Reslaj: Religion Education Social Laa Roiba Journal

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

Analisis Manajemen Risiko Aplikasi *Customer Operational Center* (COC) dengan Menggunakan Metode Nist Sp 800-30: Studi Kasus Pt.Telkom Jakarta Barat

Eva, Badie Uddin
Ilmu Komputer, Sistem Informasi, Universitas Esa Unggul
evhapuspitasari286@gmail.com, badie.uddin@esaunggul.ac.id

ABSTRACT

The Customer Operational Center (COC) information system at PT Telkom has a strategic role in supporting customer service operations, especially in the West Jakarta area. However, the existence of risks that can affect the performance of thisapplication is a challenge that must be managed properly. This research aims to analyze risk management in COC applications using the NIST SP 800-30 approach, a widely recognized method for information technology risk assessment. The research methodology includes asset identification, threats, vulnerabilities, and impact analysis on COC applications. Data was collected through interviews with the operational team, document review, and direct observation of the application work process. The analysis results show several main risks, including disruption to data integrity, the threat of cyber attacks, and the potential for application downtime that could disrupt customer service. Risk mitigation strategies are proposed based on the evaluation results, including implementation of technical controls, information security policies, and increased user awareness. Using the NIST SP 800-30 approach, this research provides systematic insights to increase the resilience of COC applications to risk, as well as supporting operational sustainability and customer service at PT Telkom West Jakarta. It is hoped that these findings can be a practical guide for companies in managing information technology risks on similar platforms.

Keywords: *Risk Analysis, NIST SP 800-30, Customer Operational Center (COC) Applications, Information Security.*

ABSTRAK

Sistem informasi *Customer Operational Center* (COC) di PT Telkom memiliki peran strategis dalam mendukung operasional layanan pelanggan, khususnya di wilayah Jakarta Barat. Namun, keberadaan risiko yang dapat memengaruhi kinerja aplikasi ini menjadi tantangan yang harus dikelola dengan baik. Penelitian ini bertujuan untuk menganalisis manajemen risiko pada aplikasi COC dengan menggunakan pendekatan NIST SP 800-30, sebuah metode yang diakui secara luas untuk penilaian risiko teknologi informasi. Metodologi penelitian meliputi identifikasi aset, ancaman, kerentanan, dan analisis dampak terhadap aplikasi COC. Data dikumpulkan melalui wawancara dengan tim operasional, tinjauan dokumen, serta observasi langsung pada proses kerja aplikasi. Hasil analisis menunjukkan beberapa risiko utama, termasuk gangguan pada integritas data, ancaman serangan siber, dan potensi *downtime* aplikasi yang dapat mengganggu layanan pelanggan. Strategi mitigasi risiko diusulkan berdasarkan hasil evaluasi, termasuk penerapan kontrol teknis, kebijakan keamanan informasi, dan peningkatan kesadaran pengguna. Dengan pendekatan NIST SP 800-30, penelitian ini memberikan wawasan sistematis untuk meningkatkan ketahanan aplikasi

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

COC terhadap risiko, serta mendukung keberlanjutan operasional dan pelayanan pelanggan PT Telkom Jakarta Barat. Temuan ini diharapkan dapat menjadi panduan praktis bagi perusahaan dalam mengelola risiko teknologi informasi pada platform serupa.

Kata kunci: Analisis Risiko, NIST SP 800-30, Aplikasi *Customer Operational Center* (COC), Keamanan Informasi.

PENDAHULUAN

Dalam kondisi persaingan yang cukup ketat antar penyedia jasa layanan telekomunikasi, perusahaan dituntut untuk meningkatkan kualitas layanan dan produk yang dihasilkan. Dengan semakin banyaknya pilihan di pasar, konsumen mempunyai kemampuan daya tawar yang lebih tinggi dalam memilih produk sesuai dengan kebutuhannya. Peta persaingan industri telekomunikasi di Indonesia in semakin ketat, selain terjadi persaingan diantara perusahaan telekomunikasi lokal juga diramaikan dengan semakin banyaknya perusahaan-perusahaan telekomunikasi asing yang masuk ke Indonesia, dimana secara umum area persaingan dilakukan dengan beragamnya fasilitas bonus, tarif murah, dan diferensiasi produk yang ditawarkan. Sejalan dengan keharusan untuk mengikuti peraturan dari pasar modal, PT Telkom Indonesia Tbk sebagai perusahaan publik (terbuka) harus mampu untuk melakukan pengelolaan bisnis perusahaan melalui praktek-praktek terbaik, yang dikenal dengan istilah *Good Corporate Governance* (GCG), dengan mengoptimalisasikan sumber daya manusia yang unggul, penggunaan teknologi yang kompetitif, dan membangun kemitraan yang saling menguntungkan dan mendukung secara sinergis (Yessika Nababan, A dkk.,2022).

Teknologi informasi, yang kian berkembang dengan cepat, dapat memiliki efek yang luar biasa dan dapat mengubah kinerja menjadi lebih efisien dan efektif. Dengan Sistem Informasi berbasis web, mereka dapat membantu orang mendapatkan informasi. Namun, penting untuk diingat bahwa risiko yang dapat terjadi di internet selalu ada. Kadang-kadang, risiko dapat dihindari, ditangani, atau diterima. Risiko—Risiko memiliki dampak yang berbeda satu sama lain. Mengendalikan risiko pada sistem informasi bertujuan terutama dapat membantu proses bisnis perusahaan menjadi lebih baik dan membuat perusahaan lebih kompetitif.

Risiko adalah situasi yang tidak menyenangkan yang menghasilkan kerugian atau kerusakan. Suatu kejadian adalah ketika seseorang melakukan sesuatu yang merugikan sehingga menimbulkan ancaman yang dapat membahayakan seseorang atau kelompok. Ancaman tidak dapat diprediksi oleh suatu perusahaan karena mereka dapat muncul kapan saja. Ancaman memiliki berbagai tingkat, dengan tingkat tertinggi, sedang, dan terendah.

Sumber daya manusia biasanya menjadi kurang produktif karena dampak buruk yang terjadi di perusahaan. Perusahaan harus berusaha menerapkan manajemen risiko untuk meminimalkan risiko dan mengurangi dampak negatifnya.

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

Manajemen risiko adalah cara untuk mengelola ancaman yang mungkin berdampak negatif pada perusahaan. Namun, risiko yang akan dihadapi perusahaan tidak selalu menimbulkan dampak negatif, tetapi kadang-kadang menimbulkan dampak positif. Akibatnya, dampak yang baik atau buruk yang akan diterima oleh perusahaan bergantung pada bagaimana perusahaan mengelola ketidakpastian. Ketidakpastian ini adalah peristiwa yang belum terjadi, sehingga dapat dianggap baik atau buruk. Namun, jika risiko diambil dengan cara yang tepat, ketidakpastian ini akan menguntungkan perusahaan. Namun jika perusahaan tidak melakukan risiko dengan dilakukannya pengelolan yang kurang baik, maka ketidakpastian tersebut nantinya akan menjadi sesuatu ancaman yang memberikan efek kerugian. Menurut buku yang ditulis oleh Ida Ayu Made Sasmita Dewi berjudul Manajemen risiko, manajemen risiko adalah bidangilmu yangmembahas bagaimana suatu organisasi menerapkan ukuran dalam memetakan berbagai masalah yang ada dengan menerapkan berbagai pendekatan manajemen secara sistematis dan menyeluruh (Dewi, 2019).

PT Telkom Indonesia (Persero) Tbk adalah Badan usaha Milik Negara (BUMN) yang bergerak dibidang penyedia jasa layanan telekomunikasi yang mana menerapkan teknologi telekomunikasi digital pada perangkat sistem telekomunkasi yangdimilikinya. PT. Telkom sendiri memilikibeberapaanak perusahaan yangsalah satunyaPT. Telekomunikasi Seluler (Telkomsel), merupakan perusahaan operator layanan telepon selulerterbesar di Indonesia. PT. Telkom sendiri menyediakan berbagai macam layanan telekomunikasi lainnya, diantaranya interkoneksi, jaringan, data, internet dan layanan terkait lainnya. Tujuannya adalah untuk memberikan layanan jaringan telekomunikasi yang baik. Hasil wawancara yang dilakukan Pada PT. Telkom Jakarta Barat terdapat unit *Fixed Broadband Access & serviceOperation* (FBB ASO) yangmenggunakan sistem informasi *Customer Operational Center* (COC) dimana sistem informasi tersebut digunakan untuk mengetahui suatu kendala atau permintaan oleh staff atau teknisi lapangan. COC juga mempunyai kendala yaitu tidak adanya notifikasi atau pemberitahuan saat permintaan kendala masuk, perusahaan juga sering mengalami insiden pemadaman listrik sehingga terhambatnya pekerjaan pada aplikasi COC yang tidak dapat beroperasi dengan baik.

Dalam melakukan kegiatan operasionalnya, PT Telkom menghadapi banyak sekali risiko-risiko yang akan menggangu, baik itu risiko internal maupun risiko eksternal. Hal ini dikarenakan PT Telkom merupakan perseroan terbatas yang berkedudukan di Indonesia yang sebagian besar operasi, asset dan pelangganya berada di Indonesia. Akibatnya kondisi politik, ekonomi, hokum, dan social di Indonesia dimasa mendatang, serta tindakan dan kebijakan tertentu yang diambil atau tidak ambil oleh Pemerintah secara material dapat berdampak negatif terhadap suatu usaha, kondisi keuangan dan hasil operasi PT Telkom. Risiko Operasional menurut PT Telkom adalah risiko-risiko yang terdapat dalam kegiatan operasional sehari-hari perusahaan yang baik secara langsung maupun tidak langsung muncul dari ketidakcukupan atau kegagalan proses internal, orang, dan system atau dari

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

kejadian di luar kendali perusahaan, termasuk bencana alam.

Metode Analisis manajemen risiko ini NIST (National Institute of Standard and Technology) SP (Publikasi Khusus) 800-30 adalah pedoman pada manajemen risiko sistem TI yang di standarisasi oleh pemerintah pusat Amerika Serikat. Desain metodologi ini didasarkan pada analisis keamanan untuk benar-benar mengidentifikasi, menilai, dan mengelola risiko pada sistem teknologi informasi. Proses ini sangat menyeluruh, yaitu mencakup semua hal mulai dari ancaman hingga penilaian berkelanjutan dan identifikasi sumber penilaian (Juliasari, Y., & Zulfikar, D. H. (n.d.)., 2022). Kerangka kerja NIST SP 800-30 menganalisis manajemen risiko pada tingkat praktik manajemen dalam kaitannya dengan model proses analitis sejalan dengan siklus hidup pengembangan sistem. Ini dirancang untuk digunakan menilai risiko dalam aktivitas manajemen risiko sistem informasi karena tujuan utamanya adalah membantu perusahaan dalam melakukan pengelolaan risiko, sehingga perusahaan mendapatkan value yang lebih baik lagi (Murniati & Nurhayati Awza, 2021).

Pada penelitian ini, peneliti memutuskan untuk menganalisis manajemen risiko sistem informasi padaPT.Telkom dengan menganalisissemua risiko yangakan datang. Hasilpada penelitian analisis ini sebagai acuan kejadian yang sudah terjadi maupun yang belum terjadi, sehingga dapat mewaspadai jika terjadi serangan dan membuat rekomendasi dengan tujuan untuk meminimalisir risiko yang mungkin terjadi dengan cara penilaian risiko dan evaluasi risiko.

Berdasarkan penjelasan di atas penulis melakukan penelitian mengenai " Analisis Manajemen Risiko Aplikasi *Customer Operational Center* (COC) dengan Menggunakan Metode NIST SP 800-30 (Studi Kasus : PT. Telkom Indonesia Jakarta Barat)".

METODE PENELITIAN

Teknik Pengumpulan data merupakan kegiatan yang bertujuan untuk mengumpulkan informasi yang diperlukan untuk mengatasi permasalahan penelitian. Untuk memperoleh data yang berkualitas, penting untuk menggunakan alat pengumpulan data yang valid dan memenuhi standar tertentu dalam perolehan data.

Observasi merupakan suatu kegiatan sistematis yang dilakukan untuk mengamati, memperhatikan, dan mencatat data mengenai objek, fenomena, atau situasi tertentu. Tujuan observasi dapat bervariasi, mulai dari penelitian ilmiah hingga evaluasi kinerja.

Observasi dapat dilakukan dengan cara pengamatan langsung terhadap objek atau kejadian mengenai apa saja yang ada pada sistem informasi COC.

Wawancara merupakan suatu bentuk interaksi verbal anatra dua atau lebih

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

orang, di mana satu pihak (pewawancara) bertanya dan pihak lainnya (responden) memberikan jawaban. Tujuan wawancara bisa bermacam-macam, seperti pengumpulan informasi, penelitian, seleksi pekerjaan, atau evaluasi. Wawancara dapat dilakukan dalam berbagai konteks dan memiliki berbagai metode, termasuk wawancara terstruktur, semi-terstruktur, atau tidak terstruktur.

Wawancara ini dilakukan untuk mencari sebuah informasi dengan cara melakukan sesi tanya jawab secara langsung kepada manajer unit FBB ASO dan pegawai yang bertanggung jawab atas aplikasi COC. Hasil wawancara tersebut ada pada lampiran 3 dan 4.

Studi pustaka meliputi kegiatan sistematis untuk memahami, menganalisis, dan menyajikan informasi yang telah dikumpulkan dari sumber-sumber tertulis yang relevan dengan suatu topik atau bidang penelitian. Ini melibatkan tinjauan dan sintesis literature yang telah ada, seperti buku, artikel jurnal, laporan penelitian, dan sumber-sumber lainnya. Studi pustaka membantu peneliti untuk memahami perkembangan pengetahuan, dan menempatkan penelitian mereka dalam konteks yang lebih luas.

HASIL DAN PEMBAHASAN

Karakteristik Sistem (*System Characterization*)

Pada tahap ini menentukan karakteristik sistem yang berisikan aset terkait dengan sistem informasi aplikasi COC pada unit FBB ASO. Hal yang paling penting dalam melakukan karakteristik sistem adalah mengidentifikasi aset yang berhubungan dengan sistem informasi aplikasi COC itu sendiri. Dalam karakteristik sistem ini masing-masing memiliki setiap aset yang dapat di akses oleh *stakeholder*, salah satunya ialah stakeholder FBB ASO yang bertugas dalam melakukan pengawasan dan pengecekan terhadap aplikasi COC serta juga berperan penting dalam menjaga ruang server dan jaringan router agar proses penginputan dapat berjalan dengan lancer. Berikut ini aset yang telah ditemukan oleh peneliti dengan melakukan observasi dan wawancara ke unit *Fixed Broadband Accses & Service Operation* (FBB ASO).

Tabel 1. Daftar Karakterisasi Sistem

Jenis Aset	Nama Aset	Deskripsi Aset	Stakeholder
Hardware	Komputer / PC	Windows	FBB ASO
	Server	Processor 4 core dengan RAM 60 GB	

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

	Router	Router bertugas menghubungkan dua atau lebih jaringan, seperti jaringan area lokal (LAN) ke jaringan yang lebih luas (WAN) atau ke internet. Dengan router, perangkat yang terhubung ke jaringan yang berbeda dapat berkomunikasi satu sama lain.	

Software	Server	OS Linux	FBB ASO
Data dan Informasi	Data Request	Informasi yang berada didalam Sistem infromasi Aplikasi COC dan merupakan sebuah data penting bagi aplikasi COC itu sendiri	FBB ASO
	Data Pelanggan		
	Data Koneksi dan Layanan		
	Data Pemantauan Real Time		
SDM / Karyawan	Manager	Pengguna yang memiliki wewenang dalam mengakses website sistem informasi aplikasi COC sesuai dengan level hak aksesnya	Manager, FBBASO
	Unit FBB ASO		

Reslaj: Religion Education Social Laa Roiba Journal
Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

Infrastruktur	Listrik	Listrik merupakan salah satu sumber energi yang sangat penting yang berperan untuk menghidupkan atau menjalankan sebuah aset pada perangkat lunak	Seluruh *Stakeholder*

Identifikasi Ancaman (*Threat Identification*)

Identifikasi ancaman yaitu melakukan identifikasi dengan mencari sumber ancaman serta melakukan analisa ancaman yang terkait dengan aplikasi *Customer Operational Center* (COC). Identifikasi ancaman ini dilakukan dengan menyesuaikan aset yang dimiliki, dampak ancaman dibuat dengan menyesuaikan fokus penelitian, yakni COC. Tujuan dari tahap ini

mengidentifikasi sumber ancaman yang berpotensi menimbulkan kerusakan serta menggangu fungsi dari proses aplikasi COC. Berikut daftar ancaman yang telah disusun oleh penulis:

Tabel 2. Identifikasi Ancaman

Jenis Asset	Peristiwa Ancaman	Sumber Ancaman	Keterangan Ancaman
Hardware	Komputer mati	*Eksternal*	Proses *backup* dan penginputan data mengalami kegagalan
	Jaringan internet mati	*Eksternal*	Kegagalan perlengkapan TI (Jaringan)
	AC diruang data center mati	*Internal*	Kehilangan data
	Pemadaman listrik secara berkala	*Eksternal*	Proses *backup* dan penginputan data mengalami kegagalan
	Kebakaran	*Internal*	Kerusakan pada infastruktur penyimpanan dan data *input*

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

Software	Serangan DDos	*Eksternal*	*Server* mengalami *down*
	Sharing password	*Eksternal*	Penyalahgunaan hak akses
Data dan informasi	Data *lost*	*Internal*	Data yang telah tersimpan mendadak hilang
	Gagalnya sinkronisasi data karena jaringan terputus	*Eksternal*	Penginputan data mengalami kegagalan karena sistem membutuhkan jaringan yang stabil
Sumber daya manusia	Lupa dalam mengganti password	Personal (pegawai	Akun dapat di akses oleh orang yang tidak memiliki hak dalam
		Divisi FBB ASO)	Mengakses aplikasi website COC
	Kelalaian penanganan data dan informasi	Personal (pegawai divisi FBB ASO)	Terhambatnya input data dikarenakan sistem informasi tersebut tidak memberikan notifikasi jika ada *request* masuk, Sehingga menyebabkan user tidak update dan data tercancel secara otomatis

Sumberancaman padaidentifikasi ancaman dibagi menjadi 2 jenis ancaman yaitu *Adversarial* dan *Non-Adversarial*. *Adversarial* merupakan peristiwa yang ditargetkan pada eksploitasi kerentanan yang disengaja sedangkan *Non-Adversarial* merupakan peristiwa yang mungkin secara tidak sengaja memicu kerentanan (*Joint Task Force Transformation Initiative*, 2012). Tabel 3 merupakan daftar kejadian ancaman yang telah diidentifikasi menurut jenis ancamannya.

Reslaj: Religion Education Social Laa Roiba Journal
Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

Tabel 3. Daftar Kejadian Ancaman Berdasarkan Jenis Ancaman

Peristiwa Ancaman	Sumber Ancaman	Jenis Ancaman	Kemungkinan Terjadinya Ancaman
Komputer mati	Kegagalan perlengkapan TI (Hardware pada server)	Non-Adversarial	*Medium*
Jaringan internet mati	Kegagalan Perlengkapan TI (Jaringan)	Non-Adversarial	*Medium*
AC diruang data center mati	Kegagalan Perlengkapan TI (Hardaware pada server)	Non-Adversarial	*Medium*
Pemadaman listrik secara berkala	Individu diluar organsasi	Adversarial	*Medium*
Kebakaran	Bencana alam	Non-adversarial	*Medium*
Serangan DDos	Individu diluar organisasi	Adversarial	*Medium*
Sharing password	Individu didalam organisasi (pegawai)	Adversarial	*Medium*
Data lost	Individu didalam atau diluar organisasi	Non-Adversarial	*High*
Gagalnya sinkronisasi data karena jaringan terputus	Kegagalan perlengkapan IT (jaringan)	Non-Adversarial	*Medium*

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

Lupa dalam mengganti password	*Previleged user* (pegawai)	Non-Adversarial	*Medium*
Kelalaian penanganan data dan informasi	Individu didalam organisasi (pegawai)	Non-Adversarial	*Low*

Berdasarkan Tabel 3 yang telah dilakukan identifikasi tingkatan ancaman yang dapat terjadi pada COC oleh pihak pegawai dan umum yaitu sebanyak 1 tingkatan *High*, 9 tingkatan *Medium* dan 1 tingkatan *Low*.

KESIMPULAN

Dari penelitian yang telah dilakukan pada COC diketahui bahwa COC belum melakukan manajamen risiko dan terdapat beberapa permasalahan selama sistem beroperasi. Oleh karena itu, untuk menghindari adanya permasalahan yang dapat memberikan kerugian yang lebih besar bagi organisasi maka dilakukan analisis manajemen risiko pada aplikasi COC. Penilaian risiko dilakukan dengan melakukan identifikasi aset TI pada COC untuk mengetahui kekritisan aset, melakukan identifikasi ancaman, melakukan identifikasi kerentanan sistem, analisis control yang sudah diterapkan, penentuan kemungkinan, analisis dampak dan penentuan risiko. Setelah dilakukan analisis sesuai tahapan NIST SP 800-30 diketahui bahwaCOC memiliki risiko dengan tingkatan *Medium* sebanyak 9 risiko dan risiko dengan tingkatan *Low* sebanyak 2 risiko.

Penyusunan rekomendasi kontrol dari risiko-risiko yang ditemukan dikelompokkan sesuai dengan tingkatan risiko dan penyusunan rekomendasi kontrol ini berdasarkan pada NIST SP 800-53 Rev 5. Rekomendasi kontrol yang digunakan untuk risiko tingkatan *Medium* sebanyak 9 kelompok sedangkan rekomendasi kontrol yang digunakan untuk risiko tingkatan *Low* sebanyak 2 kelompok.

DAFTAR PUSTAKA

Danial, & Wasriah. (2009). *Metode penulisan karya ilmiah*. Bandung: Laboratorium Pendidikan Kewarganegaraan UPI.

Dewi, I. A. M. S. (2019). *[Judul buku tidak disebutkan]*. Unhi Press.

Djojosoeharso, S. (2009). *Prinsip-prinsip manajemen risiko dan asuransi*. Jakarta: Salemba Empat.

Elky, S. (2007). *An introduction to information system risk management*. SANS Institute.

Fahmi, I. (2010). *Manajemen risiko: Teori, kasus dan solusi*. Bandung: Alfabeta.

Volume 7 Nomor 7 (2025) 1976 – 1986 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v7i7.8091

Galorath, D. (2006). Risk management success factor. *PM World Today, 8*(12).

Hanafi, M. M. (2009). *Manajemen risiko*. Yogyakarta: UUP STIM YKPN. Juliasari, Y., & Zulfikar, D. H. (2022). Analisis manajemen risiko sistem informasi pendidik dan tenaga kependidikan (SIMPATIKA) menggunakan framework NIST SP 800-30. *[Nama jurnal tidak disebutkan]*.

Jogiyanto. (2005). *Analisa dan perancangan desain sistem informasi*. Jakarta: Cempaka Warna.

Joint Task Force Transformation Initiative. (2011). *Managing information security risk: Organization, mission, and information system view* (NIST Special Publication 800-39).

Murniati, E. E. S., & Nurhayati, R. (2021). Manajemen risiko sistem informasi perpustakaan (Studi kasus di Perpustakaan Universitas Riau). *Jurnal Gema Pustakawan, 9*(2), 100–113.

Nababan, A. Y., Rahmawati, E., Saputra, E. G., Rivanti, F., & Saputra, S. (2022). Analisis financial risk pada PT. Telkom Indonesia Tbk. *YUME: Journal of Management, 5*(3), 285–292. https://doi.org/10.2568/yum.v5i3.1992

Nurochman, A. (2016). Manajemen risiko sistem informasi perpustakaan (Studi kasus di Perpustakaan Universitas Gadjah Mada). *Berkala Ilmu Perpustakaan dan Informasi, 10*(2), 1. https://doi.org/10.22146/bip.8830

Oetomo, B. S. D. (2002). *Perencanaan dan pembangunan sistem informasi*. Yogyakarta: Andi.

Permatasari, D. A., Hayuhardhika, W., Putra, N., & Perdanakusuma, A. R. (2019). Analisis manajemen risiko sistem informasi E-LKPJ pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. *[Nama jurnal tidak disebutkan], 3*(6). http://j-ptiik.ub.ac.id

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology.

Stoneburner, G., Goguen, A., & Feringa, A. (2006). Risk management guide for information technology systems NIST SP 800-30. *Expert Opinion on Therapeutic Targets, 10*(2), 289–302. https://doi.org/10.1517/14728222.10.2.289

Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of risk analysis methods: MEHARI, MAGERIT, NIST800-30 and Microsoft's security management guide. In *International Conference on Availability, Reliability and Security*, Fukuoka.

Tantra, R. (2012). *Manajemen proyek sistem informasi*. Yogyakarta: Andi.