Jurnal Ilmu Komputer & Agri-informatika

Tersedia secara *online* di:
http://journal.ipb.ac.id/index.php/jika

Volume 11 Nomor 1 halaman 27 – 38
e ISSN: 2654-9735, p ISSN: 2089-6026

# Analisis Kesenjangan Pemenuhan Standar Sistem Manajemen Keamanan Informasi pada Ina-Geoportal

# *Compliance Gap Analysis of Information Security Management System Standards on Ina-Geoportal*

EKA MARLIANA[1*], YANI NURHADRYANI[2], IRMAN HERMADI[2]

**Abstrak**

Peningkatan ancaman terhadap keamanan informasi saat ini dan tuntutan regulasi terhadap sistem Ina-geoportal sebagai sistem elektronik strategis menuntut Badan Informasi Geospasial untuk menerapkan serta memperoleh sertifikasi standar ISO/IEC 27001 pada ruang lingkup Ina-geoportal. Analisis kesenjangan dilakukan guna mengevaluasi tingkat ketersediaan persyaratan standar dan kontrol keamanan informasi yang telah ditetapkan, berdasarkan studi dokumen, observasi, dan wawancara kepada 10 responden dari Pusat Pengelolaan dan Penyebarluasan Informasi Geospasial. Hasil analisis menunjukkan bahwa mayoritas persyaratan dalam standar belum terpenuhi, dengan 20 dari 26 persyaratan masih belum terpenuhi. Hal ini terjadi karena Badan Informasi Geospasial baru menerapkan ISO/IEC 27001 pada ruang lingkup fasilitas fisik dan jaringan di pusat data. Dari 108 kontrol keamanan informasi yang ditetapkan, sebanyak 28 kontrol belum terpenuhi, meskipun sebagian besar kontrol telah terpenuhi oleh penerapan standar pada ruang lingkup saat ini.

Kata Kunci**:** analisis kesenjangan, Ina-geoportal, ISO/IEC 27001:2013.

***Abstract***

*The increasing threats to information security and regulatory demands on the Ina-geoportal system as a strategic electronic system require the National Geospatial Information Agency (Badan Informasi Geospasial) to implement and obtain ISO/IEC 27001 standard certification within the scope of the Ina-geoportal. Gap analysis is conducted to evaluate compliance with standard requirements and established information security controls, based on document studies, observations, and interviews with 10 respondents from the Center for Management and Dissemination of Geospatial Information. The analysis results show that the majority of standard requirements remain unfulfilled, with 20 out of 26 requirements still unmet. This shortfall is attributed to the National Geospatial Information Agency's limited implementation of ISO/IEC 27001, focusing solely on physical facilities and network infrastructure within data centers. Despite significant progress, with most controls met within the current scope, 28 out of 108 established information security controls remain unmet.*

Keywords: gap analysis, Ina-geoportal, ISO/IEC 27001:2013.

## PENDAHULUAN

Perkembangan dan integrasi teknologi informasi dan komunikasi dalam peradaban modern menimbulkan berbagai ancaman dan insiden keamanan informasi (Ahsan *et al*. 2022). Di Indonesia, beberapa contoh ancaman dan insiden keamanan informasi termasuk kasus kebocoran data, *web defacement*, dan anomali trafik. Contohnya, pada tahun 2020, terjadi kebocoran data sebanyak 91 juta data pengguna Tokopedia (BSSN 2021; Interpol 2021), serta 1.3 miliar data registrasi kartu *subscriber identity module* (SIM) pada tahun 2022 (Clinten 2022). Kejadian serupa juga terjadi di platform-media sosial Facebook dan Instagram pada tahun 2019 (Pleskach *et al.* 2019). Pada tahun 2022, sektor administrasi pemerintahan menjadi sektor yang paling banyak mengalami insiden *web defacement* (BSSN 2023). *Web defacement*,

[1] Pusat Pengelolaan dan Penyebarluasan Informasi Geospasial, Badan Informasi Geospasial, Bogor, 16911
[2] Departemen Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor 16680
[*] Penulis Korespondensi: Surel: eka.marliana@big.go.id.

yang merupakan serangan umum yang dilakukan oleh peretas untuk merusak situs web sebuah organisasi, dapat berdampak pada reputasi dan kredibilitas organisasi (Mao dan Bagolibe, 2019). Anomali trafik di Indonesia terus meningkat setiap tahunnya (BSSN 2019, 2020, 2021, 2022, 2023). Anomali trafik merujuk pada pola trafik yang tidak normal, yang mengindikasikan adanya serangan siber (Huo *et al.* 2019). Implementasi sistem manajemen keamanan informasi menjadi sangat penting seiring dengan meningkatnya isu-isu keamanan informasi (Pleskach *et al.* 2019).

Ina-geoportal merupakan sebuah sistem informasi yang digunakan oleh Badan Informasi Geospasial (BIG) untuk menyebarkan informasi geospasial. Sebagai portal geospasial nasional, Ina-geoportal menjalin hubungan antara berbagai mitra penghubung simpul jaringan nasional yang berasal dari kementerian, lembaga, dan pemerintah daerah. Pengguna juga dapat memanfaatkan berbagai fitur seperti analisis data, *geoprocessing*, *geotagging*, serta *drag and drop* data file dengan menggunakan teknologi *map viewer* berbasis *opensource* (BIG 2017). Ina-geoportal resmi diluncurkan pada tanggal 17 Oktober 2011.

Pada tahun 2022, Ina-geoportal diidentifikasi sebagai sistem elektronik strategis oleh Badan Siber dan Sandi Negara (BSSN). Sesuai dengan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, sistem elektronik strategis adalah sistem elektronik yang memiliki dampak pada kepentingan umum, pelayanan publik, kelancaran operasi negara, atau pertahanan dan keamanan negara, sehingga wajib menerapkan dan memperoleh sertifikat sistem manajemen pengamanan informasi.

Meskipun BIG telah memperoleh sertifikat Sistem Manajemen Keamanan Informasi berdasarkan ISO/IEC 27001:2013 untuk lingkup *physical and network facilities* di *data center* (DC) dari tahun 2018 hingga tahun 2023, namun lingkup tersebut belum mencakup seluruh komponen dari sistem informasi Ina-geoportal. Layanan sistem informasi ini sangat bergantung pada kondisi infrastruktur, seperti *network, hardware, software*, data, prosedur, dan sumber daya manusia (Whiteman dan Mattord 2011).

ISO/IEC 27001, yang merupakan standar untuk *information security management system* (ISMS), merupakan kerangka kerja yang paling terkenal dalam menjaga keamanan informasi dengan menjelaskan cara menerapkan dan mengelola ISMS (Achmadi *et al.* 2018; Hamdi *et al.* 2019; ISO 2013; Velasco *et al.* 2018). Keamanan informasi sendiri memiliki tiga aspek utama, yaitu kerahasiaan (*confidentiality*) untuk menjaga kerahasiaan informasi dan hanya dapat diakses oleh pihak yang berwenang, integritas (*integrity*) untuk memastikan keaslian informasi, dan ketersediaan (*availability*) untuk memastikan informasi tersedia dan dapat digunakan saat dibutuhkan (Achmadi *et al.* 2018; Kemkominfo 2016; Wulansari dan Novandi, 2022). ISMS merupakan bagian dari sistem manajemen yang mengelola keamanan informasi dengan pendekatan risiko bisnis (Pleskach et *al.* 2019).

Dalam konteks Ina-geoportal, penerapan ISMS menjadi sangat penting bagi BIG untuk memenuhi regulasi dan melindungi Ina-geoportal dari risiko ancaman keamanan informasi. Namun, analisis kesenjangan terhadap pemenuhan ISMS belum pernah dilakukan pada lingkup Ina-geoportal. Penelitian analisis kesenjangan terhadap standar ISO/IEC 27001:2013 telah dilakukan pada berbagai bidang seperti pendidikan (Maingak *et al.* 2018; Nasser 2017), pemerintahan (Tjirare dan Shava 2017), dan perusahaan (Candiwan *et al.* 2016), yang memberikan gambaran tentang sejauh mana pemenuhan atau penerapan standar ISO/IEC 27001 pada masing-masing bidang.

Penelitian ini bertujuan untuk melakukan analisis kesenjangan pemenuhan antara standar ISO/IEC 27001:2013 dan penerapannya pada ruang lingkup Ina-Geoportal. Sebagai penelitian terapan yang menggunakan pendekatan kualitatif, hasil dari penelitian ini diharapkan dapat memberikan kontribusi khususnya bagi BIG dalam mengidentifikasi persyaratan standar dan kontrol keamanan informasi yang belum dan perlu dipenuhi atau diterapkan pada lingkup Ina-geoportal.

# METODE

Penelitian dilakukan di BIG tepatnya di Pusat Pengelolaan dan Penyebarluasan Informasi Geospasial (Pusat PPIG) sebagai pengelola Ina-geoportal. Standar yang digunakan dalam analisis kesenjangan adalah ISO/IEC 27001:2013. Jenis penelitian ini adalah penelitian terapan dan menggunakan pendekatan kualitatif. Metode pengambilan data dan validitasnya diuji melalui wawancara terstruktur, dan teknik pengambilan data lainnya melalui observasi, dan studi dokumen (Candiwan *et al.* 2016). Tahapan dalam penelitian dibagi menjadi tiga bagian:

1. Penyusunan kertas kerja analisis kesenjangan

Kertas kerja yang digunakan, disusun berdasarkan Standar ISO/IEC 27001:2013. Standar ISO/IEC 27001:2013 terdiri dari klausul utama yang berisi persyaratan standar dan klausul kontrol keamanan informasi yang disajikan dalam tabel Annex A. Tabel kertas kerja yang digunakan dalam penelitian ini terdiri dari (Candiwan *et al.* 2016):

a. Klausul standar,
b. Persyaratan/ketentuan yang ada pada standar,
c. Status pemenuhan,
d. Bukti aktual (hasil studi dokumen, wawancara dan observasi), dan
e. Kesenjangan antara persyaratan dan kondisi aktual.

Identifikasi persyaratan yang ada pada klausul utama ditandai dengan kata "*shall*" . Penerapan persyaratan yang ada pada klausul utama bersifat wajib tanpa ada pengecualian (ISO, 2013). klausul utama pada standar ISO/IEC 27001:2013 terdiri dari:

a. Klausul 4: Konteks organisasi
b. Klausul 5: Kepemimpinan
c. Klausul 6: Perencanaan
d. Klausul 7: Dukungan
e. Klausul 8: Operasi
f. Klausul 9: Evaluasi kinerja
g. Klausul 10: Peningkatan

Tabel Annex A memuat klausul kontrol keamanan informasi yang merupakan bagian integral dari ISO/IEC 27001 dan memiliki peran krusial dalam implementasi ISMS (Shojaie *et al.* 2014). Annex A terdiri dari 14 klausul kontrol keamanan yang secara total mencakup 35 tujuan kontrol dan 114 kontrol, yang dijelaskan dalam tabel Annex A (ISO 2013). Berbeda dengan klausul utama, klausul kontrol pada tabel Annex A bersifat opsional dan disesuaikan dengan lingkup penerapan ISMS di suatu organisasi. Dari total 114 kontrol di Annex A ISO/IEC 27001:2013, BIG hanya menerapkan 108 kontrol yang relevan dengan lingkup fasilitas fisik dan jaringan. Penetapan 108 kontrol ini terdokumentasikan dalam *Statement of Applicability* (SOA) nomor 003/LAP/BTIK/09/2021. SOA tersebut memuat daftar kontrol Annex A yang ditetapkan untuk diterapkan atau dikecualikan, beserta justifikasi yang sesuai. Berikut adalah 14 klausul kontrol yang tercantum dalam Annex A ISO/IEC 27001:2013:

1. A.5: Kebijakan keamanan informasi
2. A.6: Organisasi keamanan informasi
3. A.7: Keamanan sumber daya manusia
4. A.8: Klasifikasi informasi
5. A.9: Kontrol akses
6. A.10: Kriptografi
7. A.11: Keamanan fisik dan lingkungan
8. A.12: Keamanan operasi
9. A.13: Keamanan komunikasi
10. A.14: Akuisisi, pengembangan, dan pemeliharaan sistem
11. A.15: Hubungan pemasok

12. A.16: Manajemen insiden keamanan informasi
13. A.17: Aspek keamanan informasi manajemen kelangsungan bisnis
14. A.18: Kepatuhan

2. Pengumpulan data

Pengumpulan data dilakukan melalui metode studi dokumen, observasi, dan wawancara dengan narasumber aparatur sipil negara (ASN) di Pusat PPIG BIG, terdiri dari tim pengelola Ina-geoportal dan tim infrastruktur, pada bulan Juni 2023. Studi dokumen meliputi analisis berbagai dokumen kebijakan, pedoman, prosedur, laporan, notulensi rapat, dan sumber informasi lain yang relevan yang dimiliki oleh BIG.

3. Analisis kesenjangan

Analisis kesenjangan dilakukan dengan membandingkan setiap persyaratan standar dari klausul utama dan klausul kontrol dengan situasi aktual yang ada pada lingkup Ina-geoportal. Kertas kerja yang telah disusun digunakan sebagai pedoman dalam proses identifikasi dan analisis pemenuhan standar. Identifikasi dan analisis pemenuhan standar dilakukan berdasarkan data dan informasi yang diperoleh dari studi dokumen, observasi, dan wawancara dengan narasumber.

## HASIL DAN PEMBAHASAN

Analisis kesenjangan terhadap klausul utama dilakukan berdasarkan penelitian dokumen terkait penerapan ISO/IEC 27001:2013 pada lingkup *physical dan network facilities*, serta melalui wawancara yang dilakukan pada bulan Juni 2023. Studi dokumen mencakup berbagai dokumen kebijakan, pedoman, prosedur, laporan, notulensi rapat, dan materi lain yang relevan dengan kebutuhan analisis. Responden dalam analisis kesenjangan pemenuhan terhadap klausul utama adalah tim pengelola Ina-geoportal di Pusat PPIG, yang terdiri dari 2 responden. Hasil analisis kesenjangan terhadap pemenuhan persyaratan pada klausul 4 hingga klausul 10 ISO/IEC 27001:2013 disajikan dalam Tabel 1.

Mayoritas persyaratan yang terdapat dalam klausul utama ISO/IEC 27001:2013 masih belum terpenuhi. Dari total 26 persyaratan yang ada, hanya 6 klausul yang telah terpenuhi, yang setara dengan sekitar 23% (Gambar 1). Persyaratan yang telah terpenuhi berasal dari hasil implementasi standar pada lingkup saat ini. Faktor-faktor utama yang menyebabkan ketidakpemenuhan persyaratan standar pada setiap klausul utama akan diuraikan secara singkat berikut ini:

a. Klausul 4

   Belum ditetapkannya isu internal dan eksternal, kebutuhan dan keinginan dari pihak berkepentingan yang berkaitan dengan penerapan keamanan informasi pada Ina-geoportal, dan belum ditetapkan dan diterapkannya standar ISO/IEC 27001:2013 pada ruang lingkup Ina-geoportal.

b. Klausul 6

   Belum direncanakan dan dilakukannya penilaian risiko keamanan informasi pada lingkup Ina-geoportal, dan belum ditentukannya rencana penanganan risiko keamanan keamanan informasi tersebut.

c. Klausul 7

   Belum ditetapkannya kompetensi yang diperlukan dalam penerapan ISMS untuk lingkup Ina-geoportal dan Belum disusunnya dokumentasi informasi terkait Ina-geoportal sesuai dengan persyaratan standar.

d. Klausul 8

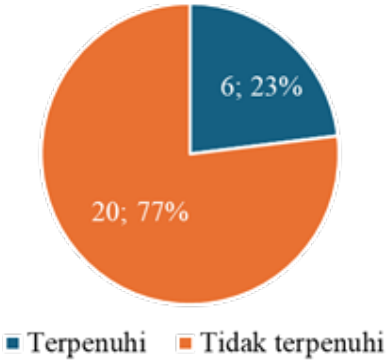
   Belum dilakukannya penilaian risiko keamanan informasi secara berkala pada lingkup Ina-geoportal dan penerapan penanganan risiko belum dapat dilakukan karena rencana penanganan risiko belum ditetapkan pada klausul 6.

e. Klausul 9
Belum diterapkannya standar ISO/IEC 27001:2013 pada lingkup Ina-geoportal menjadikan proses evaluasi kinerja ISMS belum dapat dilakukan.

f. Klausul 10
Belum diterapkannya standar ISO/IEC 27001:2013 pada lingkup Ina-geoportal menjadikan proses perbaikan terhadap ketidaksesuaian dan peningkatan ISMS yang berkelanjutan belum dapat dilakukan.

Tabel 1 Hasil analisis kesenjangan persyaratan ISO/IEC 27001:2013 pada lingkup Ina-geoportal

| Klausul ISO 27001 | | Terpenuhi | Tidak terpenuhi |
|---|---|---|---|
| Klausul 4 - Konteks organisasi | | | |
| 4.1 | Memahami organisasi dan konteksnya | | √ |
| 4.2 | Memahami kebutuhan dan harapan pihak-pihak yang berkepentingan | | √ |
| 4.3 | Menentukan ruang lingkup sistem manajemen keamanan informasi | | √ |
| 4.4 | Sistem manajemen keamanan informasi | | √ |
| Klausul 5 –Kepemimpinan | | | |
| 5.1 | Kepemimpinan dan komitmen | √ | |
| 5.2 | Kebijakan | √ | |
| 5.3 | Peran, tanggung jawab, dan wewenang organisasi | √ | |
| Klausul 6 – Perencanaan | | | |
| 6.1 | Tindakan untuk mengatasi risiko dan peluang | | |
| 6.1.1 | Umum | | √ |
| 6.1.2 | Penilaian risiko keamanan informasi | | √ |
| 6.1.3 | Perlakuan risiko keamanan informasi | | √ |
| 6.2 | Tujuan keamanan informasi dan perencanaan untuk mencapainya | | √ |
| Klausul 7 –Dukungan | | | |
| 7.1 | Sumberdaya | √ | |
| 7.2 | Kompetensi | | √ |
| 7.3 | Kesadaran | √ | |
| 7.4 | Komunikasi | √ | |
| 7.5 | Informasi terdokumentasi | | |
| 7.5.1 | Umum | | √ |
| 7.5.2 | Membuat dan memperbarui | | √ |
| 7.5.3 | Pengendalian informasi yang terdokumentasi | | √ |
| Klausul 8 –Operasi | | | |
| 8.1 | Perencanaan dan pengendalian operasional | | √ |
| 8.2 | Penilaian risiko keamanan informasi | | √ |
| 8.3 | Perlakuan risiko keamanan informasi | | √ |
| Klausul 9 –Evaluasi kinerja | | | |
| 9.1 | Pemantauan, pengukuran, analisis dan evaluasi | | √ |
| 9.2 | Audit internal | | √ |
| 9.3 | Tinjauan manajemen | | √ |
| Klausul 10 –Peningkatan | | | |
| 10.1 | Ketidaksesuaian dan tindakan perbaikan | | √ |
| 10.2 | Perbaikan berkelanjutan | | √ |
| **Jumlah klausul** | | **6** | **20** |




Gambar 1 Persentase pemenuhan persyaratan standar ISO/IEC 27001:2013 pada Ina-geoportal

Analisis kesenjangan terhadap penerapan kontrol keamanan informasi pada Ina-geoportal dilakukan berdasarkan 108 kontrol yang ditetapkan dalam dokumen SOA. Identifikasi apakah setiap kontrol telah terpenuhi atau belum dilakukan berdasarkan studi dokumen mengenai penerapan ISO/IEC 27001:2013 pada lingkup *physical dan network facilities*, serta berdasarkan justifikasi dari responden (Tabel 2). Responden yang terlibat berasal dari Pusat PPIG, yang terdiri dari tim pengelola Ina-geoportal (2 responden) dan tim infrastruktur (5 responden), dan wawancara dilakukan pada bulan Juni 2023. Persentase pemenuhan kontrol keamanan informasi pada lingkup Ina-geoportal dapat dilihat dalam Gambar 3.

Tabel 2 Penerapan kontrol keamanan informasi berdasarkan *Annex* A ISO/IEC 27001:2013

| | Klausul kontrol – Annex A | Penerapan kontrol di BIG | Terpenuhi | Tidak terpenuhi |
|---|---|---|---|---|
| A.5 | Kebijakan keamanan informasi | | | |
| A.5.1 | Arahan manajemen untuk keamanan informasi | | | |
| A.5.1.1 | Kebijakan untuk keamanan informasi | √ | √ | |
| A.5.1.2 | Reviu kebijakan informasi keamanan | √ | √ | |
| A.6 | Organisasi keamanan informasi | | | |
| A.6.1 | Organisasi internal | | | |
| A.6.1.1 | Peran dan tanggung jawab keamanan informasi | √ | √ | |
| A.6.1.2 | pemisahan tugas | √ | √ | |
| A.6.1.3 | Kontak dengan pihak berwenang | √ | √ | |
| A.6.1.4 | Kontak dengan kelompok kepentingan khusus | √ | √ | |
| A.6.1.5 | Keamanan informasi dalam manajemen proyek | √ | √ | |
| A.6.2 | Perangkat seluler dan teleworking | | | |
| A.6.2.1 | Kebijakan perangkat seluler | √ | √ | |
| A.6.2.2 | Teleworking | √ | √ | |
| A.7 | Keamanan sumber daya manusia | | | |
| A.7.1 | Sebelum bekerja | | | |
| A.7.1.1 | Penyaringan | - | | |
| A.7.1.2 | Syarat dan ketentuan kerja | √ | √ | |
| A.7.2 | Selama bekerja | | | |
| A.7.2.1 | tanggung jawab manajemen | √ | √ | |
| A.7.2.2 | Kesadaran keamanan informasi, pendidikan dan pelatihan | √ | √ | |
| A.7.2.3 | Proses disiplin | √ | √ | |
| A.7.3 | Pemutusan hubungan kerja dan perubahan pekerjaan | | | |
| A.7.3.1 | Pemutusan hubungan kerja atau perubahan tanggung jawab pekerjaan | √ | √ | |
| A.8 | Klasifikasi informasi | | | |
| A.8.1 | Tanggung jawab atas aset | | | |
| A.8.1.1 | Inventarisasi aset | √ | | √ |
| A.8.1.2 | Kepemilikan aset | √ | | √ |
| A.8.1.3 | Penggunaan aset yang dapat diterima | √ | √ | |
| A.8.1.4 | Pengembalian aset | √ | √ | |

Tabel 2 Penerapan kontrol keamanan informasi berdasarkan *Annex* A ISO/IEC 27001:2013 (Lanjutan)

| | Klausul kontrol – Annex A | Penerapan kontrol di BIG | Terpenuhi | Tidak terpenuhi |
|---|---|---|---|---|
| A.8.2 | Klasifikasi informasi | | | |
| A.8.2.1 | Klasifikasi informasi | √ | | √ |
| A.8.2.2 | Pelabelan informasi | √ | | √ |
| A.8.2.3 | Penanganan aset | √ | | √ |
| A.8.3 | Penanganan media | | | |
| A.8.3.1 | Pengelolaan media yang dapat dipindahkan | √ | √ | |
| A.8.3.2 | Pembuangan media | √ | √ | |
| A.8.3.3 | Transfer media fisik | √ | √ | |
| A.9 | Kontrol akses | | | |
| A.9.1 | Persyaratan bisnis kontrol akses | | | |
| A.9.1.1 | Kebijakan kontrol akses | √ | √ | |
| A.9.1.2 | Akses ke jaringan dan layanan jaringan | √ | √ | |
| A.9.2 | Manajemen akses pengguna | | | |
| A.9.2.1 | Pendaftaran pengguna dan de-registrasi | √ | √ | |
| A.9.2.2 | Penyediaan akses pengguna | √ | √ | |
| A.9.2.3 | Pengelolaan hak akses pribadi | √ | √ | |
| A.9.2.4 | Manajemen informasi otentikasi rahasia pengguna | √ | √ | |
| A.9.2.5 | Tinjauan hak akses pengguna | √ | | √ |
| A.9.2.6 | Penghapusan atau penyesuaian hak akses | √ | √ | |
| A.9.3 | Tanggung jawab pengguna | | | |
| A.9.3.1 | Penggunaan informasi otentikasi rahasia | √ | √ | |
| A.9.4 | Kontrol akses sistem dan aplikasi | | | |
| A.9.4.1 | Pembatasan akses informasi | √ | √ | |
| A.9.4.2 | Prosedur *log-on* yang aman | √ | √ | |
| A.9.4.3 | Sistem manajemen kata sandi | √ | √ | |
| A.9.4.4 | Penggunaan program utilitas istimewa | √ | √ | |
| A.9.4.5 | Kontrol akses ke sumber kode program | - | | |
| A.10 | Kriptografi | | | |
| A.10.1 | Kontrol kriptografi | | | |
| A.10.1.1 | Kebijakan penggunaan kontrol kriptografi | √ | √ | |
| A.10.1.2 | Manajemen kunci | √ | √ | |
| A.11 | Keamanan fisik dan lingkungan | | | |
| A.11.1 | Area aman | | | |
| A.11.1.1 | Perimeter keamanan fisik | √ | √ | |
| A.11.1.2 | Pengendalian masuk secara fisik | √ | | √ |
| A.11.1.3 | Pengamanan kantor, ruangan dan fasilitas | √ | | √ |
| A.11.1.4 | Perlindungan terhadap ancaman eksternal dan lingkungan | √ | | √ |
| A.11.1.5 | Bekerja di area aman | √ | √ | |
| A.11.1.6 | Area pengiriman dan pemuatan | √ | √ | |
| A.11.2 | Peralatan | | √ | |
| A.11.2.1 | Penempatan dan perlindungan peralatan | √ | √ | |
| A.11.2.2 | Utilitas Pendukung | √ | √ | |
| A.11.2.3 | Keamanan perkabelan | √ | √ | |
| A.11.2.4 | Pemeliharaan peralatan | √ | √ | |
| A.11.2.5 | Penghapusan aset | √ | √ | |
| A.11.2.6 | Keamanan peralatan dan aset di luar lokasi | √ | √ | |
| A.11.2.7 | Pembuangan atau penggunaan kembali peralatan secara aman | √ | √ | |
| A.11.2.8 | Peralatan pengguna tanpa pengawasan | √ | √ | |
| A.11.2.9 | Kebijakan *clear desk* dan *clear screen* | √ | √ | |
| A.12 | Keamanan operasi | | | |
| A.12.1 | Prosedur operasional dan tanggung jawab | | | |
| A.12.1.1 | Prosedur operasi yang terdokumentasi | √ | | √ |

Tabel 2 Penerapan kontrol keamanan informasi berdasarkan *Annex* A ISO/IEC 27001:2013 (Lanjutan)

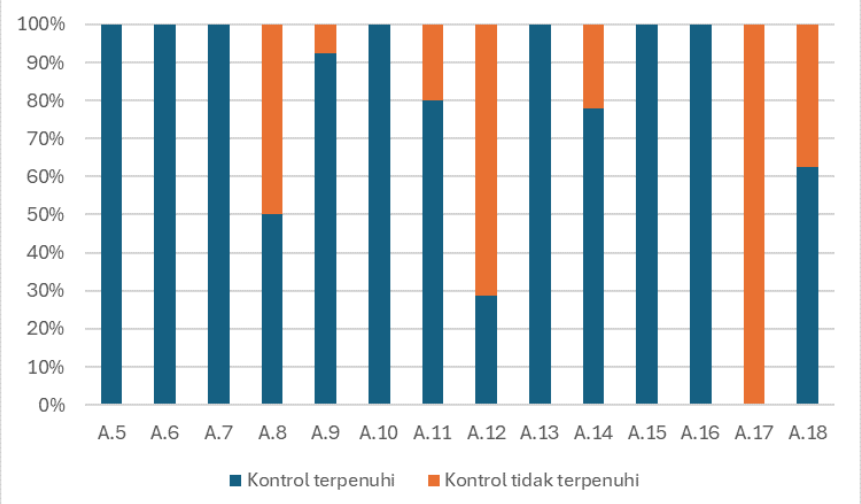
| | Klausul kontrol – Annex A | Penerapan kontrol di BIG | Terpenuhi | Tidak terpenuhi |
|---|---|---|---|---|
| A.12.1.2 | Manajemen perubahan | √ | | √ |
| A.12.1.3 | Manajemen kapasitas | √ | | √ |
| A.12.1.4 | Pemisahan lingkungan pengembangan, pengujian dan operasional | √ | | √ |
| A.12.2 | Perlindungan dari malware | | | |
| A.12.2.1 | Kontrol terhadap malware | √ | √ | |
| A.12.3 | Cadangan | | | |
| A.12.3.1 | Cadangan informasi | √ | | √ |
| A.12.4 | Pencatatan dan pemantauan | | | |
| A.12.4.1 | Pencatatan peristiwa | √ | | √ |
| A.12.4.2 | Perlindungan informasi log | √ | √ | |
| A.12.4.3 | Log administrator dan operator | √ | | √ |
| A.12.4.4 | Sinkronisasi jam | √ | √ | |
| A.12.5 | Pengendalian perangkat lunak operasional | | | |
| A.12.5.1 | Instalasi perangkat lunak pada sistem operasional | √ | | √ |
| A.12.6 | Manajemen kerentanan teknis | | | |
| A.12.6.1 | Pengelolaan kerentanan teknis | √ | | √ |
| A.12.6.2 | Pembatasan Instalasi Perangkat Lunak lunak | √ | √ | |
| A.12.7 | Pertimbangan audit sistem informasi | | | |
| A.12.7.1 | Pengendalian audit sistem informasi | √ | | √ |
| A.13 | Keamanan komunikasi | | | |
| A.13.1 | Manajemen keamanan jaringan | | | |
| A.13.1.1 | Pengendalian jaringan | √ | √ | |
| A.13.1.2 | Keamanan layanan jaringan | √ | √ | |
| A.13.1.3 | Segregasi dalam jaringan | √ | √ | |
| A.13.2 | Transfer informasi | | | |
| A.13.2.1 | Kebijakan dan prosedur transfer informasi | √ | √ | |
| A.13.2.2 | Perjanjian transfer informasi | √ | √ | |
| A.13.2.3 | Pesan elektronik | √ | √ | |
| A.13.2.4 | Kerahasiaan atau perjanjian kerahasiaan | √ | √ | |
| A.14 | Akuisisi, pengembangan, dan pemeliharaan sistem | | | |
| A.14.1 | Persyaratan keamanan sistem informasi | | | |
| A.14.1.1 | Analisis dan spesifikasi kebutuhan keamanan informasi | √ | √ | |
| A.14.1.2 | Mengamankan layanan aplikasi pada jaringan publik | - | | |
| A.14.1.3 | Melindungi transaksi layanan aplikasi | - | | |
| A.14.2 | Keamanan dalam proses pengembangan dan dukungan | | | |
| A.14.2.1 | Kebijakan pembangunan yang aman | - | | |
| A.14.2.2 | Prosedur pengendalian perubahan sistem | √ | | √ |
| A.14.2.3 | Tinjauan teknis aplikasi setelah perubahan platform operasi | √ | √ | |
| A.14.2.4 | Pembatasan perubahan pada paket perangkat lunak | - | | |
| A.14.2.5 | Prinsip rekayasa sistem yang aman | √ | | √ |
| A.14.2.6 | Lingkungan pengembangan yang aman | √ | √ | |
| A.14.2.7 | Pembangunan yang dialihdayakan | √ | √ | |
| A.14.2.8 | Pengujian keamanan sistem | √ | √ | |
| A.14.2.9 | Pengujian penerimaan sistem | √ | √ | |
| A.14.3 | Data uji | | | |
| A.14.3.1 | Perlindungan data uji | √ | √ | |
| A.15 | Hubungan pemasok | | | |
| A.15.1 | Keamanan informasi dalam hubungan pemasok | | | |
| A.15.1.1 | Kebijakan keamanan informasi untuk hubungan pemasok | √ | √ | |
| A.15.1.2 | Mengatasi keamanan dalam perjanjian pemasok | √ | √ | |
| A.15.1.3 | Rantai pasok teknologi informasi dan komunikasi | √ | √ | |
| A.15.2 | Manajemen penyampaian layanan pemasok | | | |
| A.15.2.1 | Pemantauan dan peninjauan layanan pemasok | √ | √ | |

Tabel 2 Penerapan kontrol keamanan informasi berdasarkan *Annex* A ISO/IEC 27001:2013 (Lanjutan)

| | Klausul kontrol – Annex A | Penerapan kontrol di BIG | Terpenuhi | Tidak terpenuhi |
|---|---|---|---|---|
| A.15.2.2 | Mengelola perubahan pada layanan pemasok | √ | √ | |
| A.16 | Manajemen insiden keamanan informasi | | | |
| A.16.1 | Manajemen insiden dan peningkatan keamanan informasi | | | |
| A.16.1.1 | Tanggung jawab dan prosedur | √ | √ | |
| A.16.1.2 | Melaporkan kejadian keamanan informasi | √ | √ | |
| A.16.1.3 | Melaporkan kelemahan keamanan informasi | √ | √ | |
| A.16.1.4 | Penilaian dan keputusan mengenai peristiwa keamanan informasi | √ | √ | |
| A.16.1.5 | Respon terhadap insiden keamanan informasi | √ | √ | |
| A.16.1.6 | Belajar dari insiden keamanan informasi | √ | √ | |
| A.16.1.7 | Pengumpulan bukti | √ | √ | |
| A.17 | Aspek keamanan informasi manajemen kelangsungan bisnis | | | |
| A.17.1 | Kelangsungan keamanan informasi | | | |
| A.17.1.1 | Merencanakan kelangsungan keamanan informasi | √ | | √ |
| A.17.1.2 | Menerapkan kesinambungan keamanan informasi | √ | | √ |
| A.17.1.3 | Memverifikasi, meninjau dan mengevaluasi kelangsungan keamanan informasi | √ | | √ |
| A.17.2 | Redundansi | | | |
| A.17.2.1 | Ketersediaan fasilitas pengolahan informasi | √ | | √ |
| A.18 | Kepatuhan | | | |
| A.18.1 | Kepatuhan terhadap persyaratan hukum dan kontrak | | | |
| A.18.1.1 | Identifikasi undang-undang yang berlaku dan persyaratan kontrak | √ | √ | |
| A.18.1.2 | Hak kekayaan intelektual | √ | √ | |
| A.18.1.3 | Perlindungan arsip | √ | √ | |
| A.18.1.4 | Privasi dan perlindungan informasi identitas pribadi | √ | √ | |
| A.18.1.5 | Regulasi Kontrol Kriptografi | √ | √ | |
| A.18.2 | Tinjauan keamanan informasi | | | |
| A.18.2.1 | Tinjauan independen terhadap keamanan informasi | √ | | √ |
| A.18.2.2 | Kepatuhan terhadap kebijakan dan standar keamanan | √ | | √ |
| A.18.2.3 | Kepatuhan teknis | √ | | √ |
| Jumlah kontrol | | 108 | 80 | 28 |

Status pemenuhan penerapan kontrol keamanan informasi pada setiap Annex A dapat dibagi menjadi 3 kelompok (Gambar 2), yaitu:

1. Terpenuhi seluruhnya, yaitu pada A.5, A.6, A.7, A.10, A.13, A.15, dan A.16.
2. Terpenuhi sebagian, yaitu pada A.8, A.9, A.11, A.12, A.14, dan A.18.
3. Belum terpenuhi seluruhnya, yaitu pada A.17.




Gambar 2 Persentase pemenuhan klausul kontrol pada Ina-geoportal

Total persentase pemenuhan kontrol keamanan informasi pada Ina-geoportal adalah sekitar 74%. Nilai ini dihitung dari persentase kontrol yang terpenuhi terhadap total kontrol yang ditetapkan (Tabel 2). Meskipun nilai persentase pemenuhan pada klausul utama relatif rendah, namun persentase pemenuhan pada klausul kontrol relatif tinggi. Hal ini disebabkan oleh fakta bahwa tidak semua kontrol keamanan informasi berlaku untuk seluruh area aplikasi, dan sebagian besar kontrol telah terpenuhi melalui implementasi standar ISO/IEC 27001:2013 pada lingkup saat ini. Dari Tabel 2, terlihat bahwa 5 dari 6 kontrol yang dikecualikan berkaitan dengan area aplikasi, seperti pengamanan *program source code* dan pengamanan aplikasi. Oleh karena itu, kontrol-kontrol tersebut sangat disarankan untuk diterapkan pada lingkup Ina-geoportal. Secara umum, ketidakpemenuhan sebagian atau seluruh klausul kontrol keamanan informasi pada Tabel 2 disebabkan oleh:

a. A.8: pengelolaan aset berupa inventarisasi dan penetapan penanggung jawab aset serta pengelolaan informasi berdasarkan ketentuan yang ditetapkan di BIG belum sepenuhnya diimplementasikan.
b. A.9: reviu hak akses pada Ina-geoportal belum reguler dilakukan.
c. A.11: fitur keamanan akses pada area terbatas yang sesuai dengan pedoman standar keamanan informasi yang telah ditetapkan di BIG belum seluruhnya terpenuhi.
d. A.12: prosedur operasional aplikasi belum seluruhnya terdokumentasi, prosedur manajemen perubahan belum diterapkan, pengelolaan kapasitas baru sebatas pemantauan, pemisahan area *development*, *testing*, dan *production* belum diterapkan, *backup* dan uji *restore* belum diterapkan seluruhnya, reviu *log* belum reguler dilakukan, manajemen kerentanan belum diterapkan, dan kebutuhan serta aktifitas proses audit sistem informasi belum disusun dan dilakukan.
e. A.14: prosedur manajemen perubahan belum diterapkan.
f. A.17: aspek manajemen kelangsungan bisnis pada Ina-geoportal belum terpenuhi pada aspek redudansi yang belum diterapkan pada seluruh komponan Ina-geoportal, dan belum adanya pedoman pemulihan keamanan informasi pada Ina-geoportal yang menjadi panduan jika terjadi bencana.
g. A.18: reviu terhadap penerapan kebijakan maupun standar keamanan informasi secara reguler pada Ina-geoportal belum dilakukan.

Validasi hasil penelitian dilakukan melalui proses konfirmasi ulang dalam pertemuan yang dihadiri oleh tim aplikasi (termasuk tim Ina-geoportal) dan tim infrastruktur untuk mencapai kesepakatan dan persetujuan terhadap hasil analisis yang telah dilakukan. Hasil analisis menunjukkan rendahnya pemenuhan persyaratan standar pada klausul utama dan masih terdapat kontrol keamanan informasi yang belum diterapkan pada lingkup Ina-geoportal. Kondisi ini disebabkan oleh belum dimasukkannya Ina-geoportal ke dalam ruang lingkup penerapan ISO/IEC 27001:2013 di BIG, sehingga segala aktivitas dan dokumen yang diperlukan untuk memenuhi persyaratan standar belum dilaksanakan secara komprehensif. Menurut Koordinator Sistem Informasi dan Penyebarluasan Informasi Geospasial di Pusat PPIG, penerapan ISO/IEC 27001:2013 di BIG dilaksanakan secara bertahap, dan untuk penerapan pada lingkup Ina-geoportal baru akan dipersiapkan pada tahun 2024. Kesuksesan implementasi manajemen keamanan informasi dalam suatu organisasi tidak hanya bergantung pada teknologi, tetapi juga faktor-faktor pendukung lainnya seperti komitmen dan budaya organisasi, serta kemampuan sumber daya manusia (Al-sofi *et al.* 2021).

## SIMPULAN

Analisis kesenjangan memberikan gambaran mengenai pemenuhan persyaratan standar ISO/IEC 27001:2013 dan penerapan kontrol keamanan informasi pada lingkup Ina-geoportal di BIG. Persentase pemenuhan persyaratan standar untuk lingkup Ina-geoportal baru sekitar 23%.

Sementara itu, persentase penerapan kontrol keamanan informasi sudah cukup tinggi, yaitu sekitar 74%. Tingginya persentase penerapan kontrol dibandingkan dengan pemenuhan persyaratan pada klausul utama disebabkan oleh sebagian besar kontrol telah terpenuhi melalui penerapan ISO/IEC 27001:2013 saat ini di BIG. Langkah awal yang sangat penting untuk memenuhi seluruh persyaratan standar pada lingkup Ina-geoportal adalah menetapkan Ina-geoportal ke dalam lingkup penerapan ISO/IEC 27001. Hal ini akan memastikan ketersediaan sumber daya, komitmen manajemen, dan aktivitas yang diperlukan untuk memenuhi persyaratan tersebut. Hasil analisis kesenjangan ini dapat digunakan oleh BIG untuk mengidentifikasi tindakan yang perlu dilakukan dalam memenuhi dan menerapkan standar ISO/IEC 27001:2013 pada lingkup Ina-geoportal. Selain itu, dari 6 kontrol keamanan yang dikecualikan dari penerapan pada lingkup saat ini, 5 di antaranya direkomendasikan untuk diterapkan pada lingkup Ina-geoportal karena berkaitan dengan pengamanan aplikasi.

## UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada Badan Informasi Geospasial, khususnya Pusat Pengelolaan dan Penyebarluasan Informasi Geospasial, semua narasumber, dan semua orang yang telah membantu kegiatan penelitian ini berjalan dengan baik. Kami juga mengucapkan terima kasih kepada Badan Riset dan Inovasi Nasional, yang bertindak sebagai pemberi beasiswa.

## DAFTAR PUSTAKA

Achmadi D, Suryanto Y, Ramli K. 2018. On developing information security management system (ISMS) framework for ISO 27001-based data center. *2018 International Workshop on Big Data and Information Security (IWBIS)*. 149–157. https://doi.org/10.1109/IWBIS.2018.8471700.

Ahsan M, Nygard KE, Gomes R, Chowdhury MM, Rifat N, Connolly JF. 2022. Cybersecurity threats and their mitigation approaches using machine learning—a review. *Journal of Cybersecurity and Privacy*, *2*(3). 527–555. https://doi.org/10.3390/jcp2030027.

Al-sofi TAB, Al-Shaibany NA, Al-Khulaidi AA, Almekhlafi YM. 2021. *Analysis Of Information Security Management Systems Frameworks in Organizations*. *03*.

BSSN. 2019. *Laporan Tahunan Monitoring Keamanan Siber 2018*. https://cloud.bssn.go.id/s/Y9tSycL4Pzci2qW.

BSSN. 2020. *Laporan Tahunan Monitoring Keamanan Siber 2019*. https://cloud.bssn.go.id/s/nM3mDzCkgycRx4S.

BSSN. 2021. *Laporan Tahunan Monitoring Keamanan Siber 2020*. https://cloud.bssn.go.id/s/ZSdfebRTKW7p8nW.

BSSN. 2022. *Laporan Tahunan Monitoring Keamanan Siber 2021*. https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw.

BSSN. 2023. *Lanskap Keamanan Siber Indonesia 2022*. BSSN. https://cloud.bssn.go.id/s/3S5B2ToddAFsiXs.

Candiwan, Beninda MYD, Priyadi Y. 2016. Analysis of information security audit using ISO 27001:2013 & ISO 27002:2013 at IT division - X company, in Bandung, Indonesia. *International Journal of Basic and Applied Science*. 04:77–88.

Clinten B. 2022. Kasus data bocor di indonesia sepanjang 2022, dari PLN, pertamina, hingga aksi bjorka. *Kompas*. https://tekno.kompas.com/read/2022/12/29/09020067/kasus-data-bocor-di-indonesia-sepanjang-2022-dari-pln-pertamina-hingga-aksi?page=all.

Hamdi Z, Anir NA, Nuha AMN, Hassandoust F. 2019. A comparative review of ISMS implementation based on ISO 27000 series in organizations of different business sectors. *Journal of Physics: Conference Series*. 1339(1):012103. https://doi.org/10.1088/1742-6596/1339/1/012103.

Huo X, Wu K, Miao W, Wang L, He H, Su D. 2019. Research on network traffic anomaly detection of source-network-load industrial control system based on GRU-OCSVM. *IOP Conference Series: Earth and Environmental Science*. 300(4):042043. https://doi.org/10.1088/1755-1315/300/4/042043.

Interpol. 2021. *ASEAN Cyberthreat Assessment*. https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf.

ISO. 2013. *ISO/IEC 27001:2013 - Information Security Management System*. British Standards Institution.

Maingak AZ, Candiwan C, Harsono LD. 2018. Information security assessment using ISO/IEC 27001:2013 standard on government institution. *TRIKONOMIKA*. 17(1):28. https://doi.org/10.23969/trikonomika.v17i1.1138.

Mao BM, Bagolibe KD. 2019. A contribution to detect and prevent a website defacement. *2019 International Conference on Cyberworlds (CW)*. 344–347. https://doi.org/10.1109/CW.2019.00062.

Nasser AA. 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).

Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia No. 4 Tentang Sistem Manajemen Pengamanan Informasi, Pub. L. No. 4. 2016.

Pleskach V, Pleskach M, Zelikovska O. 2019. Information security management system in distributed information systems. *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*. 300–303. https://doi.org/10.1109/ATIT49449.2019.9030484.

Shojaie B, Federrath H, Saberi I. 2014. Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A. *2014 Ninth International Conference on Availability, Reliability and Security*, 259–264. https://doi.org/10.1109/ARES.2014.41.

Tjirare DJ, Shava FB. 2017. A gap analysis of the ISO/IEC 27000 standard implementation in Namibia. *2017 IST-Africa Week Conference (IST-Africa)*. 1–10. https://doi.org/10.23919/ISTAFRICA.2017.8102376.

Velasco J, Ullauri R, Pilicita L, Jacome B, Saa P, Moscoso-Zea O. 2018. Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry. *2018 International Conference on Information Systems and Computer Science (INCISCOS)*. 294–300. https://doi.org/10.1109/INCISCOS.2018.00049.

Whiteman ME, Mattord HJ. 2011. *Principles of Information Security*. 4th ed Vol. 4. Cengage Learning.

Wulansari TT, Novandi D. 2022. Evaluation of information security management using the KAMI index framework. *2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA)*. 173–177. https://doi.org/10.1109/ICSINTESA56431.2022.10041714.