Volume 6 Issue 2 (2023) Pages 362 - 376
SEIKO : Journal of Management & Business
ISSN : 2598-831X (Print) and ISSN : 2598-8301 (Online)

Perancangan Proses Keamanan Informasi Berdasarkan *Framework* ISO27001:2022

Muhammad Rizqan Aditama, Fitriyana Dewi[2], Dhata Praditya[3]
[1,2,3]Prodi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University

Abstrak

Keamanan informasi memiliki nilai yang krusial bagi perusahaan karena informasi merupakan salah satu aset yang sangat berharga dalam menjalankan operasi bisnis. Sebagai perusahaan yang bergerak dalam bidang industri MRO (*maintenance, repair and overhaul*) mesin pesawat terbang, TurbinCorp telah sukses dalam menangani *maintenance* ribuan mesin pesawat terbang di negara-negara berbagai belahan dunia, oleh karena itu penerapan sistem manajemen keamanan informasi adalah hal yang krusial supaya perusahaan bisa terhindar dari kebocoran ataupun ancaman yang dapat mengancam informasi perusahaan. Untuk perusahaan industri MRO, pengimplementasian standar ISO/IEC 27001:2022 yang merupakan versi terbaru dari ISO/IEC 27001:2013 dapat memberikan banyak manfaat seperti perlindungan data pelanggan, meningkatkan reputasi dan membantu menjaga kepatuhan terhadap peraturan dan persyaratan hukum yang berlaku. Tujuan penelitian ini adalah untuk menilai kondisi penerapan sistem manajemen keamanan informasi yang sudah diterapkan dan yang belum diterapkan. Penelitian ini dilakukan dengan pendekatan *Design Science Research* (DSR) dengan empat (4) tahap: inisiasi, pengumpulan data, rekomendasi, dan tahap pelaporan. Pengumpulan data dilakukan melalui wawancara serta dokumen. Data kemudian dianalisis menggunakan kerangka kerja ISO/IEC 27001:2022. Penelitian ini berfokus pada klausa utama yaitu klausa 4 sampai klausa 10 dan kontrol-kontrol *annex*. Kesenjangan yang teridentifikasi kemudian dibuatkan perancangan rekomendasi berdasarkan aspek *people*, *process* dan *technology* yang mencakup pilihan sertifikasi, pilihan kelompok minat khusus, penambahan peran dan tanggung jawab, prosedur, kebijakan dan pemilihan perangkat. Hasil penelitian ini dapat digunakan sebagai referensi untuk meningkatkan efisiensi keamanan informasi dan memberi beberapa rekomendasi jika perusahaan ingin mengajukan sertifikasi ISO/IEC 27001:2022.

Kata Kunci: Sistem Manajemen Keamanan Informasi (SMKI), Kontrol Teknologi Informasi, ISO/IEC 27001:2022, *Design Science Research* (DSR)

Abstract

Information security holds crucial value for companies because information represents one of the most valuable assets in conducting business operations as a company operating in the MRO (maintenance, repair, and overhaul) aircraft engine industry, TurbinCorp have successfully managed the care of thousands of aircraft engines in countries across different parts of the world. Therefore, implementing an information security management system is pivotal to protecting the company from potential leaks or threats that could compromise company information. For MRO industry companies, implementing the ISO/IEC 27001:2022 standard, the latest version of ISO/IEC 27001:2013, can bring numerous benefits, such as safeguarding customer data, enhancing reputation, and maintaining compliance with prevailing regulations and legal requirements. This research aims to assess the status of the information security management system that has been and has yet to be implemented. This study uses the Design Science Research (DSR) approach with four (4) stages: initiation, data collection, recommendation, and

reporting. Data collection was conducted through interviews and documentation. The data was then analyzed using the ISO/IEC 27001:2022 framework. This research focuses on the primary clauses, specifically clauses 4 through 10, and the annex controls. Identified gaps were followed by the design of recommendations based on people, processes, and technology. This encompassed choices for certification, specific interest group options, additions of roles and responsibilities, procedures, policies, and equipment selection. The results of this research can serve as a reference for enhancing information security efficiency and providing recommendations if the company is considering applying for ISO/IEC 27001:2022 certification.

***Keywords**: Information Security Management System (ISMS), Information Technology Control, ISO/IEC 27001:2022, Design Science Research (DSR)*

[1]Muhammad Rizqan Aditama, [2]Fitriyana Dewi, [3]Dhata Praditya
[1]rizqanaditama@student.telkomuniversity.ac.id, [2]fitriyanadewi@telkomuniversity.ac.id , [3]dhatapraditya@telkomuniversity.ac.id

PENDAHULUAN

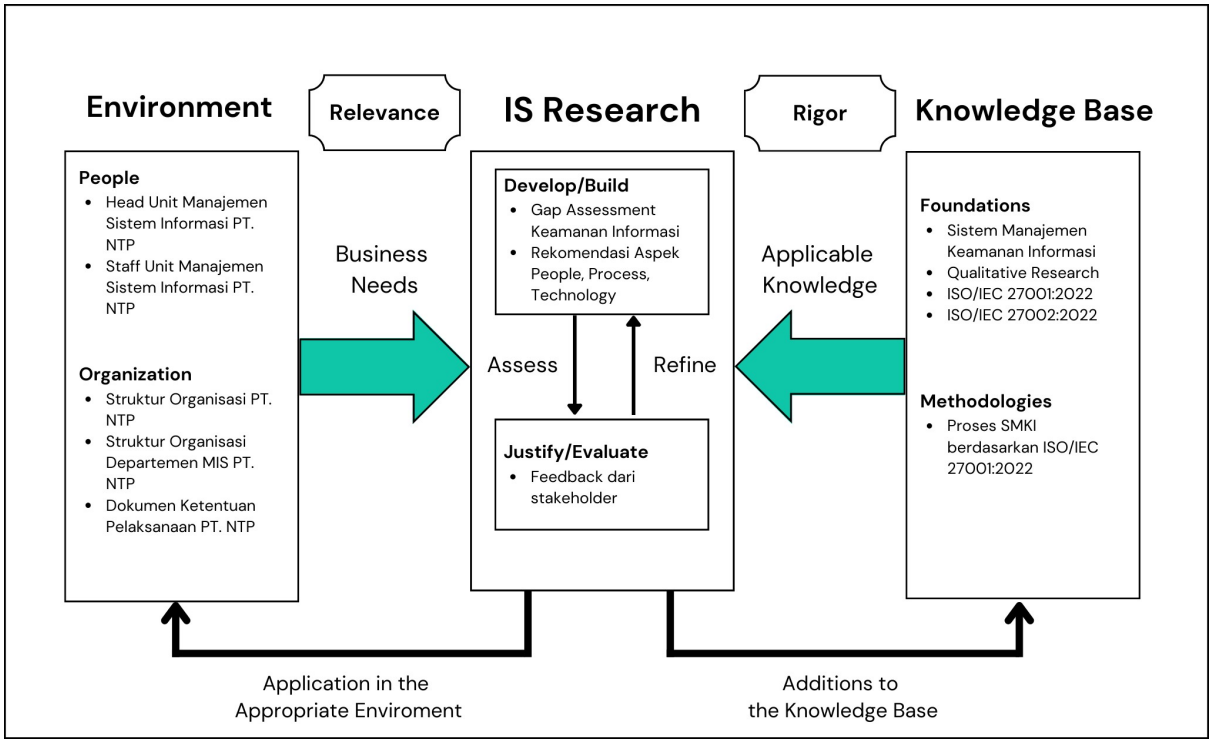
Teknologi informasi (TI) terus berkembang pesat setiap harinya, sehingga organisasi atau perusahaan harus senantiasa beradaptasi dan menerapkan perkembangan TI tersebut [1]. Dalam perkembangan teknologi yang cepat ini, terdapat data yang diproses, digunakan, dan disimpan yang merupakan aset penting perusahaan dalam pengambilan keputusan [2]. Dengan makin kompleksnya kemajuan teknologi informasi, ada banyak lubang yang dapat dimanfaatkan pihak-pihak untuk mengganggu berjalannya proses di suatu organisasi. Keamanan informasi merujuk pada tindakan untuk mencegah sumber daya informasi dari dimanfaatkan oleh pihak yang tidak sah untuk memanipulasi, mencuri, atau mengakses informasi tersebut [3]. Keamanan informasi sangat penting bagi perusahaan karena informasi merupakan salah satu aset yang sangat penting dalam menjalankan bisnis [4]. Informasi dapat mencakup data-data, rahasia, rancangan produk, serta informasi penting lainnya yang dapat membantu perusahaan untuk bersaing dan memperoleh keuntungan [5], [6]. Jika informasi ini jatuh ke tangan yang salah, maka dapat membahayakan perusahaan secara finansial, operasional, dan reputasi. Perusahaan yang mengelola informasi penting dan sensitif perlu memperhatikan keamanan informasi sebagai bagian penting dari strategi bisnis mereka [7]. Dengan mengelola keamanan informasi dengan baik, perusahaan dapat meminimalkan kemungkinan terjadinya dampak negatif dan memaksimalkan kemungkinan hasil positif dari data dan informasi yang dimilikinya [8], [9]. Oleh karena itu keamanan informasi penting dilakukan untuk memastikan bahwa informasi perusahaan efektif dan terus menjadi sesuai dengan kebutuhan perusahaan yang terus berkembang [10]. TurbinCorp adalah perusahaan yang terpercaya dan terkemuka di Asia Tenggara dan juga diakui di seluruh dunia untuk layanannya yang berkualitas tinggi dalam bidang pemeliharaan dan *overhaul* turbin gas, mesin *aero*, dan turbin industri. Untuk menjaga informasi-informasi internal TurbinCorp dalam mengelola informasi, dibutuhkan sebuah penerapan keamanan informasi karena dengan penerapannya, perusahaan dapat melindungi informasi penting dari ancaman yang berasal dari luar maupun dalam perusahaan yang dihadapi TurbinCorp. ISO 27001 merupakan standar internasional yang diakui secara luas dan dirancang untuk membantu organisasi mengidentifikasi dan mengurangi risiko keamanan informasi, serta menetapkan dan memelihara kebijakan dan prosedur keamanan yang ketat.

Arsitektur ISO 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi [11]. ISO 27001 adalah sebuah framework keamanan informasi yang dapat membantu perusahaan untuk mengembangkan dan menerapkan sistem manajemen keamanan informasi (ISMS) yang efektif [12]. Framework ini meningkatkan kepercayaan pelanggan dan meningkatkan kinerja bisnis mereka dengan mengurangi risiko dan memastikan bahwa sistem mereka dilindungi dari ancaman keamanan yang mungkin timbul. Selain itu, ISO 27001 juga membantu perusahaan memenuhi persyaratan hukum dan peraturan terkait keamanan informasi sehingga TurbinCorp dapat mengembangkan bisnis dan penetrasi pasar internasional yang lebih luas. Dalam merencanakan implementasi proses keamanan informasi menggunakan *framework* ISO 27001, perusahaan harus mempertimbangkan tujuan bisnis dan kebutuhan keamanan informasi mereka, serta sumber daya yang tersedia untuk menerapkan standar ini dengan efektif. TurbinCorp juga perlu mengidentifikasi risiko keamanan informasi yang ada dan mengembangkan strategi untuk mengurangi risiko tersebut.

METODOLOGI

1. Kerangka Konsep

Gambar 1 menjelaskan kerangka konsep yang direferensi kan oleh [13] dipergunakan untuk menghubungkan dengan kerangka teori supaya kerangka berpikir dapat terbentuk. Rancangan ini memuat secara keseluruhan terkait penelitian yang akan dikerjakan pada penelitian ini, dibagi menjadi 3 elemen, bagian *Environment* merupakan lingkungan yang digunakan sebagai sarana untuk penelitian yang terdapat 2 komponen yaitu *People* yang merupakan orang-orang berjabatan *Head Unit* dan *Staff* pada divisi Manajemen Sistem Informasi di TurbinCorp yang akan membantu mengumpulkan data untuk penelitian dan *Organization* yang merupakan objek dari penelitian, yakni TurbinCorp. Elemen selanjutnya adalah *IS Research* yang merupakan riset dari penelitian yang dilakukan yang terdapat 2 komponen yaitu *Develop/Build* yang merupakan representasi dari penelitian yang akan dilakukan dan *Justify/Evaluate* yang merupakan pengecekan dari *stakeholder* yang berkaitan terkait hasil penelitian. Terakhir, elemen *Knowledge Base* yang merupakan dasar pengetahuan penelitian yang mempunyai 2 komponen yaitu *Foundations* yang merupakan dasar pembelajaran untuk penelitian seperti keamanan informasi dan kualitatif dan *Methodologies* yang merupakan metode yang digunakan pada penelitian yaitu ISO 27001:2022.



Gambar 1. Model Konseptual
(Diadaptasi dari Hevner DSR [13])

2. Pengumpulan Data

Data yang dikumpulkan terbagi menjadi dua (2) data, yakni data primer dan data sekunder. Pengumpulan data primer dilakukan dengan cara melakukan observasi langsung ke objek penelitian yaitu TurbinCorp dengan wawancara struktural kepada supervisor dan staf dari Departemen Manajemen Sistem Informasi PT. NTP untuk mendapatkan jawaban mengenai keamanan informasi yang sudah diterapkan perusahaan. Pengumpulan data sekunder dikumpulkan dari dokumen-dokumen perusahaan seperti dokumen KP (Ketentuan Pelaksanaan) atau catatan dari perusahaan.

3. Analisis Data

Setelah data terkumpulkan, data kemudian dianalisis menggunakan *framework* ISO 27001:2022. Pertama, peneliti mengidentifikasi data seperti kontrol-kontrol yang sudah ditanyakan, apakah sudah diimplementasi atau belum oleh perusahaan. Selanjutnya, peneliti melakukan analisis kontrol yang teridentifikasi belum dan belum optimal diimplementasikan oleh PT. NTP. Setelah menganalisis kontrol tersebut, penulis akan memberikan usulan rekomendasi kontrol pada kontrol-kontrol yang belum dan belum optimal diimplementasikan. Diharapkan, jika rekomendasi tersebut diimplementasikan, maka bisa menjadi usulan dan referensi ketika perusahaan ingin mengimplementasi atau mendapatkan sertifikasi ISO 27001:2022.

4. Evaluasi

Setelah dilakukan pengumpulan dan analisis data, selanjutnya dilakukan evaluasi. Evaluasi merupakan tahapan untuk menunjukkan keabsahan atau validitas dari proses dan hasil penelitian. Untuk menunjukkan validitas, peneliti menggunakan pendapat dari *stakeholder* dari perusahaan untuk memvalidasi kembali analisis perencanaan yang telah diberikan oleh peneliti.

HASIL DAN PEMBAHASAN

1. Penilaian *Control Existing*

Dalam menentukan prioritas tujuan TKMTI yang menjadi fokus pada penelitian ini, hasil dari *design factor* COBIT 2019 [14] dikalikan dengan nilai area fokus COBIT 2019 *Information Security* [15]. Tabel 1 menampilkan hasil analisis prioritas tujuan TKMTI.

Tabel 1. Penilaian *Control Existing*

Nilai	Deskripsi
0 (N/A)	Klausa/kontrol tidak relevan untuk organisasi
0 (*None*)	Organisasi belum menerapkan klausa/kontrol tersebut sama sekali.
0,5 (*Partially*)	Organisasi belum sepenuhnya menerapkan klausa/kontrol tersebut.
1 (*Fully*)	Organisasi telah menerapkan klausa/kontrol tersebut dengan baik.

Tabel 2 menampilkan hasil penilaian *existing* terhadap klausa. Dalam hasil penilaian existing berdasarkan klausa-klausa yang ada, beberapa temuan kesenjangan telah diidentifikasi. Untuk Klausa 4 yang berkaitan dengan *Context of Organization* dan Klausa 5 tentang *Leadership*, serta Klausa 8 yang membahas *Performance Evaluation*, semua menunjukkan hasil yang memuaskan tanpa adanya kesenjangan. Namun, evaluasi terhadap Klausa 6 yang mencakup *Planning* menunjukkan adanya 1 kesenjangan. Lebih lanjut, Klausa 7 yang terkait dengan *Support dan Operation* masing-masing menunjukkan 3 kesenjangan. Terakhir, pada Klausa 7 yang fokus pada *Improvement*, terdapat 1 kesenjangan. Oleh karena itu, meskipun sebagian besar klausa telah memenuhi kriteria, masih ada beberapa area yang memerlukan perhatian dan perbaikan lebih lanjut.

Tabel 2. Hasil Penilaian Klausa

Section	Sub-Klausa	Skor
Context of Organization Existing		
4.1	*Understanding the organization and its context*	1
4.2	*Understanding the needs and expectations of interested parties*	1
4.3	*Determining the scope of the information security management system*	1
4.4	*Information security management system*	1
Leadership Existing		

Section	**Sub-Klausa**	**Skor**
5.1	*Leadership and commitment*	1
5.2	*Policy*	1
5.3	*Organizational roles, responsibilities and authorities*	1
Planning Existing		
6.1	*Actions to address risks and opportunities*	1
6.2	*Information security objectives and planning to achieve them*	1
6.3	*Planning of changes*	0,5
Support Existing		
7.1	*Resources*	0,5
7.2	*Competence*	0,5
7.3	*Awareness*	0,5
7.4	*Communication*	1
7.5	*Documented information*	1
Performance Evaluation Existing		
8.1	*Operational planning and control*	1
8.2	*Information security risk assessment*	1
8.3	*Information security risk treatment*	1
Operation Existing		
9.1	*Monitoring, measurement, analysis and evaluation*	0,5
9.2	*Internal audit*	0,5
9.3	*Management review*	0,5
Improvement Existing		
10.1	*Continual improvement*	0,5
10.2	*Nonconformity and corrective action*	1

Tabel 3 menampilkan bahwa dari hasil penilaian *existing* dari Kontrol *Annex Organizational Controls*, ditemukan 9 kesenjangan.

Tabel 3. *Organizational Controls Existing*

Section	***Controls***	**Nilai *Existing***
A.5.1	*Policies for information security*	1
A.5.2	*Information security roles and responsibilities*	1
A.5.3	*Segregation of duties*	1
A.5.4	*Management responsibilities*	1
A.5.5	*Contact with authorities*	1
A.5.6	*Contact with special interest groups*	0
A.5.7	*Threat intelligence*	1

Section	*Controls*	Nilai *Existing*
A.5.8	*Information security in project management*	0
A.5.9	*Inventory of information and other associated assets*	1
A.5.10	*Acceptable use of information and other associated assets*	1
A.5.11	*Return of assets*	1
A.5.12	*Classification of information*	1
A.5.13	*Labelling of information*	1
A.5.14	*Information transfer*	1
A.5.15	*Access control*	1
A.5.16	*Identity management*	1
A.5.17	*Authentication information*	1
A.5.18	*Access rights*	1
A.5.19	*Information security in supplier relationships*	1
A.5.20	*Addressing information security within supplier agreements*	1
A.5.21	*Managing information security in the ICT supply chain*	1
A.5.22	*Monitoring, review and change management of supplier services*	1
A.5.23	*Information security for use of cloud services*	1
A.5.24	*Information security incident management planning and preparation*	0,5
A.5.25	*Assessment and decision on information security events*	0,5
A.5.26	*Response to information security incidents*	1
A.5.27	*Learning from information security incidents*	1
A.5.28	*Collection of evidence*	0,5
A.5.29	*Information security during disruption*	1
A.5.30	*ICT readiness for business continuity*	0,5
A.5.31	*Legal, statutory, regulatory and contractual requirements*	1
A.5.32	*Intellectual property rights*	1
A.5.33	*Protection of records*	1
A.5.34	*Privacy and protection of PII*	0
A.5.35	*Independent review of information security*	0,5
A.5.36	*Compliance with policies, rules and standards for information security*	0,5
A.5.37	*Documented operating procedures*	1

Tabel 4 menampilkan bahwa dari hasil penilaian existing dari Kontrol *Annex People Controls*, ditemukan 4 kesenjangan.

Tabel 4. *People Controls Existing*

Section	*Controls*	Nilai *Existing*
A.6.1	*Screening*	0,5
A.6.2	*Terms and conditions of employment*	1
A.6.3	*Information security awareness, education and training*	0,5
A.6.4	*Disciplinary process*	1
A.6.5	*Responsibilities after termination or change of employment*	0,5
A.6.6	*Confidentiality or non-disclosure agreements*	1
A.6.7	*Remote working*	0,5
A.6.8	*Information security event reporting*	1

Tabel 5 menampilkan bahwa dari hasil penilaian existing dari Kontrol Annex *Phyisical Control*, ditemukan 1 kesenjangan.

Tabel 5. *Phyisical Control Existing*

Section	***Controls***	**Nilai *Existing***
A.7.1	*Physical security perimeters*	1
A.7.2	*Physical entry*	1
A.7.3	*Securing offices, rooms and facilities*	1
A.7.4	*Physical security monitoring*	1
A.7.5	*Protecting against physical and environmental threats*	1
A.7.6	*Working in secure areas*	1
A.7.7	*Clear desk and clear screen*	1
A.7.8	*Equipment siting and protection*	1
A.7.9	*Security of assets off-premises*	1
A.7.10	*Storage media*	1
A.7.11	*Supporting utilities*	1
A.7.12	*Cabling security*	0,5
A.7.13	*Equipment maintenance*	1
A.7.14	*Information transfer*	1

Tabel 6 menampilkan bahwa dari hasil penilaian existing dari Kontrol Annex *Technological Controls*, ditemukan 4 kesenjangan.

Tabel 6. *Technological Controls Existing*

Section	***Controls***	**Nilai *Existing***
A.8.1	*User endpoint devices*	1
A.8.2	*Privileged access rights*	1
A.8.3	*Information access restriction*	1
A.8.4	*Access to source code*	1
A.8.5	*Secure authentication*	1
A.8.6	*Capacity management*	1
A.8.7	*Protection against malware*	1
A.8.8	*Management of technical vulnerabilities*	1
A.8.9	*Configuration management*	1
A.8.10	*Information deletion*	1
A.8.11	*Data masking*	1
A.8.12	*Data leakage prevention*	1
A.8.13	*Information backup*	1
A.8.14	*Redundancy of information processing facilities*	1
A.8.15	*Logging*	1
A.8.16	*Monitoring activities*	1
A.8.17	*Clock synchronization*	1
A.8.18	*Use of privileged utility programs*	1
A.8.19	*Installation of software on operational systems*	1
A.8.20	*Networks security*	1
A.8.21	*Security of network services*	1
A.8.22	*Segregation of networks*	1

Section	*Controls*	Nilai *Existing*
A.8.23	*Web filtering*	1
A.8.24	*Use of cryptography*	0,5
A.8.25	*Secure development life cycle*	1
A.8.26	*Application security requirements*	0,5
A.8.27	*Secure system architecture and engineering principles*	0,5
A.8.28	*Secure coding*	1
A.8.29	*Security testing in development and acceptance*	1
A.8.30	*Outsourced development*	1
A.8.31	*Separation of development, test and production environments*	1
A.8.32	*Change management*	1
A.8.33	*Test information*	0
A.8.34	*Protection of information systems during audit testing*	1

2. *Gap Assessment*

Gap Assessment adalah evaluasi yang dilakukan untuk mengidentifikasi perbedaan antara kondisi saat ini dan kondisi yang diinginkan atau standar yang ditetapkan. yaitu penilaian terhadap kondisi saat ini dan kondisi yang diharapkan berdasarkan standar ISO 27001:2022. Tujuannya adalah untuk mengidentifikasi sejauh mana TurbinCorp telah mencapai pencapaian keamanan informasi mereka. Evaluasi kesenjangan ini dilakukan dengan memeriksa setiap klausa dan kontrol sesuai dengan ISO 27001:2022 yang diharapkan seluruhnya sudah memenuhi ≥80% supaya dapat mengajukan sertifikasi ISO yang direferensikan pada *best practice* ISO. Berikut hasil dari *Gap Assessment*. Tabel 7 menampilkan hasil *gap assessment* klausa.

Tabel 7. Hasil *Gap Asessment* Klausa

Area dalam Standar	Jumlah Persyaratan	Jumlah Terpenuhi	*Conformant*
Context of the Organization	4	4	100%
Leadership	3	3	100%
Planning	3	2	66,67%
Support	5	3	60%
Operation	3	3	100%
Performance Evaluation	3	0	0%
Improvement	2	1	50%
Total Klausul	**23**	**16**	**69,56%**

Tabel 8 menampilkan hasil gap assessment control annex

Tabel 8. Hasil *Gap Asessment Control Annex*

Area dalam Standar	Jumlah Persyaratan	Jumlah Terpenuhi	*Conformant*
Organizational Controls	37	28	75,68%
People Controls	8	4	50%
Physical Controls	14	13	92,86%
Technological Controls	34	30	88,24%
Total Kontrol Annex	**93**	**75**	**80,65%**

3. Perancangan Sistem Manajemen Keamanan Informasi

Perancangan Sistem Manajemen Keamanan Informasi ini melibatkan suatu usulan yang bertujuan untuk mengubah kondisi *existing* menjadi nilai yang dapat memenuhi persyaratan sertifikasi ISO 27001:2022 dengan merencanakan, menyesuaikan, dan mengatur keamanan informasi yang ada di TurbinCorp agar sesuai dengan sistem manajemen keamanan sistem informasi yang didasarkan pada ISO 27001:2022 dan menggunakan kontrol-kontrol pada ISO 27001:2022 sebagai acuan pencapaian sistem manajemen keamanan sistem informasi. Perancangan ini melibatkan aspek *people*, *process*, dan *technology* [16] dengan tipe rekomendasi seperti pada Tabel 15. Berikut persyaratan yang belum terpenuhi dan diberi rekomendasi supaya memenuhi nilai yang di targetkan supaya perusahaan bisa mengajukan sertifikasi ISO 27001:2022 yaitu ≥80% yang berdasarkan *best practice* kerangka kerja tersebut. Tabel 9 menampilkan perancangan rekomendasi SMKI.

Tabel 9. Perancangan Rekomendasi SMKI

Klausa	Temuan	Tipe
Aspek *People*		
A.5.6 *Contact with special interest groups*	Organisasi belum membangun kontak dengan kelompok minat khusus ataupun forum keamanan khusus lainnya dan asosiasi profesional.	*Skill & Awareness*
A.6.3 *Information security awareness, education and training*	Organisasi belum melakukan pelatihan tentang keamanan informasi.	*Skill and Awareness*
7.1 *Resources*	Perusahaan belum menentukan sumber daya untuk sistem manajemen keamanan informasi	*Roles and Responsibility*
Aspek *Process*		
6.3 *Planning of changes*	Organisasi belum melakukan perubahan sistem manajemen keamanan informasi terencanana	*Procedure*
9.1	Organisasi tidak menyediakan prosedur tertulis	*Procedure*

Klausa	Temuan	Tipe
Monitoring, measurement, analysis and evaluation		
9.2 *Internal audit*	tidak ada audit internal untuk keamanan informasi.	*Procedure*
9.3 *Management review*	Tidak ada peninjauan SMKI secara terencana	*Procedure*
10.1 *Continual improvement*	Organisasi meningkatkan efektivitas sistem manajemen keamanan informasi jika ada kasus atau arahan dari top *management*.	*Procedure*
A.5.28 *Collection of evidence*	Organisasi belum menetapkan prosedur tertulis terkait pengumpulan dan bukti kejadian keamanan informasi.	*Procedure*
A.6.5 *Responsibilities after termination or change of employment*	Organisasi belum menetapkan tanggung jawab dan kewajiban keamanan informasi yang tetap berlaku secara tertulis setelah pemutusan kerja, tetapi dikomunikasikan secara langsung.	*Policy*
Aspek *Technology*		
A.6.7 *Remote working*	Organisasi belum sepenuhnya menerapkan tindakan keamanan ketika bekerja dari jarak jauh dikarenakan hanya memakai *messenger* untuk berkomunikasi.	*Tools*

4. Perancangan Aspek *People*

Perancangan pada aspek *people* menghasilkan tiga (3) rekomendasi yang terbagi menjadi *roles, responsibility,* dan *skill and awareness*. Pada *roles and responsibility,* terdapat penambahan peran *information security manager* yang mengelola, merancang, mengawas, dan/atau menilai keamanan informasi [17]. Pada *skill and awareness*, terdapat rekomendasi untuk melakukan pelatihan terkait manajemen risiko, keamanan jaringan, keamanan aplikasi, penanganan insiden, kebijakan dan prosedur khusus dan audit keamanan. Selain itu, terdapat rekomendasi untuk dapat bergabung dengan kelompok kepentingan khusus, forum keamanan, maupun asosiasi professional.

5. Perancangan Aspek *Process*

Perancangan pada aspek *process* menghasilkan sembilan (9) rekomendasi, yakni penyusunan kebijakan mengenai tanggung jawab dan kewajiban keamanan informasi setelah perubahaan status kerja, kebijakan terkait praktik pelaksanaan pekerjaan jarak jauh, menyusun prosedur terkait perubahan pada keamanan TI, prosedur penentuan tanggung jawab dan pemilik untuk setiap sumber daya, prosedur pemantauan dan analisis keamanan informasi, prosedur terkait audit keamanan informasi, prosedur peninjauan SMKI, prosedur peninjauan rutin serta prosedur pengumpulan bukti kejadian keamanan informasi.

6. Perancangan Apsek *Technology*

Perancangan pada aspek *technology* menghasilkan dua (2) rekomendasi, yakni pergantian *messenger* dengan aplikasi komunikasi yang telah dilengkapi dengan enkripsi *end-to-end* serta penggunaan VPN untuk memastikan koneksi yang aman [18].

7. *Roadmap* Implementasi

Tabel 10 menampilkan *roadmap* yang merujuk pada usulan jadwal dan rencana pengimplementasian dari rekomendasi yang telah diberikan. Ini merupakan panduan yang mengarahkan langkah-langkah yang harus diambil dan menerapkan rekomendasi dengan baik. *Roadmap* ini menyediakan gambaran mengenai tahapan-tahapan yang harus diselesaikan, waktu yang diperlukan untuk setiap langkah

Tabel 10. *Roadmap* Implementasi

Kegiatan	**Jangka Waktu 2024**			
	Q1	**Q2**	**Q3**	**Q4**
Aspek *People*				
A.5.6 *Contact with special interest groups*				
6.3 *Information security awareness, education, and training*				
7.1 *Resources*				
Aspek *Process*				
6.3 Planning of Changes				
9.1 Monitoring, Measurement, Analysis and Evaluation				
9.2 Internal Audit				
9.3 Management Review				
10.1 Continual Improvement				
A.5.28 Collection of evidence				
A.6.5 Responsibilities after termination or change of employment				
Aspek *Technology*				
A.6.7 Remote Working				

8. Estimasi Usulkan Rancangan

Setelah merancang rekomendasi berdasarkan aspek *people, process,* dan *technology,* dibuatkan perbandingan untuk membandingkan keadaan TurbinCorp sebelum dan sesudah diterapkannya rekomendasi tersebut. Tabel 11 menampilkan bahwa setelah rekomendasi jumlah persyaratan yang terpenuhi pada area *Context of the Organization* adalah 4 dari 4 persyaratan, jumlah persyaratan yang terpenuhi pada area *Leadership* adalah 3 dari 3 persyaratan. jumlah persyaratan yang terpenuhi pada area *Planning* adalah 2 dari 3 persyaratan, jumlah persyaratan yang terpenuhi pada area *Support* adalah 4 dari 5 persyaratan, jumlah persyaratan yang terpenuhi pada area *Operation* adalah 3 dari 3 persyaratan, jumlah persyaratan yang terpenuhi pada area *Performance Evaluation* adalah 0 dari 3 persyaratan, dan jumlah persyaratan yang terpenuhi pada area Improvement adalah 1 dari 2 persyaratan.

Tabel 11. Estimasi Hasil *Gap Assessment* Klausa

Area dalam Standar		**Jumlah Persyaratan**	**Jumlah Terpenuhi**	**% *Conformant***
4	*Context of the Organization*	4	4	100%
5	*Leadership*	3	3	100%
6	*Planning*	3	3	100%
7	*Support*	5	4	80%
8	*Operation*	3	3	100%
9	*Performance Evaluation*	3	3	100%
10	*Improvement*	2	2	100%
Total Klausul		**23**	**22**	**95,6%**

Tabel 12 menampilkan bahwa setelah rekomendasi jumlah persyaratan yang terpenuhi pada area *Organizational Controls* adalah 30 dari 37 persyaratan, jumlah persyaratan yang terpenuhi pada area *People Controls* adalah 7 dari 8 persyaratan, jumlah persyaratan yang terpenuhi pada area *Physical Controls* adalah 13 dari 14 persyaratan, dan jumlah persyaratan yang terpenuhi pada area *Technological Controls* adalah 30 dari 34 persyaratan.

Tabel 12. Estimasi Hasil *Gap Assessment Control Annex*

Area dalam Standar		**Jumlah Persyaratan**	**Jumlah Terpenuhi**	**% *Conformant***
A.5	*Organizational Controls*	37	30	81%
A.6	*People Controls*	8	7	87,5%
A.7	*Physical Controls*	14	13	92,86%
A.8	*Technological Controls*	34	30	88,24%
A.5	*Organizational Controls*	37	30	81%
A.6	*People Controls*	8	7	87,5%

Area dalam Standar	Jumlah Persyaratan	Jumlah Terpenuhi	% *Conformant*
Total Kontrol Annex	**93**	**80**	**86%**

SIMPULAN

Hasil proses perancangan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001:2022 di TurbinCorp menunjukkan bahwa klausa utama ISO 27001:2022, yaitu Klausa 4 (Context of Organization), Klausa 5 (Leadership), dan Klausa 8 (Operation), sudah memenuhi syarat. Namun, masih ada beberapa klausa yang belum sepenuhnya memenuhi syarat, yaitu Klausa 6 (Planning), Klausa 7 (Support), Klausa 9 (Performance Evaluation), dan Klausa 10 (Improvement). Selain itu, dari 37 persyaratan dalam kontrol Annex A ISO 27001:2022 untuk Organizational Controls, terdapat 9 kontrol yang belum terpenuhi di TurbinCorp Kontrol Annex A ISO 27001:2022 untuk Pengendalian A.5 (People Controls) memiliki 4 kontrol yang belum terpenuhi. Pengendalian A.6 (Physical Controls) juga memiliki 1 kontrol yang belum terpenuhi, begitu juga dengan Pengendalian A.7 (Technological Controls) yang memiliki 4 kontrol yang belum terpenuhi di TurbinCorp. Rekomendasi untuk mengatasi masalah ini adalah untuk Pengendalian A.7 yaitu mengusulkan kelompok minat khusus, pelatihan, dan sertifikasi pada TurbinCorp Dalam hal proses, disarankan untuk membuat beberapa prosedur dan kebijakan tambahan pada TurbinCorp Sementara itu, dalam bidang teknologi, diusulkan untuk menggunakan beberapa software tambahan pada TurbinCorp untuk memenuhi persyaratan keamanan informasi.

Referensi

[1] H. T. Murti, V. Puspita, and P. Ratih, "Pemanfaatan Teknologi Informasi dan Manajemen Perubahan Organisasi dalam Mendukung Bisnis Berkelanjutan Pasca Covid-19 pada UMKM di Kota Bengkulu (Utilization of Information Technology and Organizational Change Management to support Post-Covid 19 Sustainable Business for MSMEs in Bengkulu City)," vol. 1, no. 1, 2021.

[2] F. Gunadi and S. R. Widianto, "Perbandingan Data Warehouse Cloud Computing Menggunakan Konvensional Berbasis Kriptografi," 2020.

[3] R. McLeod, *Sistem Informasi Manajemen*. Jakarta : Salemba Empat, 2008.

[4] T. Kristanto, R. Arief, and N. F. Rozi, "PERANCANGAN AUDIT KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2005 (STUDI KASUS: PT ADIRA DINAMIKA MULTI FINANCE)," 2014.

[5] J. B. Anderson and R. Johannesson, "Understanding Information Transmission".

[6] H. P. Yockey, "Information theory, evolution and the origin of life," *Information Sciences*, 2002.

[7] D. Simarmata and D. M. Situmorang, "PENERAPAN SISTEM INFORMASI AKUNTANSI KOTA BATAM," 2023.

[8] R. Budiarto, "MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI MENGGUNAKAN METODE FMEA DAN ISO 27001 PADA ORGANISASI XYZ," vol. 2, no. 2, 2017.

[9] M. Lenawati, W. W. Winarno, and A. Amborowati, "Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5," vol. 9, no. 1, 2017.
[10] F. A. Basyarahil, H. M. Astuti, and J. A. R. Hakim, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya," vol. 6, no. 1, 2017.
[11] C. Chazar, "STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005," 2015.
[12] B. Shojaie, "Implementation of Information Security Management Systems based on the ISO/IEC 27001 Standard in different cultures," Feb. 2018.
[13] Hevner, March, Park, and Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, p. 75, 2004, doi: 10.2307/25148625.
[14] ISACA, *COBIT® 2019 Implementation guide: implementing and optimizing an information and technology governance solution*. Schaumburg, Illinois: ISACA, 2018.
[15] ISACA, *COBIT Focus Area: Information Security Using COBIT 2019*. ISACA, 2020.
[16] A. Viamianni, R. Mulyana, and F. Dewi, "COBIT 2019 INFORMATION SECURITY FOCUS AREA IMPLEMENTATION FOR REINSURCO DIGITAL TRANSFORMATION," 2023.
[17] SFIA Foundation, *Skills Framework for the Information Age: Framework Reference*. 2021.
[18] Gartner, "Gartner Magic Quadrant & Critical Capabilities," 2023. https://www.gartner.com/en/research/magic-quadrant