Jurnal of Business and Audit Information System (JBASE)
Versi Online: http://journal.ubm.ac.id/index.php/jbase
DOI: dx.doi.org/ 10.24105/jbase.v8i2.9061

Vol. 8(No.2): 24 – 31. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

ANALISIS KEBIJAKAN KEAMANAN INFORMASI DI PERUSAHAAN DISTRIBUTOR MOBILE PHONE

ANALYSIS OF INFORMATION SECURITY POLICY IN MOBILE PHONE DISTRIBUTOR COMPANY

Wiyono[1)], Agus Budiyantara[2)], Irwansyah[3)], Putu Sita Witari [4)], Timothy Marpaung[5)], Gery Jordana[6)]

[1)]Program Studi Sistem Informasi, Universitas Buddhi Dharma, Tangerang
[2)] Program Studi Sistem Informasi, Institut Sosial dan Teknologi Widuri, Jakarta
[3)]Program Studi Teknik Informatika, Universitas Muhammadiyah Prof. Dr. Hamka
[4)]Program Studi Bahasa Inggris, Universitas Bunda Mulia, Jakarta
[5,6)] Program Studi Bisnis Digital, Universitas Bunda Mulia, Jakarta

15 Mei 2025 / 24 Septermber 2025

Abstrak

Perusahaan distributor *mobile phone* terkemuka yang menghadapi berbagai tantangan dalam sistem keamanan informasi dan kelangsungan operasional, seperti ketidaksesuaian data stok, keterlambatan pengiriman, dan potensi serangan siber. Permasalahan tersebut dapat mengganggu efisiensi bisnis dan keandalan sistem informasi perusahaan. Untuk mengatasi risiko-risiko tersebut, penerapan standar internasional seperti ISO 27001 dan ISO 22301 menjadi penting. Penelitian ini bertujuan untuk menganalisis kebutuhan keamanan informasi dan mengidentifikasi risiko teknologi informasi pada perusahaan dengan pendekatan *Business Continuity Management System* (BCMS). Hasilnya diharapkan memberikan rekomendasi strategis guna meningkatkan ketahanan bisnis dan menjaga integritas sistem informasi.
Kata kunci: ISO 27001, ISO 22301, keamanan informasi, Distributor *Mobile phone*, risiko TI.

Abstract

A leading mobile phone distribution company faces various challenges in its information security and operational continuity systems, such as stock data discrepancies, shipping delays, and potential cyberattacks. These issues can disrupt business efficiency and the reliability of the company's information systems. To address these risks, implementing international standards such as ISO 27001 and ISO 22301 is crucial. This study aims to analyze information security needs and identify information technology risks within the company using a Business Continuity Management System (BCMS) approach. The results are expected to provide strategic recommendations to improve business resilience and maintain the integrity of the company's information systems.
***Keywords**: ISO 27001, ISO 22301, information security, Erajaya, IT risk.*

Pendahuluan

Perusahaan distributor mobile phone merupakan perusahaan di Jakarta dan awalnya berfokus pada impor dan distribusi perangkat telekomunikasi di Indonesia (Prasetyo, 2024). Seiring waktu, perusahaan mengembangkan model bisnisnya menjadi berorientasi pada pelanggan (*customer-centric*) dengan empat vertikal bisnis utama: *Digital, Beauty & Wellness, Active Lifestyle, dan Food & Nourishment* (Rahayu, 2024).

*Korespondensi Penulis:

E-mail: wiyonopondokaren@gmail.com

Perusahaan juga menjalin kerja sama dengan merek global ternama seperti *Apple, Samsung, DJI, The Face Shop*, dan *Sushi Tei* (Ubaidillah, 2024), serta telah memperluas jangkauan distribusinya ke Malaysia dan Singapura, mencakup 83 pusat distribusi dan lebih dari 1.100 gerai ritel (Daryanto et al., 2020). Pertumbuhan bisnis yang pesat ini diiringi oleh tantangan signifikan, khususnya dalam proses *inbound* gudang pusat. Permasalahan yang sering muncul mencakup *overload*, keterlambatan pengiriman, ketidaksesuaian data stok, pelanggaran jam cut off, serta kesalahan sistem dan kebocoran data (Sholihah et al., 2023). Tantangan keamanan informasi seperti *intercept email*, kesalahan konfigurasi, dan serangan berbasis *web* juga menjadi isu penting. Selain itu, hubungan dengan pemasok (*supplier relationship*) berisiko terdampak serangan siber, seperti melalui tautan palsu yang dapat mengecoh karyawan.

Untuk mengatasi permasalahan ini, ISO 27001 dan ISO 22301 menjadi standar internasional yang penting dalam pengelolaan sistem keamanan informasi dan manajemen kelangsungan bisnis (Hsu et al., 2016; Pramudya & Fajar, 2019). ISO 22301 berfungsi menjaga kelangsungan operasional perusahaan di tengah gangguan, sementara ISO 27001 berperan dalam perlindungan informasi, menjaga kerahasiaan, integritas, dan ketersediaan data (Syahruli, 2020; Aurabillah et al., 2024).

Audit internal berperan penting dalam mengevaluasi efektivitas penerapan standar ini dan mengidentifikasi perbaikan sistem keamanan yang diperlukan (Kamal, 2023). Dalam konteks exchange of information, perusahaan perlu membangun kepercayaan dalam kolaborasi data antar vertikal bisnis (Karla et al., 2022). Untuk *development and support processes*, penguatan konfigurasi sistem dan tata kelola keamanan sangat diperlukan (LeRay, 2024). Pada aspek supplier *relationship*, pemanfaatan AI dalam sistem manajemen rantai pasok dapat membantu mendeteksi ancaman sejak dini (Earls, 2021). Sementara itu, monitoring keamanan dapat ditingkatkan melalui kontrol teknologi seperti *firewall* dan enkripsi data (Ahmad et al., 2020).

Dalam hal *business continuity*, penerapan BCMS berdasarkan ISO 22301 meningkatkan keunggulan kompetitif dan layanan tanpa gangguan kepada pelanggan (Bakar et al., 2015). *Compliance* terhadap regulasi keamanan data juga esensial agar perusahaan terhindar dari pelanggaran hukum dan membangun sistem keamanan yang kokoh (Jha, 2024). Akhirnya, implementasi BCMS dan ISO 22301 memberikan fondasi tangguh bagi perusahaan dalam menghadapi risiko operasional dan keamanan informasi (Bras et al., 2023), sekaligus meningkatkan reputasi dan efisiensi operasional secara keseluruhan.

Metode Penelitian

Tahapan Penelitian

Gambar 1. Tahapan Penelitian

Pada Gamabr 1. Tahapan penelitian, proses tahapannya sebagai berikut:

1. *Studi Literatur* Mengumpulkan dan menganalisis sumber-sumber seperti jurnal dan buku untuk membangun landasan teori dan memahami penelitian sebelumnya.
2. *Pengumpulan Data* Dilakukan melalui wawancara menggunakan media digital (Google Meet/Chat) dengan pendekatan NPLF (kapabilitas 1–5) untuk menilai tingkat implementasi ISO.
3. *Analisis Data* Mengolah data menggunakan analisis tematik dengan acuan ISO 27001 untuk menemukan wawasan mendalam dan menarik kesimpulan.
4. *Penulisan Laporan* Menyusun hasil penelitian secara sistematis dan logis dalam laporan akhir yang mencakup latar belakang, metodologi, hasil, dan kesimpulan.

Hasil Dan Pembahasan

Penelitian ini bertujuan untuk mengevaluasi penerapan sistem manajemen keamanan informasi berdasarkan standar ISO 22301 di perusahaan distributor *mobile phone*. Evaluasi dilakukan melalui beberapa domain, yaitu *Exchange of Information, Development and Support Processes, Supplier Relationships, Monitoring and Information Security Incident Management, Business and Information Security Continuity Management*, serta *Compliance*. Data dikumpulkan melalui wawancara mendalam dengan pihak terkait dan dianalisis menggunakan skala kapabilitas yang sesuai dengan standar ISO 22301. Skala kapabilitas yang digunakan meliputi:

- N (*Not Achieved*): 0–15%
- P (*Partially Achieved*): 15–50%
- L (*Largely Achieved*): 50–85%
- F (*Fully Achieved*): 85–100%

Hasil analisis menunjukkan bahwa perusahaan telah mencapai tingkat kapabilitas yang baik di beberapa domain, namun masih terdapat kesenjangan antara kondisi saat ini dengan target yang diharapkan. Berikut adalah pembahasan detail untuk setiap domain.

1. Exchange of Information

Tabel 1. Potongan Hasil Wawancara bagian *Exchange of Information*

Pertanyaan	1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Apakah perusahaan ada menerapkan information transfer *policies and procedures*?						F			
Apakah ada orang yang bertanggung jawab atas *agreement information transfer*?						F			
Apakah ada orang yang bertanggung jawab untuk email dan social media di perusahaan anda?						F			
Apakah perusahaan memiliki kebijakan terkait dengan *security risk in email*?						F			
Apakah perusahaan memiliki spesialis keamanan informasi terkait dengan spam?						F			
Apakah perusahaan pernah menyaksikan seseorang menggunakan internet secara tidak pantas di tempat kerja?	N								
Menurut perusahaan, apakah kebijakan penggunaan yang dapat diterima membantu mencegah penyalahgunaan internet?						F			
Apakah media sosial memengaruhi produktivitas di tempat kerja?						F			

Domain ini mencakup kebijakan dan prosedur transfer informasi, enkripsi data, pembatasan akses, serta manajemen email dan media sosial. Hasil wawancara menunjukkan bahwa perusahaan telah mencapai tingkat kapabilitas F (*Fully Achieved*) untuk sebagian besar aspek, seperti penerapan kebijakan transfer informasi dan keamanan email. Namun, masih ditemukan beberapa masalah, seperti:

- Human error dalam mengidentifikasi tautan phishing.
- Spam berlebihan yang memengaruhi produktivitas karyawan.

Rekomendasi:

1. Menerapkan pelatihan karyawan untuk meningkatkan kesadaran keamanan siber.
2. Menggunakan teknologi seperti *Secure Email Gateway (SEG)* dan *Sender Policy Framework (SPF)* untuk mengurangi spam.

3. Memperkuat kebijakan penggunaan internet dengan pemantauan aktivitas secara berkala.

2. Development and Support Processes

Tabel 2 . Hasil Potongan Wawancara bagian *Development and Support Process*

Pertanyaan	1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Apakah organisasi Anda memiliki kebijakan pengembangan yang aman yang diterapkan sepanjang SDLC?					F				
Apakah prinsip rekayasa sistem yang aman telah terdokumentasi dan diterapkan dalam seluruh aktivitas pengembangan sistem informasi?					F				
Apakah lingkungan pengembangan perangkat lunak Anda telah dirancang untuk mendeteksi dan mengurangi kerentanan keamanan?					F				
Apakah pengujian penerimaan keamanan dilakukan untuk memastikan bahwa aplikasi memenuhi persyaratan keamanan sebelum diterima oleh pengguna?						F			

Domain ini berfokus pada penerapan *Secure Software Development Life Cycle (SDLC)* dan prinsip rekayasa sistem yang aman. Perusahaan telah mencapai tingkat kapabilitas F (Fully Achieved) dalam pengujian keamanan aplikasi, tetapi masih menghadapi tantangan seperti:

- Kerentanan sistem eksternal dari pihak ketiga.
- Keterlambatan pengujian keamanan karena tekanan *time-to-market*.

Rekomendasi:

1. Menerapkan *DevSecOps* untuk mengintegrasikan keamanan dalam setiap tahap pengembangan.
2. Melakukan audit keamanan berkala terhadap vendor pihak ketiga.
3. Menggunakan tools seperti *SAST* dan *DAST* untuk deteksi kerentanan otomatis.

3. Supplier Relationships

Tabel 3. Hasil Potongan Wawancara bagian *Supplier Relationship*

Pertanyaan	1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Apakah sulit mengontrol keamanan informasi pada sub-pemasok (tier-2 atau lebih)?						F			
Apakah semua pemasok memiliki akses ke informasi sensitif organisasi?	N								
Apakah evaluasi berkala terhadap pemasok wajib dilakukan oleh organisasi?					F				
Apakah prinsip keamanan informasi wajib dicantumkan dalam kontrak pemasok?					F				
Apakah pemasok harus melaporkan insiden keamanan informasi?					F				

Perusahaan telah menetapkan kebijakan keamanan informasi untuk pemasok, tetapi masih mengalami kendala dalam mengontrol sub-pemasok (*tier-2 atau lebih*). Hasil wawancara menunjukkan tingkat kapabilitas F (*Fully Achieved*) untuk evaluasi pemasok, namun terdapat masalah seperti:

- Keterlambatan pengiriman produk oleh pemasok.
- Risiko keamanan data dari rantai pasok yang kompleks.

Rekomendasi:

1. Menerapkan *Balanced Scorecard* untuk mengevaluasi kinerja pemasok secara holistik.
2. Memperkuat klausul keamanan dalam kontrak dengan pemasok.
3. Menggunakan sistem *SIEM* untuk memantau aktivitas mencurigakan dari pihak eksternal.

4. Monitoring and Information Security Incident Management

Tabel 4. Hasil Potongan Wawancara bagian *Monitoring and Information Security Incident Management*

Pertanyaan	1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Apakah perusahaan secara teratur memantau log sistem untuk aktivitas yang mencurigakan?						**F**			
Apakah ada proses untuk mendeteksi dan mengklasifikasikan kejadian keamanan informasi?						**F**			
Apakah peran dan tanggung jawab untuk manajemen insiden ditetapkan dengan jelas?						**F**			
Apakah ada prosedur formal untuk melaporkan kejadian keamanan informasi?						**F**			
Dapatkah karyawan dengan mudah melaporkan masalah perangkat lunak yang mereka hadapi?						**F**			
Apakah ada tim yang ditugaskan untuk menilai dan memutuskan kejadian keamanan?						**F**			
Apakah perusahaan memiliki rencana tindakan yang siap untuk insiden keamanan?						**F**			
Apakah catatan insiden disimpan sedemikian rupa sehingga dapat digunakan sebagai bukti hukum?						**F**			

Perusahaan telah menerapkan sistem pemantauan log dan manajemen insiden dengan baik, tetapi masih terdapat tantangan dalam:

- Koordinasi tim saat menangani insiden.
- Dokumentasi insiden yang kurang lengkap untuk kepentingan hukum.

Rekomendasi:

1. Membentuk tim *CSIRT (Computer Security Incident Response Team)* dengan tanggung jawab jelas.
2. Menggunakan sistem ticketing seperti *OTRS* untuk pelaporan insiden yang terstruktur.
3. Melakukan simulasi insiden secara berkala untuk meningkatkan kesiapan tim.

5. Business and Information Security Continuity Management

Perusahaan telah mengadopsi standar ISO 22301 untuk rencana kelangsungan bisnis, tetapi masih perlu meningkatkan:

- Keterlibatan karyawan dalam pelatihan keamanan siber.
- Pengujian rutin rencana pemulihan bencana.

Rekomendasi:

1. Menerapkan model *PDCA (Plan-Do-Check-Act)* untuk evaluasi berkelanjutan.
2. Melakukan simulasi bencana minimal sekali setahun.
3. Membangun budaya keamanan informasi di seluruh organisasi.

Tabel 5. Hasil Potongan Wawancara bagian *Business and Information Security Continuity Management*

Pertanyaan	1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Apakah ISO 22301 membantu perusahaan mengembangkan prosedur respons dan pemulihan insiden yang efektif?					**F**				
Apakah perusahaan secara aktif mengidentifikasi dan menilai risiko yang dapat mempengaruhi kelangsungan bisnis?						**F**			
Apakah informasi hasil penilaian risiko digunakan dalam perencanaan kesinambungan bisnis?					**F**				
Apakah rencana kesinambungan bisnis dikembangkan dan diterapkan di setiap departemen dalam organisasi?					**F**				
Apakah perusahaan mengikuti kerangka kerja atau standar tertentu untuk perencanaan kesinambungan bisnis (seperti ISO 22301)?					**F**				
Apakah rencana kesinambungan bisnis diuji dan diperbarui secara berkala, khususnya terkait ancaman keamanan informasi?					**F**				
Apakah perusahaan memiliki mekanisme untuk mempertahankan keamanan informasi dan menangani ancaman terhadapnya?					**F**				

6. Compliance

Tabel 6. Hasil Potongan Wawancara bagian Compliance

Pertanyaan	1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Apakah perusahaan sudah mengidentifikasi dan mendokumentasikan semua hukum dan peraturan yang berlaku relevan dengan operasi organisasi Anda?						F			
Apakah perusahaan memiliki tindakan untuk melindungi dan mengelola hak kekayaan intelektual organisasi Anda?						F			
Apakah ada kebijakan formal untuk memastikan penyimpanan dan retensi catatan organisasi yang aman?						F			
Apakah perusahaan memiliki kontrol yang diterapkan untuk memastikan privasi dan perlindungan informasi identitas pribadi (PII)?						F			
Apakah kontrol kriptografi yang digunakan di organisasi perusahaan diatur dan mematuhi persyaratan hukum dan kebijakan yang relevan?						F			
Apakah organisasi perusahaan secara teratur menilai kepatuhan terhadap kebijakan dan standar keamanan internal?						F			
Apakah perusahaan melakukan audit rutin terhadap sistem informasi perusahaan untuk memastikan kepatuhan dan mendeteksi potensi masalah?						F			

Perusahaan telah mematuhi berbagai regulasi, tetapi masih perlu memperbaiki:

- Dokumentasi kebijakan kriptografi.
- Kepatuhan karyawan terhadap peraturan internal.

Rekomendasi:

1. Menerapkan *Sistem Manajemen* untuk memantau perubahan regulasi.
2. Melakukan audit internal secara mandiri, tidak hanya menunggu audit eksternal.
3. Memperkuat pelatihan karyawan tentang privasi data dan hak kekayaan intelektual.

Simpulan

Perusahaan Distributor *mobile phone* saat ini memiliki fondasi yang kuat untuk menjual barang di bidang retail dan distribusi perangkat seluler, serta memiliki banyak cabang perusahaan, dengan tata kelola perusahaan yang baik dan memenuhi standar peraturan perundang-undangan, hal ini menandakan bahwa perusahaan memiliki kompetensi untuk bersaing dengan perusahaan lain yang bergerak di bidang yang sama, hanya saja, perusahaan Erajaya perlu melakukan perbaikan regulasi yang berkaitan dengan tim Audit dan tim TI terutama di bidang tata kelola TI, kerena berdasarkan wawancara yang dilakukan karyawan memerlukan adaptasi untuk menyesuaikan regulasi keamanan sistem yang dilakukan perusahaan dengan lingkungan kerja, maka dari itu dengan menerapkan model BCMS (*Business Continuity Management System*) yang menggunakan metode PDCA(*Plan-Do-Check-Art*) tersebut perusahaan mendapatkan gambaran untuk merencanakan, melaksanakan, memeriksa dan mengambil tidakan untuk meningkatkan proses kelangsungan bisnis.

Daftar Pustaka

Ahmad, A. D. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 939–953.

Aurabillah, B. A. (2024). Implementasi Framework Iso 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature). *JATI (Jurnal Mahasiswa Teknik Informatika)*, 454–460. .

Bakar, Z. A. (2015). The effect of business continuity management factors on organizational performance: A conceptual framework. *International Journal of Economics and Financial Issues*, 128–134.

Bras, J. C. (2023). Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019. . *IEEE Access*, 134239–134258.

C. Hsu, T. W. (2016). The Impact of ISO 27001 Certification on Firm Performance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 4842–4848.

Daryanto, W. M. (2020). Financial Health Level Of Indonesian Mobile Telecommunication Device Retail During Digital Transformation: A Case Study Of Pt Erajaya . *International Journal of Business, Economics and Law,*, 23(1), 225–242. .

Earls, A. R. (2021). *Top challenges of supplier relationship management.* Retrieved from techtarget: https://www.techtarget.com/searcherp/feature/Top-challenges-of-supplier-relationshipmanagement

Jha, S. (2024). *Cyber Security Compliance 101: All You Need To Know*. Retrieved from sprinto: https://sprinto.com/blog/cyber-security-compliance/

Kamal. (2023). *Pengertian Audit: Jenis, Fungsi dan Manfaat.* Retrieved from gramedia: https://www.gramedia.com/literasi/pengertianaudit/?srsltid=AfmBOoqhowHRyp1RByr_OIAjGsQoPYsF7TSpnFDGjUdylFEHJDNJ9sZT#Fun

Karla, D. P. (2024). A Comprehensive Review on Significance of Problem-Solving Abilities in Workplace. *World Journal of English Language*, 88–95.

LeRay, M. (2024). *Understanding Modern Development Environments: A Complete Guide.* Retrieved from speedscale: https://speedscale.com/blog/modern-development-environments/

Pramudya, G. W. (2019). Business continuity plan using ISO 22301:2012 in IT solution . *International Journal of Mechanical Engineering and Technology*, 865-872.

Prasetyo, S. (2024). *PT Erajaya Swasembada Tbk (ERAA) Profil dan Sejarah Singkat.* Retrieved from pina: https://pina.id/artikel/detail/pt-erajaya-swasembada-tbk-eraa-profil-dan-sejarah-singkatejefy7dmy81

Rahayu, E. M. (2024, December 20). *Erajaya Group: Mencetak Pemimpin untuk Penuhi Kebutuhan Empat Vertikal Bisnis*. Retrieved from SWA: https://swa.co.id/read/454475/erajaya-group-mencetak-pemimpinuntuk-penuhi-kebutuhan-empat-vertikal-bisnis

Sholihah, A. M. (2023). Analisis Perbaikan Masalah Dalam Proses Inbound Di Gudang Pusat Pt Xyz Menggunakan Metode House Of Risk (Hor). *Journal of Economics and Business UBS*, 2780–2794.

Syahruli, A. (2020). *Apa Saja Manfaat Sertifikasi ISO 22301:2016 Sistem Manajemen Kelangsungan* . Retrieved from isoindonesiacenter: https://isoindonesiacenter.com/apa-saja-manfaatsertifikasi-iso-223012016-sistem-manajemen-kelangsunganbisnis/#:~:text=ISO%2022301%20membantu%20organisasi%20untuk,insiden%20sebelum%20ri

Ubaidillah, M. (2024, June 10). *Erajaya Group Gencar Berekspansi Menyokong 4 Vertikal Bisnis*. Retrieved from SWA: https://swa.co.id/read/447619/erajaya-group-gencar-berekspansi-menyokong-4-vertikalbisnis