Strategi Optimalisasi Manajemen Konfigurasi untuk Keamanan Informasi Berdasarkan ISO/IEC 27001:2022

Febri Pujiani[1], Rahadian Bisma[2]

[1,2]S1 Sistem Informasi, Fakultas Teknik, Universitas Negeri Surabaya
[1]febripujiani.20066@mhs.unesa.ac.id
[2]rahadianbisma@unesa.ac.id

***Abstrak*— Keamanan informasi merupakan salah satu aspek yang krusial bagi organisasi. Upaya peningkatan keamanan informasi juga harus menjadi fokus utama untuk meminimalisir segala risiko yang bisa saja terjadi pada organisasi. Kerentanan keamanan ini juga berkaitan dengan manajemen konfigurasi. Sering kali serangan menargetkan area yang diatur dalam manajemen konfigurasi seperti perangkat lunak, perangkat keras, maupun pengaturan jaringan. Perubahan yang tidak terkontrol juga menjadi masalah serius pada proyek perangkat lunak. Manajemen konfigurasi memberikan kontrol untuk mengelola perubahan, karena perubahan yang tidak sah dan ketidakkonsistenan dapat terhindarkan. Selain itu, manajemen konfigurasi masih menjadi pendekatan baru untuk mengelola keamanan informasi terutama pada standar ISO/IEC 27001:2022, sehingga banyak organisasi yang belum familiar dengan konsep dan penerapannya. Hal ini menjadikan manajemen konfigurasi sebagai tantangan tersendiri bagi organisasi yang ingin memperbarui atau mendapatkan sertifikasi ISO/IEC 27001:2022. Dengan permasalahan yang telah dijabarkan, maka perlu dilakukan analisis proses dari manajemen konfigurasi untuk membantu organisasi memahami bagaimana menerapkan manajemen konfigurasi yang efektif sesuai dengan standar internasional, sehingga dapat mengurangi risiko keamanan dan memastikan sistem informasi tetap aman dan terkendali. Dalam penelitian ini menghasilkan 3 aktivitas utama untuk manajemen konfigurasi dan 4 dokumen untuk mendukung implementasi manajemen konfigurasi untuk membantu organisasi dalam pengelolaan konfigurasi yang efektif sesuai dengan standar internasional ISO/IEC 27001:2022.**

***Kata Kunci*— Keamanan Informasi, Manajemen Konfigurasi, ISO/IEC 27001:2022**

I. PENDAHULUAN

Ketersediaan teknologi informasi telah menjadi kebutuhan utama dalam berbagai aspek kehidupan modern, terutama dalam konteks menjalankan aktivitas bisnis [1]. Hal ini dikarenakan teknologi informasi dapat menunjang kegiatan bisnis dalam meningkatkan efisiensi, efektivitas, dan produktivitas organisasi [2]. Oleh karena itu, keamanan informasi merupakan salah satu aspek yang paling krusial bagi organisasi. Semakin berkembangnya teknologi juga akan diikuti dengan peningkatan kerentanan keamanan yang dapat menjadi ancaman serius. Upaya peningkatan keamanan informasi juga harus menjadi fokus utama untuk meminimalisir segala risiko yang bisa saja terjadi pada organisasi.

Kerentanan keamanan ini juga berkaitan dengan manajemen konfigurasi. Sering kali serangan menargetkan area yang diatur dalam manajemen konfigurasi seperti perangkat lunak, perangkat keras, maupun pengaturan jaringan. Selain dari sisi keamanan informasi, kurangnya manajemen konfigurasi justru menyebabkan masalah serius pada keandalan, waktu kerja, dan kemampuan untuk meningkatkan skala sistem. Selain itu, minimnya dokumentasi mengenai konfigurasi dapat menyulitkan proses pemulihan ketika terjadi insiden keamanan.

Perubahan yang tidak terkontrol menjadi masalah serius pada proyek perangkat lunak. Manajemen konfigurasi memberikan kontrol untuk mengelola perubahan, karena perubahan yang tidak sah dan ketidakkonsistenan dapat terhindarkan. Tim juga dapat bekerja secara paralel dan penggabungan kode secara terkendali. Tanpa manajemen konfigurasi yang efektif, bisa saja menyulitkan tim untuk kembali ke versi perangkat lunak sebelumnya. Masalah yang sama dapat terus terjadi di versi berikutnya apabila perubahan tidak diawasi dan dicatat dengan baik.

Selain permasalahan dari sisi teknis, manajemen konfigurasi masih menjadi pendekatan baru untuk mengelola keamanan informasi terutama pada standar ISO/IEC 27001:2022. Pada versi sebelumnya yakni ISO/IEC 27001:2013 belum diterapkan, sehingga banyak organisasi yang belum familiar dengan konsep dan penerapannya. Organisasi juga harus melakukan penyesuaian internal, karena perlu mengembangkan kebijakan baru dan melatih staf untuk mengelola konfigurasi dengan baik. Hal ini menjadikan manajemen konfigurasi sebagai tantangan tersendiri bagi organisasi yang ingin memperbarui atau mendapatkan sertifikasi ISO/IEC 27001:2022.

Manajemen konfigurasi penting untuk dilakukan karena dapat menyediakan model dasar dan logis dari infrastruktur TI suatu organisasi dengan mengidentifikasi, mengendalikan, memelihara, dan memverifikasi status dan versi *Configuration Item* (CI) di lingkungan TI [3]. Elemen manajemen konfigurasi yang dijelaskan oleh ISO/IEC 27001:2022 meliputi *hardware*, *software*, layanan, dan jaringan. Seluruh elemen tersebut harus dilakukan manajemen konfigurasi agar mampu berfungsi dengan baik sesuai dengan pengaturan keamanan yang dipersyaratkan, dan konfigurasi yang telah ditentukan tidak diubah secara tidak terotorisasi dan tidak sah [4].

Berdasarkan uraian yang telah dijabarkan, penelitian ini akan menganalisis proses dari manajemen konfigurasi berdasarkan ISO/IEC 27001:2022. Standar ISO/IEC 27001:2022 akan digunakan untuk menentukan panduan yang harus dilakukan untuk melakukan pengelolaan konfigurasi. Sehingga peneliti membuat sebuah penelitian yang berjudul "Analisis Manajemen Konfigurasi Berdasarkan ISO/IEC 27001:2022" yang bertujuan untuk membantu organisasi memahami bagaimana menerapkan manajemen konfigurasi yang efektif sesuai dengan standar internasional, sehingga

dapat mengurangi risiko keamanan dan memastikan sistem informasi tetap aman dan terkendali.

II. LANDASAN TEORI

A. Keamanan Informasi

Secara sederhana keamanan informasi merupakan upaya menjaga *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan), atau yang biasa dikenal sebagai konsep C-I-A triad [5]. Keamanan informasi berarti melindungi aset dari penyerang yang menyerang jaringan, virus, bencana alam, kondisi lingkungan yang merugikan, gangguan listrik, pencurian dan perusakan, atau kondisi lain yang tidak diinginkan. Untuk mencapai tujuan keamanan informasi, langkah penting yang perlu dilakukan yakni melalui implementasi serangkaian kontrol yang sesuai, termasuk kebijakan, aturan, proses, prosedur, struktur organisasi, fungsi perangkat lunak, maupun perangkat keras [4]. Berikut adalah aspek-aspek penting yang harus diperhatikan dalam merancang sistem keamanan informasi, yang juga menjadi fokus penelitian ini:

1) Kerahasiaan (confidentiality): memastikan bahwa informasi dalam organisasi hanya dapat diakses oleh pihak yang berwenang dan diawasi dengan baik.;
2) Integritas (integrity): memastikan bahwa informasi dalam organisasi tetap akurat, lengkap, dan tidak dapat diubah oleh pihak yang tidak berwenang.
3) Ketersediaan (availability): memastikan bahwa informasi dalam organisasi selalu tersedia dan mudah diakses sesuai kebutuhan.

Jika semua aspek di atas terpenuhi, maka informasi dapat dianggap aman. Namun, jika salah satu aspek tidak terpenuhi, hal tersebut dapat mengakibatkan insiden keamanan informasi.

Berdasarkan penjabaran di atas, maka dapat disimpulkan bahwa keamanan informasi merupakan upaya untuk melindungi informasi dengan menjaga kerahasiaan, integritas, dan ketersediaannya, dengan melakukan penerapan kontrol yang meliputi kebijakan, prosedur, aturan, ataupun regulasi yang sesuai.

B. Manajemen Konfigurasi

Secara singkat, manajemen konfigurasi merujuk pada pengaturan komponen-komponen sistem komputer agar dapat berfungsi sesuai dengan tugas yang ditetapkan. Manajemen konfigurasi juga merupakan suatu proses teknis dan manajerial yang menerapkan sumber daya, metode, dan perangkat yang sesuai untuk mendefinisikan serta memastikan konsistensi antara persyaratan produk, produk itu sendiri, dan informasi terkait konfigurasi produk [6]. COBIT 2019 mendeskripsikan manajemen konfigurasi sebagai proses pendefinisian dan pemeliharaan deskripsi serta hubungan antara sumber daya utama dan kemampuan yang diperlukan untuk memberikan layanan yang didukung oleh Teknologi Informasi. Ini mencakup langkah-langkah seperti pengumpulan informasi konfigurasi, pembentukan baseline, verifikasi dan audit informasi konfigurasi, serta pembaruan repositori konfigurasi [7].

Berdasarkan beberapa pengertian di atas maka dapat disimpulkan, bahwa manajemen konfigurasi merupakan proses teknis dan manajerial yang melibatkan pengaturan, pendefinisian, pemeliharaan, verifikasi, dan pembaruan komponen serta informasi dari sistem untuk memastikan konsistensi antara persyaratan produk dan layanannya sesuai dengan standar. Manajemen konfigurasi dapat membantu mengakomodasi perubahan, mengurangi waktu penyelesaian insiden secara signifikan dengan menggunakan repositori pusat data infrastruktur, serta menyediakan informasi konfigurasi yang akurat untuk membuat sebuah keputusan [8].

C. ISO/IEC 27001:2022

ISO/IEC 27001 merupakan standar untuk Sistem Manajemen Keamanan Informasi (SMKI) yang diterbitkan oleh *The Internasional Organization for Standarization* (ISO) pada tahun 2022. Standar ini berisi mengenai spesifikasi atau persyaratan yang harus dipenuhi untuk membangun sistem manajemen keamanan informasi (SMKI). Standar ISO/IEC 27001 memberikan panduan bagi perusahaan berbagai ukuran dan sektor kegiatan untuk membangun, menerapkan, memelihara, dan peningkatan keberlanjutan sistem manajemen keamanan informasi [4]. Standar ini melakukan pendekatan berbasis manajemen risiko. Hal ini bertujuan untuk menjamin kontrol-kontrol yang diterapkan mampu melindungi aset informasi dari berbagai risiko, sehingga mampu meningkatkan keyakinan keamanan bagi pihak yang berkepentingan [5]. Untuk mengimplementasi SMKI ini harus didukung dengan perencanaan (*planning*), kebijakan keamanan (*security policy*), program (*prosedur dan proses*), penilaian risiko (*risk assessment*) dan sumber daya manusia (*people*) [9].

Standar ini menggunakan pendekatan proses "*Plan-Do-Check-Act*" (PDCA). Siklus PDCA akan memberikan gambaran untuk implementasi tata kelola dan kesesuaian dengan tujuan Perusahaan. Berikut merupakan gambaran siklus PDCA.

Gbr. 1 Siklus PDCA

Berdasarkan Gambar 1, berikut merupakan penjelasan mengenai siklus PDCA:

TABEL I
SIKLUS PDCA

Plan (establish the ISMS)	Pada tahap ini, perencanaan dan perancangan Sistem Manajemen Keamanan Informasi (SMKI) dilakukan dengan membangun komitmen, kebijakan, kontrol, prosedur, dan instruksi kerja yang berkaitan dengan pengelolaan risiko dan peningkatan keamanan informasi untuk menciptakan SMKI yang sesuai dengan tujuan yang diinginkan
Do (implement and operate the ISMS)	Pada tahap ini, kebijakan, kontrol, proses, dan prosedur SMKI yang telah dibuat diterapkan dan dioperasikan.
Check (monitor and review the ISMS)	Pada tahap ini, pelaksanaan SMKI dipantau dan dievaluasi. Audit dilakukan untuk mengukur kinerja proses terhadap kebijakan, tujuan, dan praktik SMKI yang telah dijalankan.
Act (maintain and improve the ISMS)	Pada tahap ini, tindakan perbaikan dan pencegahan diambil berdasarkan hasil audit internal dan tinjauan manajemen, serta informasi relevan lainnya, untuk mencapai peningkatan berkelanjutan dari SMKI.

ISO/IEC 27001:2022 memiliki 10 klausul dan tujuh di antaranya merupakan prasyarat utama yakni klausul 4 sampai dengan klausul 10 yang harus dipenuhi. Standar ini juga memiliki 93 kontrol dalam 4 domain kontrol yang disebut sebagai *Annex* A. *Annex* A ini mengontrol organisasi, orang, fisik, dan teknologi. Kontrol A05 Organisasi berjumlah 37 kontrol, A06 Orang berjumlah 8 kontrol, A07 Fisik berjumlah 14 kontrol, dan A08 Teknologi berjumlah 34 kontrol.

III. METODE PENELITIAN

A. *Tahapan Penelitian*

Penelitian ini menggunakan pendekatan kualitatif karena data yang dihasilkan merupakan data deskriptif tertulis dari eksplorasi yang bersumber dari standar ISO/IEC 27001:2022 mengenai manajemen konfigurasi dan studi pustaka yang terdiri dari artikel, jurnal, maupun dokumen sejenisnya serta pencarian di internet terkait dengan masalah dan tujuan penelitian. Tahapan penelitian ini meliputi:

1. Identifikasi Masalah
   Identifikasi masalah dilakukan untuk merumuskan permasalahan yang dihadapi sebagai tujuan penelitian ini. Identifikasi masalah dalam penelitian ini adalah mengenai perumusan manajemen konfigurasi sesuai dengan standar ISO/IEC 27001:2022, sehingga dapat diketahui proses seperti apa yang harus diterapkan untuk manajemen konfigurasi secara efektif.
2. Studi Literatur
   Tahap ini melibatkan pencarian sumber-sumber informasi yang relevan mengenai manajemen konfigurasi berdasarkan ISO/IEC 27001:2022 untuk mendapatkan teori terkait manajemen konfigurasi. Selain bersumber dari standar tersebut, studi literatur juga dilakukan dengan cara mencari artikel nasional dan internasional, jurnal, maupun referensi lainnya sebagai dasar pengetahuan untuk memahami landasan teori.
3. Analisis Standar ISO/IEC 27001:2022 – *Management Configuration*
   Tahap analisis *framework* ISO/IEC 27001:2022 dilakukan untuk mengetahui konsep, cakupan, panduan, maupun proses dari manajemen konfigurasi. dari hasil analisis ini nantinya akan dijadikan dasar acuan peneliti dalam menentukan panduan aktivitas maupun aspek lain untuk manajemen konfigurasi agar sesuai dengan standar ISO/IEC 27001:2022.
4. Menentukan Panduan Aktivitas Manajemen Konfigurasi
   Tahapan ini merupakan hasil dari analisis pada standar ISO/IEC 27001:2022 yang selanjutnya akan diperoleh aktivitas proses dalam manajemen konfigurasi.
5. Kesimpulan
   Tahap ini akan diperoleh perumusan manajemen konfigurasi berdasarkan standar ISO/IEC 27001:2022. Tahap ini juga menghasilkan saran untuk perbaikan dan penyempurnaan penelitian di masa mendatang.

B. *Pengumpulan Data*

Pengumpulan data merupakan tahapan yang dilakukan untuk memperoleh informasi yang dibutuhkan untuk mencapai tujuan penelitian. Pengumpulan data pada penelitian ini meliputi:

1. Studi Pustaka
   Studi pustaka dilakukan sebagai upaya untuk memperoleh data valid yang bersifat teori serta memberikan gambaran dalam penerapan manajemen konfigurasi sesuai dengan standar ISO/IEC 27001:2022. Data tersebut diperoleh dengan mempelajari *e-book*, buku, artikel, hasil penelitian terdahulu berbentuk jurnal, maupun dokumen sejenis yang berkaitan dengan topik penelitian ini.
2. Pencarian di Internet (*Internet Research*)
   Penelusuran internet dilakukan peneliti sebagai salah satu cara mengumpulkan data, karena dari penelusuran internet memiliki cakupan literatur yang lebih luas, serta terdapat banyak informasi yang relevan dengan topik ini sehingga bermanfaat sebagai penunjang penelitian yang akan dilakukan.

IV. HASIL DAN PEMBAHASAN

A. *Analisis Framework ISO/IEC 27001:2022 – Management Configuration*

Manajemen Konfigurasi pada ISO/IEC 27001:2022 merupakan kontrol terbaru yang tertuang dalam ISO/IEC 27002:2022. Manajemen konfigurasi ini termasuk dalam pengendalian teknologi yaitu pada A.8.9 *Configuration Management.* Manajemen konfigurasi dapat memproteksi dari keamanan siber secara preventif. Kontrol dari konfigurasi ini termasuk konfigurasi keamanan, perangkat keras, perangkat lunak, layanan, dan jaringan. Komponen konfigurasi ini perlu ditetapkan, didokumentasikan, diimplementasikan, dimonitor, dan ditinjau, untuk memastikan bahwa komponen tersebut berfungsi dengan benar sesuai dengan pengaturan keamanan yang dipersyaratkan, dan konfigurasi tidak diubah secara tidak terotorisasi dengan benar [4]. Berikut merupakan panduan manajemen konfigurasi berdasarkan standar ISO/IEC 27001:2022:

TABEL II
PANDUN MANAJEMEN KONFIGURASI

Objektif Kontrol	Panduan Manajemen Konfigurasi	Detail Panduan	Tipe Kontrol
A.8.9 *Configuration Management* (Manajemen Konfigurasi)	Mendefinisik-an *template* standar konfigurasi	Pendefinisian *template* konfigurasi dengan mempertimbang kan level proteksi yang dibutuhkan, kelayakan untuk diterapkan, maupun mendukung kebijakan keamanan informasi yang berlaku di organisasi.	Preventif
	Mengelola konfigurasi	Meninjau *template* konfigurasi secara periodik dan memperbarui ketika muncul ancaman atau kerentanan, maupun terdapat perubahan versi perangkat. Konfigurasi *software*, *hardware*, layanan, dan jaringan yang telah ditetapkan, dicatat dan log dikelola ketika terjadi perubahan konfigurasi.	
	Monitoring konfigurasi	*Monitoring* konfigurasi dapat menggunakan seperangkat alat manajemen sistem dan dilakukan peninjauan secara teratur untuk memastikan kepatuhan terhadap kebijakan keamanan informasi.	

1) Ruang Lingkup Manajemen Konfigurasi

Ruang lingkup manajemen konfigurasi yaitu memastikan konfigurasi hardware, software, layanan, dan jaringan dapat berfungsi sesuai dengan pengaturan keamanan yang dipersyaratkan dan mampu meminimalisir perubahan yang tidak sah. Berikut merupakan penjabaran mengenai jenis item kofigurasi:

TABEL III
JENIS ITEM KONFIGURASI

Jenis Item Konfigurasi	Keterangan
Perangkat Keras	Meliputi semua elemen fisik sistem teknologi informasi yang digunakan dalam operasional TI. Penting dipilih karena mempengaruhi kinerja dan keamanan sistem secara langsung.
Perangkat Lunak	Mencakup semua program dan aplikasi yang digunakan dalam operasional TI. Penting dipilih karena mempengaruhi kinerja dan keamanan sistem secara langsung.
Layanan	Merujuk pada layanan yang disediakan oleh atau untuk organisasi, baik untuk layanan internal maupun eksternal.

Jenis Item Konfigurasi	Keterangan
	Layanan dan jaringan penting untuk dipilih karena mendukung operasional dan konektivitas sistem secara keseluruhan.
Jaringan	Merujuk pada sistem dari perangkat keras dan perangkat lunak yang memungkinkan komputer dan perangkat lain saling terhubung dalam organisasi, untuk mendukung operasional sistem secara keseluruhan.

2) Aktivitas Manajemen Konfigurasi

Berdasarkan **Tabel II** peneliti melakukan analisis untuk menentukan panduan aktivitas yang diperlukan untuk manajemen konfigurasi. Berikut merupakan panduannya:

a) Mendefinisikan *template* standar konfigurasi

Pada aktivitas ini, organisasi perlu mendefinisikan template konfigurasi dengan mempertimbangkan level proteksi yang dibutuhkan, kelayakan untuk diterapkan, maupun mendukung kebijakan keamanan informasi yang berlaku di organisasi. Pendefinisian template ini juga dapat menggunakan panduan untuk umum seperti yang telah didefinisikan oleh vendor.

b) Mengelola konfigurasi

Pengelolaan konfigurasi dilakukan dengan melakukan peninjauan dari template konfigurasi secara periodik dan memperbarui ketika muncul ancaman, kerentanan, ataupun terdapat perubahan versi perangkat. Kegiatan pengelolaan konfigurasi ini dapat meliputi:

- Peninjauan dan pembaruan berkala
  Template konfigurasi secara rutin ditinjau dan diperbarui dengan menetapkan jadwal. Dalam rangkaian peninjauan ini, terdapat aktivitas pengidentifikasian ancaman yang mungkin mempengaruhi konfigurasi saat ini.
- Pengelolaan hak akses
  Langkah ini dilakukan dengan meminimalkan jumlah pengguna hak akses khusus atau administrator, sehingga pengguna yang tidak perlu atau tidak aman dapat dinonaktifkan.
- Pembatasan fungsi dan layanan
  Fungsi dan layanan yang sudah tidak diperlukan atau tidak digunakan dapat dibatasi atau dinonaktifkan, untuk mengurangi risiko akses tidak sah atau modifikasi sistem yang tidak diinginkan.
- Sinkronisasi waktu
  Waktu yang sinkron diperlukan untuk memastikan semua perangkat memiliki waktu yang sama agar log lebih akurat.
- Pengelolaan informasi autentikasi
  Setelah instalasi perangkat atau aset baru, segera ubah informasi autentikasi bawaan. Peninjauan dan pembaruan informasi autentikasi perlu dilakukan secara berkala untuk menghindari risiko terhadap akses tidak sah.
- Pengaturan waktu keluar otomatis
  Langkah ini digunakan untuk mencegah akses tidak sah ke perangkat, yaitu dengan mengonfigurasi sistem agar otomatis pengguna dapat keluar ketika tidak ada aktivitas pada periode tertentu.
- Kepatuhan lisensi
  Kepatuhan terhadap lisensi perlu diterapkan untuk memastikan perangkat lunak yang digunakan sah dan didukung sesuai dengan persyaratan lisensi yang berlaku.
- Pencatatan dan pengelolaan perubahan konfigurasi
  Setiap aset yang dimiliki, penting untuk dicatat dengan informasi pemilik terbaru berserta kontaknya. Ketika ada perubahan konfigurasi, tanggal perubahan terakhir harus dibubuhkan. Hal ini untuk mengidentifikasi versi terakhir pada *template* konfigurasi. Keterkaitan dengan konfigurasi aset lainnya juga perlu didokumentasikan untuk mengetahui hubungan antar aset penting dan memahami dampak perubahan konfigurasi.

Selain aktivitas diatas, pengelolaan konfigurasi ini juga perlu dilakukan pencatatan ketika terjadi perubahan pada konfigurasi. Catatan perubahan konfigurasi ini dapat meliputi:

- Pemilik terbaru atau kontak informasi tentang aset;
- Tanggal perubahan konfigurasi terakhir;
- Versi template konfigurasi;
- Keterkaitan dengan konfigurasi aset lainnya.

c) Monitoring konfigurasi

Memonitoring konfigurasi dengan seperangkat alat manajemen sistem yang komprehensif dan dilakukan peninjauan secara teratur untuk memastikan kepatuhan terhadap kebijakan keamanan informasi. Aktivitas monitoring ini dilakukan untuk memastikan bahwa pengaturan konfigurasi sesuai dengan kebutuhan dan standar keamanan yang ditetapkan, serta memantau dan mengevaluasi aktivitas yang terjadi pada sistem untuk menghindari potensi yang dapat membahayakan sistem.

Sebagai pendukung implementasi manajemen konfigurasi yang efektif, peneliti memberikan beberapa dokumen tata kelola untuk manajemen konfigurasi. Namun, dokumen ini bukanlah acuan baku yang seluruhnya harus diterapkan. Setiap organisasi dapat menyesuaikan panduan ini dengan kebijakan atau

regulasi yang berlaku agar sesuai dengan kebutuhan organisasi.

TABEL IV
JENIS ITEM KONFIGURASI

Nama Dokumen	Deskripsi
Kebijakan Manajemen Konfigurasi	Dokumen yang mengatur prinsip-prinsip dan pedoman umum dalam manajemen konfigurasi, termasuk tujuan, ruang lingkup, dan tanggung jawab.
Proses Manajemen Konfigurasi	Dokumen yang menjelaskan seluruh proses manajemen konfigurasi dari perencanaan dan identifikasi hingga audit konigurasi.
Prosedur Manajemen Konfigurasi	Prosedur yang menjelaskan langkah-langkah untuk manajemen konfigurasi.
Formulir Catatan Item Konfigurasi	Dokumen yang digunakan untuk mencatat informasi detail setiap item konfigurasi.

V. KESIMPULAN

Kesimpulan bedasarkan hasil penelitian yang telah dilakukan yaitu analisis manajemen konfigurasi yang mengacu pada standar internasional ISO/IEC 27001:2022 yang menghasilkan 3 aktivitas utama untuk manajemen konfigurasi dan 4 dokumen untuk mendukung implementasi manajemen konfigurasi untuk membantu organisasi dalam pengelolaan konfigurasi yang efektif.

REFERENSI

[1] A. Aziz, "Pemanfaatan Teknologi Informasi dalam Pengembangan Bisnis Pos information technology utilization in business post development," *Buletin Pos dan Telekomunikasi,* vol. 10 , pp. 35-50, 2012.

[2] J. Prayoga, "PENERAPAN TEKNOLOGI INFORMASI DALAM PENINGKATAN EFEKTIVITAS, EFISIENSI DAN PRODUKTIVITAS PERUSAHAAN," *Jurnal Warta,* 2017.

[3] L. Ying, X. Lijun dan S. Wei , "Configuration Management Process Design and Implementation," *ISECS International Colloquium on Computing, Communication, Control, and Management* , pp. 4-7, 2009.

[4] ISO/IEC, ISO/IEC 27002 Information Security, Cybersecurity and Privacy Protection - Information Security Controls, Switzerland: ISO, 2022.

[5] M. Lenawati, W. W. Winarno dan A. Amborowati, "Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5," *Journal Speed – Sentra Penelitian Engineering dan Edukasi,* vol. 9, pp. 44-49, 2017.

[6] U. Ali dan C. Kidd, "Configuration Management Process Capabilities," *International Through-life Engineering Services Conference* , pp. 169-172, 2013.

[7] ISACA, COBIT 2019 Governance and Management Objectives, USA, 2018.

[8] UCISA, "ITIL – A guide to service asset and configuration".

[9] S. T. Yuwono, N. Pratama dan V. Afifah, "Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK," *Jurnal IKRAITH-INFORMATIKA,* vol. 6, pp. 21-28, 2022.