Analisis dan Peningkatan Standarisasi Keamanan Informasi pada PT Pundi Mas Berjaya

Arwin Kosasih[1], Sabariman[2]
Universitas Internasional Batam
Email korespondensi: 2132004.arwin@uib.edu[1], sabariman@uib.ac.id[2]

Abstrak

ISO/IEC 27001:2013 adalah standar internasional yang menyediakan persyaratan untuk membangun, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (ISMS) dalam suatu organisasi. Pengabdian Kepada Masyarakat ini menunjukkan penerapan standar oleh penyedia teknologi terkemuka serta peranannya dalam mematuhi peraturan keamanan siber lokal. Penelitian ini bertujuan untuk merinci persyaratan sertifikasi ISO 27001 untuk PT. Pundi Mas Berjaya, mengatasi masalah standarisasi keamanan yang mendesak dan meningkatkan kepercayaan pelanggan. Pendekatan yang digunakan mencakup pelatihan, pengembangan dokumen sertifikasi, dan kolaborasi tim dalam pengujian standardisasi. Pelatihan dimulai pada bulan Oktober 2023, dengan fokus pada standar ISO 27001 dan Prosedur Operasi Standar (SOP). Proses implementasi melibatkan lebih dari 72 jam pelatihan dan kolaborasi dengan 2 karyawan mulai dari sesi pengarahan hingga penerapan dan observasi lapangan, yang melibatkan peserta magang dan karyawan perusahaan. Proyek ini berhasil membuat dokumentasi yang memenuhi standar ISO 27001 dan mengatasi masalah keamanan informasi perusahaan dengan biaya yang efektif, meskipun masih ada beberapa masalah kecil yang belum terselesaikan karena penerapan standar serupa oleh kompetitor.
Kata Kunci: ISO 27001, ISMS, SOP, Keamanan Siber

Abstract

ISO/IEC 27001:2013 is an international standard that provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within an organization. Research indicates its implementation by leading technology providers and its role in complying with local cybersecurity regulations. This study aims to detail the requirements for ISO 27001 certification for PT. Pundi Mas Berjaya, addressing urgent security standardization issues and enhancing customer trust. The approach involves training, developing necessary certification documents, and collaborating with teams for standardization testing. Training began in October 2023, focusing on ISO 27001 standards and Standard Operating Procedures (SOP). The implementation process includes comprehensive activities from briefing sessions to field deployment and observation, involving interns and company employees. The project successfully created documentation meeting ISO 27001 standards and addressed the company's information security issues cost-effectively, although minor unresolved issues remain due to competitors' earlier adoption of similar standards.
Keywords: *ISO 27001, ISMS, SOP, Cybersecurity*

Pendahuluan

(1) ISO/IEC 27001:2013 adalah standar internasional yang menyediakan persyaratan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (ISMS) dalam konteks organisasi (Culot et al., 2021; Kitsios et al., 2023; Lopes et al., 2019; Podrecca & Sartor, 2023). ISO/IEC 27001:2013 adalah standar yang paling terkenal dalam rangkaian standar ISO 27000, yang membantu organisasi menjaga aset informasi tetap aman (Eskaluspita, 2020; Zhu & Zhu, 2019).

(2) Penelitian oleh Tahani Alsahafi et al., meneliti kesesuaian tiga universitas negeri bersertifikasi ISO/IEC 27001 di Arab Saudi dengan kerangka kerja NCA-ECC, menganalisis sejauh mana implementasi ISO/IEC 27001 memastikan kesesuaiannya dengan peraturan keamanan siber setempat (Alsahafi et al., 2022).

Penelitian oleh Giovanna Culot et al., menunjukkan bahwa ISO/IEC 27001 telah diimplementasikan oleh penyedia teknologi terkemuka seperti Apple Internet Services, Amazon Web Services, GE Digital, dan unit bisnis Microsoft, serta Workplace milik Facebook (Culot et al., 2021).

Penelitian oleh Fotis Kitsios et al., menyajikan studi kasus tentang sebuah lembaga layanan konsultasi TI internasional yang menerapkan ISO 27001 untuk memastikan kepatuhan dan meningkatkan praktik keamanan informasi (Kitsios et al., 2023).

(3) Tujuan dari kegiatan PkM ini adalah untuk menyusun persyaratan sertifikasi ISO 27001 agar PT. Pundi Mas Berjaya dapat mencapai standarisasi keamanan informasi yang optimal.

Masalah

(1) PT. Pundi Mas Berjaya menghadapi tantangan mendesak terkait standarisasi keamanan informasi. Salah satu diantaranya ialah standarisasi keamanan perusahaan.

(2) Penulis menyelesaikan permasalahan keamanan perusahaan dengan menyusun sertifikasi ISO 27001 dan *Standard Operating Procedure* (SOP) terutama dalam data center.

Metode

(1) Metode yang digunakan mencakup pelatihan intensif bagi karyawan tentang ISO 27001 dan penyusunan dokumen SOP. Penulis menulis dan menyusun kebutuhan sertifikasi ISO 27001 berserta SOP yang diperlukan kepada perusahaan. Hasil tersebut akan digunakan dan diterapkan kepada karyawan yang ada di perusahaan dalam upaya melatih mereka agar perusahaan tetap berjalan dan berfungsi sesuai dengan standarisasi minimal. Seiring dengan pelatihan tersebut dijalankan, penulis juga bekerja sama dengan tim lain untuk

mencari dan mencari jasa uji coba standarisasi perusahaan. Hal tersebut dilakukan agar perusahaan dinyatakan dan mendapatkan serfitikasi ISO 27001 yang sah.

(2) Tempat pelatihan dilaksanakan dalam PT. Pundi Mas Berjaya sejak Oktober 2023 hingga Januari 2024 setiap harinya dan sesuai dengan standarisai minimum.

Pembahasan

Menjelaskan dan menguraikan tentang:

(1) Pelaksanaan/implementasi
Pelaksanaan kegiatan melibatkan serangkaian tahapan yang dimulai dengan sesi pengarahan, diikuti oleh observasi terhadap proses manajemen keamanan informasi. Kegiatan ini berlangsung dari Oktober 2023 hingga Februari 2024 dengan dua mahasiswa terlibat beserta karyawan perusahaan. Dalam sesi pembekalan, tim manajemen PT. Pundi Mas Berjaya memberikan pemahaman mendalam tentang visi, misi, nilai perusahaan, dan tujuan program magang. Penerangan rinci disampaikan mengenai peran serta tanggung jawab peserta magang dalam konteks persiapan sertifikasi ISO 27001. Penjelasan terperinci juga diberikan mengenai Standar Operasional Prosedur (SOP) dan persyaratan sertifikasi ISO 27001, disertai penekanan pada pentingnya penilaian risiko dalam manajemen keamanan informasi. Setelah sesi pembekalan, peserta magang diterjunkan untuk menerapkan pengetahuan dan pemahaman yang diperoleh dalam lingkungan kerja PT. Pundi Mas Berjaya. Mereka diberi tugas untuk memulai penelitian mengenai persyaratan sertifikasi ISO 27001 yang berlaku untuk perusahaan. Observasi dilakukan terhadap proses-proses yang terkait dengan manajemen keamanan informasi di PT. Pundi Mas Berjaya. Ini mencakup pemantauan penggunaan SOP yang telah ada dan identifikasi area-area yang memerlukan perbaikan atau peningkatan. Praktik-praktik terbaik dalam manajemen keamanan informasi diidentifikasi dan dicatat. Dilakukan penyusunan rencana kerja magang yang mencakup jadwal kegiatan, tujuan yang ingin dicapai, serta langkah-langkah konkret yang akan diambil untuk mendukung persiapan PT. Pundi Mas Berjaya dalam memperoleh sertifikasi ISO 27001. Pembuatan rencana pengumpulan dokumen pendukung, termasuk template untuk Sistem Manajemen Kualitas (QMS), Sistem Manajemen Keamanan Informasi (ISMS), dan Manajemen Layanan TI (ITSM), menjadi bagian integral dari proses sertifikasi ISO 27001.

(2) Tersedianya berbagai dokumen SOP dari kebijakan, prosedur, dan sistem yang terlah disesuaikan dan memenuhi persyaratan ISO 27001 serta

sertifikasi ISO 27001.

PT. PUNDI MAS BERJAYA

NO SURAT		TGL. REVISI	
NOMOR REVISI		TGL. TERBIT	
NAMA KEBIJAKAN	Backup Data Perusahaan		
PENANGGUNG JAWAB			

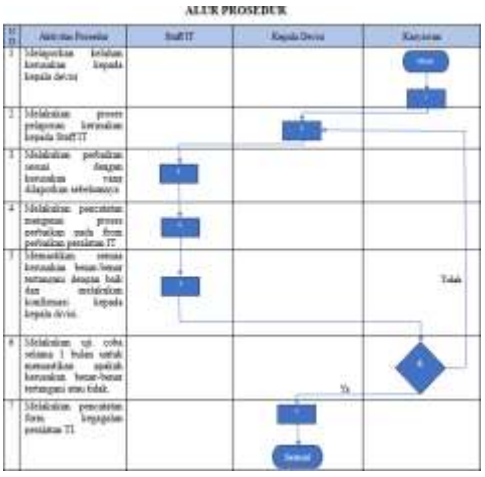
I. TUJUAN KEBIJAKAN
Kebijakan ini dibuat dengan tujuan untuk memastikan terjaminnya keamanan seluruh data dan informasi perusahaan.

II. RUANG LINGKUP
Cakupan kebijakan ini yaitu berlaku bagi seluruh pihak yang mengelola dan mengakses seluruh data dan informasi perusahaan. Data dan informasi tersebut yaitu:
1. Data keuangan
2. Data karyawan
3. Data client
4. Data aset perusahaan
5. Database

III. REFERENSI
Dalam penyusunan kebijakan ini turut menggunakan referensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan referensi ini yaitu:
1. 5.9 Inventory of information and other associated assets
2. 5.15 Access Control
3. 8.13 Information Backup

IV. KEBIJAKAN
4.1 Pengelolaan Keamanan Data
4.1.1 Seluruh pegawai wajib melakukan klasifikasi dan backup data secara berkala minimal 1 kali dalam 3 bulan sesuai jadwal yang telah ditentukan.
4.1.2 Admin wajib memeriksa data yang di-backup apakah sudah sesuai dan tidak rusak atau corrupt.
4.1.3 Admin wajib memastikan data selalu tersedia dan aktual.
4.1.4 Dilarang menyalahkan data dan informasi perusahaan.
4.1.5 Dilarang melakukan penyesatan data dengan alasan apapun jika tidak ada izin berita acara pemusnahan media.
4.1.6 Dilarang menyerjualbelikan data dan informasi kepada pihak lain dengan alasan dan keadaan apapun.
4.1.7 Dilarang menyalin atau memperbanyak data tanpa izin admin sistem dan direktur.
4.1.8 Dilarang menyampur data pribadi dengan data perusahaan.
4.1.9 Apabila kerusakan dan gangguan terjadi maka seluruh karyawan wajib menerapkan kebijakan RDF dalam waktu maksimal 1 jam setelah kerusakan terjadi.

Gambar 1 Salah satu SOP tentang kebijakan perusahaan



Gambar 2 Salah satu SOP prosedur perusahaan

Gambar 3 Invoice sertifikasi ISO 27001

(3) Perusahaan telah berhasil dan menyelesaikan keluhan yang dialami mengenai keamanan sistem informasi perusahaan. Hal ini juga terselesaikan dengan pengeluaran yang minimal dengan hasil yang cukup maksimal dan juga dalam jangka waktu yang cukup singkat. Namun sayangnya, kompetitor yang bergerak serupa dengan perusahaan sudah mendahului keperluan yang sedang perusahaan perlukan, sehingga kekurangan yang perusahaan alami tidak sepenuhnya terselesaikan meskipun tidak banyak lagi.

Simpulan

(1) PT. Pundi Mas Berjaya berhasil menyusun sertifikasi ISO 27001 dan SOP yang memenuhi standar internasional dalam waktu yang efektif.

(2) Hasil dari seluruh pengerjaan memberikan kami wawasan dan pembelajaran yang sangat banyak dan berdampak. Pengalaman yang diberikan oleh perusahaan sangat membantu penulis untuk memasuki dunia pengerjaan dalam bidang keamanan sistem informasi.

(3) Untuk PkM kedepannya yang mungkin dilaksanakan, penulis berharap agar mampu menyelesaikan masalah yang serupa dengan lebih baik, teliti, dan akurat.
(4) Penulis merasa bersyukur dan berterimakasih kepada PT. Pundi Mas Berjaya untuk segala pembelajaran dan pengalaman yang diberikan. Penulis berharap agar seluruh pembelajaran akan menjadi bekal kepada siapapun yang bersangkutan maupun kepada pembaca.

Daftar Pustaka

Alsahafi, T., Halboob, W., & Almuhtadi, J. (2022). Compliance with Saudi NCA-ECC based on ISO/IEC 27001. *Tehnicki Vjesnik*, *29*(6), 2090–2097. https://doi.org/10.17559/TV-20220307162849

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Eskaluspita, A. Y. (2020). ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University. *IOP Conference Series: Materials Science and Engineering*, *879*(1). https://doi.org/10.1088/1757-899X/879/1/012074

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability (Switzerland)*, *15*(7). https://doi.org/10.3390/su15075828

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering and Management*, *4*(2), 2–9. https://doi.org/10.29333/jisem/5888

Podrecca, M., & Sartor, M. (2023). Forecasting the diffusion of ISO/IEC 27001: a Grey model approach. *TQM Journal*, *35*(9), 123–151. https://doi.org/10.1108/TQM-07-2022-0220

Zhu, X., & Zhu, Y. (2019). Extension of ISO/IEC27001 to mobile devices security management. In *Communications in Computer and Information Science* (Vol. 970). Springer Singapore. https://doi.org/10.1007/978-981-13-6621-5_3