Analisis Risiko Penggunaan Aplikasi MyTelu Di Lingkungan Pendidikan Universitas Telkom

Rey Dylanza[1], Alfito De Vaga Mayavanny[2], Thomas Andre Pratama[3]

Abstrak

Studi ini menganalisis risiko penggunaan aplikasi MyTelu di lingkungan pendidikan Universitas Telkom dengan menggunakan metode FMEA berdasarkan framework ISO 27001 tahun 2022. Identifikasi aset kritis, ancaman, dan risiko dilakukan melalui kuis kepada pengguna aplikasi. Penilaian risiko mengacu pada tingkat keparahan, kemungkinan terjadinya, dan kemampuan deteksi, yang dihitung menjadi Risk Priority Number (RPN). Hasil perhitungan RPN menunjukkan terdapat enam risiko yang berkategori high risk, dengan nilai RPN tertinggi adalah 560 yang terkait kegagalan switch core. Mitigasi risiko yang diperlukan meliputi penyediaan redundansi, peningkatan keamanan akses, dan penerapan prosedur manajemen perubahan yang ketat. Dengan implementasi langkah-langkah mitigasi yang tepat, risiko-risiko tersebut dapat dikelola secara efektif, memastikan keberlangsungan operasional dan keamanan aplikasi MyTelu bagi pengguna di lingkungan Universitas Telkom.

Kata kunci: Analisis Risiko, Aplikasi MyTelu, Universitas Telkom

PENDAHULUAN

Dalam era digital yang semakin maju, pemanfaatan aplikasi di bidang pendidikan menjadi suatu kebutuhan yang tak terhindarkan. Dalam beberapa tahun terakhir, aplikasi telah secara signifikan mengubah cara kerja institusi pendidikan. Aplikasi ini tidak hanya mempermudah akses informasi dan meningkatkan efisiensi komunikasi, tetapi juga mengubah cara pembelajaran dan manajemen administrasi di berbagai tingkat pendidikan, mulai dari sekolah dasar hingga perguruan tinggi (Maritsa, 2021).

Di tingkat pendidikan tinggi, khususnya, aplikasi digunakan untuk berbagai tujuan seperti pengelolaan jadwal perkuliahan, pengumpulan tugas, komunikasi antara dosen dan mahasiswa, serta manajemen administrasi seperti registrasi mata kuliah dan pembayaran biaya pendidikan (Anyan, 2024). Penggunaan aplikasi ini mempercepat proses kerja, meningkatkan partisipasi mahasiswa, dan memberikan fleksibilitas yang lebih besar dalam menyampaikan materi pendidikan.

Sebagai salah satu institusi pendidikan terkemuka di bidang teknologi informasi dan komunikasi di Indonesia, Universitas Telkom telah maju dalam menerapkan teknologi tersebut dalam kegiatan akademik dan administratifnya. Untuk meningkatkan efisiensi dan kualitas layanan pendidikan, Universitas Telkom memperkenalkan aplikasi MyTelu sebagai platform terpadu yang dirancang untuk memenuhi berbagai kebutuhan internal (Hanifan 2021).

MyTelu lebih dari sekadar aplikasi biasa. Ini adalah hasil dari perencanaan dan pengembangan yang cermat, disesuaikan dengan kebutuhan spesifik Universitas Telkom. Melalui fitur-fitur yang ditawarkan, MyTelu memungkinkan mahasiswa, dosen, dan staf administrasi untuk dengan mudah mengakses informasi akademik dan administratif, berkomunikasi secara efisien, dan mengelola tugas mereka dengan lebih terstruktur (Hanifan 2021).

Namun, meskipun memiliki banyak manfaat, penggunaan MyTelu juga membawa sejumlah risiko yang perlu dipertimbangkan. Risiko-risiko ini termasuk masalah keamanan data dan privasi pengguna, kerentanan terhadap serangan siber, dan kemungkinan kegagalan sistem yang dapat mengganggu operasional universitas.

Oleh karena itu, analisis risiko terhadap penggunaan aplikasi MyTelu di Universitas Telkom sangat penting. Dengan melakukan analisis risiko yang menyeluruh, universitas dapat mengidentifikasi potensi ancaman dan kerentanan yang mungkin terjadi, serta mengambil langkah-langkah preventif yang diperlukan untuk mengurangi dampak negatifnya.

Penelitian ini bertujuan untuk mengkaji secara mendalam analisis risiko penggunaan aplikasi MyTelu di lingkungan Universitas Telkom. Tujuannya adalah untuk memberikan wawasan yang berharga bagi para pemangku kepentingan, sehingga implementasi aplikasi ini dapat berjalan dengan lancar dan memberikan manfaat maksimal bagi seluruh civitas akademika.

TINJAUAN PUSTAKA

Risiko

Risiko dapat didefinisikan sebagai kemungkinan terjadinya suatu kejadian atau situasi yang tidak diharapkan akan terjadi yang dapat menyebabkan kegagalan. Konsep ini membahas kemungkinan hasil tindakan tertentu yang dapat terjadi saat ini atau di masa depan apakah berdampak menguntungkan atau tidak. Karakteristik dari risiko sendiri adalah ketidakpastian dan mengandung unsur kerugian. (Stamatis, 2019).

Manajemen Risiko

Manajemen risiko dalam manajemen teknologi informasi adalah proses yang membantu mengelola biaya operasional dan ekonomi yang terkait dengan sistem TI. Manajemen risiko melibatkan penilaian risiko dan analisis sistematis terhadap potensi risiko yang dapat berdampak pada profitabilitas bisnis atau organisasi (Atmojo, 2020).

Tujuan manajemen risiko adalah untuk meningkatkan kinerja, mendorong inovasi, dan mendukung pencapaian tujuan perusahaan. Manajemen risiko membentuk landasan untuk mengelola risiko, dan prinsip-prinsip ini harus dipertimbangkan saat menetapkan proses dan kerangka kerja manajemen risiko.

Proses Manajemen Risiko

Proses manajemen risiko meliputi berbagai tahapan (Novianti, 2019), yaitu:

1. **Identifikasi Risiko**: Pertama, kita perlu menemukan, mengenali, dan memahami risiko yang dapat mempengaruhi proyek atau hasil proyek. Ada beberapa metode berbeda untuk mengidentifikasi risiko, seperti membuat daftar risiko.
2. **Analisis Risiko**: Setelah kita mengidentifikasi risiko, langkah selanjutnya adalah mencari tahu seberapa besar kemungkinan risiko tersebut terjadi dan apa dampaknya. Hal ini membantu kami memahami sifat dan potensi risiko terhadap tujuan proyek.
3. **Evaluasi atau Pemeringkatan Risiko**: Kami kemudian mengevaluasi atau memberi peringkat risiko berdasarkan seberapa signifikan risiko tersebut. Kami melakukan ini dengan mempertimbangkan seberapa besar kemungkinan hal tersebut terjadi dan apa konsekuensinya. Hal ini membantu kami memutuskan apakah risiko tersebut dapat diterima, dapat dikelola, atau sebaiknya ditolak.
4. **Mitigasi Risiko**: Juga dikenal sebagai rencana respons risiko. Pada tahap ini, kita menilai risiko tertinggi dan mengembangkan rencana untuk mengatasi atau memodifikasi risiko tersebut hingga mencapai tingkat yang dapat diterima. Hal ini mencakup strategi untuk meminimalkan kemungkinan risiko negatif dan memaksimalkan peluang yang ada, serta merumuskan strategi mitigasi risiko, rencana pencegahan, dan rencana darurat.

5. **Pemantauan Risiko**: Tahap ini melibatkan penggunaan daftar risiko proyek untuk mengawasi, melacak, dan meninjau risiko yang ada.

Failure Mode and Effect Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) adalah proses terstruktur yang menggunakan pendekatan top-down untuk mengidentifikasi dan mengevaluasi potensi risiko dalam suatu produk. FMEA dapat dijadikan sebagai *tools* yang berguna untuk menilai tingkat evaluasi kualitas produk serta kemungkinan mode kegagalan dan dampaknya (Kartikasari, 2019). Terdapat 3 variabel utama pembuatan FMEA yaitu:

1. Severity merupakan rating yang menunjukkan seberapa serius dampak yang muncul sebagai akibat dari *potensial failure mode*.
2. Occurance adalah rating yang menunjukkan seberapa sering terjadi kecacatan atau *bug* pada produk.
3. Detection adalah proses kontrol yang menemukan secara khusus sumber utama kegagalan.

Menurut (Stamatis, 2019), langkah-langkah dalam proses FMEA yaitu:

1. Tinjau teknik/prosedurnya.
2. Identifikasi potensi kegagalan teknik yang ditinjau.
3. Menganalisis dampak yang mungkin timbul dari kegagalan ini.
4. Menilai seberapa parah kegagalan yang mungkin terjadi.
5. Identifikasi apa yang dapat menyebabkan kegagalan tersebut.
6. Tentukan seberapa sering kegagalan ini terjadi.
7. Evaluasi pengendalian yang ada untuk mencegah kegagalan ini.
8. Menilai seberapa baik pengendalian dapat mendeteksi atau menghindari kegagalan.
9. Hitung Angka Prioritas Risiko (RPN) dengan mengalikan tingkat keparahan, kejadian, dan deteksi (RPN = S*O*D). Angka ini menunjukkan betapa seriusnya potensi kegagalan.
10. Memberikan rekomendasi untuk memperbaiki kegagalan yang paling serius.
    RPN membantu tim fokus pada kegagalan paling kritis dan memutuskan tindakan pencegahan atau perbaikan.

Keamanan Informasi

Keamanan informasi merupakan upaya perlindungan data dari serangan seperti virus dan peretas, yang menjamin keberlangsungan bisnis, mengurangi risiko bisnis, meningkatkan keuntungan investasi, dan meningkatkan peluang bisnis (Aprianti, 2023). Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu:

1. Confidentiality (kerahasiaan) merupakan aspek yang memastikan bahwa data dan informasi hanya dapat diakses oleh individu yang berwenang dengan tetap menjaga kerahasiaannya.
2. Integrity (Integritas) merupakan aspek untuk memastikan bahwa data tidak diubah tanpa izin, menjaga keakuratan dan integritasnya.
3. Availability (Ketersediaan) merupakan aspek yang memastikan bahwa data dan informasi disediakan sesuai kebutuhan, memungkinkan pengguna yang berwenang untuk mengakses informasi dan alat yang relevan.

ISO 27001

ISO 27001 merupakan standar yang dikeluarkan oleh International Organization for Standardization yang bertujuan untuk membantu perusahaan melindungi keamanan asetnya dengan memberikan rekomendasi pengelolaan sistem manajemen keamanan informasi (ISMS). ISMS adalah pendekatan sistematis yang dirancang untuk mengelola informasi penting dan sensitif perusahaan agar tetap aman. ISO 27001 mencakup klausul yang dapat digunakan untuk memitigasi dan mengendalikan risiko yang teridentifikasi (Anshori, 2019).

METODE

Metode penelitian yang diterapkan adalah metode kualitatif. Pendekatan ini dipilih karena tujuannya adalah untuk memahami pengalaman pengguna. Instrumen penelitian yang digunakan terdiri dari daftar pertanyaan. Sumber data utama yang digunakan adalah pengguna aplikasi MyTelu seperti mahasiswa, dosen, dan karyawan. Namun dalam pengumpulan data, metode yang digunakan adalah survei atau kuesioner. Proses pengumpulan data dilakukan dengan mendistribusikan survei atau kuesioner secara online. Proses analisis data meliputi langkah-langkah seperti pengorganisasian data, pengelompokan data, dan penentuan tindak lanjut.

HASIL DAN PEMBAHASAN

Identifikasi Aset Kritis

Daftar aset kritis yang dimiliki oleh aplikasi MyTelu didapatkan dengan melakukan pengumpulan review dari Google Play Store dan App Store. Berikut merupakan tabel dari hasil identifikasi aset.

Tabel 1.1 Identifikasi Aset Kritis

No.	Kategori	Aset
1	Hardware	Server
2		Switch Core
3		Router
4		UPS
6	Software	Konfigurasi
7		Interface
8		Bug
9	People	Pihak Ketiga
10		Interface
11		Fitur
12	Data/Informasi	Keamanan Data
13		Ketersediaan Informasi

Sumber: hasil olahan penulis

Identifikasi Risiko

Pada tahap identifikasi risiko, dapat dilihat dari dua aspek utama yaitu kemungkinan ancaman serta kerentanan yang dimiliki oleh aplikasi tersebut. Hasil identifikasi risiko dapat dilihat pada tabel berikut.

Tabel 1.2 Identifikasi Risiko

No.	Jenis Risiko	Risiko
1.	Perangkat Keras (Hardware)	1. Kegagalan switch core yang mengarah pada gangguan lalu lintas data. 2. Kegagalan UPS saat terjadi pemadaman listrik. 3. Kegagalan hard drive pada server database. 4. Kegagalan router dalam mencegah akses tidak sah.
2.	Perangkat Lunak (Software)	1. Aplikasi tidak berjalan lancar pada perangkat tertentu. 2. Kehilangan fitur setelah pembaruan aplikasi. 3. Ketidakmampuan aplikasi melakukan scan presensi. 4. Tampilan aplikasi yang kurang menarik atau tidak sesuai preferensi pengguna. 5. Adanya bug dalam aplikasi seperti informasi yang tidak sesuai atau tombol yang hilang.
3.	Data/Informasi	1. Konten yang ditampilkan tidak muncul. 2. Informasi tidak tersampaikan dengan baik. 3. Konten yang ditampilkan dianggap kurang relevan bagi pengguna. 4. Pencurian data di clipboard pengguna. 5. Gagal dalam menerapkan pembaruan keamanan atau perbaikan bug.
4.	Sumber Daya Manusia (People)	1. Akses tidak sah oleh pihak lain. 2. Aplikasi tidak ramah pengguna. 3. Penyalahgunaan fitur Timeline

Sumber: hasil olahan penulis

Penilaian Risiko

Penilaian risiko dilakukan dengan menggunakan metode FMEA (Failure Mode and Effect Analysis) berdasarkan framework ISO 27001 tahun 2022. Dalam penilaian ini, setiap risiko dinilai berdasarkan tiga faktor utama: Severity (tingkat keparahan), Occurrence (kemungkinan terjadinya), dan Detection (kemampuan deteksi). Hasil penilaian ini kemudian digunakan untuk menghitung Risk Priority Number (RPN).

Hasil Perhitungan RPN

Hasil perhitungan RPN memberikan gambaran mengenai prioritas risiko yang perlu segera ditangani. Berikut adalah hasil perhitungan RPN untuk beberapa risiko yang diidentifikasi:

Tabel 1.3 Perhitungan RPN

Rank	Asset	Identifikasi Risiko	Severity	Occurrence	Detection	RPN	Level
1	*Hardware*	Switch core yang bertanggung jawab mengarahkan lalu lintas data antara berbagai bagian jaringan kampus mengalami kegagalan.	8	7	10	560	Very High
2	*Software*	Aplikasi tidak berjalan lancar pada device tertentu	10	10	4	400	Very High
3	*People*	Pihak lain mengakses aplikasi secara tidak sah	8	10	5	400	Very High
4	*People*	Aplikasi tidak ramah pengguna	8	8	5	320	Very High
5	*Software*	Setelah pembaruan aplikasi, fitur untuk melihat nilai hilang atau tidak dapat diakses	10	10	3	300	Very High
6	*People*	Penyalahgunaan fitur Timeline	6	8	5	240	Very High
7	*Hardware*	UPS yang bertanggung jawab untuk memberikan daya cadangan kepada server dan perangkat jaringan kampus gagal berfungsi saat terjadi pemadaman listrik.	10	5	4	200	High
8	*People*	Penyalahgunaan fitur Timeline	10	4	5	200	High
9	*Hardware*	Salah satu hard drive pada server database kampus mengalami kegagalan.	8	6	3	144	High

Rank	Asset	Identifikasi Risiko	Severity	Occurrence	Detection	RPN	Level
10	*Information/ Data*	Konten yang ditampilkan tidak muncul	10	10	1	100	Medium
11	*Software*	Tidak dapat melakukan scan untuk presensi	10	10	1	100	Medium
12	*Software*	Tampilan aplikasi dianggap kurang menarik atau tidak sesuai dengan preferensi pengguna.	8	10	1	80	Low
13	*Information/ Data*	Informasi tidak dapat tersampaikan dengan baik	7	10	1	70	Low
14	*Information/ Data*	Konten yang ditampilkan oleh aplikasi dianggap kurang relevan bagi pengguna	8	8	1	64	Low
15	*Software*	Terdapat berbagai bug dalam aplikasi seperti informasi yang tidak sesuai, tombol yang hilang, dan sering terjadi force close	5	10	1	50	Low
16	*Hardware*	Router yang bertindak sebagai firewall gagal untuk mencegah akses yang tidak sah ke jaringan kampus.	4	9	1	36	Low
17	*Hardware*	kehilangan atau tidak dapat mengakses data pada server	7	5	1	35	Low
18	*People*	Pihak lain mengakses aplikasi secara tidak sah	5	5	1	25	Low

Sumber: hasil olahan penulis

Mitigasi Risiko

Berdasarkan hasil perhitungan RPN, langkah-langkah mitigasi risiko dirancang untuk mengurangi dampak negatif dari risiko yang diidentifikasi. Berikut adalah beberapa tindakan mitigasi yang disarankan:

Tabel 1.4 Tindak Lanjut Risiko

No.	Asset	Identifikasi Risiko	Kontrol	Tindak Lanjut
1	*Hardware*	Switch core yang bertanggung jawab mengarahkan lalu lintas data antara berbagai bagian jaringan kampus mengalami kegagalan.	8.14	Fasilitas pemrosesan informasi memerlukan redundansi untuk menjaga ketersediaan data dan layanan. Ini termasuk backup data, server cadangan, dan jaringan yang toleran terhadap kegagalan.
2	*Software*	Aplikasi tidak berjalan lancar pada device tertentu	8.1	Informasi yang diakses melalui perangkat pengguna harus dilindungi dengan enkripsi, otentikasi multi-faktor, dan kebijakan akses yang ketat untuk mencegah akses tidak sah.
3	*People*	Pihak lain mengakses aplikasi secara tidak sah	8.3	Akses ke informasi dan aset lainnya harus sesuai dengan kebijakan kontrol akses, termasuk otentikasi, izin, dan pengawasan aktif untuk mencegah penyalahgunaan.
4	*People*	Aplikasi tidak ramah pengguna	8.32	Perubahan pada fasilitas pemrosesan informasi harus melewati prosedur manajemen perubahan yang terstruktur, termasuk evaluasi risiko, pengujian, dan persetujuan sebelum implementasi.
5	*Software*	Setelah pembaruan aplikasi, fitur untuk melihat nilai hilang atau tidak dapat diakses	8.31	Lingkungan pengembangan, pengujian, dan produksi harus terisolasi untuk mencegah gangguan dan menyediakan kontrol akses yang ketat.
6	*People*	Penyalahgunaan fitur Timeline	8.16	Jaringan, sistem, dan aplikasi harus dipantau secara terus-menerus untuk mendeteksi aktivitas tidak biasa dan mengambil tindakan sesuai untuk mencegah kejadian keamanan informasi yang berpotensi.
7	*Hardware*	UPS yang bertanggung jawab untuk memberikan daya cadangan kepada server dan perangkat jaringan kampus gagal berfungsi saat terjadi pemadaman listrik.	7.11	Fasilitas pemrosesan informasi harus dilindungi dengan sumber daya cadangan, UPS, dan generator untuk mengatasi kegagalan listrik serta gangguan lainnya.
8	*People*	Penyalahgunaan fitur Timeline	8.16	Jaringan, sistem, dan aplikasi harus dipantau secara terus-menerus untuk mendeteksi aktivitas tidak biasa dan mengambil tindakan sesuai untuk mencegah kejadian keamanan

No.	Asset	Identifikasi Risiko	Kontrol	Tindak Lanjut
				informasi yang berpotensi.
9	*Hardware*	Salah satu hard drive pada server database kampus mengalami kegagalan.	7.10	Media penyimpanan harus dikelola dengan skema klasifikasi yang sesuai sepanjang siklus hidupnya, termasuk keamanan transportasi dan penghapusan sesuai dengan persyaratan organisasi.
10	*Information/ Data*	Konten yang ditampilkan tidak muncul	8.32	Perubahan pada fasilitas pemrosesan informasi harus melewati prosedur manajemen perubahan yang terstruktur, termasuk evaluasi risiko, pengujian, dan persetujuan sebelum implementasi.
11	*Software*	Tidak dapat melakukan scan untuk presensi	8.31	Lingkungan pengembangan, pengujian, dan produksi harus terisolasi untuk mencegah gangguan dan menyediakan kontrol akses yang ketat.
12	*Software*	Tampilan aplikasi dianggap kurang menarik atau tidak sesuai dengan preferensi pengguna.	8.32	Perubahan pada fasilitas pemrosesan informasi harus melewati prosedur manajemen perubahan yang terstruktur, termasuk evaluasi risiko, pengujian, dan persetujuan sebelum implementasi.
13	*Information/ Data*	Informasi tidak dapat tersampaikan dengan baik	5.10	Aturan penggunaan yang dapat diterima dan prosedur penanganan informasi serta aset lainnya harus jelas, didokumentasikan, dan diterapkan secara konsisten.
14	*Information/ Data*	Konten yang ditampilkan oleh aplikasi dianggap kurang relevan bagi pengguna	5.10	Aturan penggunaan yang dapat diterima dan prosedur penanganan informasi serta aset lainnya harus jelas, didokumentasikan, dan diterapkan secara konsisten.
15	*Software*	Terdapat berbagai bug dalam aplikasi seperti informasi yang tidak sesuai, tombol yang hilang, dan sering terjadi force close	8.31	Lingkungan pengembangan, pengujian, dan produksi harus terisolasi untuk mencegah gangguan dan menyediakan kontrol akses yang ketat.
16	*Hardware*	Router yang bertindak sebagai firewall gagal untuk mencegah akses yang tidak sah ke jaringan kampus.	8.2	Penetapan dan penggunaan hak akses istimewa harus terbatas kepada personel yang memerlukannya, dengan pengawasan ketat dan audit yang teratur.
17	*Hardware*	kehilangan atau tidak dapat mengakses data pada server	5.29	Organisasi harus memiliki rencana darurat untuk menjaga keamanan informasi selama gangguan, termasuk pemulihan sistem,

No.	Asset	Identifikasi Risiko	Kontrol	Tindak Lanjut
				pemantauan, dan komunikasi yang efektif.
18	*People*	Pihak lain mengakses aplikasi secara tidak sah	8.3	Akses ke informasi dan aset lainnya harus sesuai dengan kebijakan kontrol akses, termasuk otentikasi, izin, dan pengawasan aktif untuk mencegah penyalahgunaan.

Sumber: hasil olahan penulis

KESIMPULAN

Dalam penggunaan aplikasi MyTelu di lingkungan Universitas Telkom, risiko-risiko telah diidentifikasi melalui metode FMEA dengan framework ISO 27001 tahun 2022. Ancaman terhadap aset kritis meliputi gangguan perangkat keras dan perangkat lunak, serta akses tidak sah terhadap data sensitif pengguna. Penilaian risiko dilakukan dengan memperhitungkan tingkat keparahan, kemungkinan terjadinya, dan kemampuan deteksi, yang kemudian dihitung menjadi Risk Priority Number (RPN). Hasil perhitungan RPN mengungkapkan terdapat enam risiko yang berkategori high risk, dengan nilai RPN tertinggi adalah 560, terkait kegagalan switch core yang memiliki kategori very high. Risiko-risiko ini memerlukan tindakan mitigasi segera untuk menghindari gangguan layanan yang signifikan, kerentanan terhadap akses tidak sah, dan ketidakpuasan pengguna terhadap fitur aplikasi. Langkah-langkah mitigasi yang diperlukan mencakup penyediaan redundansi dan backup, peningkatan keamanan akses, dan penerapan prosedur manajemen perubahan yang ketat. Dengan mengimplementasikan langkah-langkah mitigasi yang tepat, risiko-risiko yang teridentifikasi dapat dikelola dengan lebih efektif, memastikan keberlangsungan operasional dan keamanan penggunaan aplikasi MyTelu di lingkungan pendidikan Universitas Telkom.

DAFTAR PUSTAKA

Anshori, F. A., Suprapto, & Reza Perdanakusuma, A. (2019). "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)." Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 3(2), 1701–1707.

Anyan, A. (2024). "PENGEMBANGAN APLIKASI MOBILE UNTUK MEMFASILITASI KOLABORASI GURU DAN SISWA DALAM PROSES PEMBELAJARAN." Jurnal Review Pendidikan dan Pengajaran (JRPP), 7(2), 3709–3716. doi: 10.31004/jrpp.v7i2.26710.

Aprianti, S., Sari, R. P., & Rusi, I. (2023). "Manajemen Risiko Keamanan Simbada Menggunakan Metode NIST SP 800-30 Revisi 1 dan Kontrol ISO/IEC 27001:2013." Jurnal Buana Informatika, 14(1), 50–59.

Atmojo, S. A., & Manuputty, A. D. (2020). "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office." Jurnal Teknik Informatika dan Sistem Informasi, 7(3), 546–558.

Kartikasari, V., & Romadhon, H. (2019). "Analisa Pengendalian dan Perbaikan Kualitas Proses Pengalengan Ikan Tuna Menggunakan Metode Failure Mode And Effect Analysis (FMEA) dan Fault Tree Analysis (FTA) Studi kasus di PT XXX Jawa Timur." Journal of Industrial View, 1(1), 1–10.

Maritsa, A., Hanifah Salsabila, U., Wafiq, M., Rahma Anindya, P., & Azhar Ma'shum, M. (2021). "Pengaruh Teknologi Dalam Dunia Pendidikan." Al-Mutharahah: Jurnal Penelitian dan Kajian Sosial Keagamaan, 18(2), 91–100. doi: 10.46781/al-mutharahah.v18i2.303.

Nurul Haq, H., Hasbi, M. F., & Maulid, H. (2021). My TelU: Aplikasi mobile untuk civitas akademia Telkom University berbasis Flutter. eProceedings of Applied Science, 7(5).

Novianti, D. (2019). "PENGEMBANGAN KERANGKA MANAJEMEN RISIKO PADA PERBANKAN SYARIAH." Asy Syar'iyyah: Jurnal Ilmu Syari'ah dan Perbankan Islam, 4(1), 46–67.

Pangestuti, D. C., Nastiti, H., & Husniaty, R. (2022). "Analisis Risiko Operasional Dengan Metode FMEA." Jurnal Akuntansi, Ekonomi dan Manajemen Bisnis, 10(2), 177–186.

Stamatis, D.H. Risk Management Using Failure Mode and Effect Analysis (FMEA). Google Books. Accessed January 30, 2019. https://books.google.com/books?hl=en&lr=&id=h-mPDwAAQBAJ&oi=fnd&pg=PT2&dq=risk+operational+fmea&ots=0mFX_cPHJp&sig=j0quh_TfWjQGkym3W4R3Ds7B_fI