ISSN 2527-3671 (*Online*)
ISSN 2087-8893 (*Print*)

Teknologi: Jurnal Ilmiah Sistem Informasi 11 (1) Januari 2021 1-15

Tersedia *online* di www.journal.unipdu.ac.id
Unipdu
Terakreditasi Sinta S5
Halaman jurnal di www.journal.unipdu.ac.id/index.php/teknologi

# Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah

# *Gap analysis of information security management system (ISMS) in preparation for ISO/IEC 27001:2013 certification in government institutions*

*Sitta Rif'atul Musyarofah [a], Rahadian Bisma [b]*

*[a,b] Sistem Informasi, Universitas Negeri Surabaya, Surabaya, Indonesia*
*email: [a] sittarifatulm@gmail.com, [b] rahadianbisma@unesa.ac.id*

**INFO ARTIKEL**

***Sejarah artikel:***
Menerima 22 Oktober 2020
Revisi 17 November 2020
Diterima 20 November 2020
*Online* 23 Januari 2021

**Kata kunci:**
analisis kesenjangan informasi
ISO/IEC 27001:2013
keamanan informasi
SMKI

***Keywords:***
*gap analysis*
*information*
*information security*
*ISMS*
*ISO/IEC 27001:2013*

***Style APA dalam menyitasi artikel ini:***
Musyarofah, S. R., & Bisma, R. (2021). Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah. *Teknologi: Jurnal Ilmiah Sistem Informasi*, 11(1), 1-15.

**ABSTRAK**

Dinas Komunikasi dan Informatika (Diskominfo) Kota Madiun merupakan lembaga pemerintahan yang memiliki tanggung jawab untuk mengelola teknologi informasi dan komunikasi di pemerintah Kota Madiun. Sebagai instansi yang bertugas untuk melayani dan memberikan informasi kepada masyarakat, Diskominfo Kota Madiun rentan terhadap ancaman keamanan informasi yang dapat menghambat kinerjanya. Sistem Manajemen Keamanan Informasi (SMKI) ISO/IEC 2701:2013 merupakan sistem yang diharapkan mampu memberikan keefektifan dan keefesienan pengelolaan keamanan informasi pada Diskominfo Kota Madiun. Penelitian ini bertujuan untuk mengetahui kondisi sistem keamanan informasi terkini dan bagaiamana kesiapan Diskominfo Kota Madiun untuk mencapai sertifikasi ISO/IEC 27001:2013. Metode *gap analysis* digunakan untuk mengetahui seberapa jauh pemenuhan persyaratan ISO/IEC 27001:2013 terpenuhi. Hasil dari analisis kesenjangan menunjukkan sejauh mana kesiapan Diskominfo Kota Madiun untuk melakukan sertifikasi ISO/IEC 27001:2013. Dari hasil analisis kesenjangan dapat diketahui persentase kesiapan Diskominfo Kota Madiun sebesar 71%, dengan *range* kesiapan antara 19% - 100%. Tingkat kesiapan tertinggi yaitu sebesar 100% pada persyaratan klausul 4 tentang konteks organisasi dan klausul 10 tentang perbaikan, di mana semua persyaratan keamanan informasi telah terpenuhi. Sedangkan persentase kesiapan terendah yaitu sebesar 19% yang ditunjukkan pada persyaratan klausul 6 tentang perencanaan. Hasil dari penelitian menunjukkan bahwa Diskominfo Kota Madiun harus meningkatkan kesiapannya untuk sertifikasi ISO/IEC 27001:2013 dengan memenuhi persyaratan-persyaratan dokumen keamanan informasi yang diperlukan berdasarkan pada standar ISO/IEC 27001:2013.

***ABSTRACT***

*The Madiun City Communication and Informatics Service (Diskominfo) is a government institution that has the responsibility for managing information and communication technology in the Madiun city government. As a government institution to serving and providing information to the public, Diskominfo Madiun City is vulnerable to information security threats that can hinder its performance. Information Security Management System ISO / IEC 2701: 2013 is a system that expected to be able to provide effectiveness and efficiency of information security management at Diskominfo Madiun city. This research aims to determine the current conditions and how the readiness of Diskominfo Madiun City to achieve ISO/IEC 27001:2013 certification. From the results of the gap analysis, it can be seen that the percentage of readiness of Diskominfo Madiun City is*

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

*71%, with a readiness range between 19% - 100%. The highest level of readiness is 100% on the requirements of clause 4 concerning the organizational context and clause 10 concerning improvements, where all information security requirements have been met. While the lowest readiness percentage is 19% which is shown in the requirements of clause 6 regarding planning. The gap analysis method is used to determine how far the ISO/IEC 27001:2013 requirements are fulfilled. The results of the gap analysis show the extent of the readiness of Diskominfo Madiun City to carry out ISO/IEC 27001:2013 certification. The results of the research indicate that Diskominfo Madiun City must improve its readiness for ISO/IEC 27001:2013 certification by fulfill the requirements of the required information security documents based on ISO/IEC 27001:2013 standards.*


## 1. Pendahuluan

Informasi menjadi suatu aset yang sangat penting dan berharga bagi keberlanjutan organisasi (Rosmiati & Riadi, 2016), sehingga kerusakan atau kebocoran informasi dapat berakibat buruk bagi organisasi. Semakin meningkatnya kebutuhan informasi, maka ancaman terhadap keamanan informasi juga terus meningkat. Kerentanan informasi yang meningkat menjadi sebuah ancaman yang lebih kompleks bagi keamanan informasi untuk bisnis, organisasi, maupun pemerintahan (Hassanzadeh, Jahangiri, & Brewster, 2014). Ancamaan keamanan informasi bukan hanya dapat merusak konfigurasi sistem dan informasi yang telah tersimpan, akan tetapi ancaman dapat berupa pelanggaran informasi individu serta pengambilan informasi yang bersifat profit (Mauladani & Siahaan, 2018). Oleh karena itu, dibutuhkan suatu sistem keamanan informasi untuk menjamin keamanan sistem secara menyeluruh (Ritzkal, Goeritno, & Hendrawan, 2016). Penerapan teknologi keamanan informasi yang selaras dengan aspek keamanan informasi yang meliputi aspek *confidentiality*, *integrity*, dan *avalilability* diperlukan untuk mendukung perlindungan keamanan informasi organisasi (Octariza, 2019). Jenis-jenis keamanan informasi dikategorikan menjadi lima aspek, yaitu keamanan fisik, keamanan pribadi, keamanan operasional, keamanan komunikasi, dan keamanan jaringan (Whitman & Mattord, 2012). Manajemen keamanan informasi merupakan bagian dari keseluruhan sistem manajemen organisasi, yang berdasarkan pendekatan risiko bisnis untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan suatu keamanan informasi (Fauzi, 2018).

Pemerintah Kota Madiun sebagai institusi pemerintahan yang telah memanfaatkan teknologi informasi dan komunikasi, rentan terhadap berbagai ancaman keamanan informasi yang dapat menghambat kinerja pemerintah Kota Madiun dalam hal pelayanan dan pemberian informasi kepada masyarakat. Kerentanan keamanan tersebut dapat berasal dari berbagai faktor, seperti faktor teknis, organisasi, lingkungan, maupun keputusan manajemen yang buruk. Semakin banyak informasi suatu organisasi yang disimpan, dikelola dan dibagikan maka semakin besar pula risiko terjadi kerusakan, kehilangan atau tereksposnya data ke pihak yang tidak diinginkan (Sarno & Iffano, 2009). Untuk menghindari kerentanan keamanan informasi pada pemerintah Kota Madiun, dibutuhkan suatu sistem keamanan informasi dengan standar operasional dan prosedur manajemen pengamanan sistem informasi. Prosedur keamanan informasi pada dasarnya bertujuan untuk meyakinkan bahwa kerahasiaan (*confidentiality)*, ketersediaan *(availability)*, dan integritas *(integrity)* dari pengolahan data pada suatu organisasi terjaga (Maulana, 2019). Standar dan undang-undang yang terkait dengan keamanan informasi antara lain yaitu ISO/IEC 27001:2013, COBIT, ITIL, dan lain sebagainya.

Berdasarkan masalah yang telah dijelaskan, untuk menjamin keamanan informasi dibutuhkan suatu standar yang terkait dengan sistem manajemen keamanan informasi sebagai panduan yang dapat memberikan arahan dalam menjaga aset informasi organisasi. Sistem manajemen keamanan informasi pada dasarnya ditujukan untuk menjamin pengamanan kerahasiaan data, integritas informasi, dan ketersediaan informasi (Putra, Nurhayati, & Windasari, 2016). Sistem Manajemen Keamanan Informasi (SMKI) merupakan proses untuk merencanakan (*plan*), mengimplementasikan (*do*), meninjau ulang atau memonitor (*check*), dan memelihara (*act*) keamanan informasi guna mencapai tujuan organisasi (Apriandari & Sasongko, 2018; ISO, 2013). Pada penerapannya, SMKI dapat menghasilkan manual keamanan informasi, prosedur keamanan informasi, instruksi kerja, dan formulir keamanan informasi (Apriandari & Sasongko, 2018). Dinas Komunikasi dan Informatika Pemerintah (Diskominfo) Kota Madiun telah menerapkan beberapa standar keamanan informasi yang diperlukan dengan tujuan untuk meningkatkan kualitas keamanan informasi organisasi sehingga kepuasan masyarakat terjaga.

S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15
ISSN 2527-3671 (*Online*)
ISSN 2087-8893 (*Print*)

Meskipun telah menerapkan standar keamanan informasi, diperlukan standarisasi keamanan informasi yang dapat meningkatkan keamanan informasi organisasi. Sistem manajemen keamanan informasi yang mengacu pada standar nasional atau internasional memberikan kualitas pengamanan yang tinggi dan mampu menanggulangi permasalahan yang terjadi (Basyarahil, Astuti, & Hidayanto, 2017). Standar keamanan informasi yang digunakan pada penelitian ini yaitu ISO/IEC 27001:2013.

ISO/IEC 27001:2013 merupakan standar keamanan informasi yang diterbitkan *International Organization for Standarization* dan *International Electrotecnical Comission* pada Oktober 2013 yang merupakan pembaruan dari versi 2005. Standar keamanan informasi menggunakan ISO/IEC 27001 direkomendasikan karena pada penerapan standar tersebut telah berbasis risiko sehingga dianggap mampu dalam mengurangi ancaman keamanan informasi dengan tepat (Basyarahil, Astuti, & Hidayanto, 2017), serta standar ini dapat berlaku pada semua bisnis dan organisasi (Hartati, 2017). ISO/IEC 27001:2013 adalah standar internasional untuk manajemen keamanan informasi yang mendefinisikan serangkaian kontrol dan persyaratan untuk membangun, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan sistem manajemen keamanan informasi (SMKI) (Nasser, 2017). ISO/IEC 27001:2013 mendefinisikan keperluan-keperluan untuk SMKI yang baik dan terstruktur sehingga dapat membantu memberikan perlindungan terhadap gangguan dan risiko aktivitas-aktivitas bisnis dan melindungi proses bisnis agar terhindar dari risiko kerugian dan kegagalan pada pengamanan informasi (Pratiwi, 2019). Sistem Manajemen Keamanan Informasi (SMKI) yang baik dapat membantu memberikan perlindungan dan pengamanan terhadap ancaman keamanan informasi yang dapat mengganggu proses bisnis organisasi agar terhindar dari risiko kerugian dan kegagalan keamanan informasi (Octariza, 2019).

SMKI pemerintah Kota Madiun dapat diterapkan dengan syarat harus memenuhi standar ISO/IEC 27001:2013 yang berisikan spesifikasi dan persyaratan SMKI. Setiap aktivitas-aktivitas keamanan informasi pada pemerintah Kota Madiun harus berdasarkan pada persyaratan klausul-klausul standar ISO/IEC 27001:2013. Oleh karena itu, perlu dilakukan analisis kesenjangan pada SMKI pada pemerintah Kota Madiun berdasarkan ISO/IEC 27001:2013. Analisis kesenjangan keamanan informasi merupakan sebuah proses perbandingan operasi keamanan informasi aktual dari organisasi dengan persyaratan hukum, peraturan, dan internal manajemen keamanan informasi internasional yang relevan dengan organisasi. Analisis kesenjangan dilakukan untuk membandingkan seberapa jauh persyaratan klausul-klausul ISO/IEC 27001:2013 terpenuhi sehingga dapat diketahui pengaturan keamanan informasi antara kondisi aktual terkini dengan standar ISO/IEC 27001:2013 (Mauladani & Siahaan, 2018). Hasil yang didapat dari analisis kesenjangan yaitu berupa perbandingan antara persyaratan keamanan informasi yang sudah ada dengan persyaratan ISO/IEC 27001:2013. Analisis kesenjangan menunjukkan seberapa jauh kesiapan Diskominfo Pemerintah Kota Madiun untuk melakukan sertifikasi ISO/IEC 27001:2013, yang kemudian dapat dilakukan perbaikan. Hasil yang didapatkan dari penelitian yaitu rekomendasi perbaikan berdasarkan ISO/IEC 27001:2013 terhadap keamanan informasi Diskominfo Kota Madiun.

## 2. *State of the Art*

Pada bagian ini, berisi literatur penelitian sebelumnya yang terkait dengan peneliti ini, diantaranya adalah sebagai berikut:

a. Nasser (2017) dalam penelitian menggunakan standar ISO/IEC 27001:2013 dan model *Maturity*. Penelitian ini bertujuan untuk mengetahui praktik keamanan informasi di Akademi Studi Pascasarjana Yaman dan menilai sejauh mana pemenuhan mereka terhadap persyaratan keamanan informasi. Selain itu, untuk mengukur kesenjangan antara tingkat praktik keamanan informasi aktual di akademi dan tingkat yang ingin dicapai sesuai dengan persyaratan ISO/IEC: 27001. Hasil dari *maturity level* menunjukkan keamanan informasi di YAGS berada pada level 2.
b. Putra, Nurhayati, dan Windasari (2016) dalam penelitiannya berfokus pada masalah keamanan informasi yang ada di Bank Nagari Sumatera Barat, yaitu risiko keamanan data yang mengancam kegiatan operasional Bank Nagari. Tujuan penelitian tersebut yaitu untuk mengevaluasi keamanan informasi pada Bank Pembangunan Daerah Sumatera Barat (Bank Nagari) dengan menggunakan Indeks KAMI. Penelitian dilakukan dengan menganalisis kondisi terkini keamanan informasi Bank Nagari kemudian dihasilkan rekomendasi perbaikan terhadap keamanan informasi. Hasil dari

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

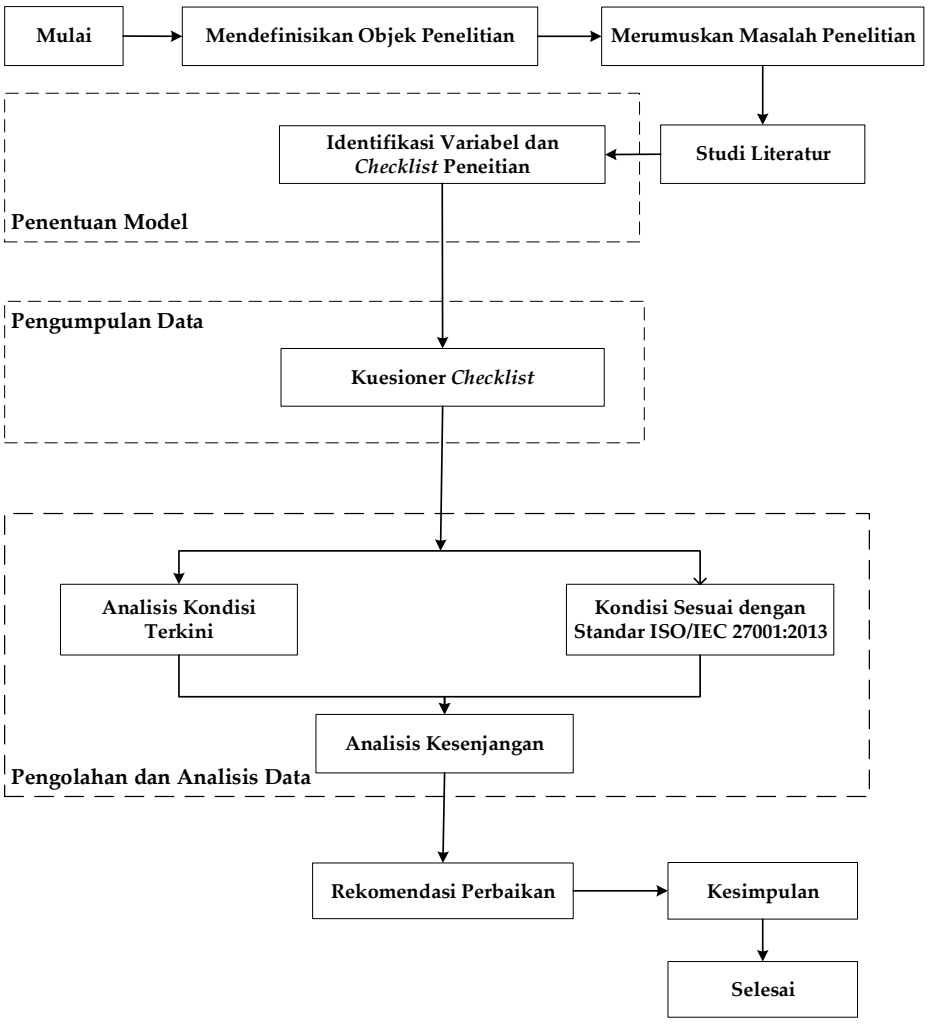
penelitian ini yaitu pada pengukuran keamanan informasi menggunakan indeks KAMI pada Bank Nagari menunjukkan tingkat kematangan keamanan informasi I+ sampai II+, sehingga masih perlu perbaikan, karena untuk mendapatkan sertifikasi ISO/IEC 27001, tingkat kematangan keamanan informasi minimal berada pada level III.

c. Pratiwi (2019) dalam penelitiannya berfokus pada pengelolaan risiko terkait keamanan informasi. Penelitian ini bertujuan untuk menghasilkan dokumen perencanaan SMKI yaitu dokumen pengelolaan risiko terkait keamanan informasi, dokumen kontrol objektif dan kontrol keamanan terkait dengan pengelolaan risiko, serta dokumen SOP (*Standar Operational Procedure)*. Kontrol yang digunakan pada penelitian ini yaitu A.5 Kebijakan keamanan informasi; A.6 Organisasi keamanan informasi; A.7 Keamanan SDM; A.9 Kontrol akses; A.11 Fisik dan keamanan lingkungan; dan A.12 Keamanan Operasional. Hasil pada penelitian ini yaitu dokumen identifikasi risiko, penilaian risiko dan respon risiko dari masing-masing aset informasi.

d. Rosmiati dan Riadi (2016) pada penelitiannya berfokus pada pengukuran keamanan informasi pada XYZ dengan metode analisis *maturity model.* Penelitian bertujuan untuk mengetahui sejauh mana kesiapan dan tingkat kematangan keamanan informasi pada perusahaan XYZ. Hasil pengukuran dengan *maturity level* menunjukkan perusahaan XYZ berada pada level 2. Untuk itu diberikan rekomendasi yang bertujuan untuk meningkatkan keamanan informasi perusahaan.

e. Fauzi (2018) pada penelitiannya berfokus pada implementasi keamanan informasi pada Usaha Kecil Menengah (UKM) yang bergerak di bidang *engineering services* dengan menggunakan standar ISO/IEC 27001:2013 dan analisis risiko menggunakan metode OCTAVE. Penelitian bertujuan untuk mengetahui bagaimana hasil analisis risiko pada UKM agar dapat diketahui kontrol apa saja yang harus ditetapkan untuk meningkatkan keamanan informasi UKM.

## 3. Metode Penelitian




Gambar 1. Tahapan penelitian

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

Metode penelitian yang digunakan dalam penelitian ini yaitu metode *gap analysis*, di mana peneliti membandingkan kondisi keamanan informasi saat ini pada instansi dengan kondisi yang sesuai dengan standar ISO/IEC 27001:2013. Penelitian bertujuan untuk untuk mengevaluasi sistem keamanan informasi yang sudah diterapkan oleh Pemerintah Madiun untuk mencapai sertifikasi ISO/IEC 27001:2013. Tahapan dari penelitian ini disajikan pada Gambar 1.

### *3.1. Tahapan penelitian*

Tahapan penelitian merupakan gambaran langkah-langkah penelitian yang digunakan untuk memperoleh dan mengumpulkan data yang diperlukan pada penelitian. Berikut merupakan tahapan penelitian yang digunakan oleh peneliti.

### *3.2. Variabel penelitian*

Variabel penelitian yang digunakan pada penelitian ini diambil berdasarkan klausul dan Annex yang terdapat pada ISO/IEC 27001:2013. Tabel 1 menunjukkan variabel penelitian yang digunakan dalam penelitian.

Tabel 1. Variabel penelitian

| No | Klausul dan Annex |
|---|---|
| 1 | 4 Konteks organisasi |
| 2 | 5 Kepemimpinan |
| 3 | 6 Perencanaan |
| 4 | 7 Dukungan |
| 5 | 8 Operasi |
| 6 | 9 Evaluasi kinerja |
| 7 | 10 Perbaikan |
| 8 | A.5 Kebijakan keamanan informasi |
| 9 | A.6 Organisasi keamanan informasi |
| 10 | A.7 Keamanan sumber daya manusia |
| 11 | A.8 Manajemen asset |
| 12 | A.9 Kontrol akses |
| 13 | A.11 Keamanan fisik dan lingkungan |
| 14 | A.12 Keamanan operasi |
| 15 | A.13 Keamanan komunikasi |
| 16 | A.14 Akuisisi, pengembangan, dan pemeliharaan sistem |
| 17 | A.15 Hubungan pemasok |
| 18 | A.16 Manajemen insiden keamanan informasi |
| 19 | A.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis |
| 20 | A.18 Kepatuhan |

### *3.3. Teknik pengumpulan data*

Pengumpulan data melalui kuesioner dilakukan dengan cara memberi seperangkat pertanyaan tertulis kepada responden untuk mendapat jawaban melalui proses komunikasi dan pengajuan pertanyaan (Ritzkal, Goeritno, & Hendrawan, 2016). Pelaksanaan kuesioner ini dilakukan untuk mendapatkan informasi mengenai analisis kesenjangan pada sistem manajemen keamanan informasi pada pemerintah Kota Madiun berdasarkan ISO/IEC 27001:2013. Kuesioner yang digunakan peneliti yaitu berupa *checklist* berdasarkan *toolkit* ISO/IEC 27001 dari CertiKit. Pada penelitian ini responden berjumlah 3 orang dari tim keamanan informasi ISO/IEC 27001:2013 pemerintah Kota Madiun.

#### *3.3.1. Observasi*

Tujuan observasi yaitu untuk mendapatkan data atau informasi yang berhubungan dengan objek penelitian. Pada penelitian ini dilakukan pengamatan secara langsung untuk mengetahui bagaimana kondisi keamanan informasi di pemerintah Kota Madiun melalui Diskominfo Kota Madiun.

#### *3.3.2. Wawancara*

Wawancara dilakukan dengan cara tanya jawab langsung terkait keamanan informasi pada pemerintah Kota Madiun yang dilakukan dengan informan yang dipilih. Wawancara bertujuan untuk mengetahui informasi mengenai permasalahan dan bagaimana manajemen keamanan informasi pada Kota Madiun.

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

Pada penelitian ini wawancara dilakukan dengan tim keamanan informasi ISO/IEC 27001:2013 pemerintah Kota Madiun.

### *3.3.3. Kuesioner*

Pengumpulan data melalui kuesioner dilakukan dengan cara memberi seperangkat pertanyaan tertulis kepada responden untuk mendapat jawaban. Pelaksanaan kuesioner ini dilakukan untuk mendapatkan informasi mengenai analisis kesenjangan pada sistem manajemen keamanan informasi pada pemerintah Kota Madiun berdasarkan ISO/IEC 27001:2013. Kuesioner yang digunakan peneliti yaitu berupa *checklist* berdasarkan toolkit ISO/IEC 27001 dari CertiKit. Pada penelitian ini responden berjumlah 3 orang dari tim keamanan informasi ISO/IEC 27001:2013 pemerintah Kota Madiun.

### *3.4. Analisis dan pengolahan data*

Analisis data dilakukan dengan metode *gap analysis*. Tujuan dilakukan dengan analisis kesenjangan yaitu untuk mengetahui seberapa besar kesenjangan yang ada antara kondisi aktual dengan kondisi yang diharapkan, serta mengetahui peningkatan kinerja yang diperlukan untuk menutupi kesenjangan yang terjadi (Muchsam & Saputro, 2011). Contoh topik persyaratan yang digunakan pada analisis kesenjangan yang berasal dari klausul dan kontrol keamanan pada Annex dapat dilihat pada Tabel 2.

Tabel 2. Contoh pertanyaan persyaratan analisis kesenjangan

| Kontrol | Persyaratan |
|---|---|
| **4 Konteks organisasi** | |
| 4.1 Memahami organisasi dan konteksnya | Sudahkah masalah eksternal dan internal yang mempengaruhi SMKI telah ditentukan? |
| 4.2 Memahami kebutuhan dan harapan pihak yang berkepentingan | Sudahkah pihak-pihak yang berkepentingan dan persyaratannya diidentifikasi? |
| **A.5 Kebijakan keamanan informasi** | |
| A.5.1.1 Kebijakan untuk keamanan informasi | Apakah ada kebijakan atau serangkaian kebijakan yang disetujui dan dikomunikasikan? |
| A.5.1.2 Tinjauan kebijakan untuk keamanan informasi | Apakah kebijakan ditinjau secara berkala? |

Tabel 3. Hasil persentase pengisian *Checklist* analisis kesenjangan

| Area | Jumlah Persyaratan | Persyaratan Terpenuhi | Persentase Penilaian |
|---|---|---|---|
| 4 Konteks organisasi | 4 | 4 | 100% |
| 5 Kepemimpinan | 6 | 5 | 83% |
| 6 Perencanaan | 16 | 3 | 19% |
| 7 Dukungan | 8 | 6 | 75% |
| 8 Operasi | 4 | 1 | 25% |
| 9 Evaluasi kinerja | 6 | 5 | 83% |
| 10 Perbaikan | 2 | 2 | 100% |
| A.5 Kebijakan keamanan informasi | 2 | 1 | 50% |
| A.6 Organisasi keamanan informasi | 7 | 4 | 57% |
| A.7 Keamanan sumber daya manusia | 6 | 5 | 83% |
| A.8 Manajemen aset | 10 | 7 | 70% |
| A.9 Kontrol akses | 14 | 9 | 79% |
| A.11 Keamanan fisik dan lingkungan | 15 | 11 | 73% |
| A.12 Keamanan operasi | 14 | 8 | 79% |
| A.13 Keamanan komunikasi | 7 | 6 | 86% |
| A.14 Akuisisi, pengembangan, dan pemeliharaan sistem | 13 | 11 | 85% |
| A.15 Hubungan pemasok | 5 | 3 | 60% |
| A.16 Manajemen insiden keamanan informasi | 7 | 6 | 86% |
| A.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis | 4 | 3 | 75% |
| A.18 Kepatuhan | 8 | 7 | 88% |
| **Rata-rata nilai** | | | 71% |

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

Pengolahan data dilakukan dengan menghitung persentase hasil pengisian *checklist* analisis kesenjangan. Hasil perhitungan persentase menunjukkan seberapa jauh kesiapan Diskominfo Kota Madiun pada masing-masing persyaratan berdasarkan ISO/IEC 27001:2013. Hasil persentase masing-masing variabel dai hasil *checklist* ditunjukan pada Tabel 3.

Dari hasil rekapitulasi penilaian pada Tabel 3, maka didapatkan persentase setiap variabel. Jumlah persyaratan merupakan skor maksimal yang dapat dicapai setiap klausul dan Annex. Kolom persyaratan terpenuhi merupakan jumlah persyaratan yang sudah dipenuhi oleh instansi. Kemudian skor persyaratan yang terpenuhi dihitung dengan skor maksimal, sehingga dari hasil perhitungan tersebut didapatkan persentase dari tiap klausul dan Annex.

## 4. Hasil dan Pembahasan

Pada bagian ini membahas tentang uraian hasil analisis yang dilakukan terhadap data yang telah diperoleh pada penelitian untuk menjawab tujuan penelitian yang dilakukan. Analisis data meliputi analisis kesenjangan untuk mengetahui seberapah jauh kesiapan organisasi untuk sertifikasi ISO/IEC 27001:2013 dan analisis terhadap rekomendasi perbaikan.

### *4.1. Analisis kesenjangan dengan persyaratan ISO/IEC 27001:2013*

Analisis kesenjangan didapat dari jawaban *checklist* yang berdasarkan persyaratan ISO/IEC 27001:2013. Hasil analisis kesenjangan pada Tabel 3 menunjukkan bahwa masih terdapat beberapa aspek yang sangat perlu dilakukan perbaikan. Pada Tabel 3 dapat dilihat *range* penilaian berada antara 19%-100%. Di mana hanya klausul 4 dan klausul 10 yang mencapai skor 100%. Hal ini menunjukkan bahwa masih banyak terdapat persyaratan yang seharusnya dipenuhi. Dengan adanya ketidaksesuaian ini, maka instansi akan lebih berkomitmen dalam penerapan ISO/IEC 27001:2013 untuk mendapatkan sertifikasi ISO/IEC 27001:2013 dan sertifikasi dapat memberikan dampak positif bagi Pemerintah Kota Madiun. Berikut akan dijelaskan hasil analisis kesenjangan pada setiap klausul dan annex.

1) Analisis Klausul 4 Konteks Organisasi
   Klausul 4 Konteks Organisasi memiliki persentase penilaian sebesar 100%. Hal ini menunjukkan bahwa semua persyaratan yang ada pada klausul konteks organisasi telah dijalankan dengan baik. Walaupun klausul 4 memenuhi persentase maksimum, hendaknya tetap diperhatikan evaluasi terhadap perbaikan/koreksi yang melibatkan pihak lain yang berkepentingan.
2) Analisis Klausul 5 Kepemimpinan
   Klausul 5 Kepemimpinan memiliki persentase penilaian sebesar 83%. Di mana klausul 5 menunjukkan bahwa penerapan telah dilakukan dengan cukup baik, tetapi terdapat beberapa ketidaksesuaian. Ketidaksesuaian terjadi pada sub klausul 5.2 tentang kebijakan, dikarenakan masih ada beberapa kebijakan yang belum didokumentasikan. Manajemen puncak telah menunjukkan komitmennya terhadap SMKI dengan menyediakan sumber daya dan berkomunikasi secara efektif mengenai keamanan informasi instansi. Hal ini terbukti dengan adanya Surat Keputusan Kepala Diskominfo Pemerintah Kota Madiun tentang Pembentukan Struktur Organisasi Sistem Manajemen Keamanan Informasi (SMKI) Pemerintah Kota Madiun Berbasis ISO/IEC 27001:2013 tahun 2020. Pada surat keputusan tersebut telah disusun pembagian tugas di semua bagian yang dibutuhkan untuk memenuhi sasaran keamanan informasi instansi.
3) Analisis Klausul 6 Perencanaan
   Klausul 6 Perencanaan memiliki persentase penilaian sebesar 19%, di mana merupakan persentase paling rendah dibandingkan dengan nilai klausul lain. Ketidaksesuaian terjadi pada sub kalusul 6.1.2 tentang penilaian risiko keamanan informasi dan sub klausul 6.1.3 tentang perlakuan risiko keamanan informasi. Hal ini dikarenakan belum adanya proses penilaian risiko keamanan informasi yang didokumentasikan dan ditetapkan dengan baik, serta belum diterapkannya opsi perawatan risiko yang sesuai untuk setiap risiko yang melebihi kriteria penerapan. Meskipun belum ada penerapan mengenai penilaian dan penerapan risiko, tetapi instansi telah menetapkan rencana keamanan informasinya dan terus meningkatkan pencapaian tujuan keamanan informasi yang sudah diterapkan.
4) Analisis Klausul 7 Dukungan
   Klausul 7 Dukungan memiliki persentase penilaian sebesar 75%. Klausul 7 menunjukkan bahwa beberapa persyaratan telah dijalankan dengan baik, tetapi dalam penerapannya masih terdapat

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

ketidaksesuaian. Ketidaksesuaian terjadi pada sub klausul 7.5.1 dan sub klausul 7.5.2, di mana semua informasi yang diperlukan oleh standar belum didokumentasikan. Berdasarkan persyaratan klausul 7, instansi telah menyediakan dan menentukan sumber daya yang dibutuhkan. Untuk meningkatkan kompetensi sumber daya manusia, telah dilakukan pelatihan kesadaran mengenai keamanan informasi, dan beberapa pelatihan lain yang dibutuhkan. Pelatihan kesadaran dilakukan dengan tujuan agar setiap pegawai yang relevan terhadap keamanan informasi mengetahui bagaimana pentingnya keamanan informasi bagi pemerintah Kota Madiun.

5) Analisis Klausul 8 Operasi

Klausul 8 Operasi memiliki persentase penilaian sebesar 25%. Klausul 8 menunjukkan bahwa lebih banyak persyaratan yang belum terpenuhi. Ketidaksesuaian terjadi pada sub klausul 8.2 tentang penilaian risiko keamanan informasi, di mana belum terdapat dokumentasi rencana penilaiain risiko yang diterapkan. Ketidaksesuaian juga terjadi pada sub klausul 8.3 tentang perawatan risiko keamanan informasi, di mana belum ada dokumentasi rencana penanganan risiko keamanan informasi dan hasilnya. Persyaratan yang terpenuhi ditunjukkan pada sub klausul perencanaan dan kontrol operasional di mana proses *outsourcing* sudah diidentifikasikan dan dikendalikan dengan cukup baik.

6) Analisis Klausul 9 Evaluasi Kinerja

Klausul 9 Evaluasi Kinerja memiliki persentase penilaian sebesar 83%. Klausul 9 menunjukkan bahwa penerapan keamanan informasi memenuhi persyaratan dengan cukup baik, walaupun masih ada beberapa persyaratan yang belum terpenuhi. Ketidaksesuaian terjadi pada subklausul 9.1 tentang pemantauan, pengukuran, analisis, dan evaluasi, di mana metode pemantauan, pengukuran, analisis, dan evaluasi belum didefinisikan dan didokumentasikan dengan jelas. Klausul 9 menunjukkan bahwa persyaratan yang terpenuhi antara lain mengenai audit internal yang sudah ditentukan dilakukan oleh orang-orang yang berkualifikasi dan tidak memihak. Untuk ulasan manajemen yang diadakan secara rutin biasanya sudah didokumentasikan.

7) Analisis Klausul 10 Perbaikan

Klausul 10 Perbaikan memiliki persentase penilaian sebesar 100%. Klausul 10 menunjukkan bahwa penerapan keamanan informasi sudah memenuhi persyaratan, dikarenakan semua persyaratan pada *checklist* yang telah terpenuhi. Hal ini ditunjukkan dengan adanya prosedur penanganan insiden dan ketidaksesuaian. Manajemen puncak juga telah memiliki komitmen untuk terus meningkatkan sistem manajemen keamanan informasi. Walaupun klausul 10 memenuhi persentase maksimum, hendaknya tetap diperhatikan evaluasi terhadap perbaikan/koreksi yang melibatkan pihak lain yang berkepentingan.

8) Analisis A5 Kebijakan Keamanan Informasi

A5 Kebijakan Keamanan Informasi memiliki persentase penilaian sebesar 50%. Annex 5 menunjukkan bahwa penerapan keamanan informasi belum sepenuhnya memnuhi persyaratan, dikarenakan masih ada persyaratan yang belum terpenuhi. Ketidaksesuaian terjadi pada kontrol 5.1.2 mengenai tinjauan keamanan informasi. A5 menunjukkan bahwa persyaratan yang telah dipenuhi yaitu adanya komitmen manajemen puncak untuk keamanan informasi yang ditunjukkan dengan adanya rencana kebijakan yang akan ditetapkan.

9) Analisis A6 Organisasi Keamanan Informasi

A6 Organisasi Keamanan Informasi memiliki persentase penilaian sebesar 57%. Hal ini menunjukkan bahwa persyaratan pada A6 telah dijalankan tetapi masih belum sepenuhnya konsisten dalam penerapannya. Ketidaksesuaian ini terjadi pada kontrol 6.2.1 (kebijakan perangkat seluler) dan 6.2.2 (*teleworking*). Manajemen puncak telah menunjukkan kepemimpinannya dengan menetapkan struktur organisasi sistem manajemen keamanan informasi, sehingga yang terlibat dengan keamanan informasi jelas tanggung jawab dan perannya. Akan tetapi, belum adanya rencana pengelolaan risiko perangkat seluler dan *teleworking*.

10) Analisis A7 Keamanan Sumber Daya Manusia

A7 Keamanan Sumber Daya Manusia memiliki persentase penilaian sebesar 83%. Hal ini menunjukkan bahwa persyaratan pada A7 telah dilaksanakan dengan cukup baik tetapi masih

ISSN 2527-3671 (*Online*)
ISSN 2087-8893 (*Print*)

belum sepenuhnya diterapkan. Manajemen puncak telah memaksimalkan fungsinya dengan menegakkan keamanan informasi melalui pelatihan kesadaran keamanan informasi kepada pegawai. Ketidaksesuaian terjadi pada kontrol 7.1.1 tentang penyaringan pegawai.

11) Analisis A8 Manajemen Aset
A8 Manajemen Aset memiliki persentase penilaian sebesar 70%. Hal ini menunjukkan bahwa persyaratan pada A8 masih belum cukup terpenuhi. Diskominfo Pemerintah Kota Madiun telah mengelola media yang dapat dilepas (*removable media*) tetapi belum ada aturan terdokumentasi mengenai bagaimana mengelola *removable media* tersebut. Klasifikasi informasi dan pelabelan informasi sudah disesuaian. Ketidaksesuaian terjadi pada kontrol 8.1.3 dan 8.2.3 di mana belum ada prosedur mengenai penggunaan aset yang dapat diterima.
12) Analisis A9 Kontrol Akses
A9 Kontrol Akses memiliki persentase penilaian sebesar 79%. Hal ini ditunjukkan bahwa akses sistem dan aplikasi sudah dibatasi sesuai dengan kebijakan, setiap orang yang memilik akses untuk masuk ke sistem/aplikasi harus memiliki kata sandi sebagai verifikasi identitas dirinya kepada sistem keamanan yang dimiliki aplikasi. Ketidaksesuaian terjadi dikarenakan proses manajemen akses pengguna belum memiliki aturan atau prosedur yang terdokumentasi sehingga dapat meningkatkan risiko kesalahan proses manajemen akses.
13) Analisis A11 Keamanan Fisik dan Lingkungan
A11 Keamanan Fisik dan Lingkungan memiliki persentase penilaian sebesar 73%. Hal ini menunjukkan bahwa persyaratan pada A11 masih belum cukup terpenuhi. Batas-batas keamanan fisik dan kontrol entri fisik sudah ditentukan, seperti adanya tulisan peringatan pada zona terbatas dan penggunaan *fingerprint* untuk masuk ke dalam area aman. Penempatan dan perlindungan peralatan sudah dilakukan pada tempatnya, serta perawatan peralatan teknologi informasi sudah dilakukan. Ketidaksesuaian terjadi pada proses perawatan dan pengamanan peralatan teknologi informasi yang belum memiliki acuan yang terdokumentasi, seperti aturan tertulis atau prosedur.
14) Analisis A12 Keamanan Operasi
A12 Keamanan Operasi memiliki persentase penilaian sebesar 79%. Hal ini menunjukkan bahwa persyaratan pada A12 masih belum cukup terpenuhi. proses manajemen perubahan telah ditentukan tetapi belum didefinisikan dalam prosedur. Proses pencadangan diatur dalam kebijakan cadangan, dan sudah ditentukan jadwal pengujiannya. Manajemen puncak telah merencanakan audit internal sistem informasi untuk meminimalkan gangguan keamanan informasi. Ketidaksesuaian terjadi pada kontrol 12.1.1 di mana prosedur yang dibutuhkan belum semuanya terdokumentasi.
15) Analisis A13 Keamanan Komunikasi
A13 Keamanan Informasi memiliki persentase penilaian sebesar 86%. Hal ini ditunjukkan pada keamanan jaringan yang sudah dikelola dengan adanya perjanjian layanan jaringan dan pemisahan dalam jaringan. Perjanjian kerahasiaan ditunjukkan dengan adanya surat pernyataan untuk setiap personel SMKI untuk mengimplementasikan SMKI dan menjaga kerahasiaan yang di dalamnya pada jangka waktu tertentu. Ketidaksesuaian ditunjukkan pada kontrol 13.2.1 di mana transfer informasi dilindungi melalui kebijakan, tetapi belum terdapat prosedur yang didokumentasikan.
16) Analisis A14 Akuisisi, Pengembangan, dan Pemeliharaan
A14 Akuisisi, Pengembangan, dan Pemeliharaan memiliki persentase penilaian sebesar 85%. Hal ini ditunjukkan pada proses menentukan sistem baru yang telah dipertimbangkan keamanan informasinya. Proses pengembangan sistem dan aplikasi diatur dalam kebijakan dan prosedur pengembangan sistem. Namun, tetap perlu dilakukan evaluasi untuk proses pengembangan sistem. Ketidaksesuaian terjadi pada kontrol 14.2.2 di mana belum ada prosedur pengendalian perubahan formal.
17) Analisis A15 Hubungan Pemasok
A15 Hubungan Pemasok memiliki persentase penilaian sebesar 60%. Hal ini menunjukkan bahwa persyaratan untuk A15 belum terpenuhi dengan baik. Kegiatan pengiriman layanan pemasok ditinjau secara berkala. Ketidaksesuaian terjadi pada kontrol 15.1.1 di mana diperlukan

ISSN 2527-3671 (*Online*)
ISSN 2087-8893 (*Print*)

identifikasi, penilaian, dan pengelolaan terhadap risiko yang terkait dengan akses pemasok, serta perubahan layanan pemasok belum dikelola.

18) Analisis A16 Manajemen Insiden Keamanan Informasi
A16 Manajemen Insiden Keamanan Informasi memiliki persentase penilaian sebesar 86%. Hal ini ditunjukkan dengan pengelolaan insiden pada Diskominfo Pemerintah Kota Madiun yang sudah sesuai dengan prosedur yang ada. Pelaporan kejadian dan insiden keamanan informasi dapat dilakukan pada *website* servicedesk.madiunkota.go.id. Ketidaksesuaian terjadi pada evaluasi insiden mengenai rpembelajaran insiden keamanan informasi yang belum didokumentasikan.

19) Analisis A17 Aspek Keamanan Informasi Manajemen Kelangsungan Bisnis
A17 Aspek Keamanan Informasi Manajemen Kelangsungan Bisnis memiliki persentase penilaian sebesar 75%. Hal ini ditunjukkan pada tingkat keamanan informasi yang diperlukan telah diidentifikasi. Rencana kesinambungan bisnis diperlukan verifikasi, tinjauan, dan evaluasi secara berkala.

20) Analisis A18 Kepatuhan
A18 Kepatuhan memiliki persentase penilaian sebesar 88%. Hal ini ditunjukkan pada subkontrol 18.1 tentang kepatuhan dengan persyaratan hukum dan kontrak. Diskominfo Pemerintah Kota Madiun telah mengidentifikasikan peraturan perundang-undangan dan persyaratan kontrak yang berlaku untuk penerapan keamanan informasinya. Manajemen puncak telah merencanakan proses audit internal sebagai tinjauan independen keamanan informasi. Ketidaksesuaian terjadi pada kontrol 18.1.5 mengenai kontrol kriptografi.

### *4.2. Rekomendasi perbaikan*

Berdasarkan hasil subbab 4.1 diketahui bahwa hampir semua klausul dan Annex yang memiliki nilai kesiapan kurang dari 100%, sehingga diperlukan perbaikan agar dapat mencapai sertifikasi ISO/IEC 27001:2013. Berikut ini merupakan rekomendasi yang dapat diberikan pada persyaratan yang memiliki nilai kesiapan di bawah 100%, yaitu:

1) Klausul 5: Kepemimpinan
Kepemimpinan dengan persentase kesiapan sebesar 83% yang memenuhi 5 dari 6 persyaratan. Berdasarkan hasil analisis klausul 5, rekomendasi yang dapat diberikan pada Diskominfo Pemerintah Kota Madiun yaitu diperlukan komunikasi untuk setiap kebijakan keamanan informasi, dan evaluasi secara berkala untuk kebijakan keamanan informasi yang ada.

2) Klausul 6: Perencanaan
Perencanaan, dengan persentase kesiapan sebesar 19% yang memenuhi 3 dari 16 persyaratan. Berdasarkan hasil analisis klausul 6, rekomendasi yang dapat diberikan pada Diskominfo Pemerintah Kota Madiun terkait dengan risiko yaitu sebagai berikut:
   - Menentukan semua risiko yang mungkin terjadi, merencanakan tindakan untuk mengatasi risiko yang sudah diidentifikasi pada dokumen identifikasi risiko.
   - Membuat dokumentasi penilaian risiko yang berisi proses penilaian risiko keamanan informasi yang berhubungan dengan kerahasiaan, integritas, dan ketersediaan informasi. Kemudian melakukan analisis, evaluasi, dan prioritas perawatan risiko.
   - Membuat dokumentasi proses penanganan risiko keamanan informasi yang berisi opsi perawatan risiko yang dipilih, kontrol yang diperlukan untuk risiko. Rencana perawatan risiko harus disetujui oleh pemilik risiko.
   - Membuat dokumen *Statement of Applicability* (SoA)

3) Klausul 7: Dukungan
Dukungan dengan persentase kesiapan sebesar 75% yang memenuhi 6 dari 8 persyaratan. Berdasarkan hasil analisis klausul 7, rekomendasi yang dapat diberikan yaitu diperlukan prosedur pengendalian informasi sebagai standar yang digunakan untuk dokumentasi informasi.

4) Klausul 8: Operasi
Operasi dengan persentase kesiapan sebesar 25% yang memenuhi 1 dari 4 persyaratan. Berdasarkan hasil analisis klausul 8, rekomendasi yang dapat diberikan terkait dengan perubahan dan risiko sebagai berikut:
   - Membuat prosedur mengenai perubahan.

ISSN 2527-3671 (*Online*)
ISSN 2087-8893 (*Print*)

- Melakukan penilaian risiko pada interval yang direncanakan.
- Membuat dokumentasi rencana dan proses penanganan risiko keamanan informasi.

5) Klausul 9: Evaluasi kinerja
Evaluasi kinerja dengan persentase kesiapan sebesar 83% yang memenuhi 5 dari 6 persyaratan. Berdasarkan hasil analisis klausul 9, rekomendasi yang dapat diberikan yang terkait dengan pemantauan, pengukuran, analisis, dan evaluasi yaitu:
- Mendefinisikan metode pemantauan, pengukuran, analisis, dan evaluasi sistem keamanan informasi.
- Membuat prosedur pemantauan, analisis, dan evaluasi sistem manajemen keamanan informasi.
- Melaksanakan audit internal secara periodik dengan orang yang berkualifikasi.
- Melakukan evaluasi pada sistem keamanan informasi yang sudah ada dengan metode yang ditentukan.

6) A5: Kebijakan keamanan informasi
Kebijakan keamanan informasi dengan persentase kesiapan sebesar 50% yang memenuhi 1 dari 2 persyaratan. Berdasarkan hasil analisis A5, rekomendasi yang dapat diberikan yaitu diperlukan tinjauan secara berkala terhadap kebijakan keamanan informasi yang telah disetujui dan dikomunikasikan.

7) A6: Organisasi keamanan informasi
Organisasi keamanan informasi dengan persentase kesiapan sebesar 57% yang memenuhi 4 dari 7 persyaratan. Berdasarkan hasil analisis A6, rekomendasi yang dapat diberikan terkait dengan keamanan informasi dalam manajemen proyek, perangkat seluler dan *teleworking* yaitu sebagai berikut:
- Proyek harus mempertimbangkan keamanan informasi secara memadai yang berdasarkan panduan keamanan informasi untuk manajemen proyek.
- Menyusun kebijakan perangkat seluler dan mengelola risiko terkait perangkat seluler.
- Menyusun kebijakan *teleworking* untuk memastikan situs *teleworking* aman.

8) A7: Keamanan sumber daya manusia
Keamanan sumber daya manusia dengan persentase kesiapan sebesar 83% yang memenuhi 5 dari 6 persyaratan. Berdasarkan hasil analisis A7, rekomendasi yang dapat diberikan terkait penyaringan pegawai, yaitu diperlukan prosedur penyaringan pegawai nonPNS yang memuat persyaratan mengenai ketersediaan mengikuti prosedur keamanan informasi.

9) A8: Manajemen aset
Manajemen aset dengan persentase kesiapan sebesar 70% yang memenuhi 7 dari 10 persyaratan. Berdasarkan hasil analisis A8, rekomendasi yang dapat diberikan yaitu:
- Menyusun aturan yang terdokumentasi untuk penggunaan yang dapat diterima, seperti prosedur penggunaan aset.
- Membuat prosedur untuk media yang dapat dilepas (*removable media*) untuk memastikan *removable media* dikelola dengan aman.
- Membuat prosedur transfer media fisik untuk melindungi media selama transportasi untuk meminimalisir risiko keamanan informasi.

10) A9: Kontrol akses
Kontrol akses dengan persentase kesiapan sebesar 79% yang memenuhi 9 dari 14 persyaratan. Berdasarkan hasil analisis A9, rekomendasi yang dapat diberikan yaitu diperlukannya dokumentasi proses manajemen akses dan tinjauan secara berkala hak akses oleh pemikik akses.

11) A11: Keamanan fisik dan lingkungan
Keamanan fisik dan lingkungan dengan persentase kesiapan sebesar 73% yang memenuhi 11 dari 15 persyaratan. Berdasarkan hasil analisis A11, rekomendasi yang dapat diberikan yaitu sebagai berikut:
- Membuat prosedur keamanan kabel sebagai acuan pengamanan kabel pada instansi.
- Membuat prosedur perawatan untuk peralatan teknologi informasi, agar meminimalisir risiko kerusakan peralatan.
- Membuat prosedur mengenai penghapusan aset.
- Membuat prosedur untuk media yang dapat dilepas (*removable media*) untuk memastikan *re-*

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

Tabel 4. Usulan rekomendasi dokumen

| Area | Rekomendasi Dokumen |
|---|---|
| 5 Kepemimpinan | Dokumen kebijakan keamanan informasi<br>Manual sistem manajemen keamanan informasi |
| 6 Perencanaan | Dokumen SoA (*Statement of Applicability*)<br>Dokumen identifikasi risiko<br>Dokumen SOP penilaian dan perawatan risiko |
| 7 Dukungan | Dokumen SOP pengembangan kompetensi keamanan informasi<br>Dokumen SOP transfer informasi |
| 8 Operasi | Dokumen SOP manajemen perubahan<br>Dokumen perawatan dan penilaian risiko |
| 9 Evaluasi kinerja | Dokumen SOP tinjauan manajemen<br>Dokumen SOP audit internal |
| A.5 Kebijakan keamanan informasi | Dokumen kebijakan keamanan informasi |
| A.6 Organisasi keamanan informasi | Dokumen kebijakan perangkat seluler<br>Dokumen kebijakan teleworking<br>Dokumen panduan keamanan informasi untuk manajemen proyek |
| A.7 Keamanan sumber daya manusia | Dokumen SOP penyaringan pegawai |
| A.8 Manajemen asset | Dokumen SOP penanganan aset<br>Dokumen SOP untuk media yang dapat dilepas (*removable media*)<br>Dokumen SOP transfer media fisik |
| A.9 Kontrol akses | Dokumen SOP manajemen hak akses<br>Dokumen kebijakan kontrol akses |
| A.11 Keamanan fisik dan lingkungan | Dokumen SOP keamanan kabel<br>Dokumen SOP perawatan peralatan teknologi informasi<br>Dokumen SOP untuk media yang dapat dilepas (*removable media*) |
| A.12 Keamanan operasi | Dokumen pedoman lingkungan pengembangan yang aman |
| A.13 Keamanan komunikasi | Dokumen SOP transfer informasi |
| A.14 Akuisisi, pengembangan, dan pemeliharaan sistem | Dokumen SOP manajemen perubahan<br>Dokumen pedoman lingkungan pengembangan yang aman |
| A.15 Hubungan pemasok | Dokumen SOP manajemen perubahan<br>Dokumen perawatan dan penilaian risiko |
| A.16 Manajemen insiden keamanan informasi | Dokumen SOP tanggap insiden keamanan informasi<br>Dokumen laporan insiden |
| A.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis | Dokumen rencana kontinuitas bisnis |
| A.18 Kepatuhan | Dokumen SOP tinjauan manajemen<br>Dokumen SOP audit internal |

*movable media* dikelola dengan aman.

12) A12: Keamanan operasi

ISSN 2527-3671 (*Online*)
ISSN 2087-8893 (*Print*)

Keamanan operasi dengan persentase kesiapan sebesar 79% yang memenuhi 8 dari 14 persyaratan. Berdasarkan hasil analisis A12, rekomendasi yang dapat diberikan yaitu diperlukan dokumentasi semua prosedur yang relevan dengan ruang lingkup.

13) A13: Keamanan komunikasi
Keamanan komunikasi dengan persentase kesiapan sebesar 86% yang emenuhi 6 dari 7 persyaratan. Berdasarkan hasil analisis A13, rekomendasi yang dapat diberikan yaitu membuat kebijakan dan prosedur transfer informasi.
14) A14: Akuisisi, pengembangan, dan pemeliharaan sistem
Akuisisi, pengembangan, dan pemeliharaan sistem dengan persentase kesiapan sebesar 85% yang memenuhi 11 dari 13 persyaratan. Berdasarkan hasil analisis A14, rekomendasi yang dapat diberikan yaitu dengan menerapkan prinsip-prinsip yang menyeluruh untuk menciptakan sistem yang aman.
15) A15: Hubungan pemasok
Hubungan pemasok dengan persentase kesiapan sebesar 60% yang memenuhi 3 dari 5 persyaratan. Berdasarkan hasil analisis A15, rekomendasi yang dapat diberikan terkait dengan kebijakan keamanan informasi untuk pemasok dan perubahan pemasok yaitu sebagai berikut:
- Mengelola dan menilai risiko yang terkait dengan akses pemasok.
- Membuat prosedur manajemen perubahan sebagai acuan untuk mengelola perubahan pada layanan pemasok.

16) A16: Manajemen insiden keamanan informasi
Manajemen insiden keamanan informasi dengan persentase kesiapan sebesar 86% yang memenuhi 6 dari 7 persyaratan. Berdasarkan hasil analisis A16, rekomendasi yang dapat diberikan yaitu dengan melakukan pembelajaran dari insiden dan ketidaksesuaian yang telah terjadi.
17) A17: Aspek keamanan informasi dari manajemen kelangsungan bisnis
Aspek keamanan informasi dari manajemen kelangsungan bisnis dengan persentase kesiapan sebesar 75% yang memenuhi 3 dari 4 persyaratan. Berdasarkan hasil analisis A17, rekomendasi yang dapat diberikan yaitu diperlukan uji dan validasi terhadap rencana kontinuitas keamanan informasi yang akan diterapkan.
18) A18: Kepatuhan
Kepatuhan dengan persentase kesiapan sebesar 88% yang memenuhi 7 dari 8 persyaratan. Berdasarkan hasil analisis A18, rekomendasi perbaikan yang dapat diberikan yaitu sebagai berikut:
- Membuat prosedur pemantauan, analisis, dan evaluasi sistem manajemen keamanan informasi.
- Persyaratan undang-undang, peraturan, kontraktual yang relevan, dan pendekatan organisasi, harus diidentifikasi, didokumentasikan dan dijaga tetap mutakhir untuk sistem informasi dan organisasi.
- Membuat dokumentasi prosedur audit internal.

Untuk usulan rekomendasi perbaikan yang diberikan berdasarkan hasil penelitian kepada Diskominfo Pemerintah Kota Madiun dalam bentuk rancangan dokumen keamanan informasi berdasarkan persyaratan ISO/IEC 27001:2013 disajikan pada Tabel 4.

## 5. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka kesimpulan yang dapat diambil berdasarkan hasil analisis kesenjangan yang dilakukan secara menyeluruh terhadap persyaratan-persyaratan ISO/IEC 27001:2013, yaitu Diskominfo Pemerintah Kota Madiun memiliki kesiapan untuk melakukan sertifikasi ISO/IEC 27001:2013 sebesar 71%. Nilai tersebut menandakan bahwa Pemerintah Kota Madiun perlu melakukan perbaikan terkait sistem keamanan informasinya berdasarkan persyaratan ISO/IEC 27001:2013. Persyaratan yang menjadi fokus perhatian yaitu Klausul 6 (perencanaan) dan Klausul 8 (operasi), di mana pada klausul ini memiliki persentase kesiapan di bawah 50%. Klausul 6 memiliki persentase kesiapan 19% dan Klausul 8 memiliki persentase kesiapan 25%.

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

Beberapa saran untuk penelitian selanjutnya adalah diharapkan peneliti dapat melakukan analisis manajemen risiko untuk persiapan sertifikasi ISO/IEC 27001:2013. Selain itu, untuk penelitian selanjutnya diharapkan dapat melakukan evaluasi penerapan keamanan informasi yang telah dilakukan analisis kesenjangan. Hal ini berfungsi untuk mengetahui bagaimana penerapan keamanan informasi setelah dilakukan analisis kesenjangan.

## 6. Referensi

Apriandari, W., & Sasongko, A. (2018). Analisis Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Di Diskominfo Kota Sukabumi). *Santika: Jurnal Ilmiah Sains dan Teknologi, 8*(1), 715-729.

Basyarahil, F. A., Astuti, H. M., & Hidayanto, B. C. (2017). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. *Jurnal Teknik ITS, 6*(1).

Fauzi, R. (2018). Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002. *JTERA (Jurnal Teknologi Rekayasa), 3*(2), . 3, No. 2, Desember 2018, Hal. 145-156.

Hartati, T. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013. *Jurnal Ilmiah Manajemen Informatika dan Komputer*, 63-70.

Hassanzadeh, M., Jahangiri, N., & Brewster, B. (2014). A Conceptual Framework for Information Security Awareness, Assessment, and Training. In B. Akhgar, & H. R. Arabnia (Eds.), *Emerging Trends in ICT Security* (pp. 99-110). Morgan Kaufmann.

ISO. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.* ISO. Retrieved from https://www.iso.org/standard/54534.html

Mauladani, F., & Siahaan, D. O. (2018). Perancangan SMKI Berdasarkan SNI ISO/IEC27001:2013 dan SNI ISO/IEC27005:2013 (Studi Kasus DPTSI-ITS). *CSRID (Computer Science Research and Its Development Journal), 10*(1), 56-67.

Maulana, M. M. (2019). *Audit Keamanan Sistem Informasi pada Dinas Komunikasi dan Informatika Kabupaten Bogor Menggunakan Standar ISO/IEC 27001: 2013 dan COBIT 5.* Jakarta: Universitas Islam Negeri Syarif Hidayatullah.

Muchsam, Y., & Saputro, F. F. (2011). Penerpaan Gap Analysis pada Pengembangan Sistem Pendukung Keputusan Penilaian Kinerja Karyawan (Studi Kasus PT. XYZ). *Seminar Nasional Aplikasi Teknologi Informasi 2011 (SNATI 2011).* Yogyakarta: Universitas Islam Indonesia.

Nasser, A. A. (2017). Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen. *International Journal of Scientific Research in Multidisciplinary Studies, 3*(11), 4-13.

Octariza, N. F. (2019). *Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 pada Kantor Pusat PT. Jasa Marga.* Jakarta: Universitas Islam Negeri Syarif Hidayatullah.

Pratiwi, W. A. (2019). *Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 pada Kominfo Provinsi Jawa Timur.* Surabaya: Institut Bisnis dan Informatika STIKOM Surabaya.

Putra, A. A., Nurhayati, O. D., & Windasari, I. P. (2016). Perencanaan dan Implementasi Informations Security Management System Menggunakan Framework ISO/IEC 20071. *Jurnal Teknologi dan Sistem Komputer, 4*(1), 60-66.

Ritzkal, R., Goeritno, A., & Hendrawan, A. H. (2016). Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) PADA Fakultas Teknik UIKA-Bogor. *Prosiding Semnastek (Seminar Nasional Sains dan Teknologi).* Jakarta: Universitas Muhammadiyah Jakarta.

Rosmiati, R., & Riadi, I. (2016). Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal dan Operasional Mengkombinasikan Standar Iso 27001:2005 dengan Maturity Level (Studi Kasus Kantor Biro Teknologi Informasi PT. XYZ). *Seminar Nasional Teknologi Informasi dan Multimedia 2016*. Yogyakarta: STMIK AMIKOM Yogyakarta.

Sarno, R., & Iffano, I. (2009). *Sistem Manajemen Keamanan Informasi.* Surabaya: ITS Press.

ISSN 2527-3671 (*Online*)
S. R. Musyarofah., & R. Bisma /Teknologi 11 (1) Januari 2021 1-15 ISSN 2087-8893 (*Print*)

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security.* Boston: Course Technology, Cengage Learning.