JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8779

ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI SISTEM LAYANAN UPA-PKK UPN "VETERAN" JAWA TIMUR MENGGUNAKAN METODE NIST SP800-30

Putu Anggi Suryantari[1*], Rangga Laksana Aryananda[2], Denisa Septalian Alhamda[3], Anggraini Puspita Sari[4], Dwi Arman Prasetya[5]

[1,2,3)]Prodi Magister Teknologi Informasi Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya, Jawa Timur, Indonesia
[4)]Prodi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya, Jawa Timur, Indonesia [5)]Prodi Sains Data Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya, Jawa Timur, Indonesia

Keywords:
Information Security; Risk Management; NIST SP 800 30; Information System

Corespondent Email:
anggraini.puspita.if@upnjatim.ac.id

Abstrak. Keamanan informasi merupakan aspek penting dalam penerapan sistem layanan berbasis teknologi informasi di lingkungan perguruan tinggi. Sistem layanan UPA PKK UPN Veteran Jawa Timur berperan dalam mendukung kegiatan pengembangan karier dan kewirausahaan mahasiswa serta alumni sehingga memerlukan pengelolaan risiko keamanan informasi yang terstruktur. Penelitian ini bertujuan untuk menganalisis risiko keamanan informasi menggunakan metode NIST SP 800-30. Tahapan penelitian meliputi identifikasi ancaman, identifikasi kerentanan, analisis pengendalian, penilaian tingkat kemungkinan dan dampak, serta penentuan tingkat risiko. Hasil penelitian menunjukkan bahwa risiko keamanan informasi pada sistem layanan UPA PKK berada pada kategori rendah, sedang, hingga tinggi, dengan risiko dominan berada pada tingkat sedang hingga tinggi, terutama pada aspek keamanan akses sistem dan pengelolaan data. Rekomendasi pengendalian difokuskan pada penguatan mekanisme autentikasi, pembaruan sistem secara berkala, serta peningkatan prosedur keamanan. Metode NIST SP 800-30 terbukti memberikan pendekatan yang sistematis dalam pengelolaan risiko keamanan informasi pada sistem layanan UPA PKK.

Abstract. *Information security is a critical aspect in the implementation of information technology–based service systems in higher education institutions. The UPA PKK service system at UPN Veteran Jawa Timur supports career development and entrepreneurship activities for students and alumni, thus requiring structured information security risk management. This study aims to analyze information security risks using the NIST SP 800-30 framework. The research stages include threat identification, vulnerability identification, control analysis, assessment of likelihood and impact, and risk determination. The results indicate that information security risks in the UPA PKK service system are classified into low, moderate, and high categories, with dominant risks falling within the moderate to high levels, particularly related to system access security and data management. Risk control recommendations focus on strengthening authentication mechanisms, implementing regular system updates, and improving security procedures. The NIST SP 800-30 framework provides a systematic approach to identifying and managing information security risks in the UPA PKK service system.*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong perguruan tinggi untuk mengintegrasikan sistem informasi dalam berbagai layanan akademik dan nonakademik [1]. Pemanfaatan sistem informasi tidak hanya berfungsi sebagai sarana pendukung operasional tetapi juga menjadi elemen strategis dalam peningkatan kualitas layanan dan pengambilan keputusan institusional [2]. Dalam konteks tersebut aspek keamanan informasi menjadi faktor penting karena sistem informasi mengelola data yang bersifat sensitif dan bernilai tinggi [3].

UPA-PKK UPN "Veteran" Jawa Timur merupakan unit yang memiliki peran strategis dalam mendukung pengembangan karier dan kewirausahaan mahasiswa serta alumni. Aktivitas layanan yang dijalankan melibatkan pengelolaan data pribadi mahasiswa alumni serta mitra eksternal yang tersimpan dalam sistem informasi berbasis teknologi. Ketergantungan terhadap sistem informasi ini menuntut adanya jaminan terhadap kerahasiaan integritas dan ketersediaan informasi agar layanan dapat berjalan secara berkelanjutan dan terpercaya.

Seiring dengan meningkatnya pemanfaatan teknologi informasi risiko terhadap keamanan informasi juga semakin kompleks [4]. Ancaman dapat berasal dari faktor internal maupun eksternal seperti kesalahan pengguna kelemahan konfigurasi sistem serangan siber serta keterbatasan pengendalian keamanan [5]. Apabila risiko tersebut tidak dikelola dengan baik maka dapat menimbulkan gangguan layanan kebocoran data serta menurunnya kepercayaan sivitas akademika dan pemangku kepentingan terhadap institusi [6].

Manajemen risiko keamanan informasi diperlukan sebagai upaya sistematis untuk mengidentifikasi menganalisis dan mengendalikan risiko yang berpotensi mengganggu keberlangsungan sistem informasi [7]. Salah satu metode yang banyak digunakan dalam penilaian risiko keamanan informasi adalah NIST SP 800 30. Metode ini menyediakan kerangka kerja yang terstruktur dan komprehensif dalam menilai risiko melalui tahapan identifikasi sistem ancaman kerentanan serta penentuan tingkat kemungkinan dan dampak risiko [8].

Berdasarkan uraian tersebut, sistem layanan UPA-PKK UPN "Veteran" Jawa Timur memiliki tingkat ketergantungan yang tinggi terhadap teknologi informasi dalam pengelolaan data layanan karier dan kewirausahaan yang bersifat penting dan sensitif. Kompleksitas ancaman serta potensi kerentanan keamanan informasi yang berasal dari faktor internal maupun eksternal menunjukkan perlunya pengelolaan risiko keamanan informasi yang terstruktur dan sistematis. Oleh karena itu, penelitian ini dilakukan untuk menganalisis manajemen risiko keamanan informasi pada sistem layanan UPA-PKK UPN "Veteran" Jawa Timur menggunakan metode NIST SP 800-30 guna mengidentifikasi tingkat risiko yang ada serta merumuskan rekomendasi pengendalian risiko yang sesuai dengan karakteristik sistem dan kebutuhan organisasi..

2. TINJAUAN PUSTAKA

Sistem Informasi

Sistem informasi merupakan sekumpulan komponen yang saling berinteraksi untuk mengumpulkan mengolah menyimpan dan mendistribusikan informasi guna mendukung proses operasional manajerial dan pengambilan keputusan dalam suatu organisasi [9]. Dalam lingkungan perguruan tinggi sistem informasi digunakan untuk menunjang berbagai layanan akademik dan nonakademik yang melibatkan pengelolaan data dalam jumlah besar dan bersifat dinamis [10]. Keandalan sistem informasi menjadi faktor penting karena berpengaruh langsung terhadap kualitas layanan yang diterima oleh pengguna [11].

Keamanan Informasi

Keamanan informasi adalah upaya untuk melindungi informasi dari berbagai ancaman agar kerahasiaan integritas dan ketersediaan informasi tetap terjaga [12]. Kerahasiaan berkaitan dengan perlindungan informasi agar hanya dapat diakses oleh pihak yang berwenang [13]. Integritas menekankan pada keakuratan dan keutuhan data dari perubahan yang tidak sah [14]. Ketersediaan berkaitan dengan jaminan bahwa informasi dapat diakses saat dibutuhkan. Ketiga aspek tersebut menjadi

dasar dalam pengelolaan keamanan informasi pada sistem informasi organisasi [15].

Risiko dan Manajemen Risiko

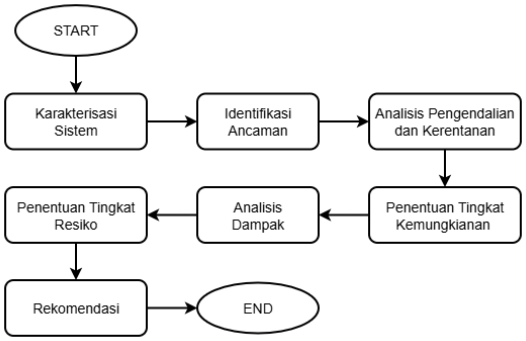
Risiko merupakan potensi terjadinya peristiwa yang dapat menimbulkan dampak negatif terhadap pencapaian tujuan organisasi [16]. Dalam konteks teknologi informasi risiko dapat muncul akibat ancaman yang memanfaatkan kelemahan sistem sehingga menyebabkan gangguan operasional kehilangan data atau kerugian lainnya [17]. Manajemen risiko adalah proses sistematis yang mencakup identifikasi analisis evaluasi dan pengendalian risiko untuk meminimalkan dampak yang mungkin terjadi [18]. Penerapan manajemen risiko memungkinkan organisasi untuk memahami tingkat risiko yang dihadapi serta menentukan langkah pengendalian yang sesuai [19].

Metode NIST SP 800 30

NIST SP 800 30 adalah panduan penilaian risiko keamanan informasi yang dikembangkan oleh *National Institute of Standards and Technology* [20]. Metode ini menyediakan pendekatan yang terstruktur dalam melakukan penilaian risiko melalui tahapan karakterisasi sistem identifikasi ancaman identifikasi kerentanan analisis pengendalian penentuan tingkat kemungkinan analisis dampak penentuan tingkat risiko rekomendasi pengendalian serta dokumentasi hasil [21]. Keunggulan metode ini terletak pada kemampuannya memberikan gambaran risiko secara komprehensif dan mudah dipahami oleh pengambil keputusan sehingga banyak digunakan dalam penilaian risiko sistem informasi di berbagai organisasi [22].

3. METODE PENELITIAN

Metode penelitian ini disusun untuk menganalisis manajemen risiko keamanan informasi pada sistem layanan UPA PKK UPN Veteran Jawa Timur dengan mengacu pada kerangka kerja NIST SP 800-30. Tahapan penelitian dirancang secara sistematis untuk mengidentifikasi risiko, menilai tingkat risiko, serta merumuskan rekomendasi pengendalian yang sesuai. Alur penelitian disajikan dalam bentuk flowchart untuk memberikan gambaran yang jelas mengenai tahapan dan keterkaitan antarproses penelitian.



Gambar 1. Metodologi Penelitian

Berdasarkan Gambar 1 Flowchart Alur Penelitian, tahap penelitian diawali dengan karakterisasi sistem, yaitu mengidentifikasi batasan, komponen utama, aset informasi, serta lingkungan sistem layanan UPA PKK UPN Veteran Jawa Timur. Tahap ini bertujuan untuk memperoleh pemahaman menyeluruh mengenai sistem yang menjadi objek penelitian sebagai dasar dalam proses analisis risiko selanjutnya.

Tahap berikutnya adalah identifikasi ancaman dan kerentanan yang berpotensi memengaruhi keamanan informasi sistem. Identifikasi dilakukan terhadap ancaman internal dan eksternal serta kelemahan sistem yang dapat dimanfaatkan oleh ancaman tersebut. Selanjutnya dilakukan analisis pengendalian untuk menilai efektivitas kontrol keamanan yang telah diterapkan dalam mengurangi kemungkinan dan dampak risiko.

Proses penilaian risiko dilanjutkan dengan penentuan tingkat kemungkinan dan analisis dampak dari setiap risiko yang teridentifikasi. Hasil dari kedua tahapan tersebut digunakan dalam penentuan tingkat risiko dengan mengombinasikan nilai kemungkinan dan dampak sesuai dengan pendekatan NIST SP 800-30. Berdasarkan tingkat risiko yang diperoleh, kemudian disusun rekomendasi pengendalian sebagai upaya mitigasi risiko keamanan informasi. Seluruh hasil analisis digunakan sebagai dasar dalam penarikan kesimpulan penelitia.

4. HASIL DAN PEMBAHASAN

4.1 Karakterisasi Sistem

Karakterisasi sistem dilakukan untuk mengidentifikasi batasan dan komponen utama

dari sistem layanan UPA PKK UPN Veteran Jawa Timur yang menjadi objek penelitian. Tahapan ini bertujuan untuk memberikan gambaran awal mengenai lingkungan sistem informasi sehingga proses identifikasi risiko dapat dilakukan secara terarah dan sesuai dengan kondisi aktual.

Sistem laanan UPA PKK UPN Veteran Jawa Timur merupakan sistem informasi berbasis teknologi yang digunakan untuk mendukung kegiatan pengembangan karier dan kewirausahaan mahasiswa serta alumni. Sistem ini dimanfaatkan dalam pengelolaan data

layanan karier data alumni data mitra serta informasi pendukung lainnya yang berkaitan dengan aktivitas UPA PKK.

Komponen perangkat keras pada sistem layanan UPA PKK meliputi server yang digunakan untuk menyimpan dan memproses data komputer klien yang digunakan oleh admin serta perangkat jaringan yang mendukung konektivitas sistem. Perangkat lunak yang digunakan mencakup sistem operasi server aplikasi sistem informasi berbasis web serta perangkat lunak pendukung lainnya yang berfungsi dalam pengelolaan dan penyajian data.

Data yang dikelola dalam sistem layanan UPA PKK mencakup data mahasiswa data alumni data mitra industri serta data administratif layanan. Data tersebut bersifat penting dan sensitif sehingga memerlukan perlindungan terhadap akses yang tidak sah kehilangan maupun perubahan data. Selain itu sumber daya manusia yang terlibat terdiri dari admin sistem dan pengguna internal yang memiliki peran dalam pengelolaan dan pemanfaatan sistem informasi.

Berdasarkan karakteristik tersebut sistem layanan UPA PKK memiliki tingkat ketergantungan yang tinggi terhadap keberlangsungan teknologi informasi. Oleh karena itu sistem ini memerlukan pengelolaan keamanan informasi yang memadai guna menjaga kelancaran layanan serta melindungi aset informasi yang dimiliki.

4.2 Identifikasi Ancaman

Identifikasi ancaman dilakukan untuk mengetahui sumber ancaman yang berpotensi mengganggu keamanan informasi pada sistem layanan UPA PKK UPN Veteran Jawa Timur. Ancaman dapat berasal dari faktor internal maupun eksternal yang memiliki motivasi dan kemampuan berbeda dalam mengeksploitasi kelemahan sistem. Tahap ini menjadi dasar dalam menentukan tingkat risiko pada tahap selanjutnya.

Tabel 1 merupakan hasil identifikasi ancaman sistem layanan UPA-PKK, sebagaimana disajikan pada Tabel berikut.

Tabel 1. Identifikasi Ancaman Sistem Layanan UPA-PKK

Sumber Ancaman	Motivasi Utama	Bentuk Ancaman	Dampak Potensial
Hacker atau Cracker	Tantangan keuntungan finansial	Peretasan sistem akses tidak sah	Kebocoran data gangguan layanan
Kriminal Siber	Keuntungan finansial	Pencurian data manipulasi informasi	Kerugian institusi dan reputasi
Human Error	Kurangnya pemahaman sistem	Salah konfigurasi lupa logout	Celah keamanan sistem
Gangguan Teknis	Faktor lingkungan dan infrastruktur	Server down gangguan jaringan	Terhentinya layanan sementara

Berdasarkan Tabel 1. tersebut terlihat bahwa ancaman dominan terhadap sistem layanan UPA PKK berasal dari faktor manusia baik yang bersifat disengaja maupun tidak disengaja. Selain itu ancaman eksternal berupa serangan siber juga berpotensi menimbulkan dampak signifikan terhadap keamanan dan keberlangsungan sistem layanan.

4.3 Identifikasi Kerentanan

Identifikasi kerentanan dilakukan untuk mengetahui kelemahan yang terdapat pada sistem layanan UPA PKK UPN Veteran Jawa Timur yang berpotensi dimanfaatkan oleh ancaman. Kerentanan dapat muncul pada aspek teknologi maupun tata kelola sistem informasi. Tahap ini bertujuan untuk memberikan gambaran mengenai kondisi sistem yang masih memerlukan peningkatan pengamanan.

Tabel 2 meerupakan hasil identifikasi kerentanan sistem Layanan UPA-PKK yang disajikan pada Tabel berikut.

Tabel 2. Identifikasi Kerentanan Sistem Layanan UPA-PKK

Area	Kerentanan	Deskripsi Kerentanan	Dampak Potensial
Website	Manajemen kata sandi lemah	Penggunaan kata sandi sederhana dan jarang diperbarui	Akses tidak sah ke sistem
Website	Otentikasi tunggal	Tidak menggunakan autentikasi berlapis	Peningkatan risiko peretasan
Jaringan	Akses publik terbuka	Sistem dapat diakses melalui internet	Eksploitasi celah keamanan
Jaringan	Enkripsi belum optimal	Transmisi data belum sepenuhnya terenkripsi	Penyadapan data
Data	Backup tidak terjadwal	Pencadangan data belum dilakukan secara rutin	Kehilangan data
Sistem	Pembaruan sistem tidak berkala	Patch keamanan belum diterapkan secara konsisten	Kerentanan terhadap eksploitasi
Prosedur	Audit akses terbatas	Tidak ada peninjauan hak akses berkala	Penyalahgunaan akun

Berdasarkan Tabel 2 tersebut, kerentanan yang dominan terdapat pada aspek aplikasi dan jaringan khususnya terkait mekanisme pengamanan akses dan pengelolaan data. Kerentanan ini dapat meningkatkan peluang terjadinya gangguan keamanan informasi apabila tidak diimbangi dengan pengendalian yang memadai.

4.4 Analisis Pengendalian

Analisis pengendalian dilakukan untuk meninjau kontrol keamanan yang telah diterapkan pada sistem layanan UPA PKK UPN Veteran Jawa Timur. Tahap ini bertujuan untuk mengetahui sejauh mana pengendalian yang ada mampu mengurangi kemungkinan dan dampak risiko yang telah diidentifikasi pada tahap sebelumnya.

Pengendalian keamanan pada sistem layanan UPA PKK sebagian besar mengikuti kebijakan dan infrastruktur teknologi informasi yang diterapkan di lingkungan UPN Veteran Jawa Timur. Pengelolaan sistem dilakukan secara terpusat dengan dukungan unit teknologi informasi sehingga akses terhadap sistem dibatasi sesuai dengan peran pengguna.

Hasil analisis terhadap pengendalian yang diterapkan disajikan pada Tabel 3 berikut ini.

Tabel 3. Analisis Pengendalian Sistem Layanan UPA-PKK

Area	Pengendalian yang Diterapkan	Kondisi Saat Ini	Tingkat Efektivitas
Akses Sistem	Akun pengguna dan kata sandi	Telah diterapkan	Cukup
Akses Sistem	Pembatasan hak akses	Berdasarkan peran pengguna	Cukup
Jaringan	Firewall jaringan kampus	Telah diterapkan	Baik
Jaringan	Pengelolaan akses internet	Terpusat oleh unit TI	Baik
Sistem	Pemeliharaan sistem	Dilakukan secara berkala	Cukup
Data	Penyimpanan data terpusat	Server institusi	Baik
Prosedur	Dokumentasi penggunaan sistem	Masih terbatas	Kurang

Berdasarkan Tabel 3, hasil analisis pengendalian menunjukkan bahwa sistem layanan UPA PKK telah memiliki pengendalian dasar yang mendukung keamanan informasi. Namun efektivitas pengendalian pada beberapa aspek masih berada pada tingkat cukup dan kurang khususnya pada pengelolaan prosedur dan dokumentasi. Kondisi ini menunjukkan bahwa pengendalian yang ada belum sepenuhnya mampu menutup seluruh kerentanan yang teridentifikasi.

4.5 Penentuan Tingkat Kemungkinan

Penentuan tingkat kemungkinan dilakukan untuk menilai peluang terjadinya risiko pada sistem layanan UPA PKK UPN Veteran Jawa Timur. Penilaian ini mempertimbangkan jenis ancaman kerentanan yang ada serta efektivitas pengendalian keamanan yang telah diterapkan. Tingkat kemungkinan digunakan sebagai salah satu parameter utama dalam penentuan tingkat risiko pada tahap selanjutnya.

Dalam penelitian ini tingkat kemungkinan diklasifikasikan ke dalam tiga kategori yaitu tinggi, sedang, dan rendah. Definisi masing masing tingkat kemungkinan disajikan pada Tabel 4 berikut.

Tabel 4. Tingkat Kemungkinan Risiko

Tingkat Kemungkinan	Deskripsi
Tinggi	Ancaman sangat mungkin terjadi dan pengendalian yang ada belum mampu mengatasi kerentanan secara efektif
Sedang	Ancaman berpotensi terjadi namun sebagian pengendalian telah diterapkan
Rendah	Ancaman jarang terjadi dan pengendalian sistem dinilai cukup efektif

Berdasarkan Tabel 4 tersebut, meunjukkan bahwa hasil identifikasi ancaman dan kerentanan serta analisis pengendalian tingkat kemungkinan risiko pada sistem layanan UPA PKK berada pada kategori sedang hingga tinggi. Kondisi ini disebabkan oleh masih adanya kerentanan pada aspek pengamanan akses sistem dan pengelolaan data meskipun pengendalian dasar telah diterapkan.

4.6 Analisis Dampak

Analisis dampak dilakukan untuk mengetahui besarnya konsekuensi yang dapat ditimbulkan apabila risiko keamanan informasi terjadi pada sistem layanan UPA PKK UPN Veteran Jawa Timur. Dampak yang dianalisis berkaitan dengan gangguan layanan kerugian aset informasi serta reputasi institusi. Hasil analisis dampak digunakan sebagai dasar dalam menentukan tingkat risiko pada tahap selanjutnya.

Dalam penelitian ini tingkat dampak diklasifikasikan ke dalam tiga kategori yaitu tinggi sedang dan rendah. Kriteria penilaian dampak disajikan pada Tabel 5 berikut ini.

Tabel 5. Tingkat Dampak Risiko

Tingkat Dampak	Deskripsi
Tinggi	Gangguan layanan utama kebocoran data penting serta penurunan reputasi institusi
Sedang	Gangguan layanan sementara dan keterlambatan operasional
Rendah	Gangguan kecil yang tidak memengaruhi layanan secara signifikan

Berdasarkan Tabel 5 tersebut menunjukkan bahwa hasil analisis dampak sistem layanan UPA PKK memiliki potensi dampak yang cukup signifikan terutama pada aspek kebocoran data dan terhentinya layanan. Hal ini disebabkan oleh ketergantungan layanan terhadap sistem informasi serta pentingnya data yang dikelola dalam mendukung kegiatan pengembangan karier dan kewirausahaan.

4.7 Penentuan Tingkat Risiko

Penentuan tingkat risiko dilakukan dengan mengombinasikan hasil penilaian tingkat kemungkinan dan tingkat dampak dari risiko keamanan informasi pada sistem layanan UPA PKK UPN Veteran Jawa Timur. Tahap ini bertujuan untuk mengetahui prioritas risiko yang perlu ditangani berdasarkan tingkat keparahannya.

Dalam penelitian ini penentuan tingkat risiko mengacu pada pendekatan NIST SP 800 30 dengan menggunakan nilai kualitatif yang dikonversi menjadi tingkat risiko rendah sedang dan tinggi. Matriks penentuan tingkat risiko disajikan pada Tabel 6 berikut ini.

Tabel 6. Matriks Penentuan Tingkat Risiko

Tingkat Kemungkinan	Dampak Rendah	Dampak Sedang	Dampak Tinggi
Tinggi	Sedang	Tinggi	Tinggi
Sedang	Rendah	Sedang	Tinggi
Rendah	Rendah	Rendah	Sedang

Berdasarkan Tabel 6, matriks risiko memiliki dampak yang tinggi dikategorikan sebagai risiko tinggi dan menjadi prioritas utama untuk dilakukan pengendalian. Risiko dengan tingkat kemungkinan dan dampak sedang dikategorikan sebagai risiko sedang dan memerlukan pengelolaan secara bertahap. Sementara itu risiko dengan tingkat kemungkinan dan dampak rendah dikategorikan sebagai risiko rendah dan dapat diterima dengan pemantauan berkala.

Hasil penentuan tingkat risiko menunjukkan bahwa sistem layanan UPA PKK memiliki beberapa risiko yang berada pada kategori sedang hingga tinggi khususnya yang berkaitan dengan keamanan akses sistem dan pengelolaan data. Oleh karena itu diperlukan langkah pengendalian yang tepat untuk menurunkan tingkat risiko ke level yang dapat diterima.

4.8 Rekomendasi Pengendalian

Rekomendasi pengendalian disusun berdasarkan hasil penentuan tingkat risiko pada sistem layanan UPA PKK UPN Veteran Jawa Timur. Rekomendasi ini bertujuan untuk menurunkan tingkat risiko keamanan informasi ke level yang dapat diterima serta meningkatkan perlindungan terhadap aset informasi dan keberlangsungan layanan.

Pengendalian yang direkomendasikan difokuskan pada risiko dengan kategori tinggi dan sedang dengan mempertimbangkan kondisi sistem dan sumber daya yang tersedia. Rekomendasi pengendalian disajikan pada Tabel 7 berikut ini.

Tabel 7. Rekomendasi Pengendalian Risiko

Area	Risiko Utama	Rekomendasi Pengendalian	Prioritas
Akses Sistem	Akses tidak sah	Penerapan autentikasi berlapis dan kebijakan kata sandi yang kuat	Tinggi
Aplikasi	Kerentanan aplikasi	Pembaruan sistem dan patch keamanan berkala	Tinggi
Data	Kehilangan data	Penjadwalan backup data secara rutin	Tinggi
Jaringan	Penyadapan data	Penerapan enkripsi komunikasi	Sedang
Prosedur	Pengelolaan akses	Audit hak akses pengguna secara berkala	Sedang
SDM	Kurangnya kesadaran keamanan	Pelatihan keamanan informasi bagi pengelola sistem	Sedang

Berdasarkan Tabel 7 tersebut, didapatkan bahwa rekomendasi pengendalian difokuskan pada penguatan mekanisme akses sistem pengamanan data serta peningkatan pengelolaan prosedur keamanan. Penerapan rekomendasi ini diharapkan dapat menurunkan tingkat risiko keamanan informasi pada sistem layanan UPA PKK serta meningkatkan keandalan dan keberlangsungan layanan.

5. KESIMPULAN

Penelitian ini dilakukan untuk menganalisis manajemen risiko keamanan informasi pada sistem layanan UPA PKK UPN Veteran Jawa Timur menggunakan metode NIST SP 800 30. Berdasarkan hasil analisis yang telah dilakukan dapat disimpulkan bahwa sistem layanan UPA PKK memiliki ketergantungan yang tinggi terhadap teknologi informasi dalam mendukung kegiatan pengembangan karier dan kewirausahaan mahasiswa serta alumni.

Hasil identifikasi ancaman dan kerentanan menunjukkan bahwa risiko keamanan informasi pada sistem layanan UPA PKK masih didominasi oleh kelemahan pada aspek pengamanan akses sistem pengelolaan data serta penerapan prosedur keamanan. Meskipun pengendalian dasar telah diterapkan efektivitasnya belum sepenuhnya mampu menurunkan tingkat risiko secara optimal.

Berdasarkan penilaian tingkat kemungkinan dan dampak diperoleh beberapa

risiko yang berada pada kategori sedang hingga tinggi. Risiko tersebut berpotensi menimbulkan gangguan layanan kebocoran data serta penurunan kepercayaan terhadap sistem layanan apabila tidak dikelola dengan baik.

Penerapan metode NIST SP 800 30 terbukti mampu memberikan gambaran risiko keamanan informasi secara sistematis dan terstruktur. Metode ini membantu dalam menentukan prioritas risiko serta menyusun rekomendasi pengendalian yang sesuai dengan kondisi sistem layanan UPA PKK. Dengan demikian hasil penelitian ini dapat dijadikan dasar dalam meningkatkan pengelolaan keamanan informasi dan keberlangsungan sistem layanan UPA PKK UPN Veteran Jawa Timur.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada UPA PKK UPN Veteran Jawa Timur atas dukungan dan kesempatan yang diberikan dalam pelaksanaan penelitian ini. Ucapan terima kasih juga disampaikan kepada pihak-pihak yang telah memberikan arahan, masukan, serta bantuan selama proses pengumpulan data dan penyusunan penelitian sehingga penelitian ini dapat diselesaikan dengan baik.

DAFTAR PUSTAKA

[1] A. A. Zulfa, T. Ibrahim, dan O. Arifudin, "Peran sistem informasi akademik berbasis web dalam upaya meningkatkan efektivitas dan efisiensi pengelolaan akademik di perguruan tinggi," Jurnal Tahsinia, vol. 6, no. 1, pp. 115–134, 2025.

[2] M. A. Azizah, S. Solikhin, dan N. Lailiyah, "Implementasi sistem informasi manajemen dalam mendukung pelayanan administrasi," Ngaos: Jurnal Pendidikan dan Pembelajaran, vol. 2, no. 2, pp. 80–94, 2024.

[3] M. F. Aska, D. P. Putra, dan C. J. M. Sinambela, "Strategi efektif untuk implementasi keamanan siber di era digital," Journal of Informatic and Information Security, vol. 5, no. 2, pp. 187–200, 2024.

[4] R. Pakina dan M. Solekhan, "Pengaruh teknologi informasi terhadap hukum privasi dan pengawasan di Indonesia: Keseimbangan antara keamanan dan hak asasi manusia," Journal of Scientech Research and Development, vol. 6, no. 1, pp. 273–286, 2024.

[5] Z. Alamin dan M. A. Mu'min, "Analisis keamanan jaringan pada sistem kendali jarak jauh untuk infrastruktur kritis," Jurnal Pengembangan Sains dan Teknologi, vol. 1, no. 1, pp. 25–41, 2025.

[6] S. Tommy dan M. I. P. Nasution, "Evaluasi manajemen risiko keamanan siber pada infrastruktur digital pemerintah: Studi kasus pusat data nasional (PDN)," Jurnal Manajemen Ekonomi dan Bisnis, vol. 4, no. 1, pp. 1–26, 2025.

[7] U. Kasma, "Identifikasi risiko keamanan data pada sistem informasi perpustakaan," dalam SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, vol. 14, no. 2, pp. 9–17, Jul. 2025.

[8] T. A. Rahmi, M. Ikhwani, dan M. Muthmainnah, "Analisis manajemen risiko pada sistem informasi manajemen rumah sakit (SIMRS) dengan ISO 31000 dan NIST SP 800-30 di RSUD H. OK Arya Zulkarnain," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 9, no. 5, pp. 8207–8215, 2025.

[9] L. Marlina dan M. S. Nugraha, "Analisis komponen utama dalam sistem informasi manajemen: Konsep, fungsi, dan implementasi," Pendas: Jurnal Ilmiah Pendidikan Dasar, vol. 9, no. 4, pp. 872–890, 2024.

[10] M. Abdullah, T. Zulfikar, dan S. I. Shadiqin, "Manajemen data akademik perguruan tinggi keagamaan Islam swasta: Studi literature review," An-Nadzir: Jurnal Manajemen Pendidikan Islam, vol. 2, no. 1, pp. 48–59, 2024.

[11] A. Adamuddin dan A. Yamin, "Pengaruh kualitas layanan dan sistem informasi terhadap kepuasan masyarakat di Kelurahan Menala Kecamatan Taliwang Kabupaten Sumbawa Barat," JIIP–Jurnal Ilmiah Ilmu Pendidikan, vol. 8, no. 5, pp. 5096–5108, 2025.

[12] D. F. Daulay dan R. Sayekti, "Strategi menjamin sistem keamanan data perpustakaan digital Universitas Negeri Medan berbasis cloud computing," Jurnal Informatika Teknologi dan Sains (Jinteks), vol. 7, no. 3, pp. 1464–1472, 2025.

[13] W. D. Novarianti, A. P. P. S. Meliala, N. A. S. Yusuf, dan B. N. C. Melati, "Kerahasiaan bank vs hak atas informasi: Mengurai konflik kepentingan dalam perlindungan data pribadi," Jurnal Multidisiplin Ilmu Akademik, vol. 2, no. 1, pp. 103–114, 2025.

[14] D. P. Adhelia dan M. I. P. Nasution, "Dampak faktor manusia dan pengoptimalisasian terhadap integritas data perusahaan dalam lingkungan bisnis," Socius: Jurnal Penelitian Ilmu-Ilmu Sosial, vol. 2, no. 11, 2025.

[15] L. A. Saputra, F. M. Akbar, F. Cahyaningtias, M. P. Ningrum, dan A. Fauzi, "Ancaman keamanan pada sistem informasi manajemen perusahaan," Jurnal Pendidikan Siber Nusantara, vol. 1, no. 2, pp. 58–66, 2023.
[16] A. Vidiarto, R. Azis, A. Mulyanto, M. Meidilah, S. Supryanto, dan H. Prasetyono, "Pengaruh budaya peduli risiko dalam meningkatkan efektivitas manajemen risiko organisasi," BULLET: Jurnal Multidisiplin Ilmu, vol. 2, no. 4, pp. 982–991, 2023.
[17] A. W. Ardhani, N. Wahyudi, dan Y. Ardilla, "Penerapan ISO 31000 dalam analisis risiko pengelolaan sistem informasi tata ruang (SITR) Jawa Timur," Journal of Information System, Applied, Management, Accounting and Research, vol. 9, no. 4, pp. 1465–1476, 2025.
[18] A. Fitriani, I. Irsyad, dan M. Setiawati, "Implementasi pengendalian risiko dalam meningkatkan efektivitas manajemen sekolah," Jurnal Ilmu Manajemen dan Pendidikan, vol. 2, no. 3, pp. 829–832, 2025.
[19] M. Agil, N. N. Sholikhah, A. Zunaidi, dan M. Ahmada, "Meminimalkan risiko dan memaksimalkan keuntungan: Strategi manajemen risiko dalam pengelolaan wakaf produktif," Al-Muraqabah: Journal of Management and Sharia Business, vol. 3, no. 2, pp. 156–175, 2023.
[20] I. P. Jovano, I. R. Padiku, dan B. Ahaliki, "Analisis manajemen risiko dan keamanan sistem informasi akademik terpadu (SIAT) Universitas Negeri Gorontalo menggunakan framework NIST SP 800-30," Diffusion: Journal of Systems and Information Technology, vol. 5, no. 1, pp. 135–144, 2025.
[21] A. Syaputra, "Penilaian IT governance dalam manajemen risiko IT menggunakan metode quantitative dan qualitative risk analysis," Jurnal Manajemen Informatika (JAMIKA), vol. 12, no. 1, pp. 63–73, 2022.
[22] A. Gunawan, F. Sulianta, dan U. Widyatama, "Penilaian risiko infrastruktur IT pada website e-learning Universitas XYZ menggunakan framework NIST SP 800-30," n.d.