 ISSN: 2830-0408

Evaluasi Kesenjangan dan Standardisasi Dokumen Keamanan Informasi Berdasarkan ISO/IEC 27001:2022 dengan Pendekatan PDCA di PT XYZ

Muhammad Ramzy Firdaus[a*], Amenda Septiala Tarigan[a]
[a] Program Studi Teknik Industri, Fakultas Teknik, Universitas Pembangunan Nasional Veteran Jakarta, Jalan Limo Raya, Depok, Jawa Barat, , 16515
* Corresponding author: 2310312051@mahasiswa.upnvj.ac.id

ABSTRAK

Penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2022 menjadi kebutuhan krusial bagi perusahaan penyedia layanan teknologi informasi di industri penerbangan guna menjamin ketersediaan, kerahasiaan, dan integritas data. Penelitian ini bertujuan mengevaluasi kesenjangan dokumen Sistem Manajemen Keamanan Informasi eksisting dan melakukan standardisasi Prosedur Operasional Standar (SOP) di PT XYZ menggunakan kerangka kerja Plan-Do-Check-Act (PDCA). Evaluasi awal melalui *gap analysis* terhadap 27 klausul yang dievaluasi dan menunjukkan tingkat kepatuhan awal sebesar 29,6% *Comply*, 59,3% *Partly Comply*, dan 11,1% *Non-Comply*. Melalui tahapan PDCA yang diintegrasikan dengan *Swimlane Diagram* dan matriks RACI (*Responsible, Accountable, Consulted, Informed*), dilakukan penyusunan dan revisi terhadap tiga SOP prioritas, yaitu SOP Identifikasi Risiko dan Peluang SMKI, SOP Sasaran Keamanan Informasi dan Pemantauan KPI Siber, serta SOP Akses Fisik *Data Center*. Hasil evaluasi akhir menunjukkan peningkatan tingkat kepatuhan menjadi 70,4% (19 klausul) *Comply* dan penurunan status *Non-Comply* menjadi 0,0%. Penelitian ini menunjukkan bahwa pendekatan PDCA terstruktur dapat mendukung penutupan kesenjangan dokumen serta memperjelas tata kelola dan wewenang lintas divisi dalam persiapan sertifikasi ISO/IEC 27001:2022.

Kata Kunci: *Gap Analysis*, ISO/IEC 27001:2022, Matriks RACI, PDCA, Standardisasi Dokumen.

ABSTRACT

The implementation of an Information Security Management System (ISMS) based on ISO/IEC 27001:2022 has become an important requirement for information technology service providers in the aviation sector to protect the integrity, and confidentiality of data. This study aimed to evaluate gaps in the existing Information Security Management System documents and to standardize Standard Operating Procedure (SOPs) at PT XYZ using the Plan-Do-Check-Act (PDCA) framework. An initial gap analysis of 27 evaluated clauses indicated compliance level of 29.6% Comply, 59.3% Partly Comply, and 11.1% Non-Comply. Through the PDCA stages integrated with Swimlane Diagrams and RACI (Responsible, Accountable, Consulted, Informed) matrix, three priority SOPs were formulated and revised: the SOP for ISMS Risk and Opportunity Identification, the SOP for Information Security Objectives and Cyber KPI Monitoring, and the SOP for Data Center Physical Access. The final evaluation showed an increase in compliance level to 70.4% (19 clauses) Comply and a reduction of Non-Comply status to 0.0%. This study showed that a structured PDCA approach can support the closure of documentation gaps and clarify cross-functional governance and responsibilities in preparation for ISO/IEC 27001:2022 certification.

Keywords: Gap Analysis, ISO/IEC 27001:2022, PDCA, RACI Matrix, Document Standardization,

ISSN: 2830-0408

1. Pendahuluan

Di era transformasi digital yang masif, manajemen mutu dan keamanan informasi telah bertransformasi dari sekadar tuntutan regulasi menjadi fondasi strategis bagi keberlangsungan bisnis di berbagai sektor industri [16]. Bagi organisasi yang mengelola layanan Teknologi Informasi (TI) bagi sektor penerbangan dan transportasi, keandalan sistem serta jaminan atas kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data operasional maupun data pelanggan memiliki tingkat kritis yang sangat tinggi [17]. Gangguan keamanan siber atau kegagalan tata kelola sistem informasi pada penyedia jasa TI penerbangan tidak hanya berpotensi menimbulkan kerugian finansial, melainkan juga berisiko memicu dampak sistemik terhadap kelancaran operasional penerbangan nasional dan internasional serta meruntuhkan kepercayaan publik [19]. Penerapan standar internasional seperti ISO/IEC 27001:2022 tentang Sistem Manajemen Keamanan Informasi (SMKI) menjadi sarana pembuktian yang krusial untuk menjamin tata kelola keamanan informasi yang terstruktur, tepercaya, dan berkelanjutan [2].

PT XYZ, sebagai penyedia solusi teknologi informasi di sektor penerbangan dan transportasi, memegang peranan vital dalam menyediakan berbagai layanan, mencakup Airline, Transportation and Travel Solutions, Infrastructure Hosting and Managed Services, System Integration, hingga Business Consultancy. Seiring dengan terbitnya standar ISO/IEC 27001:2022 sebagai acuan, diperlukan evaluasi dan penyelarasan dokumen Sistem Manajemen Keamanan Informasi untuk memastikan kesesuaiannya dengan persyaratan standar yang digunakan. Dalam hal ini, Divisi Quality Management (ECD-2) berperan sebagai pengawal tata kelola standar internal dan bertanggung jawab dalam pengelolaan standarisasi serta koordinasi proses review guna mendukung kesiapan evaluasi sertifikasi independen.

Meskipun perusahaan telah memiliki dokumentasi sistem manajemen yang berjalan, hasil identifikasi awal (*baseline assessment*) yang dilakukan dalam penelitian ini menunjukkan adanya kesenjangan (*gap*) antara dokumen eksisting terhadap klausul ISO/IEC 27001:2022. Dari total 27 klausul/kontrol inti yang dievaluasi, hanya 29,6% (8 klausul) yang telah memenuhi kriteria kepatuhan penuh (*Comply*), sementara 59,3% (16 klausul) berstatus *Partly Comply*, dan 11,1% (3 klausul) berstatus *Non-Comply*. Kesenjangan paling kritis teridentifikasi pada area tata kelola risiko, pemantauan indikator kinerja keamanan siber, dan pengendalian akses fisik ruang server (*Data Center*). Ketiga area ini tidak hanya memerlukan perumusan narasi prosedur baku, tetapi juga melibatkan koordinasi lintas unit, antara Divisi Quality Management, Divisi IT Security, Internal Audit, dan Human Capital sehingga diperlukan kejelasan alur proses dan pembagian peran untuk mengurangi potensi tumpang tindih wewenang (*overlapping authority*).

Untuk mengatasi permasalahan kesenjangan dokumen serta ketidakjelasan pembagian peran tersebut, diperlukan kerangka kerja perbaikan mutu yang terstruktur, sistematis, dan berulang (repeatable). Metodologi Plan-Do-Check-Act (PDCA) digunakan sebagai kerangka dalam penelitian ini karena keunggulannya dalam mengintegrasikan tahapan perencanaan berbasis risiko, eksekusi perancangan, pengujian lapangan, hingga standardisasi berkelanjutan [4]. Pendekatan PDCA dikombinasikan dengan pemetaan proses bisnis *Swimlane Diagram* dan perancangan matriks RACI (*Responsible, Accountable, Consulted, Informed*) untuk memastikan kejelasan alur kerja dan penugasan wewenang di setiap aktivitas operasional.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengevaluuasi kesenjangan dokumen Sistem Manajemen Keamanan Informasi di PT

ISSN: 2830-0408

XYZ terhadap persyaratan ISO/IEC 27001:2022, melakukan standarisasi dan revisi Prosedur Operasional Standar (SOP) prioritas menggunakan instrumen *flowchart* dan matriks RACI, serta mengevaluasi perubahan tingkat kepatuhan (*compliance rate*) klausul SMKI setelah penerapan siklus PDCA. Hasil penelitian ini diharapkan dapat memberikan gambaran praktis mengenai penerapan pendekatan PDCA dalam pengelolaan dan standarisasi dokumen keamanan informasi, khususnya pada organisasi penyedia layanan teknologi informasi yang melibatkan koordinasi lintas unit.

2. Tinjauan Pustaka

2.1 ISO/IEC 27001:2022 dan Sistem Manajemen Keamanan Informasi

ISO/IEC 27001:2022 merupakan standar internasional yang menetapkan persyaratan untuk membangun, menerapkan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) secara berkelanjutan [1]. Kerangka kerja ini dirancang untuk melindungi kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) aset informasi melalui penerapan proses manajemen risiko yang sistematis [2]. Standar versi 2022 melakukan restrukturisasi signifikan pada kontrol Lampiran A (Annex A), memadatkan 114 kontrol menjadi 93 kontrol yang dikelompokkan ke dalam empat tema utama: *Organizational Controls, People Controls, Physical Controls*, dan *Technological Controls* [2]. Evaluasi kematangan SMKI dalam persiapan sertifikasi kerap menemukan bahwa organisasi menghadapi tantangan utama bukan pada ketiadaan infrastruktur fisik, melainkan pada ketidaksesuaian dokumentasi prosedur operasional yang belum secara eksplisit memuat klausul kontrol keamanan terbaru [3].

2.2 Anatomi SOP: Flowchart dan Matriks RACI

Prosedur Operasional Standar (SOP) merupakan instrumen kendali mutu yang mendokumentasikan alur kerja baku untuk memastikan konsistensi operasional organisasi [4]. Dokumentasi SOP yang efektif mengintegrasikan narasi tekstual dengan dua komponen visual utama, yaitu *flowchart* dan matriks RACI (*Responsible, Accountable, Consulted, Informed*) [5]. *Flowchart* berfungsi memvisualisasikan urutan logis langkah-langkah proses [4], sedangkan matriks RACI menetapkan pembagian wewenang dan tanggung jawab kerja lintas fungsi [6]. Penugasan peran dalam matriks RACI mengikuti prinsip utama di mana setiap langkah aktivitas idealnya hanya memiliki satu pihak *Accountable* guna mencegah ambiguitas tanggung jawab saat terjadi kegagalan operasional [6]. Kombinasi *flowchart* dan matriks RACI terbukti secara empiris mampu mereduksi ketidakjelasan koordinasi antar-divisi dalam lingkungan kerja berskala kompleks [7].

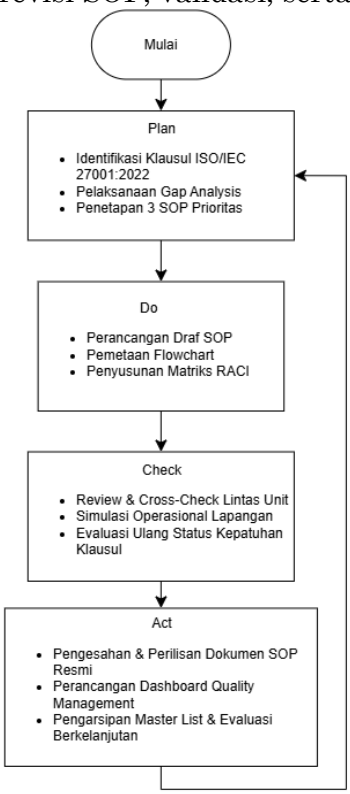
2.3 Metodologi Plan-Do-Check-Act (PDCA)

Metodologi PDCA, yang diperkenalkan oleh W. Edwards Deming, merupakan siklus empat tahap interaktif untuk perbaikan mutu berkelanjutan (*continuous improvement*) [8]. Siklus ini terdiri dari *Plan* (identifikasi masalah dan perencanaan solusi), *Do* (pelaksanaan rencana aksi pada skala uji coba), *Check* (evaluasi hasil terhadap target kriteria), dan *Act* (standardisasi solusi yang berhasil atau pengulangan siklus perbaikan) [9]. Dalam konteks SMKI, ISO/IEC 27001 menerapkan filosofi PDCA sebagai landasan operasional sistem manajemen, di mana pembaharuan dokumen mutu harus melalui pengujian dan evaluasi sebelum disahkan menjadi standar resmi korporasi [10]. Penggunaan PDCA memfasilitasi pendekatan yang fleksibel namun terukur dalam mengelola transisi dokumen kepatuhan standar internasional [11].

ISSN: 2830-0408

3. Metode Penelitian

Penelitian ini dirancang sebagai studi kasus eksploratif-evaluatif dengan menerapkan kerangka kerja *Plan-Do-Check-Act* (PDCA) pada proses evaluasi dan standarisasi dokumen Sistem Manajemen Keamanan Informasi di Divisi *Quality Management* PT XYZ, didukung oleh metode penelaahan literatur [12], kerangka manajemen proyek [13], serta prinsip kendali mutu total [14]. Tahapan penelitian ditunjukkan melalui diagram alir pada Gambar 1 yang memetakan aktivitas operasional ke dalam empat fase utama PDCA, yang masing-masing mencakup identifikasi kesenjangan, penyusunan dan revisi SOP, validasi, serta standardisasi dokumen.



Gambar. 1. Diagram Alir Metodologi PDCA

3.1 Tahap Plan (Perencanaan)

Tahap *Plan* diawali dengan inventarisasi dan evaluasi terhadap 27 klausul dan kontrol inti ISO/IEC 27001:2022, serta pelaksanaan *baseline gap analysis* terhadap dokumen mutu eksisting PT XYZ menggunakan *checklist* standar. Evaluasi ini bertujuan mengidentifikasi tingkat kepatuhan awal dan memetakan area kritis yang mengalami ketidaksesuaian. Formula perhitungan persentase tingkat kepatuhan (P) disajikan pada (1):

$$P_{category} = \frac{N_{category}}{N_{total}} \times 100\% \quad (1)$$

dengan $N_{category}$ adalah jumlah klausul dalam kategori kepatuhan tertentu (*Comply, Partly Comply,* atau *Non-Comply*) dan N_{total} adalah jumlah klausul yang dievaluasi N_{total}= 27). Berdasarkan nilai $P_{category}$, ditetapkan tiga SOP prioritas yang memiliki tingkat keterlibatan lintas divisi tinggi dan urgensi ketidaksesuaian paling kritis.

ISSN: 2830-0408

3.2 Tahap Do

Tahap *Do* berfokus pada penyusunan dan revisi draf tiga SOP prioritas, yaitu: (1) SOP Identifikasi Risiko dan Peluang SMKI, (2) SOP Sasaran Keamanan Informasi dan Pemantauan KPI Siber, dan (3) SOP Akses Fisik Data Center. Setiap SOP dilengkapi dengan alur kerja Swimlane Diagram untuk memisahkan wewenang antar-divisi serta penyusunan matriks RACI untuk memetakan peran *Responsible* (R), *Accountable* (A), *Consulted* (C), dan *Informed* (I) pada tiap butir aktivitas.

3.3 Tahap Check

Tahap *Check* dilakukan melalui validasi terhadap draf SOP yang telah dirancang. Aktivitas ini mencakup pengujian korespondensi formal, rapat penelaahan lintas unit kerja bersama *Group of Internal Audit & Risk Management* (EIA) dan Divisi IT *Security* (OIS-4), serta simulasi uji coba langsung (*walkthrough test*) pada area fisik Data Center. Hasil uji coba digunakan untuk mengidentifikasi potensi hambatan operasional sebelum pengesahan dokumen.

3.4 Tahap Act

Tahap *Act* diwujudkan melalui pengesahan (*sign-off*) resmi dokumen SOP oleh pimpinan unit kerja, penerbitan kode penomoran dokumen master, serta distribusi dokumen terkendali. Selanjutnya, dirancang *Dashboard Quality Management* berbasis *spreadsheet* terintegrasi sebagai instrumen kendali visual (*visual control tool*) untuk memantau siklus penyegaran dokumen, status persetujuan, dan pengukuran KPI kepatuhan secara berkelanjutan.

4. Hasil dan Pembahasan

4.1 Tahap Plan: Evaluasi Kesenjangan Dokumen Mutu (Baseline Gap Analysis)

Hasil evaluasi awal terhadap 27 klausul inti ISO/IEC 27001:2022 pada dokumen mutu eksisting PT XYZ dirangkum dalam Tabel 1, mengikuti metodologi studi kendali mutu industri [15].

Tabel 1
Rekapitulasi Kepatuhan Baseline Klausul ISO/IEC 27001:2022

Status Kepatuhan	Jumlah Klausul	Persentase
Comply	8	29,6%
Partly Comply	16	59,3%
Non-Comply	3	11,1%
Total	**27**	**100%**

Sebagaimana ditunjukkan pada Tabel 1, tingkat kepatuhan awal perusahaan berstatus *Comply* penuh baru mencapai 29,6%. Dominasi kategori *Partly Comply* (59,3%) mengindikasikan bahwa sebagian besar aktivitas operasional keamanan informasi sebenarnya telah dilaksanakan, namun belum didokumentasikan sesuai standar baku ISO/IEC 27001:2022. Tiga klausul yang mengalami status *Non-Comply* (11,1%) teridentifikasi pada area tata kelola risiko SMKI (Klausul 6.1.2), pemantauan sasaran keamanan informasi (Klausul 6.2), dan kendali akses fisik ruang server (Annex A.7.2). Ketiga area ini ditetapkan sebagai prioritas utama dalam siklus perbaikan PDCA.

ISSN: 2830-0408

4.2 Tahap Do: Perancangan SOP Prioritas dan Matriks RACI

Hasil evaluasi awal terhadap 27 klausul inti ISO/IEC 27001:2022 pada dokumen mutu eksisting PT XYZ dirangkum dalam Tabel 1, mengikuti metodologi studi kendali mutu industri [15].

Untuk mengatasi kesenjangan pada tahap *Plan*, dirancang perbaikan mendasar pada tiga dokumen SOP prioritas. Setiap SOP dilengkapi dengan matriks RACI untuk memperjelas wewenang operasional. Hal ini relevan dengan tantangan umum adopsi SMKI pada sektor penyedia jasa TI [16] dan sektor penerbangan [17], di mana keterandalan infrastruktur komunikasi penerbangan [18] serta keamanan digital bandara [19] menuntut pemenuhan prinsip kualitas yang ketat [20]. Sebagai sampel keterwakilan perancangan wewenang lintas divisi, Tabel 2 menampilkan matriks RACI yang disusun untuk SOP Akses Fisik Data Center.

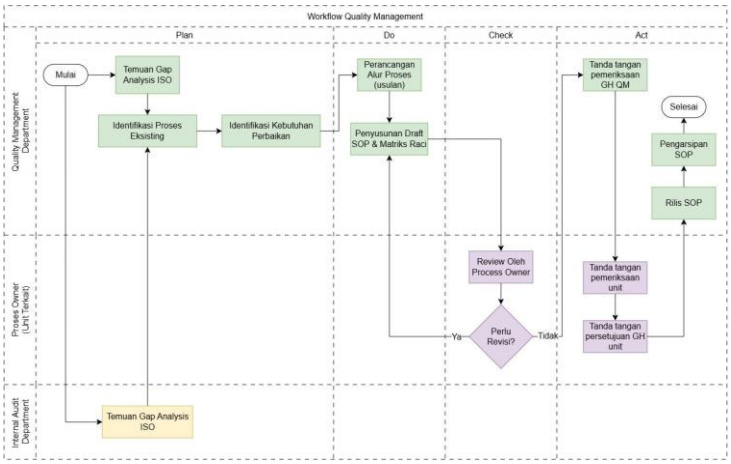
Tabel 2
Matriks RACI pada SOP Akses Fisik Data Center

No	Aktivitas	XYZ	OIS	EHB	EIA
1	Pengajuan permohonan akses	A/R	C	C	
2	Verifikasi dan persetujuan permohonan	I	A/R	C	
3	Menjadwalkan pendampingan dan/atau memproses kartu akses sementara	I	A/R	C	
4	Verifikasi indetitas dan zona masuk	I	A/R	C	
5	Pencatatan log		A/R	C	
6	Personel/pengunjung melaksanakan aktivitas di dalam Data Center	R	A	I	
7	Pengembalian kartu akses dan pencatatan waktu keluar	R	A	I	
8	Peninjauan akses berkala		A/R	C	
9	Investigasi dan tindakan korektif		A/R	C	I

Analisis terhadap Tabel 2 menunjukkan penerapan prinsip *single accountability* pada seluruh alur kerja. Divisi IT *Security* (OIS) memegang peran *Accountable/Responsible* (A/R) utama pada tahap verifikasi, pengendalian log, dan pemantauan berkala (Aktivitas 2-5, 8, dan 9). Struktur ini memastikan bahwa tanggung jawab keamanan fisik Data Center terpusat pada unit teknis yang kompeten. Sementara itu, *Group of Internal Audit & Risk Management* (EIA) secara sengaja diposisikan hanya sebagai pihak *Informed* (I) pada penanganan insiden (Aktivitas 9). Hal ini penting secara teoritis untuk menjaga pemisahan tugas (*segregation of duties*) agar independensi fungsi audit internal tidak terkompromikan akibat keterlibatan langsung dalam kegiatan operasional harian.

Selain matriks RACI, alur tata kelola antar-divisi dipetakan menggunakan Swimlane Diagram pada workflow Divisi *Quality Management*. Pemetaan ini mengintegrasikan fungsi *Internal Audit*, *Process Owner*, dan *Quality Management* ke dalam satu lintasan proses yang selaras dengan siklus PDCA.

 ISSN: 2830-0408



Gambar. 2. Swimlane Diagram Workflow *Quality Management*

4.3 Tahap Check: Validasi Lapangan, Simulasi Akses, dan Peninjauan Audit

Tahap *Check* mengevaluasi kelayakan operasional dari draf dokumen yang telah dirancang pada tahap Do. Uji coba simulasi dilaksanakan secara langsung pada fasilitas Data Center dengan melibatkan personel Divisi IT *Security* dan *Human Capital*.

Simulasi akses fisik mengungkapkan beberapa potensi hambatan operasional (*bottleneck*), antara lain ketidakjelasan durasi maksimal izin akses sementara bagi kontraktor pihak ketiga dan ketiadaan formulir serah-terima kartu akses fisik. Temuan simulasi tersebut langsung ditindaklanjuti dengan merevisi draf SOP Akses Fisik Data Center sebelum memasuki tahap persetujuan final. Proses verifikasi ini membuktikan bahwa tahap *Check* dalam PDCA berfungsi kritis sebagai pengujian hipotesis operasional untuk mencegah timbulnya kondisi di mana prosedur terdokumentasi rapi di atas kertas namun tidak memungkinkan untuk diterapkan di lapangan.

4.4 Tahap Act: Standardisasi Dokumen dan Pengendalian Berkelanjutan

Setelah seluruh draf SOP disempurnakan berdasarkan hasil pengujian tahap Check, pimpinan unit kerja memberikan pengesahan resmi. Dokumen yang telah disahkan diterbitkan dalam *Document Master List* dan didistribusikan ke unit-unit terkait.

Untuk menjamin pemantauan status dokumen secara *real-time*, dirancang *Dashboard Quality Management*. *Dashboard* ini menampilkan indikator visual mengenai status riwayat dokumen (*Completed, In Progress, Need Refreshment*), tenggat waktu peninjauan (SLA *Tracking*), serta persentase kepatuhan klausul per divisi. Karakteristik siklikal PDCA terbukti dalam tahap ini: ditemukannya kebutuhan penyesuaian baru pada instrumen identifikasi risiko saat penyusunan *dashboard* secara otomatis memicu iterasi siklus *Plan* baru untuk pembaruan SOP Identifikasi Risiko dan Peluang SMKI pada periode berikutnya.

4.5 Evaluasi Dampak Implementasi PDCA

Efektivitas penerapan metodologi PDCA diukur melalui evaluasi ulang kepatuhan (*post-implementation assessment*) terhadap 27 klausul ISO/IEC 27001:2022. Perbandingan tingkat kepatuhan sebelum dan sesudah intervensi disajikan pada Tabel 3.

ISSN: 2830-0408

Tabel 3
Rekapitulasi Kepatuhan Baseline Klausul ISO/IEC 27001:2022

Status Kepatuhan	Jumlah Klausul	Persentase
Comply	19	70,4%
Partly Comply	8	29,6%
Non-Comply	0	0,0%
Total	**27**	**100%**

Tabel 3 menunjukkan perbaikan signifikan pada profil kepatuhan dokumen mutu PT XYZ. Kategori *Comply* mengalami lonjakan dari 29,6% (8 klausul) menjadi 70,4% (19 klausul), atau meningkat sebesar +40,8%. Kenaikan ini bersumber dari konversi total 3 klausul *Non-Comply* dan 8 klausul *Partly Comply* yang berhasil ditingkatkan mutunya.

Eliminasi total status *Non-Comply* dari 11,1% menjadi 0,0% memiliki arti strategis yang sangat penting dalam kerangka audit sertifikasi. Dalam kriteria penilaian audit independen ISO/IEC 27001:2022, temuan berkategori *Non-Comply* pada kontrol tata kelola utama dan akses fisik tergolong sebagai Ketidaksesuaian Mayor (*Major Non-Conformity*) yang berpotensi menggagalkan kelulusan sertifikasi. Dengan meniadakan seluruh status *Non-Comply*, risiko kegagalan audit eksternal berhasil ditekankan secara signifikan, sekaligus memberikan landasan tata kelola keamanan informasi yang tegar bagi ekosistem TI penerbangan nasional.

5. Kesimpulan

Penelitian studi kasus ini berhasil membuktikan bahwa penerapan metodologi *Plan-Do-Check-Act* (PDCA) yang diintegrasikan dengan *Swimlane Diagram* dan matriks RACI efektif mengevaluasi dan menutup kesenjangan dokumen mutu ISO/IEC 27001:2022 di PT XYZ. Pelaksanaan evaluasi kesenjangan awal (*Plan*) berhasil mengidentifikasi area kritis dan menetapkan tiga SOP prioritas. Perancangan draf prosedur dan matriks RACI (*Do*) terbukti mampu mengeliminasi ambiguitas wewenang antar-divisi. Tahapan simulasi lapangan dan verifikasi lintas unit (*Check*) efektif mencegah terjadinya *paper compliance*, sementara pengesahan dokumen dan perancangan *Dashboard Quality Management* (*Act*) menjamin keberlanjutan kontrol sistem manajemen mutu. Dampak kuantitatif dari intervensi PDCA ini ditunjukkan oleh peningkatan tingkat kepatuhan penuh (*Comply*) dari 29,6% (8 klausul) menjadi 70,4% (19 klausul), serta pencapaian kepatuhan parsial (*Partly Comply*) turun menjadi 29,6% dan pengeliminasian total status Non-Comply dari 11,1% menjadi 0,0%.

Saran untuk pengembangan penelitian selanjutnya mencakup: (1) melakukan evaluasi dan standardisasi terhadap 8 klausul sisa yang masih berstatus *Partly Comply*; (2) mengukur tingkat kepatuhan aktual (*compliance rate in practice*) di lapangan setelah SOP diimplementasikan secara penuh selama kurun waktu 6 hingga 12 bulan; serta (3) mengintegrasikan *Dashboard Quality Management* dengan sistem manajemen insiden keamanan informasi berbasis otomatisasi untuk meningkatkan kecepatan respon operasional.

ISSN: 2830-0408

Pustaka

[1] ISO/IEC, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO/IEC Standard 27001:2022, Oct. 2022.
[2] A. Górka–Chowaniec and A. Popek, "Attempt to Use the Deming Cycle (PDCA) in the Process of Implementing an Information Security Management System," International Journal for Quality Research, vol. 19, no. 2, pp. 371–386, 2025. https://doi.org/10.24874/IJQR19.02-01
[3] J. Jevelin and A. Faza, "Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification," Journal of Information Systems and Informatics, vol. 5, no. 4, pp. 1240–1256, 2023. [Online]. Available: https://doi.org/10.51519/journalisi.v5i4.572
[4] S. Isniah, F. Debora, and H. Purba, "Plan do check action (PDCA) method: literature review and research issues," Jurnal Sistem dan Manajemen Industri, vol. 4, no. 1, pp. 72–81, 2020. https://doi.org/10.30656/jsmi.v4i1.2186
[5] F. Purwani, "Penerapan Model RACI pada Layanan TI Aplikasi Gramedia Digital," Jurnal Riset Teknik Komputer, vol. 2, no. 1, pp. 1–8, 2025. https://doi.org/10.69714/dxxg9771
[6] H. Abushama and H. Elhady, "RACI Scrum model for controlling of change user requirement in software projects," International Journal of Software Engineering and Its Applications, vol. 9, no. 2, pp. 115–128, 2015.
[7] T. R. Peltier, Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton, FL, USA: CRC Press, 2016.
[8] W. E. Deming, Out of the Crisis. Cambridge, MA, USA: MIT Press, 1986.
[9] R. S. Russell and B. W. Taylor, Operations and Supply Chain Management, 10th ed. Hoboken, NJ, USA: Wiley, 2020.
[10] 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, 2023. https://doi.org/10.47065/josh.v4i2.2552
[11] M. Podrecca, "ISO/IEC 27001: An empirical multi-method research," Doctoral Dissertation, Dept. of Engineering, University of Udine, Italy, 2023.
[12] B. A. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," Keele University Technical Report, TR/SE-0701, 2007.
[13] H. Kerzner, Project Management: A Systems Approach to Planning, Scheduling, and Controlling, 13th ed. Hoboken, NJ, USA: Wiley, 2022.
[14] J. M. Juran and J. A. De Feo, Juran's Quality Handbook: The Complete Guide to Performance Excellence, 7th ed. New York, NY, USA: McGraw-Hill Education, 2017.
[15] D. H. Besterfield, Total Quality Management, 5th ed. Pearson Education India, 2018.
[16] M. Mirtsch, J. Kinne, and K. Blind, "Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis," IEEE Transactions on Engineering Management, vol. 68, no. 1, pp. 87–100, Feb. 2021. https://doi.org/10.1109/TEM.2020.2977815
[17] A. A. Elmarady and K. Rahouma, "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment," IEEE

ISSN: 2830-0408

Access, vol. 9, pp. 143997–144016, 2021. https://doi.org/10.1109/ACCESS.2021.3121230

[18] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, "Security in digital aeronautical communications: A comprehensive survey," International Journal of Critical Infrastructure Protection, vol. 38, p. 100549, 2022. https://doi.org/10.1016/j.ijcip.2022.100549

[19] B. Metin, H. B. Dumer, and M. G. Wynn, "Aviation Cybersecurity Governance: Towards an Operational Framework and Solutions Agenda for the Airport Domain," Information, vol. 17, no. 2, art. 177, pp. 1–21, 2026. https://doi.org/10.3390/info17020177

[20] D. A. Garvin, Managing Quality: The Strategic and Competitive Edge. New York, NY, USA: Free Press, 1988.