Indonesian Journal of Digital Business

Journal homepage: https://ejournal.upi.edu/index.php/IJDB

# Praktik Manajemen Resiko Keamanan Siber: Wawasan Dari Organisasi Bersertifikat ISO 27001

*Shevani Resta Maulana Putri[1], Marceli Putri Bernandy[2*], Cindy Aulia[3], Muhammad Ghaza Raihan Fikri[4], Jasvanie Jasmine[5]*

[1,2,3,4,5] Department of Digital Business, Faculty of Economics, Universitas Negeri Surabaya

Jalan Ketintang, Surabaya 60231, Indonesia

Correspondence: E-mail: shevaniresta.22020@mhs.unesa.ac.id

## ABSTRAK

*Di era digital yang semakin kompleks dan dinamis, manajemen risiko keamanan siber telah menjadi aspek penting yang berdampak pada operasional dan keberlanjutan organisasi. Studi ini mengkaji praktik manajemen risiko keamanan siber dari sudut pandang organisasi yang telah memperoleh sertifikasi ISO 27001, standar internasional yang menetapkan standar sistem manajemen keamanan informasi (ISMS). Fokus penelitian ini adalah ISO 27001, salah satu standar keamanan informasi terkemuka di dunia. Studi ini menyelidiki makna ISO 27001, manajemen risiko, dan proses penerapan sertifikasi ini dalam organisasi melalui tinjauan literatur.Temuan menunjukkan bahwa penerapan ISO 27001 memiliki dampak yang signifikan terhadap tingkat kesadaran organisasi terhadap keamanan manajemen informasi. Proses penerapan ISO 27001 mencakup serangkaian langkah dan pendekatan yang dirancang untuk membantu organisasi mengelola risiko keamanan siber secara efektif. Studi ini menyoroti pentingnya penerapan ISO 27001 ke dalam praktik manajemen risiko keamanan siber untuk meningkatkan keamanan informasi dan mencegah ancaman siber. Studi ini juga menilai tingkat kesadaran organisasi terhadap standar ISO 27001 dan bagaimana dampaknya terhadap penerapan praktik manajemen risiko keamanan siber. Temuan kami menunjukkan bahwa organisasi dengan sertifikasi ISO 27001 memiliki kesadaran yang lebih tinggi akan pentingnya*

## INFO ARTIKEL

***Riwayat Artikel:***
*Received 11 Januari 2025*
*First Revised 15 Januari 2025*
*Accepted 20 April 2025*
*Available online 30 April 2025*
*Publication Date 30 April 2025*

***Kata Kunci:***
*Cybersecurity Risk Management; ISO 27001; ISO Implementation; Information Security; Organizational Awareness.*

*manajemen risiko keamanan siber, sehingga mendukung penerapan praktik manajemen risiko yang lebih efektif. Studi ini diharapkan dapat memberikan wawasan dan panduan praktis bagi organisasi dalam menerapkan dan memanfaatkan manajemen risiko keamanan siber sesuai dengan standar ISO 27001. Oleh karena itu, penelitian ini berkontribusi terhadap peningkatan kesadaran dan penerapan standar keamanan informasi yang lebih baik di era digital saat ini.*



## 1. PENDAHULUAN

Menurut Anwar dan Gill (2021) manajemen risiko dalam konteks kebutuhan organisasi untuk memahami konteks organisasi, kebutuhan pemangku kepentingan, dan harapan merupakan suatu pendekatan yang penting dalam memastikan bahwa organisasi dapat mengidentifikasi, menilai, dan mengelola risiko yang terkait dengan informasi pribadi secara efisien dan efektif . Manajemen risiko bertujuan untuk mengoptimalkan hasil dengan meminimalkan risiko negatif dan memaksimalkan peluang positif. Sedangkan Manajemen keamanan informasi adalah pendekatan yang terstruktur, hemat biaya, dan sistematis untuk mendirikan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi melalui adopsi Sistem Manajemen Keamanan Informasi (ISMS).

ISMS membantu organisasi dari berbagai ukuran dan industri untuk melindungi informasi mereka dengan cara yang terencana dan terjangkau (Junaid, 2023). Manajemen risiko dan manajemen keamanan informasi saling terkait karena manajemen risiko keamanan informasi melibatkan proses identifikasi, evaluasi, dan pengelolaan risiko yang dapat mempengaruhi keberlangsungan operasional dan reputasi perusahaan terkait dengan keamanan informasi.

Dengan menerapkan manajemen risiko keamanan informasi, organisasi dapat mengidentifikasi potensi ancaman keamanan informasi, mengevaluasi dampaknya, dan mengembangkan strategi untuk mengurangi risiko tersebut, sehingga membantu melindungi informasi dari serangan dan kerugian yang mungkin terjadi (Junaid, 2023). Perlindungan informasi juga harus ditekankan dengan menerapkan kontrol keamanan administratif, teknis, fisik, dan legal sesuai dengan prinsip-prinsip privasi. Organisasi perlu mendefinisikan, menetapkan, dan mengimplementasikan kontrol keamanan yang tepat di semua domain praktik untuk melindungi informasi yang sedang diproses (Allendevaux, 2021).

Kesadaran terhadap pentingnya manajemen risiko sangat penting dalam perlindungan data pribadi dan keamanan informasi, terutama di era digital yang semakin berkembang. Organisasi perlu meningkatkan kesadaran dan implementasi manajemen risiko di berbagai tingkatan, baik negara bagian maupun federal, untuk melindungi keamanan dan privasi warga. Salah satu sistem manajemen keamanan dengan standar internasional yaitu ISO 27001.

Menurut Liao dan Chueh (2012) ISO 27001 adalah standar internasional untuk manajemen keamanan informasi yang menetapkan persyaratan untuk mendirikan, menerapkan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (ISMS) dalam suatu organisasi. Standar ini dirancang untuk membantu organisasi melindungi informasi penting dan mengelola risiko keamanan informasi dengan efektif. Manajemen risiko keamanan cyber dan wawasan dari organisasi bersertifikat ISO sangat penting bagi sebuah organisasi karena membantu melindungi informasi, aset, dan reputasi perusahaan dari serangan keamanan yang dapat merugikan secara ekonomi dan reputasi dari bentuk-bentuk ancaman keamanan informasi meliputi serangan siber seperti malware, phishing, ransomware, serangan DDoS, pencurian data, dan insider threats (Junaid, 2023).

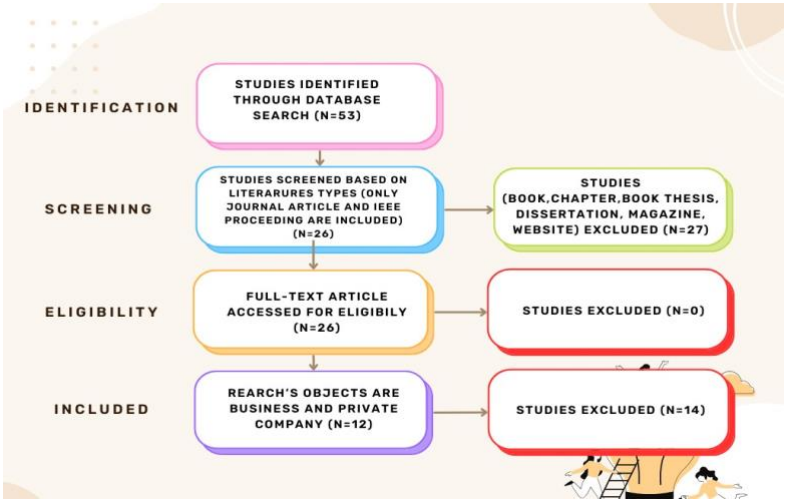
Ancaman-ancaman ini dapat merugikan secara ekonomi dan reputasi bagi sebuah organisasi jika tidak ditangani dengan baik. Dengan menerapkan praktik manajemen risiko keamanan cyber dan standar ISO 27001, organisasi dapat mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi secara sistematis dan terstruktur, sehingga meningkatkan keamanan informasi secara keseluruhan. Selain itu, sertifikasi ISO 27001 juga memberikan keyakinan kepada klien, mitra bisnis, pelanggan, dan pemegang saham bahwa langkah-langkah perlindungan telah diambil untuk melindungi aset organisasi.

Untuk membentuk mekanisme manajemen keamanan informasi berdasarkan standar ISO27001, beberapa upaya yang dapat dilakukan termasuk menyusun dan menetapkan kebijakan keamanan informasi yang sesuai dengan persyaratan standar, memiliki prosedur operasional yang ketat untuk memastikan sistem yang memproses data pribadi tunduk pada prinsip-prinsip keamanan, menerapkan kontrol keamanan dalam siklus pengembangan sistem, memastikan bahwa vendor pihak ketiga yang digunakan oleh organisasi juga tunduk pada standar keamanan yang cukup tinggi, dan mengukur dan mengevaluasi tingkat kepatuhan organisasi terhadap persyaratan standar ISO27001 (Allendevaux, 2021).

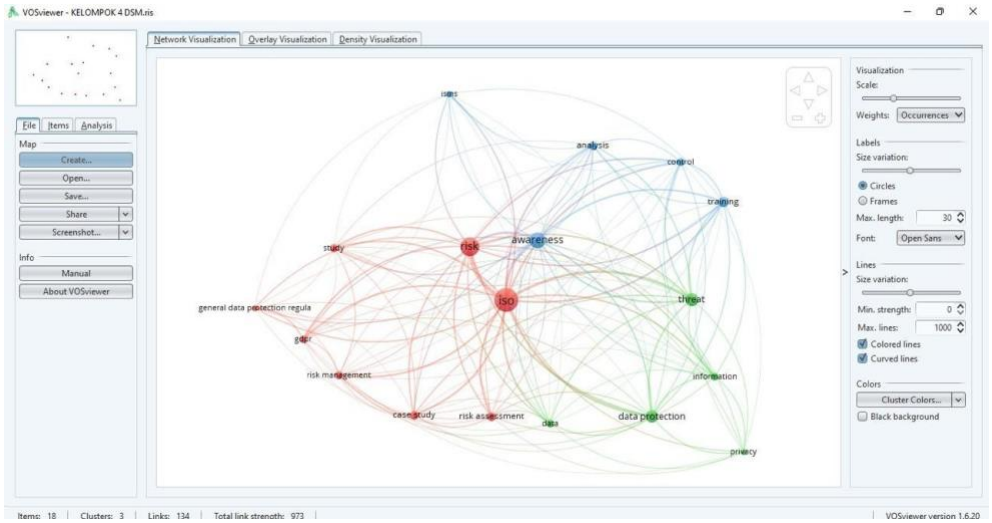
Dengan demikian, manajemen risiko keamanan cyber dan wawasan dari organisasi bersertifikat ISO sangat penting untuk menjaga keberlangsungan operasional dan reputasi perusahaan.

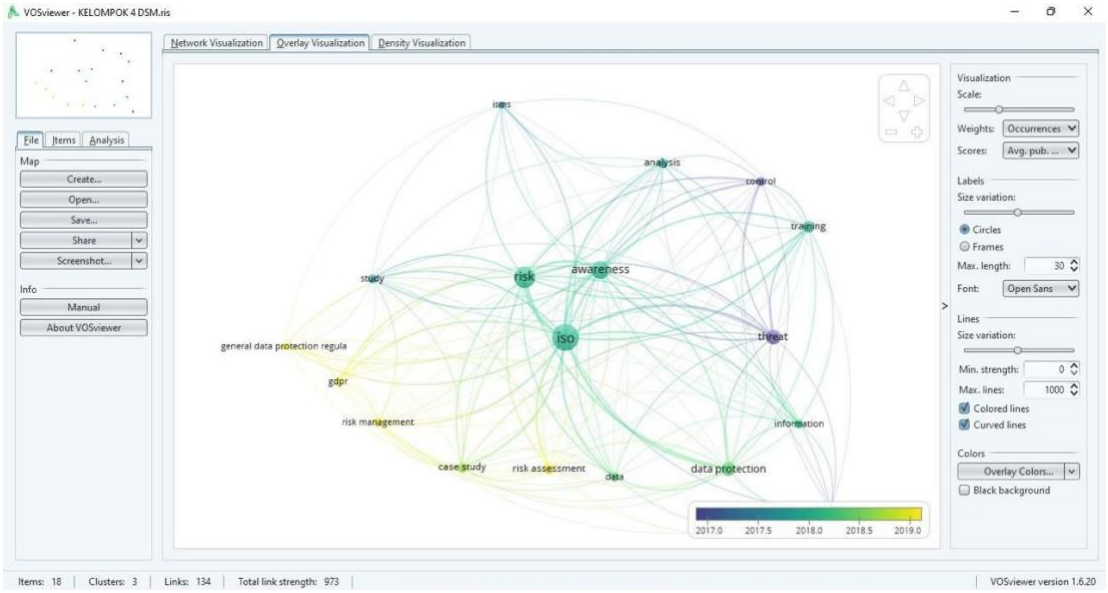
## 2. METODE

Metode penelitian ini menggunakan PRISMA adalah panduan yang digunakan untuk melakukan penilaian terhadap sebuah systematic reviews dan atau meta analysis. PRISMA membantu para penulis dan peneliti dalam menyusun sebuah systematic review dan meta analysis yang berkualitas dengan langah-Langkah yang ditunjukkan dengan bagan sebagai berikut**:**




**Gambar 1**. Metode Penelitian PRISMA






**Gambar 2**. Systematic review dan meta analysis

## 3. HASIL DAN PEMBAHASAN

### Pengertian Data Security Management

Dalam konteks bisnis saat ini, keamanan data yang lebih dikenal sebagai data security tidak boleh diabaikan. Dengan meningkatnya kompleksitas ancaman siber, perlindungan data menjadi prioritas utama bagi setiap organisasi. Berbagi strategi digunakan, seperti enkripsi, autentikasi, kontrol akses, pencadangan data, dan penggunaan firewall, yang semuanya menjadi pondasi krusial dalam membangun pertahanan terhadap serangan siber yang dapat merugikan. Selain dari aspek pencegahan serangan, penting untuk dicatat bahwa keamanan data juga memiliki dampak signifikan dalam menjaga produktivitas perusahaan dan memperkuat kepercayaan konsumen. Dengan sistem keamanan yang terintegrasi dengan baik, organisasi dapat menjalankan operasionalnya tanpa adanya ketakutan akan gangguan yang diakibatkan oleh serangan siber yang merusak. Lebih lanjut, perlindungan data yang efektif dapat meningkatkan citra perusahaan dimata pelanggan, menunjukkan komitmen perusahaan dalam menjaga kerahasiaan dan keamanan informasi yang mereka kelola.

### ISO 27001

ISO 27001 merupakan standar internasional yang menetapkan persyaratan untuk Sistem Manajemen Keamanan Informasi (ISMS) dalam sebuah organisasi. Standar ini memberikan kerangka kerja yang komprehensif untuk mengelola keamanan informasi dan melindungi aset informasi organisasi dari berbagai ancaman dan risiko keamanan cyber (Al-Mayahi, I., & Sa'ad, P. M, 2012). Sedangkan, menurut Junaid (2023) ISO 27001 adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (ISMS) yang memberikan kerangka kerja yang terstruktur dan sistematis untuk mendirikan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi dalam sebuah organisasi. ISO 27001 membantu organisasi melindungi informasi mereka dengan cara yang terencana dan terjangkau. Maka dapat disimpulkan bahwa ISO 27001

adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (ISMS) yang memberikan kerangka kerja yang komprehensif untuk mengelola keamanan informasi dalam sebuah organisasi.

Standar ini membantu organisasi dalam mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi yang dapat mempengaruhi keberlangsungan operasional dan reputasi perusahaan. Dengan menerapkan ISO 27001, organisasi dapat memastikan bahwa sistem informasi mereka dilindungi secara efektif dari ancaman keamanan. Sertifikasi ISO 27001 juga memberikan manfaat tambahan seperti peningkatan efisiensi operasional, pengurangan biaya akibat insiden keamanan, dan peningkatan reputasi perusahaan. Dengan demikian, sertifikasi ISO 27001 adalah langkah penting untuk membantu organisasi mengelola risiko keamanan informasi dengan lebih efektif dan terstruktur.

Tujuan keamanan dari ISO 27001 adalah memastikan kerahasiaan, integritas, dan ketersediaan informasi, sementara tujuan perlindungan adalah untuk mencegah akses tidak sah, memastikan informasi tidak diubah secara tidak sah, dan memastikan informasi tersedia ketika dibutuhkan . ISO 27001 juga bertujuan untuk mengelola risiko keamanan informasi dengan menerapkan kontrol organisasional, manusia, fisik, dan teknologi, yang mana proses sertifikasi untuk ISO 27001 melibatkan beberapa langkah. Pertama, organisasi perlu mendefinisikan cakupan Sistem Manajemen Keamanan Informasi (ISMS) dengan melakukan penilaian awal, analisis persyaratan, perencanaan manajemen risiko, dan evaluasi manajemen. Selanjutnya, organisasi akan menjalani audit pra-sertifikasi dan penilaian untuk memastikan bahwa proses-proses mereka sudah sesuai dengan standar. Setelah itu, organisasi akan menerima sertifikat resmi ISO 27001 untuk ISMS mereka, yang memiliki masa berlaku selama tiga tahun. Organisasi juga dapat mengajukan rekertifikasi setelah masa berlaku sertifikat berakhir. Standar ISO 27001 direkomendasikan untuk mengimplementasikan Sistem Manajemen Keamanan Informasi (ISMS) guna mengatasi risiko keamanan. Integrasi persyaratan keselamatan dengan ancaman keamanan diusulkan untuk manajemen yang lebih baik. Referensi yang disediakan memberikan informasi lebih lanjut tentang standar ISO dan studi kasus terkait keamanan cyber dan keselamatan (Junaid, 2023).

Manfaat memperoleh sertifikasi ISO 27001 termasuk manfaat ekonomi dan reputasi yang besar. Sertifikasi ini membantu mengurangi kerugian ekonomi dan reputasi akibat serangan keamanan, serta memberikan keyakinan kepada klien, mitra bisnis, pelanggan, dan pemegang saham bahwa langkah-langkah perlindungan telah diambil untuk melindungi aset organisasi dalam kasus serangan keamanan. Sertifikasi ISO 27001 juga dapat meningkatkan struktur keseluruhan organisasi, membantu menghindari denda regulasi, dan mengurangi kebutuhan audit yang sering. Dengan demikian, manfaat memperoleh sertifikasi ISO 27001 meliputi perlindungan aset, peningkatan reputasi, dan kepatuhan terhadap standar keamanan informasi yang diakui secara internasional.

**Pengertian Manajemen Resiko**

Manajemen risiko Herman Darmawi adalah suatu usaha untuk mengetahui, menganalisis serta mengendalikan risiko dalam setiap kegiatan perusahaan dengan tujuan untuk memperoleh efektivitas dan efisiensi yang lebih tinggi. Sedangkan Pendapat ahli ekonomi Joseph Dorfman mendefinisikan manajemen risiko sebagai suatu proses logis dalam usahanya untuk memahami eksposur terhadap suatu kerugian.

Risiko diartikan sebagai suatu peluang terjadinya dampak buruk yang tidak diinginkan, ataupun tidak terduga. Manajemen risiko bertujuan untuk memperoleh efektivitas,

meminimalkan kerugian, dan memastikan perusahaan tetap hidup dengan perkembangan yang berkesinambungan. Proses manajemen risiko meliputi identifikasi risiko, analisis risiko, pengendalian risiko, dan evaluasi dan peningkatan manajemen risiko.

**Proses Implementasi ISO 27001 Langkah-langkah dan Pendekatan yang Digunakan Organisasi saat Penyerangan Siber**

Tentang adanya tindakan selama terjadinya serangan siber memunculkan jawaban dari narasumber berikut ini. tdari hasil penelitian terdapat beebrapa perbandingan natara perusahaan yang menerapkan atau mengimplementasikan ISO 27001 dan perusahaan yang tidak. Ketika perusahaan tidak memiliki langkah-langkah keamanan apa pun selama serangan siber, biasanya karena keyakinan bahwa firewall internet dan perangkat lunak antivirus merupakan perlindungan mutlak, semua profesional TI lainnya menyatakan bahwa mereka memiliki prosedur jika terjadi serangan siber.

Di Perusahaan lainnya, tindakan tersebut mencerminkan keputusan untuk mematikan server Internet karena semua data perusahaan disimpan di tempat itu. Selain itu, jika karyawan di organisasi ini melihat adanya aktivitas dunia maya yang tidak biasanya terjadi, mereka akan memberi tahu profesional TI mereka. Terdapat juga cara yang lain dimana jika terjadi serangan siber, profesional TI mematikan akses internet. Situasi ini sedikit berbeda di perusahaan lain dimana karyawan, jika mereka tidak dapat menemukan profesional IT mereka, mereka mempunyai hak untuk mematikan komputer mereka dengan menekan tombol power lebih lama dari biasanya.

Beberapa perusahaan menjelaskan bahwa server Internet juga perlu dimatikan karena tidak mengetahui apakah ada virus atau malware yang sudah ditempatkan di sistem. Tema dominan dalam fase ini adalah PTC yang menunjukkan bahwa sebagian besar profesional TI telah menciptakan langkah-langkah keamanan siber organisasi yang akan digunakan jika terjadi keamanan siber.

Dari penjelasan di atas Menyoroti pentingnya penerapan standar keamanan siber, seperti ISO 27001, dalam organisasi untuk meningkatkan kesadaran dan praktik keamanan siber. Menekankan bahwa organisasi yang bersertifikat ISO 27001 cenderung memiliki tingkat kesiapan yang lebih tinggi dalam mengelola risiko keamanan siber. Bab ini juga memberikan gambaran tentang implementasi standar keamanan siber, kerjasama antara manajemen dan staf TI, serta upaya untuk meningkatkan kesadaran dan praktik keamanan siber dalam organisasi yang bersertifikat ISO 27001.

**Pentingnya Kesadaran Organisasi Terhadap Keamanan Manajemen Informasi dengan Standar ISO 27001**

Pentingnya kesadaran akan manajemen risiko sebagai perlindungan data pribadi dan juga keamanan informasi, terutama pada era yang serba digital seperti sekarang ini yang setiap waktunya mengalami perkembangan. Perlunya meningkatan kesadaran dalam sebuah organisasi beserta mengimplementasikan manajemen risiko dalam berbagai tingkatan, baik negera bagian maupun federal. sebagai pelndung keamanan dan privasi warga.

Implementasi kebijakan prosedur yang sesuai dengan strandart ISO/IEC 27001:2013 dan ISO/IEC 27701:2019. Organisasi yang memiliki sertifikasi ISO biasanya memiliki kebijakan yang memastikan keamanan operasional, manajemen risiko, dan kepatuhan terhadap

standart keamanan dan privasi yang di tetapkan. Organisasi bersertifikat ISO memiliki pemahaman yang lebih baik tentang perlindungan data dan informasi sensitif. Mereka mengadopsi prinsip desain ke amanan dan privasi secara default serta memiliki prosedur untuk memastikan penyedia layanan pihak ketiga mematuhi standart ke amanan yang sama.

Meskipun demikian,evaluasi dan peningkatan praktik keamanan cyber tetap penting mengikuti perkembangan teknologi dan ancaman. Sebelum itu perlu diketahui bahwa manajemen risiko dalam konteks organisasi memastikan identifikasi, penilaian, dan pengelolaan risiko terkait informasi pribadi secara efisien. Dalam penelitian mengenai model kepatuhan ISO/IEC 27701:2019 dan GDPR, pemahaman konteks organisasi, kebutuhan pemangku kepentingan, dan harapan menjadi kunci kepatuhan yang kuat terhadap regulasi perlindungan data global.

Dalam dokumen yang disajikan, terdapat penjelasan tentang praktik manajemen risiko keamanan cyber dan wawasan dari organisasi bersertifikat ISO terhadap organi sasi tersebut. Dokumen tersebut menunjukan bahwa hampir semua negara bagian dam Amerika Serikat memiliki undang-undang keamanan yang lemah dibandingkan dtandart IO/IEC 270001. Dan bisa kita lihat bahwa hal ini juga merupakan salahsatu bentuk kurangnya kesadaran akan pentingnya manajemen risiko.

Dan juga mengindikasikan perlunya langkah-langkah keamanan yang lebih baik dalam melindungi informasi setelah terjadinya pelanggaran keamanan. Dokumen tersebut juga mencatat bahwa undang-undang di Amerika Serikat umumnya tidak mewajibkan organisasi untuk memastikan pihak ketiga yang mereka libatkan telah diverifikasi dengan baik dan dapat menjamin tingkat perlindungan yang memadai. Oleh karena itu, rekomendasi dalam dokumen termasuk implementasi kebijakan yang aman, manajemen ketahan bisnis yang efektif, dan pengadaan serta pengembangan sistem dengan prinsip keamanan, untuk meningkatkan tingkat ke amanan dan privasi data.

## 4. KESIMPULAN

Implementasi ISO 27001 dalam berbagai konteks, termasuk organisasi yang telah memperoleh sertifikasi ISO 27001 dan lingkungan pendidikan, membantu meningkatkan kesadaran organisasi terhadap keamanan informasi, efisiensi operasional, mengurangi biaya akibat insiden keamanan, meningkatkan reputasi perusahaan, melindungi aset informasi, dan memastikan operasional yang aman. Dengan demikian, penerapan standar ISO 27001 dalam manajemen risiko keamanan siber di berbagai sektor dapat memberikan manfaat yang signifikan bagi organisasi.

Manfaat memperoleh sertifikasi ISO 27001 termasuk manfaat ekonomi dan reputasi yang besar. Sertifikasi ini membantu mengurangi kerugian ekonomi dan reputasi akibat serangan keamanan, serta memberikan keyakinan kepada klien, mitra bisnis, pelanggan, dan pemegang saham bahwa langkah-langkah perlindungan telah diambil untuk melindungi aset organisasi dalam kasus serangan keamanan. Sertifikasi ISO 27001 juga dapat meningkatkan struktur keseluruhan organisasi, membantu menghindari denda regulasi, dan mengurangi kebutuhan audit yang sering.

Penerapan standar keamanan siber, seperti ISO 27001, dalam organisasi dapat meningkatkan kesadaran dan praktik keamanan siber. Organisasi yang bersertifikat ISO 27001 cenderung memiliki tingkat kesiapan yang lebih tinggi dalam mengelola risiko keamanan siber. Kesadaran organisasi terhadap keamanan informasi dengan standar ISO 27001 penting untuk melindungi data pribadi dan informasi, terutama dalam era digital saat ini. Keamanan data, yang dikenal sebagai data security, tidak boleh diabaikan dalam konteks bisnis saat ini. Perlindungan data menjadi prioritas utama bagi setiap organisasi mengingat kompleksitas ancaman siber yang semakin meningkat. Strategi keamanan data seperti enkripsi, autentikasi.

## 7. REFERENSI


Al-Mayahi I. M. Sp (2012). Analisis GAP ISO 27001-Studi Kasus, Konferensi Internasional tentang Keamanan dan Manajemen (SAM 12), Las Vegas.

Behnia A., Rashid RA, dan Chaudhry J.A (2012, Februari). Survei Metode Analisis Risiko Keamanan Informasi, Smart Computing Review, vol. 2, no. 1.

Lembaga Standar Inggris. ISO/IEC 27001:2013 (2013). Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan. Swiss. BSI Standard Limited.

Ghazouani M., Medromi H., Sayouti A. (2014, April). Benhadou S., Penggunaan Terpadu ISO27005 Mehari dan Sistem Multi-Agent untuk Merancang Alat Manajemen Risiko Keamanan Informasi yang Komprehensif, International Journal of Applied Information System (IJAIS), Volume 7 - No. 2, Foundation of Computer Science, New York, Amerika Serikat, www.ijais.org.

Candiwan, PKS, & Sebastian, J. Analisis Perbandingan Risiko Keamanan Informasi dan Penerapan ISO27001 pada Perguruan Tinggi di Indonesia.

Zec, M. (2015). Cyber security Measures in SME's: a study of IT professionals' organizational cyber security awareness. *Linnaeus University, Kalmar. Zugriff unter http://www. divaportal. org/smash/get/diva2*, *849211*.

Liao, K. H., & Chueh, H. E. (2012). Medical Organization Information Security Management Based on ISO27001 Information Security Standard. *J. Softw.*, *7*(4), 792-797.

Al-Mayahi, I., & Sa'ad, P. M. (2012). Iso 27001 gap analysis-case study. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Junaid, T. S. (2023). *ISO 27001: information security management systems* (Doctoral dissertation, Ph. D. thesis, Unspecified Institution. https://doi. org/10.13140/RG. 2.2. 36267.52005).

Iskandar, Syamsul. Bank dan Lembaga Keuangan Lainnya. Jakarta: IN MEDIA. 2013.Kasmir. Bank dan Lembaga Keuangan Lainnya. 2014.

Latumaerissa, Julius R. Bank dan Lembaga Keuangan Lain. Jakarta: Salemba Empat. 2013. PT. Bank Rakyat Indonesia (Persero), Tbk.

Sales Kit BRI April 2015. Jakarta: Bank Rakyat Indonesia. 2015.