IMPLEMENTASI FRAMEWORK ISO 27001 SEBAGAI PROTEKSI KEAMANAN INFORMASI DALAM PEMERINTAHAN *(SYSTEMATIC LITERATURE REVIEW)*

Bilqis Aurabillah, Lintang Aprillia Putri, Novia Citra Fadhlilla, Anita Wulansari
Sistem Informasi, Universitas Pembangunan Nasional "Veteran" Jawa Timur
Jl. Rungkut Madya No.1, Surabaya, Jawa Timur, Indonesia
22082010207@student.upnjatim.ac.id

ABSTRAK

Era globalisasi, ditandai oleh kemajuan pesat dalam teknologi dan teknologi informasi, memberikan kemudahan akses informasi bagi masyarakat. Namun, keberlanjutan ini menimbulkan risiko terhadap privasi. Indonesia mengalami rendahnya keamanan informasi, terutama dalam lembaga pemerintahan. ISO 27001 memiliki kebermanfaatan dalam menjaga keamanan informasi pada lembaga pemerintah yaitu pemerintah dapat mengelola tata kelola yang baik, adanya pengukuran keberhasilan apakah tercapai tujuan dari keamanan informasi, mengetahui apa saja perbaikan dan pengelolaan yang harus dilakukan dalam keamanan informasi. Tujuan dari penelitian ini adalah untuk menganalisis kebutuhan sistem keamanan informasi dalam lembaga pemerintahan, terutama dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Metode yang digunakan dalam artikel jurnal ini adalah metode Systematic Literature Review atau sering disingkat dengan (SLR), merupakan metode yang melakukan pengumpulan, penelusuran berbagai artikel yang sesuai dengan topik atau tema yang dikaji setelah itu dievaluasi ditafsirkan dan kemudian dilakukan penyajian data. Hasil penelitian adalah Framework ISO 27001 selain mengamankan informasi, framework ini juga dapat mengevaluasi serta memelihara dari kebocoran keamanan data. Aturan yang baku dan formal membuat pelaksanaan keamanan sistem informasi lebih teratur dan dapat mengetahui kesalahan atau perbaikan yang harus dilakukan ketika skor yang didapatkan tidak sesuai dengan standar dari SNI ISO 20071.

Kata kunci : *ISO 27001, keamanan informasi, pemerintahan*

1. PENDAHULUAN

Era globalisasi ditandai dengan pesatnya perkembangan teknologi dan teknologi informasi, perkembangan teknologi dan teknologi informasi mempermudah manusia untuk mendapatkan segala informasi dari berbagai sumber, baik di dalam negeri maupun luar negeri. Masyarakat dapat mudah untuk mengakses dan mendapatkan informasi dengan cepat mengenai apapun yang dia kehendaki. Banyak sekali dampak positif yang didapatkan dari perkembangan teknologi dan informasi, namun terdapat kekurangan yang bisa mengancam privasi seseorang. Perlunya menjaga keamanan dan kerahasiaan informasi pada saat berkomunikasi secara online atau dalam media sosial.

Indonesia sendiri dalam keamanan informasi masih berada di angka yang sangat rendah, dibandingkan negara asia tenggara lainnya. Kebocoran informasi bukan hanya terjadi pada individu saja, namun dalam lembaga pemerintahan masih banyaknya peretas-peretas yang dapat mengakses informasi yang ada dalam aspek pemerintahan. Keamanan sistem informasi pada pemerintahan sangat penting karena menjaga data-data penting masyarakat, keamanan pemerintahan, menjaga pandangan masyarakat kepada pemerintahan publik dan lain sebagainya.

Sistem keamanan informasi perlu menerapkan prinsip-prinsip seperti kerahasiaan, orang yang memiliki kewenangan yang hanya bisa mengakses informasi-informasi tersebut. Integritas, keamanan dalam menjaga kelengkapan dan atau kerusakan informasi dari virus atau peretas. Ketersediaan, seluruh masyarakat dapat kapan saja dimana saja mengakses informasi yang ada di website atau platform yang disediakan oleh pemerintah. Pemenuhan prinsip tersebut dapat membantu menjaga keamanan data-data pemerintah dan juga masyarakat.

Untuk dapat mengelola, menjaga dan juga menerapkan prinsip-prinsip keamanan informasi pemerintah dapat menggunakan ISO 27001. ISO 27001 merupakan sistem manajemen keamanan informasi yang berstandarkan internasional dapat membantu untuk kebutuhan keamanan informasi dari sebuah lembaga pemerintahan atau informasi kebutuhan lainnya. ISO 27001 berstandarkan dan diakui oleh internasional karena prosesnya yang sistematis terdapat kebijakan, struktur organisasi dan lainnya.

ISO 27001 memiliki kebermanfaatan dalam menjaga keamanan informasi pada lembaga pemerintah yaitu pemerintah dapat mengelola tata kelola yang baik, adanya pengukuran keberhasilan apakah tercapai tujuan dari keamanan informasi, mengetahui apa saja perbaikan dan pengelolaan yang harus dilakukan dalam keamanan informasi. ISO 27001 juga merupakan hal yang efektif dan efisiensi untuk digunakan penggunaan waktu, dan biaya yang lebih rendah dibandingkan sistem lainnya.

Dengan demikian pada jurnal ini, penulis membahas secara detail, rinci, dan jelas mengenai bagaimana Implementasi Framework ISO 27001 sebagai Proteksi Keamanan Informasi Dalam Pemerintahan pusat daerah atau yang memiliki keterkaitan dengan pemerintahan.

2. TINJAUAN PUSTAKA

2.1. Framework ISO 27001

ISO/IEC 27001 adalah standar keamanan yang sering digunakan dan paling terkenal di dunia untuk sistem manajemen keamanan informasi (ISMS). Standar ISO/IEC 27001 memberikan panduan kepada perusahaan atau lembaga organisasi pemerintahan dari berbagai ukuran dan dari semua sektor aktivitas untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi [1]. Dengan menerapkan ISO/IEC 27001 berarti suatu organisasi atau bisnis telah menerapkan sistem untuk mengelola risiko terkait keamanan data yang dimiliki atau ditangani oleh perusahaan atau lembaga, dan sistem ini menghormati semua praktik dan prinsip terbaik yang tertuang dalam Standar Internasional ini.

ISO 27001, yang secara resmi dikenal sebagai ISO/IEC 27001:2022, adalah standar keamanan informasi yang dibuat oleh Organisasi Internasional untuk Standardisasi (ISO), yang memberikan kerangka kerja dan pedoman untuk menetapkan, menerapkan, dan mengelola sistem manajemen keamanan informasi (ISMS). Menurut dokumentasinya, ISO 27001 dikembangkan untuk "menyediakan model untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan sistem manajemen keamanan informasi." Spesifikasi tersebut mencakup rincian dokumentasi, tanggung jawab manajemen, audit internal, perbaikan berkelanjutan, dan tindakan perbaikan dan pencegahan. Standar ini memerlukan kerja sama antara seluruh bagian organisasi [2].

Untuk melakukannya, ISO 27001 menyediakan kerangka kerja komprehensif yang membantu organisasi mengembangkan dan memelihara SMKI yang aman. ISO 27001 dibagi menjadi 14 fase [3]:

1) Kebijakan Keamanan Informasi
2) Organisasi Keamanan Informasi
3) Penilaian dan Perawatan Risiko
4) Manajemen asset
5) Kontrol akses
6) Kriptografi
7) Keamanan fisik
8) Keamanan Operasi
9) Keamanan Komunikasi
10) Akuisisi, Pengembangan dan Pemeliharaan Sistem
11) Hubungan Pemasok
12) Kepatuhan terhadap Persyaratan Hukum dan Standar Industri
13) Manajemen Kualitas Informasi
14) Pemantauan dan Peninjauan Risiko

2.2. Keamanan Informasi

Keamanan informasi adalah praktik melindungi informasi dengan memitigasi risiko informasi. Hal ini melibatkan perlindungan sistem informasi dan informasi yang diproses, disimpan dan dikirimkan oleh sistem ini dari akses, penggunaan, pengungkapan, gangguan, modifikasi atau penghancuran yang tidak sah. Hal ini mencakup perlindungan informasi pribadi, informasi keuangan, dan informasi sensitif atau rahasia yang disimpan baik dalam bentuk digital maupun fisik. Keamanan informasi yang efektif memerlukan pendekatan yang komprehensif dan multidisiplin, yang melibatkan manusia, proses, dan teknologi [4].

Keamanan Informasi tidak hanya tentang mengamankan informasi dari akses yang tidak sah. Keamanan Informasi pada dasarnya adalah praktik mencegah akses, penggunaan, pengungkapan, gangguan, modifikasi, inspeksi, pencatatan, atau penghancuran informasi yang tidak sah. Informasi dapat berbentuk fisik atau elektronik. Informasi dapat berupa apa saja seperti detail Anda atau kami dapat mengatakan profil Anda di media sosial, data Anda di ponsel, biometrik Anda, dll. Jadi Keamanan Informasi mencakup begitu banyak bidang penelitian seperti Kriptografi, Komputasi Seluler, Forensik Siber, Media Sosial Online, dll.

Kami menggunakan keamanan informasi untuk melindungi aset informasi berharga dari berbagai ancaman, termasuk pencurian, spionase, dan kejahatan dunia maya. Keamanan informasi diperlukan untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi, baik disimpan secara digital maupun dalam bentuk lain seperti dokumen kertas. Berikut adalah beberapa alasan utama mengapa keamanan informasi itu penting [5]:

a. Melindungi informasi sensitif: Keamanan informasi membantu melindungi informasi sensitif agar tidak diakses, diungkapkan, atau dimodifikasi oleh individu yang tidak berwenang. Ini mencakup informasi pribadi, data keuangan, dan rahasia dagang, serta informasi rahasia pemerintah dan militer
b. Mitigasi risiko: Dengan menerapkan langkah-langkah keamanan informasi, organisasi dapat memitigasi risiko yang terkait dengan ancaman dunia maya dan insiden keamanan lainnya. Hal ini termasuk meminimalkan risiko pelanggaran data, serangan penolakan layanan, dan aktivitas jahat lainnya.

3. METODE PENELITIAN

Metode yang digunakan dalam artikel jurnal ini adalah metode Systematic Literature Review atau sering disingkat dengan (SLR), merupakan metode yang melakukan pengumpulan, penelusuran berbagai artikel yang sesuai dengan topik atau tema yang dikaji setelah itu dievaluasi ditafsirkan dan kemudian dilakukan penyajian data. Metode literature review merupakan metode yang sistematis karena adanya proses identifikasi, pengkajian, pengevaluasi dan penafsiran mengenai kumpulan artikel yang memiliki kriteria untuk menunjang pembuatan artikel jurnal sehingga mendapatkan hasil penelitian yang memuaskan.

3.1. Research Question

Setelah menentukan judul dan latar belakang permasalahan topik, pada tahap ini menentukan pertanyaan penelitian yang nantinya akan dibahas secara detail pada tahap penyajian data atau hasil dan pembahasan.

1. **RQ1**: Bagaimana Framework ISO 27001 Membantu Keamanan Informasi dalam Pemerintahan?
2. **RQ2**: Bagaimana Perbedaan Sebelum dan Sesudah menggunakan Framework ISO 27001?
3. **RQ3**: Bagaimana Rencana Perbaikan atau Pengelolaan Risiko Keamanan ISO 27001?

3.2. Inclusion and Exclusion Criteria

Tahap ini memberikan kemudahan dalam penelusuran artikel yang akan dicari, dan menentukan data artikel yang sesuai dengan topik masalah yang diangkat dalam penelitian ini. Adanya kriteria dapat memudahkan penulis untuk mengetahui apakah artikel ini layak digunakan atau tidak.

Tabel.1 Kriteria Artikel/Paper

No	Kriteria	Tipe
1	Tahun terbit artikel atau paper pada tahun 2019-2023	Inclusion
2	Artikel dan paper termasuk jenis publikasi full paper	Inclusion
3	Pembahasan artikel sesuai dengan topik atau tema yang diambil	Inclusion
4	Artikel bukan merupakan jenis literatur review	Exclusion
5	Artikel tidak termasuk ke dalam pembahasan atau topik yang diambil dalam jurnal ini	Exclusion
6	Pembahasan mengenai sistem informasi dan ilmu komputer	Exclusion

3.3. Quality Assessment

Tahap untuk mengevaluasi artikel yang telah didapatkan oleh penulis berdasarkan kriteria-kriteria yang telah ditentukan

1. Apakah artikel terbit pada jangka waktu 2019-2023?
2. Apakah artikel memuat topik Implementasi Framework ISO 27001 sebagai Proteksi Keamanan Informasi Dalam Pemerintahan?
3. Apakah artikel merupakan jenis full paper yang dapat diakses pada Google Scholar?

Setiap paper memiliki penilaian berdasarkan quality assessment di atas dengan poin sebagai berikut:

1. Nilai 1 : artikel atau paper memenuhi keseluruhan quality assessment
2. Nilai 0.5 : artikel atau paper yang hanya memenuhi sebagian quality assessment
3. Nilai 0 : artikel tidak memenuhi quality assessment

4. HASIL DAN PEMBAHASAN

4.1. Hasil evaluasi berdasarkan Kriteria Artikel

Berdasarkan hasil penelusuran ditemukan sebanyak 20 jurnal yang dicari dalam situs Google Scholar dengan memenuhi topik yang diambil dalam jurnal ini. 25 jurnal dengan jarak waktu yang up-to-date dimulai dari 2019 hingga 2023, dengan jenis artikel atau paper full paper.

Tabel. 2 Hasil Quality Assessment

No. Reference	Penulis	Judul	Tahun	QA1	QA2	QA3	Hasil
[6]	Nofry Arman, Widhy Hayuhardika, Aditya Rachmadi	Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI)	2019	1	1	1	3
[7]	Nabilla Diva Ramadhani, Widhy Hayuhardhika, Admaja Dwi Herlambang	Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)	2020	1	1	1	3
[8]	Greenhard Sitorus, Rokhman Fauzi, ST.,MT. , Ryan Adhitya ST., MT.	Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro Pada Dinas Komunikasi dan Informatika Jawa Barat	2020	1	1	1	3
[9]	Sitta Rif'atul Musyarofah, Rahadian Bisma	Analisis Kesenjangan Sistem Manajemen Keamanan Informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah	2021	1	1	1	3
[10]	Topan Nurdiansyah, M. Hendayun	Analisis dan Penerapan Manajemen Risiko Aplikasi Pemantauan Serta Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013	2022	1	1	1	3
[11]	Reynaldo Adi Putra Pratama Gala, Rizal Sengkey, Charles Punusingon	Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI	2020	1	1	1	3

No. Reference	Penulis	Judul	Tahun	QA1	QA2	QA3	Hasil
[12]	Faradhiya Aulia, Najwa Hamidah, Bintang Nuari, Reisa Permatasari	Analisis Keamanan Informasi Menggunakan Aplikasi Indeks KAMI pada Sektetariat DPRD Kabupaten Jombang	2023	1	1	1	3
[13]	Ala Aprila Ipungkarti	Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta	2023	1	1	1	3
[14]	Fadzri Ahdi Anshori, Suprapto, Andi Reza	Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)	2019	1	1	1	3
[15]	Marinda Yunella, Admaja Dwi Herlambang, Widhy Hayuhardhika	Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI	2019	1	1	1	3
[16]	Fahmi Rifai	Design of Application Information Security Self-Assessment Using VBA and MSXML2.XMLHTTP (Case Study: Diskominfo Kabupaten Kampar	2022	1	1	1	3
[17]	Anindhita Firdani, Suprapto, Andi Reza	Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 menggunakan Indeks KAMI Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang	2019	1	1	1	3
[18]	Shella Indah Dwi Octaviani, Suprapto, Admaja Dwi Herlambang	Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi dan Informatika Kota Batu Dengan Menggunakan Indeks KAMI	2019	1	1	1	3
[19]	Hadiati Agus Pratiwi, Lily Wulandari,	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor	2021	1	1	1	3
[20]	Tutik Tutik, Nurul Mutiah, Ibnur Rusi	ANALISIS DAN MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS (FMEA) DAN KONTROL ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas)	2022	1	1	1	3
[21]	Rezky Alkais Putra Rudiyanto, Vera Suryani	Analisis Sistem Manajemen Keamanan Informasi Pada Dinas Komunikasi Informasi Dan Statistik Kabupaten Lampung Tengah Menggunakan ISO/IEC 27001	2023	1	1	1	3
[22]	Lili Saputri, Mirna Annifah, Tursina Juliani	Analisis Manajemen Resiko Keamanan Informasi pada Kantor Dinas Pendidikan Gunung Tua	2023	1	1	1	3
[23]	Adi Muhajirin, Khamami Heru Santoso	KAJIAN TINGKAT KEMATANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI STUDI KASUS: SUKU DINAS KOMUNIKASI DAN INFORMATIKA JAKARTA SELATAN	2019	1	1	1	3
[24]	Faizah Salsabila Hidayat, Arfan Bachtiar	EVALUASI SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN PENILAIAN INDEKS KAMI v.4.2 PADA DINAS XYZ PROVINSI JAWA TENGAH	2023	1	1	1	3
[25]	Dian Saputra, Rizky Yulizar, Muhammad Said Saibuan, Ghivar Javad	PENILAIAN TINGKAT KESIAPAN KEAMANAN INFORMASI PADA DINAS KOMINFO KABUPATEN XYZ DENGAN INDEKS KAMI VERSI 4.2	2023	1	1	1	3

4.2. Hasil Analisis Data

RQ 1 : Bagaimana Framework ISO 27001 Membantu Keamanan Informasi dalam Pemerintahan

Berdasarkan beberapa penelitian di atas, bahwa Framework ISO 27001 dapat digunakan dengan efektif pada dinas atau kota/kabupaten di beberapa provinsi di Indonesia, karena mereka dapat menerapkan prinsip dari kriteria keamanan informasi. Dengan framework

ISO 27001, lembaga pemerintahan dapat mengetahui penilaian mengenai keamanan resiko informasi dengan diberi kategori dan peringkat level, sehingga mengetahui mana yang harus diperbaiki, dievaluasi, dan ditingkatkan. Menggunakan ISO 27001 sangat sistematis karena para lembaga pemerintah menjadi mengikuti kebijakan serta prosedur sesuai dengan standar ISO 27001, aturan yang formal sehingga memudahkan langkah yang harus dilakukan dari keamanan informasi, dan lembaga pemerintahan tidak harus dilakukan dengan terburu-buru atau spontanitas yang akan memberikan dampak tidak sesuai dengan tujuan yang ingin dicapai. Dengan Framework ISO 27001 juga dapat membantu dari beberapa ruang lingkup keamanan informasi seperti, tata kelola dari keamanan informasinya, meminimalisir resiko keamanannya, struktur atau kerangka dari keamanan, dan juga teknologi dari keamanan informasi. Dengan demikian, adanya ISO 27001 memberikan kemudahan dan sangat membantu secara efektif pada lembaga pemerintah untuk menjaga dan mengelola keamanan informasi dari data-data atau informasi yang ada di pemerintah sehingga tidak dapat diretas, dan bocor sehingga mengakibatkan kerahasiaan data negara atau masyarakat tersebar, dan image dari pemerintahan menjadi berkurang dalam faktor kepercayaan.

RQ2 : Bagaimana Perbedaan Sebelum dan Sesudah menggunakan Framework ISO 27001?

Berdasarkan beberapa evaluasi artikel atau paper di atas, sebelum menggunakan Framework ISO 27001, lembaga pemerintahan mencoba menggunakan Framework lain seperti NIST, KAMI dan lainnya namun dalam hasil sebelumnya, standar atau aturan tidak dimiliki secara sistematis, dan terkadang dilakukan secara spontanitas. Selain itu sebelum menggunakan Framework ISO 27001, dalam pelaksanaan manajemen risiko dengan standar yang diterapkan framework sebelumnya dapat membahayakan dan membocorkan kemana informasi dari lembaga pemerintahan. Sedangkan menggunakan ISO 27001 segala hal aspek memiliki standar nya masing-masing dan selalu disesuaikan dengan kebutuhan kontrol yang dibutuhkan, standar Framework ISO 27001 selain mengamankan informasi, framework ini juga dapat mengevaluasi serta memelihara dari kebocoran keamanan data. Aturan yang baku dan formal membuat pelaksanaan keamanan sistem informasi lebih teratur dan dapat mengetahui kesalahan atau perbaikan yang harus dilakukan ketika skor yang didapatkan tidak sesuai dengan standar dari SNI ISO 20071.

RQ3 : Bagaimana Rencana Perbaikan atau Pengelolaan Risiko Keamanan ISO 27001?

Pengelolaan risiko keamanan menggunakan ISO 20071 sebuah lembaga pemerintahan memiliki standar internasional yang diterbitkan dan diberi oleh ISO karena telah memenuhi persyaratan untuk menggunakan ISO 27001. pengelolaan risiko keamanan pada ISO mencakup seluruh aspek pada lembaga pemerintahan, tata kelola, struktur, infrastruktur dan lainnya, sehingga lebih sistematis dan semua lini aspek terjamin keamanannya. Selain itu, dalam pengelolaan risiko keamanan rencana dalam penerapannya menggunakan prinsip-prinsip yang harus dilakukan oleh lembaga pemerintahan. Karyawan dalam lembaga pemerintahan diberikan pedoman untuk menggunakan dan menyesuaikan kebutuhan dari lembaga pemerintahan. Dengan pengelolaan risiko keamanan ISO 27001 lembaga lebih efektif dan juga efisien untuk melindungi informasi.

5. KESIMPULAN DAN SARAN

Dengan menggunakan framework ISO 27001, lembaga pemerintahan dapat mengetahui penilaian mengenai keamanan resiko informasi dengan diberi kategori dan peringkat level, sehingga mengetahui mana yang harus diperbaiki, dievaluasi, dan ditingkatkan. Menggunakan ISO 27001 sangat sistematis karena para lembaga pemerintah menjadi mengikuti kebijakan serta prosedur sesuai dengan standar ISO 27001, aturan yang formal sehingga memudahkan langkah yang harus dilakukan dari keamanan informasi. Sebelum menggunakan Framework ISO 27001, dalam pelaksanaan manajemen risiko dengan standar yang diterapkan framework sebelumnya dapat membahayakan dan membocorkan kemana informasi dari lembaga pemerintahan. Sedangkan menggunakan ISO 27001 segala hal aspek memiliki standar nya masing-masing dan selalu disesuaikan dengan kebutuhan kontrol yang dibutuhkan.

DAFTAR PUSTAKA

[1] M. Bakri and N. Irmayana. 2017."Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001," *J. Tekno Kompak*, vol. 11, no. 2, p. 41, 2017, doi: 10.33365/jtk.v11i2.162.

[2] H. Sama *et al.*2021. "Studi Komparasi Framework Nist Dan Iso 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 6, no. 2, pp. 116–121, doi: 10.36341/rabit.v6i2.1752.

[3] S. T. Yuwono, N. Pratama, and V. Afifah, "Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001: 2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK," *J. IKRAITH-Informatika*, vol. 6, no. 2, pp. 21–28, 2022, [Online]. Available: https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/download/1570/1285.

[4] D. Rutanaji, S. S. Kusumawardani, and W. W. Winarno, "ISO 27001 sebagai Metode Alternatif bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan untuk Diterapkan di Arsip Nasional RI)," *Pros. Semin. Nas. ReTII ke-12 2017*, pp. 168–173, 2017, [Online]. Available:

https://journal.itny.ac.id/index.php/ReTII/article/view/604.

[5] A. Arini, "Pendeteksian Dini Tingkat Keamanan Informasi Berbasis Iso 27001 : 2013 Menggunakan Metode Ahp (Analytical Hierarchy Process)," *Cyber Security. dan Forensik Digit.*, vol. 2, no. 2, pp. 57–64, 2019, doi: 10.14421/csecurity.2019.2.2.1480.

[6] N. Arman, W. H. N. Putra, and A. Rachmadi, "Evaluasi Keamanan Informasi pada Diskominfo Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 6, pp. 5750–5755, 2019.

[7] N. D. Ramadhani, W. Hayuhardhika, N. Putra, and A. D. Herlambang, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)," vol. 4, no. 5, pp. 1490–1498, 2020.

[8] R. F. St, R. Adhitya, and N. St, "Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro Pada Dinas Komunikasi Dan Informatika," *e-Proceeding Eng.*, vol. 7, no. 2, pp. 7003–7008, 2020.

[9] S. R. Musyarofah and R. Bisma, "Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah," *Teknologi*, vol. 11, no. 1, pp. 1–15, 2021, doi: 10.26594/teknologi.v11i1.2152.

[10] M. H. Topan Nurdiansyah, "ANALISIS DAN PENERAPAN MANAJEMEN RISIKO APLIKASI PEMANTAUAN SERTA SISTEM MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN SNI ISO/IEC 27001:2013," *Sci. REGENDI*, vol. 3, no. 8.5.2017, pp. 2003–2005, 2022.

[11] R. A. P. P. Gala, R. Sengkey, and C. Punusingon, "Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI," *J. Tek. Inform.*, vol. 15, no. 3, pp. 189–198, 2020, [Online]. Available: https://ejournal.unsrat.ac.id/index.php/informatika.

[12] F. A. Rahma, N. H. Erwin, B. N. A. Nichada, and ..., "Analisis Keamanan Informasi Menggunakan Aplikasi Indeks Kami Pada Sekretariat Dprd Kabupaten Jombang," *... dan Sist. Inf.*, no. September, pp. 6–7, 2023, [Online]. Available: https://sitasi.upnjatim.ac.id/index.php/sitasi/article/view/396%0Ahttps://sitasi.upnjatim.ac.id/index.php/sitasi/article/download/396/111.

[13] A. A. Ipungkarti, "Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta," *J. Media Infotama*, vol. 19, no. 1, pp. 103–110, 2023, doi: 10.37676/jmi.v19i1.3481.

[14] F. A. Anshori and A. R. Perdanakusuma, "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 2, pp. 1701–1707, 2019, [Online]. Available: http://j-ptiik.ub.ac.id.

[15] M. Yunella, A. Dwi Herlambang, W. Hayuhardhika, and N. Putra, "Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI," *J. Pengemb. Teknol. Inf. Dan Ilmu Komputer.*, vol. 3, no. 10, pp. 9552–9559, 2019, [Online]. Available: http://j-ptiik.ub.ac.id.

[16] F. Rifai, M. Jazman, C. Studi, and D. Kabupaten, "DESIGN OF APPLICATION INFORMATION SECURITY SELF-ASSESSMENT USING VBA AND MSXML2 . XMLHTTP CASE STUDY : DISKOMINFO KABUPATEN KAMPAR PERANCANGAN APLIKASI KEAMANAN INFORMASI SELF-ASSESSMENT MENGGUNAKAN VBA DAN MSXML2 . XMLHTTP," vol. 4, no. 6, pp. 1523–1534, 2023.

[17] A. Firdani, Suprapto, and A. R. Perdanakusuma, "Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 Menggunakan Indeks KAMI (Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang)," *J. Pengemb. Teknol. Inf. dan Ilmu Komputer.*, vol. 3, no. 6, pp. 6009–6015, 2019, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/5617.

[18] S. I. D. Octaviani, Suprapto, and A. D. Herlambang, "Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Batu Dengan Menggunakan Indeks KAMI," *J. Pengemb. Teknol. Inf. dan Ilmu Komputer.*, vol. 3, no. 3, pp. 2741–2745, 2019, [Online]. Available: http://j-ptiik.ub.ac.id.

[19] W. L. Pratiwi Hadiati Agus, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor," *J. Pengemb. Teknol. ...*, vol. 2, no. 5, pp. 146–163, 2021, [Online]. Available: https://www.jiemar.org/index.php/jiemar/article/view/196.

[20] Tutik, N. Mutiah, and I. Rusi, "ANALISIS DAN MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS (FMEA) DAN KONTROL ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas)," *CODING J. Komputer. dan Apl.*, vol. 10, no. 02, pp. 249–261, 2022, [Online]. Available:

https://jurnal.untan.ac.id/index.php/jcskommipa/article/view/55082%0Ahttps://jurnal.untan.ac.id/index.php/jcskommipa/article/viewFile/55082/75676595021.

[21] R. A. P. Rudiyanto and V. Suryani, "Analisis Sistem Manajemen Keamanan Informasi Pada Dinas Komunikasi Informasi Dan Statistik Kabupaten Lampung Tengah Menggunakan ISO/IEC 27001," *Anal. Sist. Manaj. Keamanan Informasi Pada Dinas Komun. Inf. Dan Stat. Kabupaten Lampung Tengah. Menggunakan ISO/IEC 27001*, vol. 9, no. No.5, pp. 2039–2047, 2022.

[22] L. Saputri, M. A. Hsb, T. Juliani, and M. D. Irawan, "Analisis Manajemen Resiko Keamanan Informasi pada Kantor Dinas Pendidikan Gunung Tua," *J. Educ.*, vol. 5, no. 2, pp. 3437–3443, 2023, doi: 10.31004/joe.v5i2.1024.

[23] A. U. B. J. R. Muhajirin and K. H. S. N. M. J. Santoso, "Kajian Tingkat Kematangan Sistem Manajemen Keamanan Informasi Studi Kasus: Suku Dinas Komunikasi Dan Informatika Jakarta Selatan," *Proc. SNIT Salemba Raya Jakarta Pus.*, no. 5, pp. 159–163, 2012, [Online]. Available: http://www.nusamandiri.ac.id.

[24] A. Bakhtiar and F. Salsabila Hidayat, "EVALUASI SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN PENILAIAN INDEKS KAMI v.4.2 PADA DINAS XYZ PROVINSI JAWA TENGAH," *Ind. Eng. Online J.*, vol. 12, no. 4, 2023, [Online]. Available: https://ejournal3.undip.ac.id/index.php/ieoj/article/view/41401.

[25] M. H. D Saputra, RY Rahman, "PENILAIAN TINGKAT KESIAPAN KEAMANAN INFORMASI PADA DINAS KOMINFO KABUPATEN XYZ DENGAN INDEKS KAMI VERSI 4.2," *J. ILMU KOMPUTER, Sist. INFORMASI, Tek. Inform.*, vol. 2, no. 2, 2023.