PENILAIAN RISIKO KEAMANAN SISTEM INFORMASI DI DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN TRENGGALEK

Wafiq Alfin Kamil
NPP. 33.0584
Program Studi Teknologi Rekayasa Informasi Pemerintahan
Email: 33.0584@praja.ipdn.ac.id

Pembimbing Skripsi: Wenty Zahrati,S.Kom.,M.Kom,
Email: wenty@ipdn.ac.id

ABSTRACT

Problem Statement (Research Gap): *This study focuses on the research object gap concerning information system security risk assessment within a regional government agency that has a strategic role in managing information technology and digital public services. Existing literature is generally dominated by studies conducted in the healthcare, education, insurance sectors, and government organizations in general. Consequently, studies specifically examining information system security risks at the Trenggalek Regency Communication and Informatics Office remain limited. In addition, this research addresses a methodological gap through the application of the NIST SP 800-30 Revision 1 framework without combining it with other frameworks commonly used in previous studies.* ***Purpose:*** *his study aims to identify information system security risks, determine their risk levels, and analyze the efforts undertaken to minimize information system security risks at the Trenggalek Regency Communication and Informatics Office using the NIST SP 800-30 Revision 1 framework.* ***Method:*** *This research employed a descriptive quantitative approach. Data were collected through interviews, observations, and documentation. Risk assessment was conducted based on the NIST SP 800-30 Revision 1 framework.* ***Result:*** *The findings indicate that there are seven information system security risks at the Trenggalek Regency Communication and Informatics Office, namely data breach with a very high risk level; web defacement and server down with high risk levels; and brute force, misconfiguration, content injection, and cross-site scripting with moderate risk levels.* ***Conclusion:*** *The study concludes that the information system security risks at the Trenggalek Regency Communication and Informatics Office comprise seven risks with varying levels of severity. To mitigate these risks, the agency has implemented several security measures, including firewall deployment, information system security training programs, penetration testing using Burp Suite, and the establishment of a Computer Security Incident Response Team (CSIRT).*

Keywords: *Information System Security, NIST SP 800-30 Revision 1, Risk Assessment.*

ABSTRAK

Permasalahan (Kesenjangan Penelitian/Research Gap): Penulis berfokus pada kesenjangan objek penelitian mengenai penilaian risiko keamanan sistem informasi pada organisasi perangkat daerah yang memiliki fungsi strategis dalam pengelolaan teknologi informasi dan layanan digital pemerintah daerah. Literatur yang ada umumnya didominasi oleh penelitian pada sektor kesehatan, pendidikan, asuransi, maupun organisasi pemerintahan secara umum, sehingga kajian yang secara khusus menelaah risiko keamanan sistem informasi di Dinas Komunikasi dan Informatika Kabupaten Trenggalek masih terbatas. Selain itu, penelitian ini juga mengisi kesenjangan metodologis melalui penerapan framework NIST SP 800-30 Revision 1 tanpa mengombinasikannya dengan framework lain yang banyak digunakan dalam penelitian terdahulu. **Tujuan:** Penelitian ini bertujuan untuk mengetahui risiko keamanan dan tingkat risiko serta upaya untuk meminimalisir risiko keamanan sistem informasi di Dinas Komunikasi dan Informatika Kabupaten Trenggalek menggunakan framework NIST SP 800-30 Revision 1. **Metode:** Penelitian ini menggunakan pendekatan kuantitatif deskriptif. Pengumpulan data dilakukan melalui wawancara, observasi, dan dokumentasi. Penilaian risiko dilakukan berdasrkan framework NIST SP 800-30 Revision 1. **Hasil/Temuan:** Temuan penelitian menunjukkan bahwa risiko keamanan sistem informasi di Dinas Komunikasi dan Informatika Kabupaten Trenggalek terdiri atas tujuh risiko, yaitu data breach dengan tingkat risiko sangat tinggi, web defacement dan server down dengan tingkat risiko tinggi, serta brute force, misconfiguration, content injection, dan cross-site scripting dengan tingkat risiko sedang. **Kesimpulan:** Peneliti menyimpulkan bahwa risiko keamanan sistem informasi di Dinas Komunikasi dan Informatika Kabupaten Trenggalek terdiri atas tujuh risiko dengan tingkat risiko yang beragam.Untuk meminimalisir dampak dari risiko-risiko tersebut, Dinas Komunikasi dan Informatika Kabupaten Trenggalek telah melakukan berbagai upaya mitigasi, antara lain melalui penerapan firewall, penyelenggaraan bimbingan teknis keamanan sistem informasi, pelaksanaan tes penetrasi menggunakan aplikasi Burp Suite, serta pembentukan Computer Security Incident Response Team (CSIRT).

Kata kunci: Keamanan Sistem Informasi, NIST SP 800-30 Revision 1, Penilaian Risiko.

I. PENDAHULUAN

1.1. Latar Belakang

Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government menjadi landasan awal penerapan e-government secara resmi di Indonesia. Penerapan e-government di Indonesia semakin diperkuat dengan hadirnya Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Upaya tersebut sejalan dengan perkembangan transformasi digital yang telah menjadi agenda global, di mana pemerintah di berbagai negara, termasuk Indonesia, terus mengintegrasikan teknologi dalam penyelenggaraan layanan publik (Abrory et al., 2025).

Percepatan digitalisasi layanan publik melalui kebijakan Sistem Pemerintahan Berbasis Elektronik membuka peluang untuk meningkatkan kualitas pelayanan kepada masyarakat. Sejalan dengan itu Purwanto menegaskan bahwa transformasi digital di sektor administrasi publik telah mendorong perubahan dalam tata kelola pemerintahan melalui penerapan e-Government (Purwanto et al., 2025). Tetapi disisi lain Integrasi berbagai platform digital, pemanfaatan data secara masif, serta keterhubungan antarinstansi dalam ekosistem pemerintahan digital menyebabkan eksposur sistem informasi pemerintah semakin luas dan kompleks. Menurut Muliati et al (2025) seiring bertambahnya ketergantungan terhadap teknologi, tingkat dan kompleksitas risiko yang dihadapi juga meningkat. Kemudian menurut Sema et al (2024) percepatan digitalisasi menyebabkan setiap individu dan organisasi menghadapi ancaman siber yang terus berubah.

Hasil pemantauan Cyber Threat Intelligence dalam surface web, deepweb, dan darkweb,ditemukan sebanyak 285 insiden siber pada tahun 2022, meningkat menjadi 343 insiden pada tahun 2023, dan melonjak signifikan hingga 593 insiden pada tahun 2024. Dari keseluruhan data tersebut, sektor administrasi pemerintahan tercatat sebagai sektor dengan jumlah insiden tertinggi dibandingkan sektor lainnya, yaitu 120 insiden pada tahun 2022, 186 insiden pada tahun 2023, dan meningkat tajam menjadi 352 insiden pada tahun 2024. Temuan ini mengindikasikan bahwa sektor Administrasi Pemerintahan merupakan area yang paling rawan terhadap insiden siber, sehingga memerlukan perhatian lebih dalam pengelolaan risiko serta penguatan keamanan siber. Kemudian berdasarkan data yang dirilis oleh Badan Siber Sandi Negara pada tahun 2024 jumlah trafik anomali serangan siber di Indonesia tercatat mencapai 330.527.636 anomali. Trafik anomali tertinggi terjadi pada bulan desember dengan jumlah 112.085.045 anomali, mengalami peningkatan yang sangat signifikan dibandingkan bulan november yang tercatat sebanyak 49.429.682 anomali. Jumlah yang begitu besar ini mencerminkan betapa luas dan tingginya serangan yang dapat mengancam keamanan sistem digital di berbagai sektor, mulai dari sektor pemerintahan, kesehatan, pendidikan, hingga sektor bisnis dan industri.

Fenomena tingginya trafik anomali dan meningkatnya insiden siber tersebut menjadi sinyal penting bagi sektor pemerintahan, khususnya pemerintah daerah,untuk

meningkatkan kewaspadaan terhadap ancaman siber. Serangan siber dipemerintahan dapat berpotensi mengganggu keberlangsungan layanan publik. Selain berdampak pada keberlangsungan layanan publik, serangan siber juga dapat menimbulkan konsekuensi yang lebih luas terhadap aspek sosial. Ancaman utama dari serangan siber tidak terletak pada potensi kehancuran fisik yang berskala besar, melainkan pada risiko sosial yang lebih subtil, seperti berkurangnya tingkat kepercayaan publik terhadap pemerintah (Shandler & Gomez, 2023). Kondisi tersebut menunjukkan bahwa perlindungan sistem informasi di lingkungan pemerintahan menjadi sangat penting karena sistem informasi menyimpan data dan informasi yang merupakan aset berharga (Adi Saputra et al., 2023)

Kerentanan sistem informasi digital pemerintah daerah terhadap serangan siber tercermin dari kasus yang menimpa Pemerintah Kabupaten Trenggalek.Pada bulan april tahun 2022, 50 situs website milik Pemerintah Kabupaten Trenggalek, terutama situs-situs organisasi perangkat daerah, dilaporkan berhasil diretas. Selain itu, insiden yang lebih baru pada tahun 2024 website Survei Kepuasan Masyarakat dan website Sistem Pengembangan Kompetensi Aparatur milik Pemerintah Kabupaten Trenggalek terdampak akibat peretasan pada Pusat Data Nasional. Akibat serangan tersebut, beberapa data mengalami enkripsi paksa sehingga tidak dapat diakses dan sebagian data lainnya bahkan hilang. Peristiwa tersebut menunjukan bahwa, sistem informasi pemerintah daerah berada pada posisi yang rentan, oleh karena itu diperlukan pendekatan yang lebih sistematis, terukur, dan berkelanjutan untuk mengelola keamanan sistem informasi melalui penilaian risiko keamanan sistem informasi.Penilaian risko keamanan informasi sangat penting dalam mengidentifikasi dan memprioritaskan aset informasi serta mengidentifikasi dan memantau ancaman spesifik yang dihadapi organisasi, khususnya kemungkinan terjadinya ancaman dan dampaknya terhadap bisnis (Devi et al., 2022). Proses seperti penilaian risiko dan rencana mitigasi sangat krusial untuk memastikan layanan operasional dan bersiap menghadapi gangguan (Casaril, 2025).cDengan demikian, diharapkan dapat mengurangi peluang terjadinya insiden keamanan serta membatasi dampak ketika ancaman benar-benar terjadi.

1.2. Kesenjangan Masalah yang Diambil (Research Gap)

Percepatan implementasi Sistem Pemerintahan Berbasis Elektronik menuntut setiap organisasi pemerintah untuk mampu menjamin keamanan sistem informasi yang digunakan dalam penyelenggaraan pelayanan publik. Namun, kondisi aktual menunjukkan bahwa ancaman dan insiden siber pada sektor pemerintahan terus mengalami peningkatan, bahkan Pemerintah Kabupaten Trenggalek pernah mengalami kasus web defacement pada puluhan website Organisasi Perangkat Daerah serta terdampak insiden peretasan Pusat Data Nasional. Peristiwa tersebut menunjukan bahwa, pemerintah belum mampu menjamin keamanan sistem informasi yang digunakan dalam penyelenggaraan pelayanan publik, oleh karena itu diperlukan pendekatan yang lebih sistematis, terukur, dan

berkelanjutan untuk mengelola keamanan sistem informasi melalui penilaian risiko keamanan sistem informasi menggunakan *framework NIST SP 800 30 Revision 1*.

1.3. Urgensi Penelitian

Penelitian ini penting mengingat Berbagai insiden yang pernah terjadi pada sistem informasi Pemerintah Kabupaten Trenggalek, seperti web defacement terhadap puluhan website pemerintah daerah serta dampak peretasan Pusat Data Nasional yang menyebabkan gangguan akses dan kehilangan data, menunjukkan adanya risiko keamanan sistem informasi. Oleh karena itu, penelitian ini diperlukan untuk memberikan gambaran mengenai risiko keamanan sistem informasi yang dihadapi Dinas Komunikasi dan Informatika Kabupaten Trenggalek. Apabila penelitian ini tidak dilaksanakan, maka Pemerintah Kabupaten Trenggalek, khususnya Dinas Komunikasi dan Informatika Kabupaten Trenggalek, akan mengalami keterbatasan dalam memperoleh informasi yang komprehensif mengenai risiko keamanan sistem informasi yang dapat menyebabkan pengambilan keputusan terkait keamanan sistem informasi tidak didasarkan pada tingkat prioritas risiko yang sebenarnya, sehingga upaya pengamanan berpotensi kurang tepat sasaran dan kurang efektif.

1.4. Penelitian Terdahulu

1. **Penelitian Rahmi et al (2024)** menerapkan ISO 31000 dan NIST SP 800-30 untuk menganalisis manajemen risiko Sistem Informasi Manajemen Rumah Sakit (SIMRS) RSUD H. OK Arya Zulkarnain dan menemukan 15 risiko yang terdiri atas 5 risiko tinggi, 8 risiko sedang, dan 2 risiko rendah.
2. **Penelitian Tjahjono et al (2023)** menggunakan NIST SP 800-30 untuk menganalisis risiko pada sistem informasi di Diskominfo dan menemukan bahwa ancaman manusia, gangguan listrik, serta risiko teknis merupakan sumber risiko utama.
3. **Penelitian M. Fadhli Ma'arif et al (2025)** menganalisis keamanan implementasi QRIS menggunakan ISO 31000:2018 dan mengidentifikasi risiko berupa manipulasi QR code, phishing, koneksi internet yang tidak stabil, serta rendahnya literasi digital pengguna.
4. **Penelitian Putro et al (2021)** mengenai analisis manajemen risiko E-Learning EdLink menggunakan NIST SP 800-30 Revisi 1 yang menemukan tujuh risiko kritis yang terdiri dari tiga risiko very high dan empat risiko high.
5. **Penelitian Putra & Soewito (2023)** yang mengintegrasikan ISO/IEC 27005:2018 dan NIST SP 800-30 pada sistem ERP di sektor asuransi mengidentifikasi 142 skenario risiko dengan dominasi kategori low dan moderate serta merekomendasikan penguatan kontrol keamanan berdasarkan ISO/IEC 27002:2022.

1.5. Pernyataan Kebaruan Ilmiah

Kebaruan ilmiah penelitian ini terletak pada aspek objek penelitian dan metode yang digunakan. Dari aspek objek penelitian, penelitian sebelumnya umumnya menerapkan penilaian risiko keamanan sistem informasi pada sektor kesehatan, pendidikan, asuransi, maupun organisasi pemerintahan secara umum. Sementara itu, penelitian ini secara khusus berfokus pada Dinas Komunikasi dan Informatika Kabupaten Trenggalek sebagai organisasi perangkat daerah yang memiliki peran strategis dalam pengelolaan teknologi informasi, komunikasi, serta layanan digital pemerintah daerah. Dari aspek metode, penelitian ini menggunakan *framework NIST SP 800-30 Revision 1* yang merupakan versi pembaruan dari versi sebelumnya yaitu *NIST SP 800-30*. Selain itu penelitian ini tidak mengombinasikannya dengan framework lainnya, seperti *ISO 31000* atau *ISO 27005* yang banyak digunakan pada penelitian terdahulu.

1.6. Tujuan

Penelitian ini bertujuan untuk mengetahui risiko keamanan dan tingkat risiko serta upaya untuk meminimalisir risiko keamanan sistem informasi di Dinas Komunikasi dan Informatika Kabupaten Trenggalek.

II. METODE

Metode penelitian merupakan cara ilmiah yang digunakan untuk memperoleh data dengan tujuan dan manfaat tertentu (Ardieansyah et al., 2023). Pada penelitian kali, peneliti menggunakan pendekatan penelitian kualitatif deskriptif. Pendekatan kualitatif dipandang sebagai metode yang memiliki sifat fleksibel dalam meneliti, karena memungkinkan adanya perubahan guna memperoleh keselarasan dengan rencana yang telah dibuat pada lokus penelitian yang sebenarnya (Simangunsong, 2017). Pendekatan penelitian kualitatif diskriptif dipilih dalam penelitian ini karena proses penilaian risiko keamanan sistem informasi yang mengacu pada NIST SP 800-30 Revision 1, menuntut pemahaman yang mendalam terhadap kondisi keamanan sistem informasi, kebijakan keamanan informasi, prosedur keamanan informasi, sumber ancaman, peristiwa ancaman serta kerentanan sistem informasi. yang tidak dapat diungkap secara komprehensif dengan pendekatan kuantitatif. Data dikumpulkan melalui wawancara, observasi, dan dokumentasi dengan informan dipilih dengan tehnik *purposive sampling*. Proses penilaian risiko keamanan sistem informasi dilakukan menggunakan *framework NIST SP 800-30 Revision 1* melalui tahapan sebagai berikut

Tahap identifikasi sumber ancaman

Tahap identifikasi sumber ancaman dilakukan untuk mengetahui sumber risiko yang berpotensi mengganggu sistem informasi. Setelah sumber ancaman teridentifikasi, dilakukan penilaian terhadap kemampuan, niat, dan penargetan untuk ancaman yang berasal dari luar seperti hacker, sedangkan ancaman tidak dari luar dinilai berdasarkan

rentang efeknya. Skala penilaian karakteristik kemampuan, niat, penargetan, dan rentang efek sumber ancaman disajikan sebagai berikut

Tabel 1.
Penilaian karakteristik kemampuan lawan

Kemampuan	Keterangan
Sangat Tinggi	Memiliki tingkat keahlian yang sangat tinggi, sumber daya yang sangat memadai, serta mampu menciptakan peluang untuk mendukung berbagai serangan yang berhasil, berkelanjutan, dan terkoordinasi.
Tinggi	Memiliki tingkat keahlian yang canggih, dengan sumber daya dan peluang yang signifikan untuk mendukung berbagai serangan yang berhasil dan terkoordinasi.
Sedang	Memiliki sumber daya, keahlian, dan peluang yang cukup untuk mendukung beberapa serangan yang berhasil.
Rendah	Memiliki sumber daya, keahlian, dan peluang yang terbatas untuk mendukung serangan yang berhasil.
Sangat Rendah	Memiliki sumber daya, keahlian, dan peluang yang sangat terbatas untuk mendukung serangan yang berhasil.

Sumber: NIST SP 800-30 Revision 1

Tabel 2.
Penilaian karakteristik niat lawan

Niat	Keterangan
Sangat Tinggi	Berupaya untuk secara serius mengganggu, menghentikan, atau menghancurkan misi inti atau fungsi bisnis organisasi dengan dengan mengeksploitasi keberadaannya di dalam sistem informasi atau infrastruktur organisasi, serta hanya peduli terhadap pembongkaran teknik sejauh hal itu dapat menghambat kemampuannya untuk menyelesaikan tujuan yang telah ditetapkan.
Tinggi	Berupaya merusak beberapa aspek dari misi inti atau fungsi bisnis organisasi, atau mempertahankan keberadaan dalam sistem informasi atau infrastruktur organisasi untuk melakukan hal tersebut di masa depan, serta sangat peduli untuk meminimalkan deteksi serangan, terutama saat mempersiapkan serangan di masa depan.
Sedang	Berupaya memperoleh atau memodifikasi informasi kritis atau sensitif, atau mengganggu sumber daya siber organisasi dengan memanfaatkan keberadaan dalam sistem informasi atau infrastruktur organisasi, serta peduli untuk meminimalkan deteksi serangan, terutama saat melakukan serangan dalam jangka waktu lama.
Rendah	Berupaya secara aktif berupaya memperoleh informasi kritis atau sensitif, atau mengganggu sumber daya siber organisasi, dan melakukannya tanpa memperhatikan kemungkinan deteksi atau pengungkapan metode serangan.
Sangat Rendah	Lawan berupaya menggunakan, mengganggu, atau merusak tampilan (deface) sumber daya siber organisasi tanpa memperhatikan kemungkinan deteksi atau pengungkapan metode serangan.

Sumber: NIST SP 800-30 Revision 1

Tabel 3.
Penilaian karakteristik penargetan lawan

Penargetan	Keterangan
Sangat Tinggi	Menganalisis informasi yang diperoleh melalui pengintaian dan bertindak secara sangat persisten untuk menargetkan organisasi, perusahaan, program, misi, atau fungsi bisnis tertentu. Penargetan difokuskan pada informasi, sumber daya, alur kerja, atau fungsi yang bernilai tinggi atau sangat penting bagi misi.
Tinggi	Menganalisis informasi yang diperoleh melalui pengintaian untuk secara persisten menargetkan organisasi, perusahaan, program, misi, atau fungsi bisnis tertentu. Penargetan difokuskan pada informasi atau sumber daya yang bernilai tinggi atau penting bagi misi.
Sedang	Menganalisis informasi yang tersedia secara publik untuk menargetkan organisasi bernilai tinggi tertentu seperti program, atau informasi penting.
Rendah	Menggunakan informasi yang tersedia secara publik untuk menargetkan berbagai organisasi bernilai tinggi atau informasi tertentu, serta mencari peluang target dalam kelompok tersebut.
Sangat Rendah	Menargetkan atau tidak menargetkan organisasi atau kelompok organisasi tertentu.

Sumber: NIST SP 800-30 Revision 1

Tabel 4.
Penilaian rentang efek

Rentang Efek	Keterangan
Sangat Tinggi	Efeknya bersifat menyeluruh, melibatkan hampir semua sumber daya siber.
Tinggi	Efeknya bersifat luas,melibatkan sebagian besar sumber daya, termasuk banyak sumber daya kritis.
Sedang	Efeknya bersifat cukup luas melibatkan sebagian besar sumber daya siber, termasuk beberapa sumber daya kritis.
Rendah	Efeknya bersifat terbatas melibatkan beberapa sumber daya siber, tetapi tidak melibatkan sumber daya kritis.
Sangat Rendah	Efeknya bersifat minimal, melibatkan sedikit atau bahkan tidak ada pada sumber daya siber, tidak melibatkan sumber daya kritis.

Sumber: NIST SP 800-30 Revision 1

Indentifikasi peristiwa ancaman

Tahap identifikasi kejadian ancaman dilakukan untuk mengetahui peristiwa ancaman yang pernah terjadi. Setelah peristiwa ancaman teridentifikasi, dilakukan penilaian relevansi ancaman. Kriteria penilaian relevansi peristiwa sebagi berikut

Tabel 5.
Kriteria relevansi ancaman

Relevansi	Keterangan
Confirmed (Terkonfirmasi)	Peristiwa ancaman telah terlihat/terdeteksi oleh organisasi.
Expected (Diduga)	Peristiwa ancaman telah terlihat oleh rekan sejawat atau mitra organisasi.
Anticipated (Diantisipasi)	Peristiwa ancaman telah dilaporkan oleh sumber yang tepercaya.
Predicted (Diprediksi)	Peristiwa ancaman telah diprediksi oleh sumber yang tepercaya.
Possible (Mungkin)	Peristiwa ancaman telah dijelaskan oleh sumber yang cukup kredibel.

Sumber: NIST SP 800-30 Revision 1

Identifikasi kerentanan

Tahap identifikasi kerentanan merupakan tahapan untuk mengetahui kerentanan dalam sistem informasi dan faktor-faktor yang sudah ada sebelumnya dalam organisasi atau sistem yang membuat organisasi menjadi lebih rentan terhadap ancaman.

Penentuan tingkat kemungkinan

Tahap penentuan tingkat kemungkinan merupakan tahapan untuk mengetahui seberapa besar peluang terjadinya suatu peristiwa ancaman. Berikut merupakanm kriteria penentuan tingkat kemungkinan berdasarkan NIST SP 800-30 Revision 1 dengan rujukan dari penelitian (Putri & Hakim, 2018).

Tabel 6.
Kriteria terjadinya peristiwa ancaman

Kemungkinan	Keterangan
Sangat Tinggi	Kejadian hampir pasti terjadi atau subjek hampir selalu memulai kejadian ancaman.
Tinggi	Kejadian sangat mungkin terjadi atau subjek berpotensi tinggi memulai kejadian ancaman.
Sedang	Kejadian cukup mungkin terjadi atau subjek terkadang mungkin memulai kejadian ancaman.
Rendah	Kejadian kemungkinannya kecil terjadi atau subjek tidak mungkin memulai kejadian ancaman.
Sangat Rendah	Kejadian kemungkinannya sangat kecil terjadi atau subjek sangat tidak mungkin memulai kejadian ancaman.

Sumber: NIST SP 800-30 Revision 1 (Putri & Hakim, 2018).

Tabel 7.
Kriteria kemungkinan menimbulkan dampak buruk

Kemungkinan	Ketereangan
Sangat Tinggi	Jika kejadian ancaman dimulai atau terjadi, hampir pasti akan menimbulkan dampak merugikan.
Tinggi	Jika kejadian ancaman dimulai atau terjadi, sangat mungkin akan menimbulkan dampak merugikan.
Sedang	Jika kejadian ancaman dimulai atau terjadi, cukup mungkin akan menimbulkan dampak merugikan.
Rendah	Jika kejadian ancaman dimulai atau terjadi, tidak mungkin akan menimbulkan dampak merugikan.
Sangat Rendah	Jika kejadian ancaman dimulai atau terjadi, sangat tidak mungkin akan menimbulkan dampak merugikan.

Sumber: NIST SP 800-30 Revision 1 (Putri & Hakim, 2018).

Tabel 8.
Matriks penilaian keseluruhan kemungkinan

Kemungkinan Terjadinya Peristiwa Ancaman	Kemungkinan Peristiwa Ancaman Mengakibatkan Dampak Buruk				
	Sangat Rendah	**Rendah**	**Sedang**	**Tinggi**	**Sangat Tinggi**
Sangat Tinggi	Rendah	Sedang	Tinggi	Sangat Tinggi	Sangat Tinggi
Tinggi	Rendah	Sedang	Sedang	Tinggi	Sangat Tinggi
Sedang	Rendah	Rendah	Sedang	Sedang	Tinggi
Rendah	Sangat Rendah	Rendah	Rendah	Sedang	Sedang
Sangat Rendah	Sangat Rendah	Sangat Rendah	Rendah	Rendah	Rendah

Sumber: NIST SP 800-30 Revision 1

Penentuan tingkat dampak

Tahap penentuan tingkat dampak merupakan tahapan untuk menilai besarnya tingkat dampak yang dapat ditimbulkan apabila suatu peristiwa ancaman terjadi pada sistem informasi. Berikut merupakan kriteria penilaian tingkat dampak berdasarkan *NIST SP 800-30 Revision 1* dengan rujukan dari penelitian (Putri & Hakim, 2018).

Tabel 9.
Kriteria penentuan tingkat dampak

Kemungkinan	Ketereangan
Sangat Tinggi	Ancaman menimbulkan dampak yang masif, beragam, dan ekstrem bagi operasional, aset, individu, serta entitas lain (organisasi/negara).
Tinggi	Ancaman menyebabkan dampak yang signifikan (besar) terhadap operasional, aset, individu, dan organisasi lain atau negara.
Sedang	Ancaman menimbulkan dampak yang moderat (cukup) bagi operasional, aset, individu, dan organisasi lain atau negara.
Rendah	Ancaman mengakibatkan dampak yang ringan (kecil) pada operasional, aset, individu, serta organisasi lain atau negara.
Sangat Rendah	Ancaman memiliki dampak yang sangat kecil (minimal) pada operasional, aset, individu, dan entitas lain, hingga pada tingkat yang bisa diabaikan.

Sumber: NIST SP 800-30 Revision 1 (Putri & Hakim, 2018).

Penentuan tingkat risiko

Tahapan penentuan tingkat risiko merupakan tahapan mengkombinasikan antara tingkat kemungkinan keseluruhan dan tingkat dampak untuk memberikan gambaran seberapa besar tingkat risiko. Berikut merupakan tabel penentuan risiko berdasarkan *NIST SP 800-30 Revision 1*.

Tabel 10.
Matriks penentuan tingkat risiko

Kemungkinan Keseluruhan	Tingkat Dampak				
	Sangat Rendah	**Rendah**	**Sedang**	**Tinggi**	**Sangat Tinggi**
Sangat Tinggi	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Tinggi	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Sedang	Sangat Rendah	Rendah	Sedang	Sedang	Tinggi
Rendah	Sangat Rendah	Rendah	Rendah	Rendah	Sedang
Sangat Rendah	Sangat Rendah	Sangat Rendah	Sangat Rendah	Rendah	Rendah

Sumber: NIST SP 800-30 Revision 1

III. HASIL DAN PEMBAHASAN

3.1. Identifikasi Sumber Ancaman

Berdasarkan hasil identifikasi sumber peristiwa ancaman terdapat 3 sumber peristiwa ancaman di Dinas Komunikasi dan Informatika Kabupaten Trenggalek yaitu sebagai berikut

Tabel 12.
Sumber ancaman dari luar

No	Sumber ancaman	Kemampuan	Niat	Penargetan
1.	Hacker	Sangat tingggi	Sangat rendah	Sedang

Sumber: Diolah oleh peneliti 2026

Tabel 13.
Sumber ancaman dari dalam

No	Sumber ancaman	Rentang efek
1.	Administrator dengan hak khusus	Tinggi
2.	Kapasitas server	Sedang

Sumber: Diolah oleh peneliti 2026

3.2. Identifikasi Peristiwa Ancaman

Berdasarkan hasil identifikasi peristiwa ancaman terdapat 7 peristiwa ancaman di Dinas Komunikasi dan Informatika Kabupaten Trenggalek yaitu sebagai berikut

Tabel 14.
Peristiwa ancaman

No	Peristiwa ancaman	Sumber ancaman	Relevansi
1.	*Web defacement*	*Hacker*	Terkonfirmasi
2.	*Brute froce*	*Hacker*	Terkonfirmasi
3.	*Data breach*	*Hacker*	Terkonfirmasi
4.	*Misconfiguration*	Administrator dengan hak khusus	Terkonfirmasi
5.	*Content injection*	*Hacker*	Terkonfirmasi
6.	*Cross site scripting*	*Hacker*	Terkonfirmasi
7.	*Server down*	Kapasitas server	Terkonfirmasi

Sumber: Diolah oleh peneliti 2026

3.3. Identifikasi Kerentanan

Berdasarkan hasil identifikasi kerentanan terdapat 7 kerentanan pada keamanan sistem informasi di Dinas Komunikasi dan Informatika Kabupaten Trenggalek yaitu sebagai berikut

Tabel 15.
Kerentanan

No	Kerentanan
1.	Belum semua sistem pengelola *website* diperbarui secara berkala
2.	Belum semua menggunakan password yang kuat
3.	Belum semua menerapkan pembatasan percobaan login
4.	Belum semua menerapkan *multi factor authentication*
5.	Belum semua data terenkripsi
6.	Belum semua menerapkan validasi dan sanitasi input dan output
7.	Kapasitas server terbatas

Sumber: Diolah oleh peneliti 2026

3.4. Penentuan Tingkat Kemungkinan

Berdasarkan hasil penentuan tingkat kemungkinan dari 7 peristiwa ancaman yang teridentifikasi, diperoleh bahwa dua peristiwa ancaman berada pada tingkat kemungkinan tinggi, yaitu web defacement dan data breach. Selanjutnya, lima peristiwa ancaman berada pada tingkat kemungkinan sedang, yaitu brute force, misconfiguration, content injection, cross site scripting, dan server down. Hasil tersebut menunjukkan bahwa sebagian besar peristiwa ancaman memiliki tingkat kemungkinan sedang untuk terjadi dan menimbulkan dampak terhadap sistem informasi. Rincian tingkat kemungkinan untuk masing-masing peristiwa ancaman dapat dilihat pada tabel berikut

Tabel 16.
Tingkat kemungkinan

No	Peristiwa ancaman	Kemungkinan terjadinya peristiwa ancaman	Kemungkinan peristiwa ancaman memberikan dampak buruk	Tingkat kemunkinan seluruhnya
1.	*Web defacement*	Tinggi	Tinggi	Tinggi
2.	*Brute froce*	Sedang	Sedang	Sedang
3.	*Data breach*	Sedang	Sangat tinggi	Tinggi
4.	*misconfiguration*	Sedang	Sedang	Sedang
5.	*Content injection*	Sedang	Sedang	Sedang
6.	*Cross site scripting*	Sedang	Sedang	Sedang
7.	*Server down*	Rendah	Sangat tinggi	Sedang

Sumber: Diolah oleh peneliti 2025

3.5. Penentuan Tingkat Dampak

Berdasarkan penentuan tingkat dampak peristiwa ancaman, diperoleh bahwa terdapat dua peristiwa ancaman dengan tingkat dampak sangat tinggi, yaitu data breach dan server down. Selanjutnya, dua peristiwa ancaman memiliki tingkat dampak tinggi, yaitu web defacement dan content injection. Adapun tiga peristiwa ancaman lainnya

memiliki tingkat dampak sedang, yaitu brute force, misconfiguration, dan cross site scripting. Hasil tersebut menunjukkan bahwa sebagian peristiwa ancaman berpotensi menimbulkan dampak yang signifikan terhadap keamanan dan keberlangsungan sistem informasi apabila terjadi. Rincian tingkat dampak masing-masing peristiwa ancaman dapat dilihat pada tabel berikut

Tabel 17.
Tingkat dampak

No	Peristiwa ancaman	Rentang maksimal dampak
1.	*Web defacement*	Tinggi
2.	*Brute froce*	Sedang
3.	*Data breach*	Sangat tinggi
4.	*Misconfiguration*	Sedang
5.	*Content injection*	Sedang
6.	*Cross site scripting*	Sedang
7.	*Server down*	Sangat tinggi

Sumber: Diolah oleh peneliti 2025

3.6. Penentuan Tingkat Risiko

Berdasarkan penentuan tingkat risiko peristiwa ancaman, diperoleh bahwa terdapat satu peristiwa ancaman dengan tingkat risiko sangat tinggi, yaitu data breach. Selanjutnya, dua peristiwa ancaman berada pada tingkat risiko tinggi, yaitu web defacement dan server down. Adapun empat peristiwa ancaman lainnya memiliki tingkat risiko sedang, yaitu brute force, misconfiguration, content injection, dan cross site scripting. Rincian tingkat risiko masing-masing peristiwa ancaman dapat dilihat pada tabel berikut

Tabel 18.
Tingkat risiko

No	Peristiwa ancaman	Kemungkinan keseluruhan	Tingkat dampak	Risiko
1.	*Web defacement*	Tinggi	Tinggi	Tinggi
2.	*Brute froce*	Sedang	Sedang	Sedang
3.	*Data breach*	Tinggi	Sangat tinggi	Sangat tinggi
4.	*Misconfiguration*	Sedang	Sedang	Sedang
5.	*Content injection*	Sedang	Tinggi	Sedang
6.	*Cross site scripting*	Sedang	Sedang	Sedang
7.	*Server down*	Sedang	Sangat tinggi	Tinggi

Sumber: Diolah oleh peneliti 2025

3.7. Diskusi Temuan Utama Penelitian

Pada penelitian ini ditemukan tujuh risiko keamanan sistem informasi dengan tingkat risiko yang beragam. Temuan ini sejalan dengan penelitian Rahmi et al (2024) yang juga menemukan risiko dengan tingkat yang beragam, mulai dari tinggi, sedang, hingga rendah, serta penelitian Tjahjono et al (2023) yang menunjukkan bahwa sistem informasi

pada instansi pemerintah menghadapi berbagai ancaman dengan tingkat risiko yang berbeda-beda. Temuan ini juga memperkuat penelitian penelitian Putra dan Soewito (2023) yang menyatakan bahwa *misconfiguration* merupakan salah satu kerentanan utama yang dapat meningkatkan risiko keamanan informasi. Namun, berbeda dengan beberapa penelitian sebelumnya, penelitian ini menemukan data breach sebagai risiko dengan tingkat sangat tinggi, yang menunjukkan bahwa perlindungan data menjadi isu yang lebih krusial.

3.8. Diskusi Temuan Menarik Lainya

Temuan lain yang menarik menunjukkan bahwa Dinas Komunikasi dan Informatika Kabupaten Trenggalek telah melakukan berbagai upaya untuk meminimalisir dampak risiko keamanan sistem informasi melalui penerapan *firewall,* bimbingan teknis keamanan sistem informasi, tes penetrasi menggunakan aplikasi *Burp Suite* dan pembentukan *Computer Security Incident Response Team (CSIRT).*

IV. KESIMPULAN

Peneliti menyimpulkan bahwa risiko keamanan sistem informasi di Dinas Komunikasi dan Informatika Kabupaten Trenggalek terdiri atas tujuh risiko, yaitu data breach dengan tingkat risiko sangat tinggi, *web defacement* dan *server down* dengan tingkat risiko tinggi, *serta brute force, misconfiguration, content injection*, dan *cross site scripting* dengan tingkat risiko sedang. Untuk meminimalisir dampak dari risiko-risiko tersebut, Dinas Komunikasi dan Informatika Kabupaten Trenggalek telah melakukan berbagai upaya mitigasi, antara lain melalui penerapan *firewall*, penyelenggaraan bimbingan teknis keamanan sistem informasi, pelaksanaan tes penetrasi menggunakan aplikasi *Burp Suite*, serta pembentukan *Computer Security Incident Response Team (CSIRT).*

Keterbatasan Penelitian: Penelitian ini terbatas pada penilaian risiko menggunakan *framework NIST SP 800-30 Revision 1* sehingga belum mengintegrasikan framework lain seperti *ISO/IEC 27005, ISO 31000,* atau *NIST Cybersecurity Framework*. Selain itu, identifikasi kerentanan masih berdasarkan hasil wawancara, observasi, serta dokumentasi, sehingga belum didukung oleh penggunaan alat *vulnerability assessment* seperti *Acunetix, Nessus, OpenVAS,* maupun *Burp Suite*. Penelitian ini juga hanya menggambarkan kondisi risiko pada saat penelitian dilakukan sehingga perubahan ancaman dan kerentanan di masa mendatang belum dapat terakomodasi secara menyeluruh.

Arah Masa Depan Penelitian *(Future work)*: Diharapkan penelitian selanjutnya disarankan untuk mengombinasikan *NIST SP 800-30 Revision 1* dengan *framework* lain seperti *ISO/IEC 27005, ISO 31000,* atau *NIST Cybersecurity Framework* agar menghasilkan penilaian risiko yang lebih komprehensif. Selain itu, identifikasi kerentanan dapat didukung dengan penggunaan alat *vulnerability assessment* seperti *Acunetix, Nessus, OpenVAS,* maupun *Burp Suite*.

V. UCAPAN TERIMA KASIH

Ucapan terima kasih terima kasih yang sebesar-besarnya kepada Dinas Komunikasi dan Informatika Kabupaten Trenggalek yang telah memberikan izin, dukungan, serta kesempatan kepada peneliti untuk melaksanakan penelitian. Ucapan terima kasih juga peneliti sampaikan kepada seluruh pegawai dan informan di lingkungan Dinas Komunikasi dan Informatika Kabupaten Trenggalek yang telah meluangkan waktu, memberikan informasi, serta membantu proses pengumpulan data sehingga penelitian ini dapat terselesaikan dengan baik.

VI. DAFTAR PUSTAKA

Abrory, Y., Kamil, W. A., & Zahrati, W. (2025). Usability Testing Website Pelayanan Publik SILETON Usability Testing Website Pelayanan Publik SILETON Kabupaten Agam Dengan Metode SEQ dan SUS. *Jurnal Terapan Pemerintahan Minangkabau*, *5*(1), 41–55. https://ejournal.ipdn.ac.id/jtpm/article/view/4867

Adi Saputra, L., Muhammad Akbar, F., Cahyaningtias, F., Puspa Ningrum, M., & Fauzi, A. (2023). Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan. *Jurnal Pendidikan Siber Nusantara*, *1*(2), 58–66. https://doi.org/10.38035/jpsn.v1i2.48

Ardieansyah, Asmungi, & Latip. (2023). *Metodologi Penelitian Sosial*. Deepublish Digital. https://inlislite.ipdn.ac.id/opac/detail-opac?id=11197

Casaril, F. (2025). International Journal of Critical Infrastructure Protection Developing security metrics for space systems : A study considering the NIST Cybersecurity Framework 2 . 0 and the NIS2. *International Journal of Critical Infrastructure Protection*, *51*(September), 100805. https://doi.org/10.1016/j.ijcip.2025.100805

Devi, R. K., Sensuse, D. I., Kautsarina, & Suryono, R. R. (2022). Information Security Risk Assessment (ISRA): A Systematic Literature Review. *Journal of Information Systems Engineering and Business Intelligence*, *8*(2), 207–217. http://dx.doi.org/10.20473/jisebi.8.2.207-217

M. Fadhli Ma'arif, Melwin Syafrizal, Jeki Kuswanto, & Aiko Nur Hendry Yansyah. (2025). Security Risk Analysis of QRIS Implementation in Public Locations Using ISO 31000:2018 Framework. *Journal of Applied Informatics and Computing*, *9*(4), 1670–1680. https://doi.org/10.30871/jaic.v9i4.9877

Muliati, S. F., Supriadi, F., & Junaedi, D. I. (2025). Strategi Manajemen Risiko Teknologi Informasi Berbasis Studi Literatur. *Publikasi Ilmu Keteknikan Industri, Teknik Elektro Dan Informatika*, *3*, 27–39. https://doi.org/10.61132/jupiter.v3i2.780

Purwanto, B. A., Putri, T. S., Indrayani, E., & Abrory, Y. (2025). Governance Innovation Through SiMAWAS. *Jurnal Bina Praja*. https://doi.org/10.21787/jbp.17.2025-2671

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005 : 2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, *14*(4), 625–633. http://dx.doi.org/10.14569/IJACSA.2023.0140468

Putri, M. K., & Hakim, A. R. (2018). Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO / IEC. *Jurnal Info Kripto*, *15*(3). https://doi.org/10.56706/ik.v15i3.34

Putro, A. A., A Ambarwati, & E Setiawan. (2021). Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1. *Jurnal Teknologi Dan Informasi (JATI)*, *11*(September), 125–136. https://doi.org/10.34010/jati.v11i2

Rahmi, T. A., Ikhwani, M., & Sistem, M. (2024). Analisis Manajemen Risiko Pada Sistem Informasi Manajemen Rumah Sakit(SIMRS) dengan ISO 31000 dan NIST 800-30 DI

RSUD H. Ok Arya Zulkarnain. *Jurnal Mahasiswa Teknik Informatika*, *9*(5), 8207–8215. https://doi.org/10.36040/jati.v9i5.15069

Sema, W., Yayeh, Y., & Abeshu, A. (2024). Cyber Security and Applications Cyber security : State of the art , challenges and future directions. *Cyber Security and Applications*, *2*(September 2023), 100031. https://doi.org/10.1016/j.csa.2023.100031

Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks - undermining public confidence in government. *Journal of Information Technology & Politics*, *20*(4). https://doi.org/10.1080/19331681.2022.2112796

Simangunsong, F. (2017). *Metodologi Penelitian Pemerintahan* (3rd ed.). Alfabeta, Bandung. https://inlislite.ipdn.ac.id/opac/detail-opac?id=776

Tjahjono, B., Ardiansyah, M., Firmansyah, G., & Akbar, H. (2023). *RISK MANAGEMENT OF INFORMATION SYSTEM IN DISKOMINFO STATISTIC AND ENCODING USING NIST SP 800-30*. *9*(1), 134–142. https://ejournal.nusamandiri.ac.id/index.php/jitk/article/view/4080