaya operasional dan ekonomi sebagai langkah pengamanan bisnis dalam melindungi sistem teknologi informasi dan data yang mendukung atau mengatur misi dalam suatu perusahaan (Atmojo and Manuputty 2020).

Manajemen risiko memiliki tujuan untuk meningkatkan kinerja, menciptakan inovasi terbaru dan mendukung pencapaian dari suatu tujuan perusahaan. Manajemen risiko membangun dasar dalam pengelolaan risiko dan beberapa prinsip yang harus dipertimbangkan pada saat menetapkan proses dan konsep kerja dalam manajemen risiko (Dylanza, Mayavanny, and Pratama 2024).

### **Pengertian ISO 31000**

ISO (*International Organization for Standardization*) merupakan badan gabungan standar nasional di seluruh dunia. ISO 31000 adalah dokumen standar internasional yang menyatakan bahwa ISO 31000 adalah prinsip dan kerangka kerja yang dapat digunakan untuk manajemen risiko. Kerangka kerja ISO 31000 dapat membantu organisasi dalam menyelesaikan strategi mereka untuk mencapai tujuan, mengidentifikasi peluang atau ancaman terhadap proses bisnis saat ini dalam organisasi dan kemudian menentukan langkah-langkah untuk meminimalkan risiko yang berdampak negatif terhadap organisasi (Alamsyah and Rolliawati 2025).

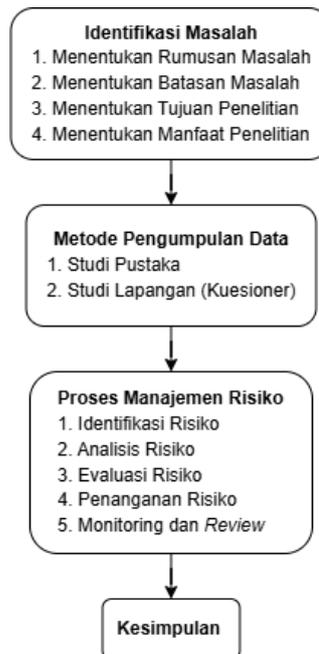
### **Pengertian LMS Sevima Edlink**

*Learning Management System* (LMS) adalah aplikasi yang digunakan untuk membantu dalam merencanakan dan melaksanakan proses kegiatan pembelajaran. *Learning Management System* (LMS) memfasilitasi pemilik untuk mengelola, mengajar, dan memantau peserta didik mereka. *Learning Management System* (LMS) menggabungkan pembelajaran tradisional dengan media digital dan alat interaktif, termasuk pembelajaran daring, kelas virtual, dan forum diskusi (Fitriani 2020).

Sevima Edlink adalah aplikasi yang digunakan sebagai media pendukung proses penilaian dalam kegiatan pembelajaran pada sektor pendidikan, khususnya pendidikan perguruan tinggi. Aplikasi ini bertujuan untuk menyediakan ruang belajar di mana para pendidik dan peserta didik memiliki kesempatan untuk menyesuaikan waktu mereka untuk terlibat dalam kegiatan proses pembelajaran (Mawarsih, Kurniawati, and Darni 2024).

## METODE

Peneliti menggunakan sebuah konsep untuk menyelesaikan masalah pada penelitian ini.



**Gambar 1. Tahapan Penelitian**

Dari kerangka Gambar 1 di atas, maka dapat dijelaskan sebagai berikut:

### 1. Identifikasi Masalah

Identifikasi masalah merupakan langkah awal yang digunakan peneliti untuk mempelajari tema yang diangkat. Di mana identifikasi masalah yang dilakukan peneliti adalah sebagai berikut:

#### a. Menentukan Rumusan Masalah

Pada tahap ini peneliti menentukan rumusan masalah, yaitu bagaimana melakukan analisis manajemen risiko teknologi informasi pada aplikasi LMS Sevima Edlink menggunakan *Framework ISO 31000* di Prodi Teknologi Informasi, Universitas Bangka Belitung.

#### b. Menentukan Batasan Masalah

Pada tahap ini peneliti memfokuskan pada risiko yang terjadi dalam penggunaan aplikasi LMS Sevima Edlink dan faktor-faktor yang mempengaruhi risiko dari aplikasi menggunakan *Framework ISO 31000* di Prodi Teknologi Informasi, Universitas Bangka Belitung.

#### c. Menentukan Tujuan Penelitian

Penelitian ini bertujuan untuk melakukan tahapan dan proses analisis manajemen risiko pada aplikasi LMS Sevima Edlink sesuai dengan standar *Framework ISO 31000*.

#### d. Menentukan Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat bagi Prodi Teknologi Informasi, Universitas Bangka Belitung.

### 2. Metode Pengumpulan Data

Metode yang dilakukan peneliti untuk mengumpulkan data yaitu, studi pustaka dan studi lapangan (kuesioner).

### 3. Proses Manajemen Risiko *Framework ISO 31000*

Dalam proses manajemen risiko terdapat serangkaian aktivitas, yaitu:

#### a. **Assessment Risiko**

ISO 31000 mendefinisikan *asesment* risiko sebagai identifikasi risiko, analisis risiko, serta evaluasi risiko.

##### 1. **Identifikasi Risiko**

Identifikasi pada penelitian ini menggunakan kuesioner yang dibagikan secara langsung kepada mahasiswa teknologi informasi yang mencakup berdasarkan pengalaman. Berikut proses dari identifikasi risiko:

- a) Identifikasi aplikasi LMS Sevima Edlink yang dimiliki mahasiswa.
- b) Identifikasi kemungkinan risiko yang terjadi pada aplikasi LMS Sevima Edlink.
- c) Identifikasi dampak yang akan diterima oleh mahasiswa.

##### 2. **Analisis Risiko**

Pada penelitian ini peneliti melakukan analisis risiko secara kualitatif. Secara umum analisis kualitatif merupakan analisis yang digunakan untuk jangkauan identifikasi dampak dan kemungkinan yang luas, sehingga dapat digunakan sebagai bahan evaluasi pemeringkatan risiko. Dengan melakukan analisis risiko secara kualitatif dapat ditentukan prioritas dalam analisis dengan mengukur dan menggabungkan probabilitas terjadinya risiko dan dampak dari hal tersebut. Dengan begitu analisis risiko kualitatif dianggap sebagai tahapan yang paling efektif, di mana dapat melakukan evaluasi yang berfokus pada risiko yang memiliki prioritas tinggi. Hal tersebut juga dapat digunakan sebagai dasar dalam melakukan analisis risiko kualitatif. Sehingga setelah teridentifikasi probabilitas serta dampak, maka akan dilakukan evaluasi guna untuk mengetahui risiko yang menjadi prioritas untuk ditangani terlebih dahulu.

<i>Likelihood</i> Rating Kriteria	Keterangan	Frekuensi
1 <i>Rare</i>	Risiko hampir tidak pernah terjadi	>2 tahun
2 <i>Unlikely</i>	Risiko jarang terjadi	1 – 2 tahun
3 <i>Possible</i>	Risiko kadang-kadang terjadi	7 – 12 bulan / tahun
4 <i>Likely</i>	Risiko sering terjadi	4 -6 bulan/ tahun
5 <i>Certain</i>	Risiko pasti terjadi	1 -3 bulan / tahun

**Gambar 2 Tabel Likelihood**

<i>Impact</i> Rating	Kriteria	Keterangan
1	<i>Insignificant</i>	Tidak mengganggu aktivitas mahasiswa
2	<i>Minor</i>	Proses aplikasi LMS Sevima Edlink mengalami gangguan, namun tidak menghambat aktivitas pembelajaran mahasiswa
3	<i>Moderate</i>	Proses aplikasi LMS Sevima Edlink mengalami gangguan, sehingga menghambat aktivitas pembelajaran mahasiswa
4	<i>Major</i>	Menghambat hampir seluruh aktivitas mahasiswa
5	<i>Catastrophic</i>	Proses aplikasi LMS Sevima Edlink mengalami gangguan total sehingga aktivitas mahasiswa berhenti total dan proses aktivitas tidak tercapai

**Gambar 3 Tabel Impact**

### 3. Evaluasi Risiko

Pada tahap ini peneliti melakukan evaluasi risiko dengan kriteria risiko yang sudah distandarkan.

<i>Certain / Pasti Terjadi</i> (5)	Moderate	Moderate	High	High	High
<i>Likely / Sering</i> (4)	Low	Moderate	High	High	High
<i>Possible / Kadang</i> (3)	Low	Low	Moderate	High	High
<i>Unlikely / Jarang</i> (2)	Low	Low	Moderate	Moderate	High
<i>Rare / Sangat Jarang</i> (1)	Low	Low	Low	Moderate	Moderate
	<i>Insignificant / Sangat Kecil</i> (1)	<i>Minor / Kecil</i> (2)	<i>Moderate / Biasa</i> (3)	<i>Major / Besar</i> (4)	<i>Catastrophic / Sangat Besar</i> (5)

Gambar 4 Matriks Evaluasi Risiko

Level Risiko	Keterangan
<i>High Risk - Risiko Tinggi</i>	Risiko yang berbahaya yang harus diatasi secepatnya.
<i>Moderate Risk - Risiko Sedang</i>	Risiko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan.
<i>Low Risk - Risiko Rendah</i>	Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil.

Gambar 5 Level Risiko

#### 4. Penanganan Risiko

Pada tahapan ini terdapat beberapa strategi yang digunakan peneliti untuk melakukan penanganan risiko, yaitu:

##### 1) *Transfer*

Strategi ini berfungsi untuk memindahkan dampak negatif yang terdapat pada ancaman risiko, serta bersamaan dengan tanggung jawab kepada pihak ketiga.

##### 2) *Mitigate*

Strategi ini digunakan untuk mengurangi probabilitas dan dampak dari risiko hingga menjadi batas bisa diterima serta analisis melalui kontrol preventif (pencegahan), kontrol korektif (perbaikan), kontrol direktif (pengarahan), dan kontrol deteksi.

##### 3) *Avoidance*

Strategi ini digunakan guna untuk menghilangkan kemungkinan terjadinya risiko terhadap risiko-risiko yang berdampak sangat besar pada aplikasi LMS Sevima Edlink.

##### 4) *Acceptance*

Strategi ini digunakan untuk risiko yang terjadi pada aplikasi LMS Sevima Edlink, namun masih dalam batas wajar.

#### 5. Monitoring dan Review

*Pelaksanaan monitoring dan review* dilakukan terhadap seluruh proses manajemen risiko termasuk konteksnya. Hasil dari catatan dan pengkajian ulang disimpan guna sebagai bukti dan laporan bahwa kegiatan itu telah dilaksanakan dan disiapkan sebagai masukan untuk *Risk Management Framework*.

## HASIL DAN PEMBAHASAN

### Proses Manajemen Risiko

#### 1) Identifikasi Aset

Peneliti melakukan tahapan identifikasi aset terhadap aplikasi LMS Sevima Edlink. Di mana pada tahapan ini diawali dengan melakukan proses studi pustaka dan studi lapangan (kuesioner). Sehingga berfokus pada identifikasi aset dari pengguna, data, hingga *software* yang berkaitan dengan aplikasi LMS Sevima Edlink. Detail aset yang terkait dengan aplikasi LMS Sevima Edlink dapat dilihat pada Tabel 1.

**Tabel 1 Identifikasi Aset LMS Sevima Edlink**

No.	Kategori	Aset
1	Pengguna	Mahasiswa Pengguna LMS Sevima Edlink Dosen Pengguna LMS Sevima Edlink Admin LMS Sevima Edlink
2	Data	Data Akun Pengguna Data Pembelajaran Data Aktivitas Pengguna
3	<i>Software</i>	Aplikasi <i>Mobile</i> LMS Sevima Edlink Website LMS Sevima Edlink Sistem <i>Database</i> LMS Sevima Edlink
4	<i>Hardware</i>	Perangkat Pengguna Server Penyimpanan LMS Sevima Edlink Perangkat Akses Jaringan ( <i>Wifi/Lan</i> ) Perangkat Infrastruktur Jaringan ( <i>Router/Switch</i> )

Sumber: Olahan Peneliti (2025)

#### 2) Identifikasi Kemungkinan Risiko

Setelah melakukan proses identifikasi aset terhadap aplikasi LMS Sevima Edlink, hal yang akan dilakukan selanjutnya ialah identifikasi kemungkinan risiko. Di mana identifikasi kemungkinan risiko berfungsi untuk mengidentifikasi berbagai kemungkinan risiko yang muncul terhadap aset aplikasi LMS Sevima Edlink yang terdiri dari berbagai faktor. Kemungkinan-kemungkinan yang terjadi dari berbagai faktor dapat dilihat pada Tabel 2.

**Tabel 2 Identifikasi Kemungkinan Risiko**

ID	Risiko	Faktor
IR01	Penyalahgunaan hak akses oleh pengguna	Manusia (SDM)
IR02	Kesalahan pengguna dalam menggunakan sistem	
IR03	Pegawai tidak mengikuti aturan standar operasional prosedur (SOP)	
IR04	Data dan informasi yang tidak sesuai	
IR05	Data rusak dan tidak bisa digunakan	Sistem dan Infrastruktur
IR06	Tampilan antarmuka dan fitur LMS Sevima Edlink kurang ramah pengguna	
IR07	Kerusakan <i>software</i> pada sistem	
IR08	Server mengalami <i>down</i>	
IR09	Penggunaan <i>database</i> melebihi kapasitas	
IR10	Serangan <i>virus</i> dan <i>malware</i> terhadap sistem	
IR11	Kegagalan jaringan terhadap sistem	
IR12	Ruang server mengalami kebakaran	Lingkungan dan Alam
IR13	Banjir	
IR14	Gempa bumi	

Sumber: Olahan Peneliti (2025)

### 3) Identifikasi Dampak Risiko

Tahap selanjutnya yaitu melakukan identifikasi dampak risiko. Di mana pada tahapan ini terdapat proses mengidentifikasi dampak apa yang akan dialami oleh aplikasi LMS Sevima Edlink jika kemungkinan risiko yang sudah diidentifikasi sebelumnya terjadi.

**Tabel 3 Dampak Risiko**

IDE	Risiko	Dampak
IR01	Penyalahgunaan hak akses oleh pengguna	Data yang terdapat di dalam sistem LMS Sevima Edlink bisa diakses atau diubah oleh pihak yang tidak bertanggung jawab.
IR02	Kesalahan pengguna dalam menggunakan sistem	Kesalahan oleh pengguna akan berdampak pada ketidaksesuaian data dan kegagalan pada proses sistem.
IR03	Pegawai tidak mengikuti aturan standar operasional prosedur (SOP)	Layanan LMS Sevima Edlink tidak bisa digunakan sesuai dengan ketentuan yang telah ditetapkan.
IR04	Data dan informasi yang tidak sesuai	Ketidaksesuaian data yang tersedia menyebabkan pengambilan keputusan menjadi tidak tepat.
IR05	Data rusak dan tidak bisa digunakan	Data atau informasi terkait pembelajaran tidak bisa diakses dalam proses kegiatan akademik.
IR06	Tampilan antarmuka dan fitur LMS Sevima Edlink kurang ramah pengguna	Pengguna kesulitan dalam menggunakan fitur yang tersedia.
IR07	Kerusakan <i>software</i> pada sistem	Sistem tidak bisa diakses yang mengakibatkan terjadinya gangguan operasional.
IR08	Server mengalami <i>down</i>	Layanan LMS Sevima Edlink tidak bisa digunakan untuk sementara waktu, yang mengakibatkan proses pembelajaran terganggu.
IR09	Penggunaan <i>database</i> melebihi kapasitas	Sistem LMS Sevima Edlink menjadi lambat atau tidak merespon yang menghambat proses kegiatan akademik.
IR10	Serangan <i>virus</i> dan <i>malware</i> terhadap sistem	Data yang tersedia bisa mengalami kerusakan ataupun kehilangan, serta berisiko dicuri oleh pihak yang tidak bertanggung jawab.
IR11	Kegagalan jaringan terhadap sistem	

		Kegagalan jaringan, seperti koneksi terputus mengakibatkan pengguna tidak bisa mengakses sistem.
IR12	Ruang server mengalami kebakaran	Data yang tersimpan pada server bisa hilang secara permanen dan seluruh sistem LMS Sevima Edlink tidak bisa digunakan.
IR13	Banjir	Perangkat keras ( <i>Hardware</i> ) bisa mengalami kerusakan dan sistem LMS Sevima Edlink tidak bisa digunakan.
IR14	Gempa bumi	Infrastruktur mengalami kerusakan yang sangat parah, sehingga sistem LMS Sevima Edlink tidak bisa digunakan dalam rentang waktu yang lama.

Sumber: Olahan Peneliti (2025)

### Analisis Risiko

Setelah melakukan tahap identifikasi risiko, kemudian tahap yang akan dilakukan selanjutnya yaitu analisis risiko. Pada tahap peneliti akan melakukan penilaian terhadap kemungkinan risiko yang telah diidentifikasi. Dengan menentukan nilai berdasarkan *Likelihood* dan *impact* pada tabel 4.

**Tabel 4 Analisis Risiko**

ID	Risiko	Likelihood	Impact
IR01	Penyalahgunaan hak akses oleh pengguna	2	3
IR02	Kesalahan pengguna dalam menggunakan sistem	4	3
IR03	Pegawai tidak mengikuti aturan standar operasional prosedur (SOP)	2	3
IR04	Data dan informasi yang tidak sesuai	2	3
IR05	Data rusak dan tidak bisa digunakan	2	3
IR06	Tampilan antarmuka dan fitur LMS Sevima	2	2

	Edlink kurang ramah pengguna		
IR07	Kerusakan <i>software</i> pada sistem	2	4
IR08	Server mengalami <i>down</i>	2	3
IR09	Penggunaan <i>database</i> melebihi kapasitas	2	3
IR10	Serangan <i>virus</i> dan <i>malware</i> terhadap sistem	1	3
IR11	Kegagalan jaringan terhadap sistem	3	3
IR12	Ruang server mengalami kebakaran	1	5
IR13	Banjir	1	4
IR14	Gempa bumi	1	4

Sumber: Olahan Peneliti (2025)

**Evaluasi Risiko**

Tahap evaluasi risiko merupakan tahap terakhir dalam *risk assesment*. Di mana pada tahap ini terdapat acuan berupa matriks risiko, di mana pada matriks tersebut terdapat 3 *risk level* yaitu *low*, *medium* dan *high*. Sehingga pada tahap ini akan membedakan kemungkinan risiko dengan berdasarkan nilai *likelihood* dan nilai *impact* pada proses sebelumnya terhadap matriks yang ada.

**Tabel 5 Matriks Risiko**

Certain/ Pasti Terjadi (5)					
	Likely / Sering (4)			IR02	
	Possible / Kadang (3)			IR11	
	Unlikely / Jarang (2)		IR06	IR01 IR03 IR04 IR05 IR08 IR09	IR07

Rare Hampir Tidak Pernah (1)			IR10	IR13 IR14	IR12
	<i>Insignificant /</i>	<i>Minor /</i>	<i>Moderate /</i>	<i>Major /</i>	<i>Catastrophic /</i>
	Sangat Kecil	Kecil	Biasa	Besar	Sangat Besar
	(1)	(2)	(3)	(4)	(5)
<b>IMPACT</b>					

Sumber: Olahan Peneliti (2025)

Setelah kemungkinan – kemungkinan risiko didata ke dalam matriks evaluasi berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*), proses selanjutnya adalah menjabarkan dari 14 kemungkinan risiko ke dalam *level of risk* dengan tingkatan *high*, *medium* dan *low*.

**Tabel 6 Evaluasi Risiko**

ID	Risiko	Likelihood	Impact	Risk Level
IR02	Kesalahan pengguna dalam menggunakan sistem	4	3	High
IR07	Kerusakan <i>software</i> pada sistem	2	4	Medium
IR11	Kegagalan jaringan terhadap sistem	3	3	Medium
IR01	Penyalahgunaan hak akses oleh pengguna	2	3	Medium
IR03	Pegawai tidak mengikuti aturan standar operasional prosedur (SOP)	2	3	Medium
IR04	Data dan informasi yang tidak sesuai	2	3	Medium
IR05	Data rusak dan tidak bisa digunakan	2	3	Medium
IR08	Server mengalami <i>down</i>	2	3	Medium
IR09	Penggunaan <i>database</i> melebihi kapasitas	2	3	Medium
IR12	Ruang server mengalami kebakaran	1	5	Medium
IR13	Banjir	1	4	Medium
IR14	Gempa bumi	1	4	Medium

IR06	Tampilan antarmuka dan fitur LMS Sevima Edlink kurang ramah pengguna	2	2	Low
IR10	Serangan <i>virus</i> dan <i>malware</i> terhadap sistem	1	3	Low

Sumber: Olahan Peneliti (2025)

### Penanganan Risiko

Tahapan yang akan dilakukan selanjutnya yaitu penanganan risiko. Di mana pada tahap ini penulis akan memberikan saran terhadap perlakuan risiko untuk memungkinkan risiko yang ada pada aplikasi LMS Sevima Edlink. Hal ini bertujuan untuk mengurangi dan mencegah terhadap kemungkinan yang mungkin akan muncul.

**Tabel 7 Penanganan Risiko**

ID	Risiko	Risk Level	Penanganan Risiko
IR02	Kesalahan pengguna dalam menggunakan sistem	High	Mengadakan pelatihan penggunaan terhadap sistem dan menyediakan fitur akses bantuan.
IR07	Kerusakan <i>software</i> pada sistem	Medium	Selalu memantau kondisi <i>software</i> yang digunakan dan mengganti <i>software</i> lama dengan yang baru agar tidak terjadi kerusakan.
IR11	Kegagalan jaringan terhadap sistem	Medium	Menyiapkan jaringan cadangan dan menggunakan layanan penyedia internet yang terpercaya serta melakukan pemantauan secara <i>real-time</i> .
IR01	Penyalahgunaan hak akses oleh pengguna	Medium	Melakukan pengaturan terhadap hak akses (siapa saja yang bisa mengakses) serta mencatat dan mengawasi setiap aktivitas pengguna dalam sistem.
IR03	Pegawai tidak mengikuti aturan standar operasional prosedur (SOP)	Medium	Memberikan pelatihan terhadap pegawai serta mencetak SOP berbentuk poster maupun panduan singkat pada area kerja.
IR04	Data dan informasi yang tidak sesuai	Medium	Data yang masuk ke dalam sistem harus diperiksa dan divalidasi terlebih dahulu, kemudian melakukan audit data secara berkala guna menjaga kualitas.
IR05	Data rusak dan tidak bisa digunakan	Medium	Melakukan <i>backup</i> data secara rutin dan menggunakan sistem penyimpanan terbaru untuk mencegah kerusakan data.

IR08	Server mengalami <i>down</i>	Medium	Selalu melakukan pemeliharaan server dan menyiapkan server cadangan apabila terjadi gangguan pada server utama.
IR09	Penggunaan <i>database</i> melebihi kapasitas	Medium	Pemantauan sistem <i>database</i> supaya tidak kelebihan beban. Jika terdapat kelebihan beban, maka perlu melakukan peningkatan kapasitas serta optimasi penggunaan.
IR12	Ruang server mengalami kebakaran	Medium	Ruang server harus dilengkapi dengan alat pemadam kebakaran otomatis dan sistem pendingin untuk menjaga suhu ruangan.
IR13	Banjir	Medium	Menyimpan infrastruktur perangkat di tempat yang tinggi agar tidak terkena air banjir.
IR14	Gempa bumi	Medium	Menyimpan server pada bangunan yang strukturnya kuat sehingga tahan akan terhadap guncangan gempa.
IR06	Tampilan antarmuka dan fitur LMS Sevima Edlink kurang ramah pengguna	Low	Memperbaharui tampilan sistem secara rutin berdasarkan pengalaman dan saran dari pengguna.
IR10	Serangan <i>virus</i> dan <i>malware</i> terhadap sistem	Low	Menggunakan antivirus, <i>firewall</i> terbaru dan melakukan <i>update</i> sistem keamanan secara rutin.

Sumber: Olahan Peneliti (2025)

### Monitoring dan Review

Hasil yang diperoleh dari proses monitoring *dan riview* yaitu berupa kritik dan saran dari berbagai pihak yang terlibat langsung dalam penggunaan serta pengelolaan aplikasi LMS Sevima Edlink. Di mana proses ini bertujuan untuk memastikan bahwa pengelolaan risiko dilakukan secara berkelanjutan. Sehingga dapat membantu kelancaran proses akademik pada Prodi Teknologi Informasi. Proses pelaksanaan manajemen risiko dikelola dan di monitoring oleh tim pengelola sistem informasi dan teknologi pada Prodi Teknologi Informasi yaitu akademik, dosen serta tim teknis teknik IT kampus. Pelaksanaan proses monitoring *dan review* dilakukan dengan mengadakan rapat dan pertemuan yang berfungsi untuk melaporkan terkait implementasi aplikasi LMS Sevima Edlink termasuk kendala yang berpotensi untuk menghambat proses penggunaan aplikasi. Serta pembahasan terkait bagaimana langkah penanganan dan pencegahan risiko yang muncul. Hal tersebut dilakukan untuk meminimalkan risiko yang akan datang.

### KESIMPULAN

Berdasarkan penelitian yang dilakukan di Prodi Teknologi Informasi terhadap penggunaan aplikasi LMS Sevima Edlink melalui beberapa tahapan mulai dari identifikasi aset, penilaian risiko, analisis risiko, evaluasi risiko, hingga penanganan risiko. Sehingga mendapatkan 14 risiko yang ada pada aplikasi LMS Sevima Edlink.

Dalam penelitian ini ditemukan 1 kemungkinan risiko dengan tingkatan *high* yaitu, kesalahan pengguna dalam menggunakan sistem. Kemudian terdapat 11 risiko dengan tingkatan

*medium*, meliputi kerusakan *software* pada sistem, kegagalan jaringan terhadap sistem, penyalahgunaan hak akses oleh pengguna, pegawai tidak mengikuti aturan standar operasional prosedur (SOP), data dan informasi yang tidak sesuai, data rusak dan tidak bisa digunakan, server mengalami *down*, penggunaan *database* melebihi kapasitas, ruang server mengalami kebakaran, banjir, dan gempa bumi. Selain itu juga terdapat 2 risiko dengan tingkat *low*, antara lain yaitu tampilan antar muka dan fitur LMS Sevima Edlink kurang ramah pengguna, serta serangan *virus* dan *malware* terhadap sistem.

Dengan adanya penelitian ini diharapkan supaya dapat mengurangi kemungkinan risiko yang dapat disebabkan oleh berbagai faktor, seperti yang sudah dijelaskan pada halaman pembahasan dengan menerapkan penanganan risiko dari Tabel 7. Sehingga proses aktivitas pembelajaran mahasiswa Prodi Teknologi Informasi dapat berjalan dengan baik.

## DAFTAR PUSTAKA

- Alamsyah, Muhammad Ramdhany, and Dwi Rolliawati. 2025. "Analisis Manajemen Risiko Sistem Informasi Pelayanan Perlindungan Perempuan Dan Anak DP3APPKB Surabaya Dengan ISO 31000:2018." *JATI (Jurnal Mahasiswa Teknik Informatika)* 9 (1): 1322–27.
- Aprianto, Khrisna, Supeno Mardi Susiki Nugroho, Teknik Elektro, Fakultas Teknologi Elektro dan Informatika Cerdas, and Its Surabaya. 2021. "Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk Dan ISO 31000:2018 Di Kabupaten Magetan." *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*. Vol. 23. Surabaya.
- Aprikasari, Manda, Laurence Benedicta, Nathanael Abel Adrielvino, and Afifah Trista Ayunda. 2024. "Penerapan ISO 31000:2018 Untuk Manajemen Risiko IT Pada Sistem Penerbitan PT. X." *Jurnal Informasi, Sains Dan Teknologi* 7 (2): 154–67.
- Atmojo, Sukma Arta, and Augie David Manuputty. 2020. "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office." *Jurnal Teknik Informatika Dan Sistem Informasi* 7 (3): 546–58.
- Bima Mahardika, Krisdana, Agustinus Fritz Wijaya, Ariya Dwika Cahyono, Program Studi, Sistem Informasi, Teknologi Informasi, Universitas Kristen, and Satya Wacana. 2019. "Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000:2018 (Studi Kasus: CV. XY)." *Sebatik* 23 (1): 277–84.
- Desy Ria, Marinda, and Arief Budiman. 2021. "PERANCANGAN SISTEM INFORMASI TATA KELOLA TEKNOLOGI INFORMASI PERPUSTAKAAN." *Jurnal Informatika Dan Rekayasa Perangkat Lunak (JATIKA)* 2 (1): 122–33.
- Dylanza, Rey, Alfito De Vaga Mayavanny, and Thomas Andre Pratama. 2024. "Analisis Risiko Penggunaan Aplikasi MyTelu Di Lingkungan Pendidikan Universitas Telkom ." *Jurnal Manajemen Risiko* 5 (1): 1–11.
- Fachrezi, Muhammad Ilham, Ariya Dwika Cahyono, and Penidas Fiodinggo Tanaem. 2021. "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga." *Jurusan Sistem Informasi* 8 (2): 764–73.
- Fahlepi, Ridho, Mona Fronita, Eki Saputra, Muhammad Luthfi Hamzah, Arif Marsal, Suandi Daulay, Universitas Islam Negeri Sultan Syarif Kasim Riau, and Sekolah Tinggi Teknologi Pekanbaru. 2023. "Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000." *Jurnal Sains Komputer & Informatika J-SAKTI*. Vol. 7. Riau.
- Fitriani, Yuni. 2020. "Analisa Pemanfaatan Learning Management System (LMS) Sebagai Media Pembelajaran Online Selama Pandemi Covid-19." *Journal of Information System, Informatics and Computing* 4 (2): 1–8.

- Haryani, Endang. 2024. "Penerapan ISO 31000:2018 Untuk Analisis Manajemen Risiko Pada Sistem Informasi Smart Operation Di PT. XYZ." *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)* 9 (2): 947.
- Lionel, Eric, Leonard, Nico Fernando, Toni Ong, and Vikhri Septama. 2023. "Analisis Manajemen Risiko Pada Malaya Cafe." *CEMERLANG : Jurnal Manajemen Dan Ekonomi Bisnis* 3 (1): 251–66.
- Mawarsih, Putri Beny, Erika Kurniawati, and Darni. 2024. "Perancangan Aplikasi Sevima Edlink Sebagai Media Evaluasi Sumatif Di SMK." *Jurnal Kajian, Penelitian Dan Pengembangan Kependidikan* 15 (3): 369–75.
- Nurhadi, Erik, Endang Chumaidiyah, and Luciana Andrawina. 2023. "Penilaian Risiko Eksternal (Market Dan Lingkungan) Berdasarkan Kerangka ISO 31000: 2018 Yang Terintegrasi ISO 9001: 2015." *Jurnal INTECH Teknik Industri Universitas Serang Raya* 9 (1): 22–32.
- Risnaeni, Umi Suswati, Muhammad Baharudin Rois, and Shinta Nuriah Ramadhani. 2019. "Efektivitas Manajemen Risiko Dan Hasil ." *Jurnal Akuntansi Dan Keuangan Islam* 1 (2): 1–12.
- Sulistiani, Heni, and Dedi Darwis. 2020. "Penerapan Metode Agile Untuk Pengembangan Online Analytical Processing (OLAP) Pada Data Penjualan (Studi Kasus: CV Adilia Lestari)." *Jurnal CoreIT* 6 (1).
- Thenu, Prilly Peshaulia, Agustinus Fritz Wijaya, Christ Rudianto, Universitas Kristen, and Satya Wacana. 2020. "Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 (Studi Kasus PT Global Infotech)." *Jurnal Bina Komputer JBK*. Vol. 2. Salatiga.