JIMT | Jurnal Informatika Multimedia dan Teknik
e-ISSN: 3089-6010
OPEN ACCESS
URL Jurnal : https://yptb.org/index.php/jimt | e-mail : jurnalq17@gmail.com | https://doi.org/10.71456/jimt/v1i2.1340

SYSTEMATIC LITERATURE REVIEW: IMPLEMENTASI ISO/IEC 27001 DALAM PENGUATAN KEAMANAN INFORMASI DI INDONESIA

Systematic Literature Review: Implementation of ISO/IEC 27001 in Strengthening Information Security in Indonesia

Rifki Maulana[1*]

[*1]Universitas Sebelas April Sumedang, Sumedang, Jawa Barat, Indonesia

*email: rifkkimaulana@gmail.com

Abstrak

Perkembangan transformasi digital yang pesat di Indonesia membawa konsekuensi meningkatnya kebutuhan akan keamanan informasi yang andal. Berbagai organisasi, baik publik maupun swasta, mulai menyadari pentingnya membangun sistem keamanan informasi yang terstruktur dan berstandar internasional. ISO/IEC 27001 menjadi salah satu standar yang banyak diadopsi karena menyediakan kerangka kerja sistematis dalam manajemen risiko, perlindungan data sensitif, dan kepatuhan terhadap regulasi nasional seperti Undang-Undang Perlindungan Data Pribadi. Penelitian ini bertujuan mengkaji bagaimana implementasi ISO/IEC 27001 dilakukan di Indonesia serta sejauh mana standar ini berkontribusi pada penguatan keamanan informasi. Metode yang digunakan adalah *Systematic Literature Review* (SLR) dengan mengikuti pedoman PRISMA. Dari 58 artikel yang terindentifikasi pada tahap awal, enam artikel terpilih berdasarkan kriteria inklusi untuk dianalisis lebih lanjut. Hasil tinjauan menunjukkan bahwa ISO/IEC 27001 telah diterapkan di berbagai sektor (Pemerintahan, Pendidikan, Kesehatan, Lembaga sosial, dan swasta) dan memberikan dampak positif terhadap peningkatan keamanan informasi organisasi. Tantangan utama dalam implementasi mencakup rendahnya Tingkat kesiapan awal, keterbatasan sumber daya manusia, serta kurangnya kebijakan internal yang mendukung. Namun demikian, komitmen kuat dari manajemen puncak dan kedisiplinan dalam mematuhi kerangka kerja standar terbukti menjadi faktor kunci keberhasilan implementasi. Studi ini diharapkan dapat menjadi rujukan bagi akademisi, praktisi, dan pembuat kebijakan dalam merumuskan strategi keamanan informasi yang lebih efektif dan berkelanjutan di Indonesia.

Kata Kunci:
ISO/IEC 27001
Keamanan Informasi
SLR

Keywords:
ISO/IEC 27001
Information Security
SLR

Abstract

The rapid development of digital transformation in Indonesia has resulted in an increasing need for reliable information security. Various organizations, both public and private, are beginning to realize the importance of building a structured and internationally standardized information security system. ISO/IEC 27001 is one of the most widely adopted standards because it provides a systematic framework for risk management, sensitive data protection, and compliance with national regulations such as the Personal Data Protection Act. This study aims to examine how the implementation of ISO/IEC 27001 is carried out in Indonesia and the extent to which this standard contributes to strengthening information security. The method used is the Systematic Literature Review (SLR) following the PRISMA guidelines. Of the 58 articles identified in the initial stage, six articles were selected based on inclusion criteria for further analysis. The results of the review show that ISO/IEC 27001 has been implemented in various sectors (Government, Education, Health, Social Institutions, and the private sector) and has had a positive impact on improving organizational information security. The main challenges in implementation include low levels of initial readiness, limited human resources, and lack of supporting internal policies. However, strong commitment from top management and discipline in adhering to the standard framework have proven to be key factors in successful implementation. This study is expected to be a reference for academics, practitioners, and policy makers in formulating more effective and sustainable information security strategies in Indonesia.

Submit Tgl.: 25-Juni-2025 | Diterima Tgl.: 26-Juni-2025 | Diterbitkan Tgl.: 28-Juni-2025

Cara mengutip Maulana, R. (2025). Systematic Literature Review: Implementasi ISO/IEC 27001 dalam Penguatan Keamanan Informasi di Indonesia. *JIMT: Jurnal Informatika, Multimedia Dan Teknik*, *1*(2), 196–201. https://doi.org/10.71456/jimt.v1i2.1340

PENDAHULUAN

Transformasi digital telah menjadi pendorong utama modernisasi di Indonesia yang mencakup berbagai sektor seperti pemerintahan *(e-government),* keuangan, pendidikan, kesehatan, dan lain-lain. Perkembangan ini menjanjikan peningkatan efisiensi operasional dan kualitas layanan. Namun, dibalik manfaat tersebut muncul tantangan besar di ranah keamanan informasi. Meningkatnya konektivitas dan volume data yang memperluas permukaan serangan, membuat organisasi rentan terhadap ancaman siber yang saat ini kian canggih. Kasus kebocoran data pribadi, serangan ransomware yang dapat melumpuhkan layanan, dan berbagai bentuk penipuan digital kini semakin marak terjadi, mengancam kepercayaan publik serta menimbulkan kerugian finansial dan reputasi yang serius. Keamanan informasi dengan demikian tidak lagi dipandang semata sebagai isu teknis, namun sudah menjadi komponen strategis yang krusial bagi kelangsungan operasional organisasi di era digital.

Sebagaimana respons terhadap meningkatnya ancaman ini, banyak organisasi di Indonesia mulai mengadopsi kerangka kerja standar internasional **ISO/IEC 27001** untuk membangun **Sistem Manajemen Keamanan Informasi (SMKI)** yang lebih kuat. Standar ini menawarkan pendekatan berbasis risiko dalam pengelolaan keamanan aset informasi secara holistik, mencakup aspek manusia, proses, dan teknologi. Adopsi ISO/IEC 27001 tidak hanya didorong oleh kebutuhan internal untuk mitigasi risiko, namun juga oleh tuntutan regulasi eksternal. Di Indonesia, hal ini diperkuat dengan disahkannya Undang-Undang No.27 tahun 2022 tentang **Perlindungan Data Pribadi (UU PDP)**. Regulasi tersebut mengharuskan organisasi menerapkan langkah-langkah teknis dan organisatoris yang memadai. Implementasi standar seperti ISO/IEC 27001 dimana hal tersebut merupakan salah satu cara terbaik untuk menunjukkan kepatuhan terhadap regulasi dan tata kelola data yang bertanggung jawab.

Bukti penerapan ISO/IEC 27001 dapat ditemukan di berbagai sektor penting di Indonesia yang menunjukkan relevansi luas tentang standar ini. Misalnya, di sektor pemerintahan, sebuah badan kepegawaian daerah menerapkan ini untuk mengukur keamanan informasi menggunakan Indeks KAMI yang memberikan evaluasi objektif dan dasar perbaikan sistem keamanan (Rochmadi & Pasa, 2021). Di sektor pendidikan ISO/IEC 27001 digunakan untuk melakukan penilaian risiko yang terorganisir pada sistem informasi akademik demi melindungi data mahasiswa (Ardius & Syamsuar, 2023). Sementara itu, di sektor kesehatan, standar ini diterapkan untuk evaluasi keamanan data pasien di rumah sakit (Daniswara et al., 2023). Pada sektor sosial, lembaga amil zakat nasional dengan ratusan ribu data donatur mengadopsi ISO/IEC 27001 guna memastikan perlindungan data pribadi donatur yang mereka kelola. Contoh ini menggambarkan bahwa standar ISO/IEC 27001 diimplementasikan secara luas, mulai dari institusi pemerintah, universitas, rumah sakit, hingga organisasi sosial.

Walaupun telah banyak studi kasus implementasi, pemahaman menyeluruh mengenai penerapan ISO/IEC 27001 di Indonesia masih terbatas dan terfragmentasi. Temuan dari berbagai penelitian cenderung terpisah dalam konteks sektoral masing-masing dan belum terhimpun dalam sintesis komprehensif yang menggambarkan tantangan, faktor keberhasilan, serta dampak implementasi standar ini lintas sektor. Sebagai contoh, sudi pada perusahan ekspedisi menyoroti tantangan pada perubahan proses bisnis dan tata kelola selama implementasi (Sinaga & Taan, 2024), sementara penelitian di sektor pendidikan atau kesehatan lebih fokus pada aspek teknis dan manajerial spesifik seperti pengelolaan risiko teknis atau peningkatan kesadaran SDM akan keamanan informasi (Ardius & Syamsuar, 2023; Daniswara et al., 2023). Keterbatasan-keterbatasan ini menciptakan research

Gap, dimana organisasi yang berniat mengadopsi standar tersebut kesulitan mengambil pembelajaran dari pengalaman implementasi sebelumnya secara menyeluruh.

Untuk menjembatani celah pengetahuan tersebut, penelitian ini menggunakan metode Tinjauan Literatur Sistematis *(Systematic Literature Review/SLR)*. Dalam pendekatan SLR dilakukan identifikasi, evaluasi, dan sintesis terhadap bukti penelitian yang relevan secara terstruktur. Penelitian ini berupaya memberikan analisis komprehensif terhadap literatur yang ada dan menjawab tiga pertanyaan utama, yaitu: (1) Bagaimana implementasi ISO/IEC 27001 dapat memperkuat keamanan informasi di berbagai sektor di Indonesia?, (2) Apa saja tantangan utama yang dihadapi dan faktor-faktor yang berkontribusi terhadap keberhasilan implementasinya?, (3) Bagaimana standar ini berperan dalam pengelolaan risiko keamanan data?. Hasil penelitian ini diharapkan dapat membentuk peta jalan berbasis bukti bagi praktisi, akademisi, dan regulator dalam upaya penguatan keamanan informasi secara efektif.

METODE PENELITIAN

Penelitian ini menggunakan **Tinjauan Literatur Sistematis** atau ***Systematic Literature Review (SLR)*** yang mengikuti pedoman **PRISMA** *(Preferred Reporting Items for Systematic Reviews and Meta-Analyses)*. Metode ini bertujuan untuk mengidentifikasi, mengevaluasi, dan menggabungkan bukti-bukti empiris mengenai implementasi ISO/IEC 27001 di Indonesia. Penelitian ini ingin menjawab tiga pertanyaan utama (RQ):(RQ1) Bagaimana implementasi ISO/IEC 27001 dapat memperkuat keamanan informasi di sektor-sektor di Indonesia?, (RQ2) Apa saja tantangan utama yang dihadapi dan faktor-faktor apa saja yang berkontribusi pada keberhasilan implementasinya?, (RQ3) Bagaimana standar ini berperan dalam pengelolaan risiko keamanan data?. Proses Pencarian Literatur dilakukan dengan cermat untuk mencakup publikasi dari tahun 2020 sampai 2025 perangkat lunak **Publish or Perish (PoP)** yang menargetkan basis data Google Scholar dan Crosreff. Kata kunci yang digunakan dalam pencarian adalah *("ISO 27001" OR "ISO 27001 Indonesia"*. Proses seleksi artikel mengikuti kriteria yang telah ditentukan. Kriteria inklusi utama adalah artikel yang terindeks, membahas implementasi ISO/IEC 27001 di Indonesia, menggunakan data yang dapat diverifikasi, serta membahas tentang atau dampak dari implementasi tersebut. Sementara itu, artikel yang hanya berisi opini, tidak fokus pada standar ISO/IEC 27001, atau memiliki metodologi penelitian yang kurang kuat, disaring menggunakan kriteria eksklusi. Semua artikel yang ditemukan kemudian dikelola menggunakan manajer referensi Mendeley.

Pada awalnya, 58 artikel berhasil diidentifikasi. Setelah dilakukan penyaringan berdasarkan kriteria yang telah ditentukan, akhirnya terpilih 6 artikel yang memenuhi syarat. Keenam artikel ini kemudian di evaluasi kualitasnya menggunakan instrumen penilaian kualitas *(Quality Assesment/QA)* yang telah dirancang. Instrumen ini terdiri dari lima pertanyaan yang menilai relevansi kontekstual, validitas metodologi, kontribusi praktis, dan kualitas publikasi dari setiap artikel. Setiap artikel dinilai dengan sistem skor (1 = terpenuhi sepenuhnya, 0,5 = terpenuhi sebagian, 0 = tidak terpenuhi) untuk memastikan hasil studi berkualitas tinggi yang dianalisis.

Tahap terakhir adalah ekstraksi dan sintesis data dari artikel yang telah lolos penilaian kualitas. Informasi yang relevan dengan setiap pertanyaan penelitian diekstraksi menggunakan formulir yang telah disiapkan. Data kualitatif yang terkumpul kemudian di sintesis dengan menggunakan analisis tematik. Proses ini bertujuan untuk mengidentifikasi dan menganalisis pola atau tema yang muncul terkait tantangan, faktor keberhasilan, serta dampak dari implementasi ISO/IEC 27001 di berbagai sektor di Indonesia, yang nantinya akan disajikan dalam bagian hasil dan pembahasan.

HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil dari tinjauan literatur sistematis yang telah dilakukan. Paparan disusun secara sekuensial mengikuti tahapan metodologi, dimulai dari hasil seleksi dan penilaian kualitas studi, yang dilanjutkan dengan sintesis temuan utama untuk menjawab pertanyaan studi.

Hasil Seleksi dan Kualitas Studi

Proses seleksi studi yang mengikuti alur PRISMA dimulai dengan identifikasi 58 artikel melalui proses pencarian. Setelah melalui proses penyaringan duplikat, judul, abstrak, dan penilaian kelayakan teks lengkap, sebanyak 6 studi primer terpilih. Dari ke enam studi ini kemudian dinilai kualitasnya menggunakan instrumen *Quality Assesment (QA)* yang telah ditetapkan.

Tabel I. Hasil Penilaian Kualitas dan Karakteristik Studi

No	Penulis (Tahun)	Sektor	QA 1	QA 2	QA 3	QA 4	QA 5
1	Daniswara et al. (2023)	Kesehatan	1	1	1	1	1
2	Ardius & Syamsuar (2023)	Pendidikan	1	1	1	1	1
3	Rochmadi & Pasa (2021)	Pemerintahan	1	1	1	1	1
4	Kamal et al. (2024)	Lembaga Sosial	1	1	1	1	1
5	Sinaga & Taan (2024)	Swasta	1	1	1	1	1
6	Mude & Masyur (2025)	Umum	1	1	1	1	1

Tabel 2. Sintesis Temuan berdasarkan pertanyaan

RQ	Penulis (Tahun)	Sektor	Fokus	Temuan
RQ 1	Rochmadi & Pasa (2021)	Pemerintah	Indeks KAMI	Kesiapan rendah (Skor 1,75) butuh kebijakan tambahan
RQ 1	Ardius & Syamsuar (2023)	Pendidikan	Penilaian Risiko Sistem Informasi	Risiko tinggi, kontrol keamanan ditentukan berdasarkan hasil penelitian
RQ 1	Kamal et al. (2024)	Sosial	Audit keamanan data donator	Kontrol risiko baik, tetapi manajemen insiden masih lemah
RQ 2	Daniswara et al. (2023)	Kesehatan	Evaluasi kesiapan kebijakan	Tidak ada kebijakan keamanan formal, perlu pelatihan
RQ 2	Sinaga & Taan (2024)	Swasta	Resistensi SDM dan Pelatihan	SDM belum siap, pegawai enggan mengikuti prosedur
RQ 3	Ardius & Syamsuar (2023)	Pendidikan	Pengelolaan risiko informasi academia	ISO Efektif mengidentifikasi risiko akademik, bantu mitigasi
RQ 3	Kamal et al. (2024)	Sosial	Audit risiko dan insiden	Audit bantu tata kelola data donatur berbasis risiko
RQ 3	Mude & Masyur (2025)	Umum	Deteksi Ancaman Otomatis	Sistem bantu deteksi dini serangan siber secara otomatis

RQ1: Penguatan Keamanan Informasi di Berbagai Sektor

ISO/IEC 27001 terbukti berkontribusi signifikan dalam memperkuat sistem keamanan informasi organisasi lintas sektor di Indonesia. Standar ini menghadirkan menghadirkan kerangka kerja yang sistematis untuk menilai kesiapan, mengidentifikasi celah, dan menetapkan kontrol pengamanan informasi secara terukur. Studi (Rochmadi & Pasa, 2021) menunjukkan bahwa penggunaan Indeks KAMI di instansi pemerintah menghasilkan skor kesiapan 1,75, angka tersebut menunjukkan masih rendahnya kapabilitas awal namun memberikan arah perbaikan konkret. Di sektor pendidikan, (Ardius & Syamsuar, 2023) menggunakan ISO/IEC 27001 untuk melakukan penilaian risiko sistem informasi akademik, sehingga kontrol keamanan dapat ditetapkan berdasarkan klasifikasi risiko. Studi (Kamal et al., 2024) membuktikan bahwa penerapan ISO di lembaga zakat YDSF memperkuat kontrol akses dan manajemen risiko, walaupun manajemen insiden masih menjadi titik lemah. Sintesis lintas studi ini memperlihatkan bahwa ISO/IEC 27001 mampu disesuaikan dengan karakteristik sektor yang berbeda dan membantu organisasi mencapai peningkatan keamanan informasi yang terstruktur.

RQ2: Tantangan dan Faktor Keberhasilan Implementasi

Implementasi ISO/IEC 27001 di Indonesia masih menghadapi sejumlah tantangan, terutama pada organisasi yang berada dalam tahap kematangan rendah. (Daniswara et al., 2023) menemukan bahwa rumah sakit kekurangan kebijakan informasi dan belum memiliki pelatihan internal. Di sektor swasta, (Sinaga & Taan, 2024) mencatat bahwa resistensi pegawai dan kurangnya SDM menjadi hambatan utama. Namun, studi lain menyoroti faktor-faktor keberhasilan implementasi. (Kamal et al., 2024) menegaskan bahwa dukungan dari manajemen puncak seringkali didorong oleh tekanan regulasi seperti UU Perlindungan Data Pribadi (UU PDP). (Ardius & Syamsuar, 2023) juga menunjukkan bahwa organisasi yang menjalankan siklus *Plan-Do-Check-Act (PDCA)* dengan disiplin memiliki efektivitas implementasi yang lebih tinggi. Oleh karena itu, keberhasilan ini sangat tergantung pada sinergi antara kesiapan internal, dukungan pimpinan, dan kepatuhan regulatif.

RQ3: Peran Standar dalam pengelolaan Risiko dan Keamanan Data

ISO/IEC 27001 memberikan peran kunci dalam mengelola risiko dan melindungi data organisasi. Standar ini memandu organisasi untuk mengidentifikasi aset informasi, mengevaluasi ancaman dan kerentanan, dan menyusun kontrol mitigasi risiko yang relevan. Studi (Ardius & Syamsuar, 2023) menunjukkan bahwa penerapan ISO di sektor pendidikan membantu melindungi data mahasiswa melalui penilaian risiko sistematis. (Kamal et al., 2024) menambahkan bahwa ISO memfasilitasi pengelolaan data donatur di lembaga sosial secara komprehensif dan berbasis risiko. Selain itu, (Mude & Masyur, 2025) menghadirkan inovasi sistem deteksi ancaman otomatis berbasis ISO 27001. Sistem tersebut merupakan deteksi dini serangan keamanan informasi dan memperkuat respons organisasi. Dalam temuan-temuan tersebut membuktikan bahwa ISO bukan sekedar alat audit, melainkan fondasi strategis pengelolaan risiko dan pengamanan data yang berkelanjutan

KESIMPULAN

Berdasarkan hasil dan pembahasan studi, maka dapat disimpulkan bahwa implementasi ISO/IEC 27001 memberikan kontribusi yang signifikan dalam memperkuat keamanan informasi di berbagai sektor di Indonesia melalui pendekatan manajemen risiko yang terstruktur, adaptif, dan menyeluruh. Standar ini mampu membantu organisasi dalam menilai kesiapan keamanan informasi, mengidentifikasi ancaman dan kerentanan, serta menetapkan kontrol yang relevan untuk melindungi aset informasi. Temuan menunjukkan bahwa keberhasilan implementasi sangat dipengaruhi oleh komitmen manajemen, kedisiplinan dalam menjalankan siklus PDCA, dan dukungan regulasi yang jelas. Meskipun terdapat tantangan berupa keterbatasan sumber daya manusia, rendahnya kesadaran keamanan, serta resistensi terhadap perubahan, organisasi yang mampu mengatasi hambatan tersebut cenderung memperoleh manfaat jangka panjang dari sisi efisiensi, keandalan sistem, dan kepatuhan hukum. Oleh karena itu, disarankan agar organisasi yang belum menerapkan ISO/IEC 27001 segera mempertimbangkan adopsi standar ini sebagai bagian dari strategi keamanan digital. Selain itu, pemerintah dan regulator diharapkan terus mendorong dan memfasilitasi proses implementasi melalui insentif, panduan nasional, serta program peningkatan kapasitas SDM. Penelitian lanjutan juga perlu dilakukan untuk mengeksplorasi model implementasi yang paling efektif di masing-masing sektor, agar standar ini tidak hanya menjadi alat formal kepatuhan, namun juga menjadi motor penggerak transformasi digital yang aman dan berkelanjutan.

REFERENSI

Ardius, E., & Syamsuar, D. (2023). ASSESSMENT RISK TERHADAP PENGGUNAAN SISTEM INFORMASI AKADEMIK UNIVERSITAS EA MENGGUNAKAN METODE ISO 27001. *Jurnal Teknologi Informasi Mura*, *15*(1), 1–13. https://doi.org/10.32767/jti.v15i1.1948

Daniswara, M. C., Putrawanto, D. I., Najib, M., Achmadha, Z., Islami, M. C. S., & Mukaromah, S. (2023). Evaluasi Keamanan Informasi di Lingkungan Rumah Sakit: Pendekatan Audit ISO 27001 di RS Rahman Rahim Sidoarjo. *Journal of Digital Ecosystem for Natural Sustainability*, *3*(2), 64–69. https://doi.org/10.63643/jodens.v3i2.192

Kamal, M., Muhamad, M., Sudianto, Y., Fauzan, M. A., Anggito, Y., Yasin, W., & Hermawan, H. (2024). Information Technology Security Audit at the YDSF National Zakat Institution Using the ISO 27001 Framework. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *13*(1), 98–103. https://doi.org/10.32736/sisfokom.v13i1.1987

Mude, M. A., & Masyur, S. H. (2025). Perancangan Aplikasi Untuk Mendeteksi Keamanan Sistem Komputer Berbasis ISO 27001. *Journal Automation Computer Information System*, *5*(1), 45–56. https://doi.org/10.47134/jacis.v5i1.97

Rochmadi, T., & Pasa, I. Y. (2021). PENGUKURAN RISIKO DAN EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI DI BKD XYZ BERDASARKAN ISO 27001 / SNI. *Cyber Security Dan Forensik Digital*, *4*(1), 38–43. https://doi.org/10.14421/csecurity.2021.4.1.2439

Sinaga, R., & Taan, F. (2024). Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala. *NUANSA INFORMATIKA*, *18*(2), 46–54. https://doi.org/10.25134/ILKOM.V18I2.205