ANALISIS KEAMANAN SISTEM INFORMASI PENJUALAN PADA PT ARTA BOGA CEMERLANG CABANG KEDIRI DENGAN MENGGUNAKAN STANDAR ISO 27001:2013

SALES INFORMATION SYSTEM ANALYSIS AT PT ARTA BOGA CEMERLANG USING ISO 27001:2013 STANDARD

Ericko Wicaksono[1*], M. Ailza Sifaul Anam [1], Rizky Alamsyah Bimantara[1], Reisa Permatasari[1]
*E-mail: 21082010219@student.upnjatim.ac.id

[1]Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

PT Arta Boga Cemerlang menunjukkan kesadaran yang kuat terhadap keamanan informasi dalam sistem penjualan mereka. Penelitian ini menggunakan wawancara dan studi literatur untuk mendapatkan data yang komprehensif. Hasilnya menunjukkan bahwa perusahaan memiliki kebijakan keamanan informasi yang mendukung penjualan, melindungi data pelanggan, mengelola aset informasi, mengatur akses sistem, dan menangani insiden keamanan. PT Arta Boga Cemerlang juga disarankan untuk mengadopsi standar global seperti ISO 27001:2013 dan memperbarui kebijakan dan prosedur keamanan informasi secara teratur. Dengan melakukan itu, perusahaan dapat menjaga kerahasiaan, integritas, dan ketersediaan data pelanggan, serta meningkatkan kepercayaan dan kepuasan pelanggan dalam proses penjualan.
Kata kunci: PT Arta Boga Cemerlang, ISO 27001:2013, sistem informasi penjualan, perlindungan data.

Abstract

PT Arta Boga Cemerlang demonstrates a strong awareness of information security in their sales system. This study uses interviews and literature studies to obtain comprehensive data. The results show that the company has an information security policy that supports sales, protects customer data, manages information assets, regulates system access, and handles security incidents. PT Arta Boga Cemerlang is also advised to adopt global standards such as ISO 27001:2013 and update its information security policies and procedures regularly. By doing so, companies can maintain the confidentiality, integrity and availability of customer data, as well as increase customer trust and satisfaction in the sales process.
***Keywords**: PT Arta Boga Cemerlang, ISO 27001:2013, sales information system, data protection.*

1. PENDAHULUAN

PT Arta Boga Cemerlang merupakan perusahaan yang bergerak di bidang penjualan makanan dan minuman. Informasi yang dimiliki oleh perusahaan ini sangat penting dan sensitif, termasuk data pelanggan, data inventaris, dan data transaksi penjualan [1]. Oleh karena itu, perusahaan perlu menerapkan sistem informasi penjualan yang efektif dan efisien untuk menjaga keamanan informasi dan integritas system [2]. ISO/IEC 27001:2013 adalah sebuah standar internasional yang memberikan persyaratan untuk mendirikan, menerapkan, menjaga, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (SMKI)[3]. Standar ini juga mencakup persyaratan untuk penilaian dan manajemen risiko keamanan informasi yang dapat disesuaikan dengan kebutuhan organisasi [4]

Penelitian ini bertujuan untuk menganalisis sistem informasi penjualan PT Arta Boga Cemerlang dengan menggunakan standar ISO 27001:2013. Implementasi standar ini diharapkan dapat

memperkuat keamanan informasi, mencegah kebocoran data, dan memastikan kinerja yang andal dan efisien dari sistem informasi penjualan[5]. Dalam penelitian ini, empat domain utama standar ISO 27001:2013 akan digunakan, yaitu kebijakan keamanan informasi, manajemen aset, kontrol akses, dan manajemen insiden keamanan informasi[6]. Dengan demikian, PT Arta Boga Cemerlang dapat mengoptimalkan keamanan informasi, melindungi integritas sistem informasi penjualan, dan mengurangi risiko terkait kebocoran data yang dapat merugikan perusahaan dan merusak kepercayaan pelanggan[7].

2. METODOLOGI

Metode penelitian ini melibatkan pengumpulan data melalui metode kualitatif (wawancara) dengan karyawan PT ARTA BOGA CEMERLANG dan studi literatur[12]. Wawancara digunakan untuk memperoleh pemahaman mendalam dari narasumber, sementara studi literatur membantu dalam memperoleh pemahaman yang lebih luas tentang topik penelitian dan temuan dari penelitian sebelumnya[13]. Dengan menggabungkan kedua metode ini, penelitian ini dapat memperoleh data yang kaya dan validitas yang kuat dengan memadukan perspektif empiris dan teoritis[14].

3. HASIL DAN PEMBAHASAN

STANDAR ISO 27001:2013 ISO 27001:2013 adalah versi yang telah direvisi dari standar sebelumnya, yaitu ISO 27001:2005[8]. Meskipun telah mengalami revisi, ISO 27001:2013 masih dapat diadopsi oleh organisasi seperti versi sebelumnya. Sistem Manajemen Keamanan Informasi ISO 27001:2013 telah ditetapkan oleh Badan Standarisasi Nasional dengan Nomor 61/KEP/BSN/4/2016 dan juga diatur oleh Peraturan Menteri Komunikasi dan Informatika Nomor 4 tahun 2016 Pasal 7[8]. ISO 27001:2013 menetapkan persyaratan dan panduan yang diperlukan untuk mengembangkan, menerapkan, memelihara, dan terus meningkatkan keamanan informasi dalam suatu organisasi[9]. Tujuan utama dari ISO 27001:2013 adalah membantu organisasi dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi yang dimiliki [10]. Standar ini mencakup beberapa domain terkait keamanan informasi. Dalam penelitian ini, akan digunakan empat domain utama yang tercakup dalam standar ISO 27001:2013. domain domain tersebut meliputi A.5: kebijakan keamanan informasi, A.8 : manajemen aset, A.9 : kontrol akses, dan A.16 : manajemen insiden keamanan informasi[11].

Pertanyaan yang diajukan kepada karyawan PT ARTA BOGA CEMERLANG

1. Domain A.5
   1.1. Bagaimana kebijakan keamanan informasi perusahaan mempengaruhi atau mendukung proses penjualan produk atau layanan perusahaan? (A.5.1.1)
   1.2. Bagaimana perusahaan mengelola risiko keamanan informasi terkait dengan penjualan, khususnya dalam hal perlindungan data pelanggan dan transaksi pembayaran? (A.5.1.2)
   1.3. Apakah perusahaan memiliki kebijakan atau prosedur khusus dalam kebijakan keamanan informasi yang berkaitan dengan penggunaan informasi pelanggan atau data penjualan untuk kepentingan pemasaran atau tujuan bisnis lainnya? (A.5.1.2)
2. Domain A.8
   2.1. Bagaimana perusahaan mengelola aset informasi yang terkait dengan penjualan, seperti data pelanggan, informasi produk, atau data transaksi? (A.8.1.1)
   2.2. Apakah perusahaan memiliki kebijakan atau prosedur khusus dalam manajemen aset yang terkait dengan penjualan, seperti manajemen inventaris produk atau perlindungan terhadap penyalahgunaan aset informasi? (A.8.1.3)
   2.3. Bagaimana perusahaan melakukan pengelolaan risiko terkait dengan aset informasi yang terlibat dalam proses penjualan? Apa langkah-langkah yang diambil untuk melindungi aset tersebut dari ancaman atau kerentanan potensial? (A.8.1.2)

3.Domain A.9

3.1.Bagaimana perusahaan mengelola akses terhadap sistem dan data yang terkait dengan proses penjualan, baik dari internal perusahaan maupun pihak eksternal? (A.9.1.1)

3.2.Apakah perusahaan memiliki prosedur atau kebijakan khusus dalam mengelola akses pengguna terhadap informasi pelanggan atau data penjualan? (A.9.2.2)

3.3.Bagaimana perusahaan memastikan bahwa hanya orang yang berwenang yang memiliki akses ke sistem atau data penjualan? Apa langkah-langkah yang diambil untuk mencegah akses yang tidak sah atau tidak pantas? (A.9.2.3)

4.Domain A.16

4.1.Bagaimana perusahaan mengidentifikasi dan menangani insiden keamanan informasi yang terkait dengan proses penjualan, seperti pelanggaran data pelanggan atau pencurian informasi transaksi? A.(16.1.1)

4.2.Apakah perusahaan memiliki prosedur atau rencana respons insiden keamanan informasi yang spesifik untuk insiden yang terkait dengan penjualan? Bagaimana proses pemulihan dan pemulihan bisnis dilakukan setelah insiden terjadi? (A.16.1.5)

4.3.Bagaimana perusahaan meningkatkan kesiapsiagaan dan pencegahan insiden keamanan informasi yang dapat mempengaruhi proses penjualan? Apa langkah-langkah yang diambil untuk mencegah insiden keamanan terjadi kembali di masa mendatang? A.(16.1.6)

Jawaban dari karyawan PT ARTA BOGA CEMERLANG

1.Domain A.5

1.1.Kebijakan keamanan informasi perusahaan memiliki dampak positif dalam mendukung proses penjualan produk atau layanan perusahaan dengan melindungi data pelanggan, mengendalikan akses, menjaga keamanan transaksi, mengelola risiko, dan menjaga keandalan sistem untuk memastikan kelancaran penjualan dan kepercayaan pelanggan. (A.5.1.1)

1.2.Perusahaan memiliki sistem yang sistematis dalam melindungi data penjualan semua pelanggan. Proses penjualan dimulai dengan orderan yang masuk melalui tablet sales dan secara langsung terhubung ke sistem komputer di kantor masing-masing kota. Seluruh data penjualan tersebut dilindungi dengan password dan hanya tim pusat yang memiliki kendali akses ke data tersebut. Setiap hari, admin di kantor cabang hanya mendapatkan password baru untuk mencetak orderan toko. (A.5.1.2)

1.3.Perusahaan memiliki kebijakan pengelolaan data pelanggan dan penjualan. Tim Data Analis di wilayah Jawa Timur bertanggung jawab mengelola data tersebut. Mereka bekerja sama dengan tim pemasaran pusat untuk strategi promosi produk. Kebijakan keamanan informasi memastikan data dikelola dengan hati-hati dan hanya diakses oleh pihak berwenang untuk analisis dan pengembangan bisnis. Kebijakan ini mendukung penggunaan data untuk kepentingan pemasaran dan tujuan bisnis, sambil menjaga keamanan dan privasi informasi. (A.5.1.2)

2.Domain A.8

2.1.Perusahaan memiliki pendekatan komprehensif dalam mengelola aset informasi terkait penjualan. Tim Data Analis di wilayah Jawa Timur bertanggung jawab dalam menjaga dan mengelola data pelanggan, informasi produk, dan data transaksi. Mereka memastikan bahwa data tersebut terjaga kerahasiaannya dan tidak diakses oleh pihak yang tidak berwenang. Perusahaan juga menerapkan kebijakan keamanan informasi yang ketat untuk melindungi kerahasiaan data dan menjaga data tersebut dari kompetitor. Dengan demikian, perusahaan secara cermat mengelola aset informasi terkait penjualan, menjaga kerahasiaan data, dan melindungi informasi dari akses yang tidak sah.(A.8.1.1)

2.2.Perusahaan memiliki tim audit internal yang memeriksa data penjualan secara rutin di setiap kantor cabang. Tim ini bertanggung jawab untuk memastikan keakuratan data, kepatuhan terhadap kebijakan, dan mengidentifikasi potensi risiko atau kelemahan dalam pengelolaan aset informasi penjualan. Mereka mengambil tindakan perbaikan jika ditemukan

ketidaksesuaian atau penyalahgunaan. Keberadaan tim audit internal ini memastikan bahwa manajemen aset informasi penjualan berjalan sesuai kebijakan perusahaan dan mendukung keberlanjutan serta kepercayaan pelanggan. (A.8.1.3)

2.3. Perusahaan melibatkan tim audit internal untuk mengelola risiko aset informasi dalam proses penjualan. Tim audit ini melakukan pemeriksaan rutin di setiap kantor cabang, termasuk memiliki satu orang anggota tim audit di setiap kantor cabang. Memastikan kepatuhan kebijakan keamanan informasi, mengidentifikasi risiko dan memberikan rekomendasi perbaikan. Audit internal membantu mengurangi risiko, meningkatkan langkah-langkah pengamanan, dan melindungi aset informasi dari ancaman potensial. (A.8.1.2).

3. Domain A.9

3.1. Perusahaan mengelola akses terhadap sistem dan data penjualan dengan hati-hati. Tim Data Analis bertanggung jawab untuk menganalisis dan mengelola data pelanggan dan penjualan, dengan izin akses yang sesuai. Perusahaan juga memperoleh data eksternal dari lembaga independen dengan perjanjian kerahasiaan dan kontrol akses. Pendekatan ini memastikan keamanan dan kerahasiaan data internal dan eksternal terjaga baik dari internal perusahaan maupun pihak eksternal. (A.9.1.1)

3.2. Tim data analis penjualan pusat mengelola data penjualan dan pelanggan dengan prosedur khusus. Mereka menganalisis data secara mendalam, mengidentifikasi tren pembelian, dan memberikan wawasan kepada tim marketing. Prosedur ini memastikan kebijakan tim marketing didasarkan pada data akurat dan relevan, meningkatkan efektivitas promosi, dan berpotensi meningkatkan penjualan. Tim data analis penjualan pusat mendukung pengambilan keputusan yang tepat oleh tim marketing dan berkontribusi pada kesuksesan perusahaan. (A.9.2.2)

3.3. Perusahaan menjaga keamanan akses ke sistem dan data penjualan dengan mengatur akses khusus di ruang tim data analis. Tim audit rutin memeriksa kantor cabang untuk kepatuhan terhadap kebijakan keamanan informasi. Pelanggaran akan ditindak tegas, termasuk interogasi dan surat peringatan sesuai jenis pelanggaran. Tujuannya adalah memastikan akses terbatas hanya bagi pengguna yang berwenang dan memberikan efek jera terhadap pelanggaran. (A.9.2.3)

4. Domain A.16

4.1. Perusahaan melibatkan tim audit kantor cabang dan wilayah untuk melakukan pengecekan rutin sesuai jadwal yang telah ditentukan. Jika ditemukan pelanggaran, pemeriksaan lebih lanjut dilakukan sesuai dengan SOP yang berlaku. Pelanggaran dapat mengakibatkan pemberian surat peringatan kepada karyawan terlibat. Tujuan langkah-langkah ini adalah menegakkan kepatuhan kebijakan keamanan informasi dan mencegah pelanggaran data pelanggan dan pencurian informasi transaksi. (A.16.1.1)

4.2. Perusahaan memiliki tim Audit pusat di Jakarta yang menangani insiden keamanan di kantor cabang. Tim Audit akan melakukan interogasi intensif dan proses pemulihan secara berkelanjutan. Pemulihan dilakukan dalam waktu 24 jam setelah insiden sesuai dengan standar perusahaan. Tindakan ini memastikan penanganan cepat dan efektif terhadap insiden keamanan informasi terkait penjualan, untuk meminimalkan dampaknya. (A.16.1.5)

4.3. Perusahaan menggabungkan langkah-langkah untuk meningkatkan kesiapsiagaan dan pencegahan insiden keamanan informasi dalam proses penjualan. Tim audit pusat dan cabang melakukan pengecekan berkala untuk mengidentifikasi dan menangani pelanggaran data pelanggan atau pencurian informasi. Ruangan tim data analis memiliki akses khusus, dan tim audit pusat memeriksa kepatuhan terhadap kebijakan. Pelanggaran diinterogasi dan dapat diikuti dengan surat peringatan bertingkat. Perusahaan memiliki prosedur respons insiden keamanan informasi yang terkait dengan penjualan dan pemulihan bisnis dalam 24 jam setelah insiden. Semua langkah ini diambil untuk mencegah insiden keamanan informasi di masa mendatang dan menjaga keamanan data pelanggan serta kelancaran proses penjualan. (A.16.1.6)

Berdasarkan hasil wawancara, peneliti telah membuat tabel analisis kesenjangan (*gap analysis*) yaitu Tabel 1, 2, dan 3[15]. Tabel *gap analysis* ini berisi temuan-temuan yang didapatkan dari wawancara dan dikaitkan dengan empat domain yang terdapat dalam standar ISO 27001:2013, dimana setiap domain tersebut berisikan tiga pertanyaan. Domain yang digunakan disebutkan dalam tabel analisis kesenjangan.

Tabel 1. Domain 5

Klausal	Kondisi
A.5.1.1	**Terkini:** Perusahaan memiliki kebijakan keamanan informasi yang mempengaruhi dan mendukung proses penjualan produk atau layanan perusahaan dengan melindungi data pelanggan, mengendalikan akses, menjaga keamanan transaksi, mengelola risiko, dan menjaga keandalan sistem. **Global:** Standar global mengharuskan organisasi untuk memiliki kebijakan keamanan informasi yang komprehensif, mengidentifikasi aset informasi, menetapkan tanggung jawab dan kewenangan, mengelola risiko keamanan informasi, dan memastikan kepatuhan terhadap kebijakan dan prosedur yang ditetapkan **Kesimpulan :** Meskipun Perusahaan telah memiliki kebijakan keamanan informasi yang mendukung proses penjualan, perlu diperhatikan untuk memastikan bahwa kebijakan tersebut mencakup seluruh aspek yang disyaratkan oleh standar global. Evaluasi ulang kebijakan keamanan informasi perlu dilakukan untuk memastikan kesesuaian dan kelengkapan dengan standar ISO 27001:2013.
A.5.1.2	**Terkini:** Perusahaan memiliki sistem yang sistematis dalam melindungi data penjualan pelanggan. Data penjualan dilindungi dengan password dan hanya tim pusat yang memiliki kendali akses ke data tersebut. **Global :** Standar global mendorong organisasi untuk mengadopsi pendekatan yang komprehensif dalam pengelolaan risiko keamanan informasi, termasuk identifikasi risiko, analisis risiko, evaluasi risiko, dan pengelolaan risiko yang tepat sesuai dengan kebijakan yang ditetapkan. **Kesimpulan:** Perusahaan telah melakukan langkah yang baik dalam mengelola risiko keamanan informasi terkait penjualan. Namun, perlu diperhatikan untuk memastikan bahwa proses identifikasi dan penanganan risiko dilakukan secara menyeluruh dan sesuai dengan standar global. Peningkatan dalam pemantauan, pengendalian akses, dan manajemen insiden keamanan dapat diterapkan untuk meminimalkan risiko yang mungkin timbul
A.5.1.2	**Terkini:** Perusahaan memiliki kebijakan keamanan informasi yang mempengaruhi dan mendukung proses penjualan produk atau layanan perusahaan dengan melindungi data pelanggan, mengendalikan akses, menjaga keamanan transaksi, mengelola risiko, dan menjaga keandalan sistem. **Global:** Standar global mewajibkan organisasi untuk memiliki kebijakan keamanan informasi yang mencakup aspek-aspek seperti identifikasi dan penilaian risiko, penetapan kontrol keamanan, pendidikan dan pelatihan karyawan, pengelolaan keamanan sistem, dan manajemen insiden keamanan. **Kesimpulan:**

	Perusahaan telah mengimplementasikan kebijakan keamanan informasi yang baik dan relevan dengan proses penjualan. Dalam upaya meningkatkan kepatuhan terhadap standar ISO 27001:2013, perlu dilakukan evaluasi lebih lanjut terhadap kebijakan yang ada untuk memastikan kesesuaian dan kelengkapan dengan standar tersebut.

Tabel 2. Domain 8

Klausal	Kondisi
A.8.1.1	**Terkini:** Perusahaan memiliki pendekatan yang komprehensif dalam mengelola aset informasi terkait penjualan, seperti data pelanggan, informasi produk, dan data transaksi. Data penjualan dilindungi dengan password dan hanya tim pusat yang memiliki kendali akses ke data tersebut. **Global:** Standar global mendorong organisasi untuk memiliki kebijakan dan prosedur yang jelas dalam mengelola aset informasi terkait penjualan. Hal ini mencakup identifikasi aset, kepemilikan aset, penggunaan aset, pemeliharaan aset, dan pemutakhiran inventaris aset secara teratur. **Kesimpulan :** Perusahaan telah melaksanakan pengelolaan aset informasi terkait penjualan dengan baik, namun perlu diperhatikan untuk memastikan bahwa semua aset teridentifikasi dengan jelas dan ada proses yang terstruktur dalam pengelolaan aset tersebut. Evaluasi dan pemutakhiran inventaris aset secara berkala juga perlu dilakukan untuk memastikan keakuratan dan kelengkapan data aset informasi.
A.8.1.3	**Terkini:** Perusahaan memiliki tim audit internal yang bertanggung jawab untuk melakukan pengecekan terhadap data inventaris produk di setiap kantor cabang. Audit rutin dilakukan untuk memverifikasi keakuratan data dan mengidentifikasi potensi risiko atau kelemahan dalam manajemen inventaris produk. **Global :** Standar global menekankan pentingnya memiliki proses yang terdokumentasi dan terstruktur dalam manajemen inventaris produk. Ini meliputi pencatatan produk, pemantauan stok, pengendalian perubahan, dan peninjauan berkala terhadap inventaris produk. **Kesimpulan:** Perusahaan telah melaksanakan manajemen inventaris produk dengan baik dengan adanya tim audit internal yang melakukan pengecekan secara rutin. Namun, perlu diperhatikan untuk memastikan bahwa semua proses terdokumentasi secara jelas dan terstruktur. Peningkatan dalam pemantauan stok, pengendalian perubahan, dan peninjauan berkala terhadap inventaris produk dapat meningkatkan efektivitas manajemen aset.
A.8.1.2	**Terkini:** Perusahaan memiliki pendekatan yang komprehensif dalam mengelola aset informasi terkait penjualan, seperti data pelanggan, informasi produk, dan data transaksi. Data penjualan dilindungi dengan password dan hanya tim pusat yang memiliki kendali akses ke data tersebut. **Global:** Standar global mendorong organisasi untuk memiliki kebijakan dan prosedur yang jelas dalam mengelola aset informasi terkait penjualan. Hal ini mencakup identifikasi aset, kepemilikan aset, penggunaan aset, pemeliharaan aset, dan pemutakhiran inventaris aset secara teratur.

	Kesimpulan: Perusahaan telah melaksanakan manajemen aset informasi terkait penjualan dengan baik. Namun, perlu dilakukan pemantauan dan evaluasi lebih lanjut untuk memastikan semua aset teridentifikasi secara jelas dan ada proses yang terstruktur dalam pengelolaan aset tersebut, serta pemutakhiran inventaris aset secara berkala.

Tabel 3. Domain 9

Klausal	Kondisi
A.9.1.1	**Terkini:** Perusahaan mengelola akses terhadap sistem dan data yang terkait dengan proses penjualan dengan pendekatan yang hati-hati, baik dari internal perusahaan maupun pihak eksternal. Tim Data Analis memiliki izin akses yang sesuai untuk menjaga keamanan dan kerahasiaan data internal, dan perusahaan menjalin perjanjian kerahasiaan dan kontrol akses dengan lembaga independen seperti Nielsen untuk melindungi data eksternal. **Global:** Standar global menekankan pentingnya mengelola akses pengguna terhadap informasi pelanggan dan data penjualan. Ini meliputi pengenalan pengguna, otorisasi akses, pengelolaan hak akses, dan pemantauan aktivitas pengguna. **Kesimpulan :** Perusahaan telah mengelola akses terhadap sistem dan data penjualan dengan baik. Namun, perusahaan perlu memastikan kepatuhan terhadap standar global dengan menerapkan prosedur dan kebijakan yang khusus dalam mengelola akses pengguna terhadap informasi pelanggan dan data penjualan. Hal ini termasuk pengenalan dan otorisasi pengguna, pengelolaan hak akses secara terstruktur, dan pemantauan aktivitas pengguna untuk mencegah akses yang tidak sah atau tidak pantas.
A.9.1.2	**Terkini:** Perusahaan memastikan keamanan akses ke sistem dan data penjualan dengan mengatur akses khusus di ruang tim data analis wilayah dan pusat. Tim audit secara rutin melakukan pemeriksaan kepatuhan terhadap kebijakan keamanan informasi, dan langkah-langkah tegas akan diambil jika ada pelanggaran yang ditemukan. **Global :** Standar global mendorong organisasi untuk menerapkan langkah-langkah pencegahan akses yang tidak sah atau tidak pantas, seperti pengendalian fisik, pengelolaan identitas, dan tindakan penegakan disiplin. **Kesimpulan:** Perusahaan telah melakukan langkah-langkah pencegahan yang baik untuk memastikan hanya orang yang berwenang yang memiliki akses ke sistem dan data penjualan. Namun, perusahaan perlu memastikan implementasi pengendalian fisik yang memadai, pengelolaan identitas yang lebih terstruktur, dan tindakan penegakan disiplin yang konsisten dalam rangka mencegah akses yang tidak sah atau tidak pantas.
A.9.1.3	**Terkini:** Perusahaan memiliki prosedur khusus yang telah ditentukan oleh tim data analis penjualan pusat untuk mengelola data penjualan dan pelanggan. Prosedur ini membantu memastikan bahwa kebijakan tim marketing didasarkan pada data yang akurat dan relevan. **Global:** Standar global menekankan pentingnya memiliki prosedur dan kebijakan yang jelas dalam mengelola akses pengguna terhadap informasi pelanggan dan data penjualan.

	Hal ini mencakup pengenalan pengguna, otorisasi akses, pemantauan aktivitas pengguna, serta pembaruan dan penghapusan hak akses. **Kesimpulan:** Perusahaan telah memiliki prosedur khusus yang membantu dalam pengelolaan data penjualan dan pelanggan. Namun, perusahaan perlu memastikan kepatuhan terhadap standar global dengan mengadopsi prosedur dan kebijakan yang lebih komprehensif dalam mengelola akses pengguna, termasuk pengenalan dan otorisasi pengguna, pemantauan aktivitas pengguna, serta pembaruan dan penghapusan hak akses secara terstruktur dan teratur.

Tabel 3. Domain 16

Klausal	Kondisi
A.16.1.1	**Terkini:** Perusahaan memiliki prosedur dan rencana respons insiden keamanan informasi yang spesifik untuk insiden yang terkait dengan penjualan. Tim Audit pusat turun langsung ke kantor cabang yang mengalami insiden untuk melakukan tindakan penanganan secara berkelanjutan, termasuk interogasi yang intensif dan proses pemulihan. Proses pemulihan dilakukan dalam waktu 24 jam setelah insiden terjadi. **Global:** Standar global mendorong organisasi untuk memiliki prosedur dan rencana respons insiden keamanan informasi yang khusus untuk meminimalkan dampak dan memulihkan bisnis setelah terjadinya insiden. Ini meliputi identifikasi, respons, mitigasi, dan pemulihan. **Kesimpulan:** Perusahaan telah memiliki prosedur dan rencana respons insiden keamanan informasi yang spesifik untuk insiden yang terkait dengan penjualan. Perusahaan memiliki tindakan penanganan yang cepat dan efektif, serta target waktu pemulihan yang sesuai dengan standar global. Namun, perusahaan perlu memastikan pembaruan dan pengujian berkala terhadap prosedur dan rencana respons insiden untuk menjaga kesiapsiagaan dan keefektifan dalam menghadapi insiden keamanan di masa mendatang.
A.16.1.5	**Terkini:** Perusahaan telah mengambil langkah-langkah untuk mencegah insiden keamanan informasi yang dapat mempengaruhi proses penjualan. Tim audit melakukan pengecekan berkala untuk mengidentifikasi dan menangani potensi pelanggaran data pelanggan atau pencurian informasi transaksi. Akses khusus di ruangan tim data analis wilayah dan pusat juga membatasi akses hanya bagi mereka yang berwenang. **Global:** Standar global mendorong organisasi untuk meningkatkan kesiapsiagaan dan pencegahan insiden keamanan informasi yang dapat mempengaruhi bisnis. Ini melibatkan identifikasi risiko, pengendalian akses, pemantauan keamanan, dan prosedur pencegahan. **Kesimpulan:** Perusahaan telah mengambil langkah-langkah yang baik dalam mencegah insiden keamanan informasi yang dapat mempengaruhi proses penjualan. Perusahaan memiliki prosedur dan kebijakan yang melibatkan identifikasi risiko, pengendalian akses, dan pemantauan keamanan. Namun, perusahaan perlu terus meningkatkan kesiapsiagaan dengan melakukan pembaruan dan pengujian berkala terhadap langkah-langkah pencegahan yang ada, serta mempertimbangkan penerapan

	standar global untuk meningkatkan keamanan informasi secara keseluruhan.
A.16.1.6	**Terkini:** Perusahaan memiliki tim audit yang melakukan pemeriksaan berkala untuk meningkatkan kesiapsiagaan dan pencegahan insiden keamanan informasi terkait dengan penjualan. Tim audit pusat dan tim audit di setiap kantor cabang melakukan pengecekan untuk mengidentifikasi potensi pelanggaran data pelanggan atau pencurian informasi transaksi. Perusahaan juga memiliki prosedur dan rencana respons insiden keamanan informasi yang terkait dengan penjualan, serta melakukan pemulihan dan pemulihan bisnis dalam waktu 24 jam setelah insiden terjadi. **Global:** Standar global mendorong organisasi untuk meningkatkan kesiapsiagaan dan pencegahan insiden keamanan informasi melalui identifikasi risiko, pengendalian akses, pemantauan keamanan, pemulihan bisnis, dan pelaksanaan langkah-langkah pencegahan yang komprehensif. **Kesimpulan:** Perusahaan telah mengambil langkah-langkah yang baik dalam meningkatkan kesiapsiagaan dan pencegahan insiden keamanan informasi yang dapat mempengaruhi proses penjualan. Perusahaan memiliki tim audit yang melakukan pemeriksaan berkala dan prosedur respons insiden yang efektif. Namun, perusahaan perlu memastikan pembaruan dan pengujian berkala terhadap langkah-langkah pencegahan yang ada, serta mempertimbangkan penerapan standar global yang lebih komprehensif untuk meningkatkan kesiapsiagaan dan keefektifan dalam menghadapi insiden keamanan informasi.

4. KESIMPULAN DAN SARAN

PT Arta Boga Cemerlang menjaga keamanan informasi dan aset penjualan dengan baik. Mereka memiliki prosedur akses dan tim analisis data yang sesuai. Perusahaan juga memiliki rencana respons insiden dan pemulihan bisnis yang cepat. PT Arta Boga Cemerlang meningkatkan kesiapsiagaan dan pencegahan insiden keamanan melalui pengujian dan pemeriksaan rutin serta kepatuhan terhadap kebijakan keamanan informasi.
Bagi penelitian selanjutnya hasil riset kami ini berpotensi untuk dikembangkan menjadi penelitian yang sesungguhnya berbasis hipotesa dan hasil-hasil penelitian yang diperoleh oleh peneliti sebelumnya

5. DAFTAR RUJUKAN

[1] A. Nasiri, “Audit Keamanan Aplikasi E-Cash Menggunakan ISO 27001 Audit Security Application for E-Cash Using ISO 27001,” *Citec Journal*, vol. 5, no. 4, 2018.
[2] Jowan Kho, “Cara Efektif Menerapkan Sistem Informasi Manajemen dalam Bisnis,” *SIMPLIDOTS*, 2023.
[3] 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, Jan. 2021, doi: 10.26594/teknologi.v11i1.2152.
[4] M. Lenawati, W. Wahyu Winarno, and A. Amborowati, “Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5,” CDROM.
[5] A. Yulianti, C. Rudianto, and A. F. Wijaya, “Analisis dan Perancangan Tata Kelola Persandian Pengamanan Informasi Menggunakan Standar ISO 27001:2013 (Studi Kasus di Diskominfo Kota Salatiga),” Journal Speed, 2018.

[6] WILDA AYU PRATIWI, "PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDARISO 27001:2013 PADA KOMINFO PROVINSI JAWA TIMUR," STIKOM, 2019.
[7] Yosepha S., "ANALISISFAKTOR-FAKTOR YANGMEMPENGARUHI KEPUASAN PENGGUNA SISTEMINFORMASI AKUNTANSI DAN KINERJA INDIVIDUMENGGUNAKAN THEORY DELONE DANMCLEANE," Universitas Diponegoro, 2016.
[8] S. Nasional, "Teknologi informasi-Teknik keamanan-Sistem manajemen keamanan informasi-Persyaratan l.nformation technology-Security techniques-lnformation security management systems-Requirements," 2016.
[9] E. Riana, M. E. S. Sulistyawati, and O. P. Putra, "Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013," *Journal of Information System Research (JOSH)*, vol. 4, no. 2, pp. 632–640, Jan. 2023, doi: 10.47065/josh.v4i2.2552.
[10] D. Rutanaji, S. Suning Kusumawardani, and W. Wahyu Winarno, "ISO 27001 Sebagai Metode Alternatif Bagi Perancangan Tata KelolaKeamanan Informasi(Sebuah Usulan Untuk Diterapkan diArsip Nasional RI)," Universitas Gajah Mada, 2017.
[11] ADI TIATAMA, "PERENCANAAN TATA KELOLA MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) v3. PADA D~NET SURABAYA," INSTITUT TEKNOLOGI SEPULUH NOPEMBER, 2016.
[12] A. Saputra and Y. G. Sucahyo, "Rancangan Tata Kelola Organisasi Sistem Manajemen Keamanan Informasi Dinas Komunikasi dan Informatika Kabupaten Bekasi Organization Governance Design of Information Security Management System Bekasi Communications and Information Technology Agency," 2018.
[13] I. Yustiana, "PERANCANGAN TATA KELOLA KEAMANAN INFORMASI MENGGUNAKAN KERANGKA KERJA COBIT 5," UNIVERSITAS NUSA PUTRA, 2017
[14] Muhammad Bakri, "ANALISIS DAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SIMHP BPKP MENGGUNAKAN STANDAR ISO 27001" *TEKNOKOMPAK*, vol. 11, p. 2, 2017.
[15] R. Sukmawati and Y. Priyadi, "Perancangan Proses Bisnis Menggunakan UML Berdasarkan Fit/Gap Analysis Pada Modul Inventory Odoo," *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 3, no. 2, p. 104, Apr. 2019, doi: 10.29407/intensif.v3i2.12697.