JURNAL
Pendidikan, Sains, Sosial dan Agama
SEKOLAH TINGGI AGAMA BUDDHA NEGERI RADEN WIJAYA WONOGIRI

Transformasi Perilaku Organisasi melalui Implementasi ISO 27001:2022 pada Industri Pialang Berjangka: Studi Kasus PT. Century Investment Futures

Shinta Sacha[1], Sri Sundari[2], Bambang Rismadi[3], Marisi Pakpahan[4]
1,2,3,4 Institut Bisnis dan Multimedia Asmi
sacha_ss2000@yahoo.com

Article History:
Accepted: 12 December 2024 ***Revised: 20 July 2025*** *Published: 29 July 2025*

Abstract

Penerapan ISO 27001:2022 sebagai standar sistem manajemen keamanan informasi (SMKI) menjadi kebutuhan mendesak dalam menghadapi ancaman siber di sektor keuangan, khususnya pada perusahaan pialang berjangka. Penelitian ini bertujuan untuk menganalisis bagaimana kebijakan keamanan informasi diimplementasikan dan bagaimana pengaruhnya terhadap perilaku organisasi. Penelitian dilakukan dengan pendekatan kualitatif-deskriptif menggunakan model implementasi kebijakan George C. Edward III yang mencakup variabel komunikasi, sumber daya, disposisi, dan struktur birokrasi. Data dikumpulkan melalui observasi, wawancara mendalam, dan studi dokumentasi terhadap karyawan dan manajemen PT. Century Investment Futures. Hasil penelitian menunjukkan bahwa implementasi ISO 27001:2022 mendorong peningkatan kesadaran terhadap keamanan informasi, keterlibatan karyawan dalam perlindungan data, serta penguatan budaya organisasi berbasis risiko. Namun, tantangan tetap ada seperti keterbatasan infrastruktur dan kebutuhan sumber daya manusia dengan kompetensi teknologi informasi lanjutan. Penelitian ini menyimpulkan bahwa ISO 27001:2022 efektif diterapkan dalam meningkatkan tata kelola keamanan informasi sekaligus mempengaruhi perilaku organisasi secara positif.

Kata kunci: *ISO 27001:2022, implementasi kebijakan, keamanan informasi, perilaku organisasi, pialang berjangka*

PENDAHULUAN

Perkembangan teknologi digital yang pesat dalam lima tahun terakhir telah menghadirkan tantangan besar dalam hal pengelolaan keamanan informasi, terutama di sektor keuangan yang sangat bergantung pada sistem informasi yang andal dan aman. Ancaman siber seperti serangan ransomware, pencurian data, manipulasi sistem, hingga kebocoran informasi sensitif telah menjadi isu kritis yang mengancam keberlangsungan bisnis dan kepercayaan stakeholder (Alshaikh, 2020; Ahmad et al., 2021).

Dalam konteks ini, penerapan Information Security Management System (ISMS) menjadi langkah strategis yang tidak dapat ditunda. Salah satu standar

internasional yang paling banyak diadopsi adalah ISO/IEC 27001:2022, yang memberikan kerangka kerja sistematis untuk mengelola risiko keamanan informasi. Standar ini menekankan pentingnya pendekatan berbasis risiko, komitmen manajemen puncak, dan pembentukan budaya organisasi yang berorientasi pada keamanan data (Karokola & Kowalski, 2021; Paananen & Kuusisto, 2022).

Namun demikian, efektivitas implementasi ISO 27001 tidak hanya bergantung pada dokumentasi teknis atau kepatuhan formal, tetapi juga pada aspek perilaku organisasi dan kemampuan internalisasi kebijakan oleh seluruh elemen perusahaan (Choi & Lee, 2021; Siponen et al., 2020). Hal ini terutama penting di industri pialang berjangka yang menghadapi tekanan regulasi dan ekspektasi publik terhadap integritas sistem transaksi berbasis digital.

Regulasi terbaru di Indonesia seperti Peraturan Bappebti No. 6 Tahun 2023 menegaskan pentingnya penerapan standar keamanan informasi bagi perusahaan pialang berjangka sebagai bagian dari tata kelola yang baik dan perlindungan konsumen. Komitmen terhadap keamanan informasi menjadi indikator kepercayaan dalam ekosistem pasar berjangka yang sangat kompetitif dan sensitif terhadap isu kebocoran data.

Penelitian-penelitian sebelumnya menekankan bahwa keberhasilan penerapan ISO 27001 sangat dipengaruhi oleh faktor-faktor seperti komunikasi kebijakan, kesiapan sumber daya manusia, struktur organisasi, dan disposisi individu terhadap perubahan (Siregar, 2022; Widodo & Prasetyo, 2020). Kerangka implementasi kebijakan George C. Edward III menjadi salah satu pendekatan yang dapat digunakan untuk menganalisis keberhasilan kebijakan secara komprehensif, melalui empat variabel utama yaitu komunikasi, sumber daya, disposisi, dan struktur birokrasi (Subarsono, 2015; Siregar, 2022).

Dengan latar belakang tersebut, penelitian ini berfokus pada analisis implementasi ISO 27001:2022 pada industri pialang berjangka, dengan studi kasus di PT. Century Investment Futures. Tujuannya adalah untuk mengidentifikasi bagaimana kebijakan keamanan informasi diinternalisasi dalam perilaku organisasi, serta faktor-faktor pendukung dan penghambat dalam proses implementasinya. Perkembangan teknologi digital yang pesat dalam lima tahun terakhir telah menghadirkan tantangan besar dalam pengelolaan keamanan informasi, terutama di sektor keuangan yang sangat bergantung pada sistem informasi yang andal dan aman. Ancaman siber seperti serangan ransomware, pencurian data, manipulasi sistem, hingga kebocoran informasi sensitif telah menjadi isu kritis yang mengancam keberlangsungan bisnis dan kepercayaan stakeholder (Alshaikh, 2020; Ahmad et al., 2021; Baskerville et al., 2020).

Sebagai respons terhadap tantangan tersebut, sistem manajemen keamanan informasi (Information Security Management System/ISMS) menjadi kerangka kerja penting yang diadopsi banyak organisasi untuk menjamin keberlanjutan dan integritas informasi. Salah satu standar internasional yang paling banyak

digunakan adalah ISO/IEC 27001:2022, yang menyediakan pendekatan sistematis untuk mengidentifikasi, mengelola, dan mengurangi risiko keamanan informasi melalui kebijakan, prosedur, dan pengendalian teknologi (Karokola & Kowalski, 2021; Calder & Watkins, 2023).

Namun demikian, efektivitas implementasi ISO 27001 tidak hanya bergantung pada kepatuhan administratif atau kelengkapan dokumentasi teknis, tetapi lebih dalam pada aspek perilaku organisasi serta kapasitas internalisasi kebijakan oleh seluruh level perusahaan. Hal ini menjadi sangat penting dalam organisasi jasa keuangan seperti pialang berjangka, yang menghadapi tekanan regulasi dan ekspektasi tinggi dari pemangku kepentingan terhadap tata kelola yang akuntabel dan sistem informasi yang aman (Choi & Lee, 2021; Siponen et al., 2020; Widodo & Prasetyo, 2020). Di Indonesia, pentingnya penguatan sistem keamanan informasi di sektor pialang berjangka ditegaskan dalam Peraturan Bappebti No. 6 Tahun 2023, yang mewajibkan penerapan standar keamanan informasi sebagai bagian dari kepatuhan dan integritas sistem transaksi. Selain itu, penguatan budaya keamanan informasi juga menjadi bagian dari transformasi digital organisasi, yang memerlukan keterlibatan aktif seluruh karyawan dan manajemen (Paananen & Kuusisto, 2022; Safira & Santosa, 2023)

Penelitian-penelitian sebelumnya menunjukkan bahwa implementasi ISO 27001 dapat mendorong peningkatan perilaku pro-keamanan jika didukung oleh komunikasi yang efektif, pelatihan berkelanjutan, dan dukungan struktural dari manajemen puncak (Rahim & Mohamed, 2020; Alzahrani, 2020). Untuk menganalisis proses implementasi kebijakan secara menyeluruh, pendekatan George C. Edward III dinilai relevan karena memuat empat variabel utama yang menentukan keberhasilan kebijakan, yaitu: komunikasi, sumber daya, disposisi pelaksana, dan struktur birokrasi (Siregar, 2022; Subarsono, 2015).

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan untukmengeksplorasi secara mendalam proses implementasi kebijakan keamanan informasi berbasis ISO 27001:2022 di lingkungan organisasi jasa keuangan. Pendekatan ini dipilih karena dinilai mampu menangkap realitas sosial dan perilaku organisasi yang kompleks, serta menjelaskan interaksi antara aktor kebijakan dalam proses internalisasi kebijakan keamanan informasi (Ahmad et al., 2021; Paananen & Kuusisto, 2022). Desain penelitian ini mengacu pada model implementasi kebijakan dari George C. Edward III, yang mengidentifikasi empat variabel kunci yang mempengaruhi efektivitas kebijakan, yaitu komunikasi, sumber daya, disposisi pelaksana, dan struktur birokrasi (Siregar, 2022; Subarsono, 2015). Model ini dianggap relevan dalam konteks organisasi sektor keuangan yang menerapkan kebijakan formal seperti ISO 27001:2022, namun menghadapi tantangan pada tahap penerapan teknis dan budaya organisasi.

Lokasi penelitian adalah PT. Century Investment Futures, sebuah perusahaan pialang berjangka yang telah menerapkan ISO 27001:2022 sebagai bagian dari sistem tata

kelola keamanan informasinya. Subjek penelitian terdiri dari manajemen puncak (direktur operasional dan manajer divisi), tim implementasi ISMS (Information Security Management System), serta staf operasional dari berbagai unit kerja. Pemilihan informan dilakukan secara purposive untuk mendapatkan data yang relevan dan mendalam dari pihak-pihak yang terlibat langsung dalam perencanaan dan pelaksanaan kebijakan keamanan informasi (Yusof & Ismail, 2019).

Data dikumpulkan melalui tiga teknik utama. Pertama, wawancara mendalam dilakukan secara semi-terstruktur untuk menggali persepsi, pengalaman, dan pandangan para informan terkait proses implementasi ISO 27001:2022, terutama dalam hal hambatan, dukungan, dan perubahan perilaku organisasi (Alzahrani, 2020; Rahim & Mohamed, 2020). Kedua, observasi partisipatif dilakukan terhadap aktivitas pelatihan internal, rapat koordinasi keamanan informasi, dan kegiatan operasional harian yang berkaitan dengan penerapan SOP keamanan. Observasi ini bertujuan menangkap dinamika interaksi serta pola perilaku yang muncul selama proses implementasi (Siponen et al., 2020). Ketiga, studi dokumentasi dilakukan dengan menganalisis dokumen resmi perusahaan seperti kebijakan keamanan informasi, laporan audit internal, laporan pelatihan, dan SOP yang berkaitan dengan ISO 27001:2022. Dokumen-dokumen ini digunakan untuk menguatkan data primer dan memberikan gambaran kebijakan secara tertulis (Putri & Rahayu, 2021).

Data yang diperoleh dianalisis menggunakan metode tematik-naratif. Tahapan analisis dilakukan melalui proses reduksi data, penyajian data, dan penarikan kesimpulan yang disusun dalam tema-tema utama sesuai dengan empat variabel model George C. Edward III. Reduksi data dilakukan untuk memilah informasi yang relevan, penyajian data dilakukan dalam bentuk matriks dan narasi, serta kesimpulan ditarik secara induktif untuk menemukan pola dan dinamika implementasi kebijakan (Grunig & Hunt, 1984; Edmondson, 2018). Keabsahan data dijaga melalui triangulasi teknik dan sumber, serta konfirmasi hasil (member checking) kepada informan kunci agar interpretasi peneliti tetap akurat (Jaatun & Snekkenes, 2019; Widodo & Prasetyo, 2020).

Penelitian ini dilaksanakan dalam kurun waktu Agustus 2024 hingga Februari 2025, mencakup tahap persiapan, pengumpulan data lapangan, analisis, dan validasi hasil. Rentang waktu tersebut memungkinkan peneliti untuk melakukan observasi berkelanjutan dan memahami proses adaptasi organisasi terhadap penerapan ISO 27001:2022 secara lebih komprehensif.

HASIL DAN PEMBAHASAN

Komunikasi

Hasil penelitian menunjukkan bahwa komunikasi kebijakan ISO 27001:2022 dilakukan melalui surat edaran, pelatihan rutin, dan distribusi dokumen digital. Pendekatan ini mencerminkan model komunikasi dua arah simetris (Grunig & Hunt, 1984), yang mendorong dialog antara manajemen dan karyawan. Pelatihan internal disesuaikan per divisi, mencerminkan konsep organizational learning

(Argyris & Schön, 1996). Namun, hambatan komunikasi teknis dan kesenjangan pemahaman antarunit masih menjadi tantangan yang perlu ditangani

Sumber Daya

Kesiapan sumber daya ditunjukkan melalui pelatihan rutin, pembentukan tim khusus (ISMS), dan pendekatan investasi berbasis risiko. Tantangan utama adalah keterbatasan infrastruktur dan kebutuhan tenaga kerja dengan kompetensi TI tingkat lanjut. PT. Century Investment Futures mengatasi hal ini dengan pelatihan internal dan penguatan soft-skill keamanan data bagi seluruh staf

Disposisi

Pada tahap awal, proses koordinasi mengalami resistensi akibat ketidaksiapan menyatukan pemahaman antar departemen. Hal ini menimbulkan ketidakseimbangan dalam pelaksanaan kebijakan baru. Namun melalui pendekatan kolaboratif, sosialisasi rutin, dan pembentukan forum diskusi lintas unit, perlahan tercipta sinergi fungsional dan peningkatan kesadaran kolektif terhadap pentingnya keamanan informasi

Struktur Birokrasi

Struktur birokrasi yang diterapkan bersifat partisipatif dan kolektif, melibatkan berbagai pemangku kepentingan, mulai dari manajemen puncak, divisi IT, hingga unit operasional. Meskipun ada jalur komunikasi dua arah, masih terdapat kesenjangan persepsi antara level strategis dan pelaksana. Konsep psychological safety (Edmondson, 2018) menjadi relevan dalam menciptakan lingkungan kerja yang mendukung keterbukaan pelaporan dan kesadaran risiko

Dampak Implementasi

Implementasi ISO 27001:2022 menunjukkan dampak positif dalam membentuk budaya organisasi yang lebih disiplin, peningkatan pemahaman terhadap SOP keamanan, serta peningkatan reputasi perusahaan di mata klien. Namun, implementasi ini masih belum sepenuhnya menjadi budaya organisasi karena waktu adaptasi yang singkat (6 bulan). Masih dibutuhkan proses pembelajaran kolektif jangka panjang untuk memastikan keberlanjutan

Rangkuman Implementasi Kebijakan Standar Keamanan

ISO 27001:2022 Di PT.Century Investment Futures

No.	Pertanyaan	Temuan
A. Komunikasi (*Communication*)		
1	Bagaimana kebijakan keamanan informasi berdasarkan ISO27001:2022 dikomunikasikan kepada	Komunikasi kebijakan keamanan informasi telah dilaksanakan secara terstruktur melalui pelatihan, briefing, dan distribusi dokumen oleh tim ISMS. Seluruh divisi menerima pelatihan wajib yang disesuaikan dengan

	seluruh karyawan di PT.Century Investment Futures ?	kebutuhan. Terdapat kesenjangan pemahaman antar departemen dan resistensi terhadap prosedur baru.di level karyawan. Perusahaan mengatasinya dengan memperkuat

2	Apakah ada pelatihan atau workshop khusus yang diberikan kepada karyawan terkait kebijakan ISO27001:2022 ?	pelatihan dan forum diskusi. Secara umum, terdapat kesinambungan antara kebijakan manajemen puncak dan pelaksanaan operasional, menunjukkan komitmen terhadap budaya keamanan informasi meski masih perlu peningkatan dalam efektivitas komunikasi.
3	Apakah ada hambatan dalam mengkomunikasikan kebijakan ini? Jika ada, bagaimana cara perusahaan mengatasinya?	
B. Sumber Daya (*Resources*)		
1	Bagaimana kesiapan SDM perusahaan dalam memahami dan menerapkan standar keamanan informasi berdasarkan ISO 27001?	Kesiapan sumber daya perusahaan dalam menerapkan kebijakan ISO 27001 menunjukkan arah positif disertai tantangan. Manajemen puncak menetapkan pelatihan, sosialisasi, dan pembentukan tim khusus sebagai langkah strategis. Pendekatan berbasis risiko digunakan untuk mengatasi keterbatasan sumber daya. Di sisi karyawan, adaptasi awal bersifat resisten, kebingungan dan tekanan, namun secara bertahap menunjukkan penerimaan berkat dukungan pelatihan dan bimbingan. Ada kesinambungan antara komitmen manajemen dan respons karyawan, dengan pelatihan dan komunikasi sebagai faktor kunci penguatan kesiapan SDM.
2	Bagaimana perusahaan menangani keterbatasan sumber daya (baik SDM, teknologi, maupun anggaran) dalam penerapan standar ini?	
3	Bagaimana respon dari karyawan dengan diterapkan nya standar keamanan informasi ISO 27001?	
C. Disposisi (*Disposition*)		
1	Bagaimana koordinasi antara berbagai departemen dalam penerapan kebijakan keamanan informasi berdasarkan ISO 27001?	Proses koordinasi antar departemen dan mekanisme pelaporan pelanggaran kebijakan keamanan informasi di PT. Century Investment Futures dalam penerapan ISO 27001:2022 menunjukkan perkembangan positif meski masih di fase transisi.Tantangan awal berupa miskomunikasi dan ketidaksesuaian peran mulai teratasi

		melalui forum koordinasi, sosialisasi, dan pendampingan tim keamanan informasi. Mekanisme pelaporan telah dipahami dan dijalankan oleh karyawan, namun efektivitas penindaklanjutannya masih perlu diperkuat. Secara umum, terdapat komitmen nyata dari manajemen dan staf untuk menjadikan keamanan informasi sebagai budaya kerja, bukan sekadar kewajiban administratif.
2	Bagaimana mekanisme pelaporan jika terjadi pelanggaran terhadap kebijakan keamanan informasi?	
3	Apakah ada evaluasi berkala terhadap penerapan kebijakan ini? Jika ya, bagaimana prosesnya?	

D. Birokrasi (*Bureaucracy*)		
1	Siapa saja pihak yang terlibat dalam pengambilan keputusan terkait kebijakan keamanan informasi di perusahaan?	Struktur birokrasi dalam penerapan ISO 27001:2022 di perusahaan bersifat kolaboratif, melibatkan manajemen puncak, tim teknis, dan unit operasional. Keputusan diambil secara kolektif, dengan dukungan manajemen yang bersifat strategis dan operasional. Namun, masih terdapat kesenjangan antara arah strategis dan pemahaman di tingkat pelaksana, menunjukkan bahwa internalisasi budaya keamanan informasi belum merata. Jalur komunikasi dua arah telah dibentuk melalui forum dan pelatihan, namun tantangan teknis dan keterbatasan waktu manajemen menghambat efektivitasnya. Keberhasilan implementasi sangat bergantung pada harmonisasi persepsi lintas level dan penguatan kesadaran akan pentingnya keamanan informasi bagi keberlanjutan bisnis.
2	Sejauh mana peran manajemen puncak dalam mendukung kebijakan keamanan informasi?	
3	Bagaimana cara perusahaan mengatasi hambatan komunikasi di level top management dan karyawan kaitannya dengan penerapan kebijakan ISO 27001	

Sumber Data: Diolah oleh Peneliti (2025)

KESIMPULAN

Penelitian ini menunjukkan bahwa implementasi kebijakan keamanan informasi ISO 27001:2022 di PT. Century Investment Futures telah berjalan secara sistematis dengan pendekatan kebijakan yang mencakup aspek komunikasi, sumber daya, disposisi, dan struktur birokrasi. Komunikasi internal yang intensif dan pelatihan rutin berhasil meningkatkan pemahaman karyawan terhadap pentingnya keamanan data. Ketersediaan sumber daya manusia dan teknologi masih menghadapi tantangan, namun telah dikelola melalui penguatan kapasitas internal.

Disposisi atau sikap para pelaksana kebijakan mengalami pergeseran positif dari resistensi menuju partisipasi aktif, menandakan terbentuknya budaya kerja yang lebih adaptif terhadap kebijakan keamanan informasi. Struktur birokrasi perusahaan yang mendukung dan kolaboratif menjadi katalisator penting dalam implementasi kebijakan ini.

Secara umum, penerapan ISO 27001:2022 tidak hanya meningkatkan kepatuhan terhadap regulasi, tetapi juga memberikan dampak positif terhadap perilaku organisasi, budaya keamanan informasi, dan kepercayaan stakeholder eksternal. Namun, proses ini membutuhkan keberlanjutan dalam bentuk pelatihan berkala, investasi infrastruktur, dan evaluasi sistematis untuk menjaga efektivitas dan relevansi kebijakan dalam jangka panjang.

REFERENSI

Ahmad, A., Maynard, S. B., & Park, S. (2021). Information security strategies: Towards an organizational multilevel security framework. Information Systems Frontiers, 23(2), 457–474. https://doi.org/10.1007/s10796-020-10000-z

Alshaikh, M. (2020). Information security management standards: A comparative study of ISO/IEC 27001 and NIST frameworks. Journal of Information Security and Applications, 55, 102582. https://doi.org/10.1016/j.jisa.2020.102582

Alzahrani, A. (2020). The role of top management in ISO 27001 implementation in Saudi Arabia: A qualitative study. Journal of Cybersecurity, 6(1), taaa001. https://doi.org/10.1093/cybsec/taaa001

Baskerville, R., Spagnoletti, P., & Kim, J. (2020). Risk management in digital environments: Cybersecurity and human factors. MIS Quarterly Executive, 19(2), 127–144.

Calder, A., & Watkins, S. (2023). ISO 27001: An introduction to information security and the ISO/IEC 27001 standard (Updated ed.). IT Governance Publishing.

Choi, S. Y., & Lee, H. (2021). Effects of organizational support on ISO 27001 compliance in financial institutions. Information Systems Frontiers, 23, 255–270. https://doi.org/10.1007/s10796-020-09988-5

Edmondson, A. (2018). The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth. Wiley.

Grunig, J. E., & Hunt, T. (1984). Managing public relations. Holt, Rinehart & Winston.

Jaatun, M. G., & Snekkenes, E. (2019). Organizational learning and ISO 27001. Information Management & Computer Security, 27(2), 232–245.

Karokola, G., & Kowalski, S. (2021). A systematic review of ISO/IEC 27001 implementation challenges. Journal of Cyber Security Technology, 5(3), 165–181. https://doi.org/10.1080/23742917.2020.1781433

Li, Y., & Zhao, L. (2023). The integration of ISO 27001 into enterprise risk management systems. Journal of Risk and Financial Management, 16(2), 75. https://doi.org/10.3390/jrfm16020075

Paananen, H., & Kuusisto, R. (2022). Organizational readiness and employee engagement in implementing ISO 27001. Journal of Organizational Change Management, 35(4), 700–720.

Putri, A., & Rahayu, S. (2021). Analisis kepatuhan karyawan terhadap kebijakan keamanan informasi di lembaga keuangan. Jurnal Teknologi dan Keamanan Siber, 9(1), 44–51.

Rahim, H. A., & Mohamed, H. (2020). Security awareness and compliance behavior: An empirical investigation in Malaysian organizations. Computers & Security, 90, 101707. https://doi.org/10.1016/j.cose.2019.101707

Safira, N., & Santosa, P. (2023). Pengaruh ISO 27001 terhadap reputasi dan kepercayaan stakeholder di perusahaan digital. Jurnal Teknologi dan Sistem Informasi, 11(3), 210–218.

Siregar, N. (2022). Evaluasi implementasi kebijakan penguatan SDM berbasis pelatihan: Pendekatan teori implementasi George C. Edward III. Jurnal Administrasi dan Kebijakan Publik, 17(2), 112–127.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2020). Employees' adherence to information security policies: An empirical study. Information & Management, 57(2), 103212.

Subarsono, A. G. (2015). Analisis kebijakan publik: Konsep, teori, dan aplikasi. Yogyakarta: Pustaka Pelajar.

Widodo, A., & Prasetyo, D. (2020). Strategi implementasi ISO 27001 dalam perspektif manajemen perubahan organisasi. Jurnal Sistem Informasi, 16(2), 120–133.

Yusof, Z. M., & Ismail, R. (2019). Measuring the effectiveness of ISO 27001 ISMS implementation in Malaysian public sectors. Journal of Information and Communication Technology, 18(1), 55–74.