Jurnal Praktik
**Keinsinyuran**
e-ISSN:3063-7449

Jurnal **Praktik Keinsinyuran** Vol.3 No.2 (Maret 2026)
journal homepage: http://ejournal.atmajaya.ac.id/index.php/jpk

# Evaluasi *Statement of Applicability* ISO 27001:2022 melalui Audit *Surveilans* pada Pusat Data Internal

Christiaan Widharto*, Maria Angela Kartawidjaja

Program Studi Program Profesi Insinyur, Fakultas Biosains, Teknologi, dan Inovasi, Universitas Katolik Indonesia Atma Jaya, Jalan Jenderal Sudirman 51 Jakarta 12930

Article Info

*Article history:*

Received
January, 08 2026

Accepted
January, 08 2026

*Keywords: ISO/IEC* 27001:2022*, Surveillance Audit, Statement of Applicability, Information Security Management System, Data Center Security.*

Abstract

*This study evaluates the effectiveness of the Statement of Applicability (SoA) through an ISO/IEC 27001:2022 surveillance audit on the internal data center infrastructure of PT ABC. The audit was conducted by an independent certification body to verify continual compliance, assess the effectiveness of the Information Security Management System (ISMS), review previous audit results, and identify opportunities for improvement. The audit program was developed in accordance with ISO 19011:2018 and ISO/IEC 17021-1:2015 using a systematic and risk-based approach. The evaluation focused on the alignment between implemented controls and the documented SoA, based on Annex A control domains. No nonconformities or discrepancies were identified, although three Opportunities for Improvement (OFIs) were recorded. The results confirm that the ISMS is compliant and effective, supporting the continuation of ISO/IEC 27001:2022 certification.*

Info Artikel

*Histori Artikel:*

Diserahkan:
08 Januari 2026

Diterima:
08 Januari 2026

Kata Kunci: ISO/IEC 27001:2022, Pengawasan Audit, Penerapan Pernyataan, Sistem Manajemen Keamanan Informasi, Keamanan Pusat Data.

Abstrak

Audit *surveilans* ISO/IEC 27001:2022 pada PT ABC dilaksanakan oleh lembaga sertifikasi independen untuk memastikan kepatuhan berkelanjutan, menilai efektivitas Sistem Manajemen Keamanan Informasi (SMKI), meninjau tindak lanjut audit sebelumnya, serta mengidentifikasi peluang peningkatan. Program audit disusun sesuai ISO 19011:2018 dan ISO/IEC 17021-1:2015 guna menjamin pelaksanaan audit yang sistematis dan konsisten. Evaluasi dilakukan terhadap kesesuaian SMKI dengan persyaratan ISO/IEC 27001:2022, khususnya melalui penelaahan *Statement of Applicability* (SoA) dan penerapan kontrol Annex A yang mencakup kontrol organisasi, sumber daya manusia, fisik, dan teknologi. Hasil audit menunjukkan tidak ditemukan n*on-conformity* maupun d*iscrepancy*, namun tercatat tiga *Opportunities for Improvement* (OFI). Secara keseluruhan, SMKI PT. ABC dinyatakan sesuai dan efektif, sehingga kelanjutan sertifikasi ISO/IEC 27001:2022 direkomendasikan.

## 1. PENDAHULUAN

Seiring dengan meningkatnya risiko kebocoran dan penyalahgunaan informasi, perlindungan terhadap data organisasi, data karyawan, dan data nasabah menjadi prioritas strategis bagi setiap perusahaan, khususnya di sektor jasa keuangan dan asuransi. Peningkatan ancaman siber serta tuntutan kepatuhan terhadap regulasi mendorong organisasi untuk menerapkan Sistem Manajemen Keamanan Informasi (SMKI) yang terstruktur dan berkelanjutan. Salah satu standar internasional yang banyak diadopsi untuk tujuan tersebut adalah ISO/IEC 27001:2022.

PT ABC merupakan perusahaan yang bergerak di bidang asuransi umum sesuai dengan Peraturan Otoritas Jasa Keuangan nomor 36 tahun 2024 (Otoritas Jasa Keuangan Republik

*Corresponding author. Christiaan Widharto
Email address: chris.ctr210@gmail.com

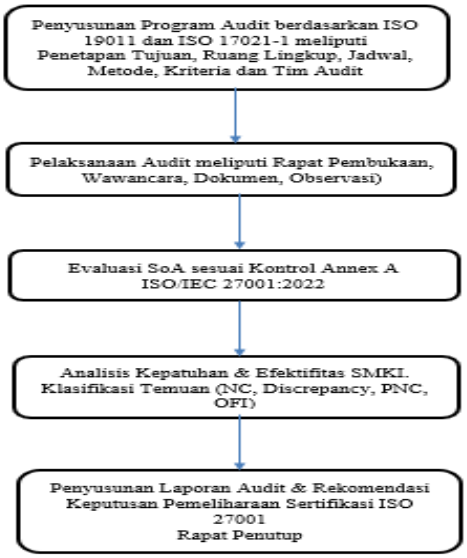
Indonesia, 2024) dan telah menerapkan serta memperoleh sertifikasi ISO/IEC 27001:2022. Untuk memastikan bahwa penerapan SMKI tetap berjalan secara konsisten dan efektif, organisasi yang telah tersertifikasi diwajibkan menjalani *surveilans* audit secara berkala oleh lembaga sertifikasi independen. Audit ini bertujuan untuk memverifikasi kepatuhan berkelanjutan terhadap persyaratan standar serta menilai efektivitas pengendalian keamanan informasi yang telah diterapkan.

Pelaksanaan audit *surveilans* ISO/IEC 27001:2022 pada PT ABC memiliki beberapa tujuan utama, yaitu memverifikasi kepatuhan berkelanjutan dengan memastikan bahwa seluruh elemen kunci dan persyaratan standar tetap dipenuhi, menilai efektivitas SMKI dalam mendukung pencapaian tujuan organisasi, pemenuhan peraturan perundang-undangan yang berlaku, serta kebutuhan dan harapan pelanggan, mengidentifikasi area perbaikan melalui evaluasi bukti kepatuhan dan penemuan peluang peningkatan terhadap sistem keamanan informasi, efisiensi proses, dan kinerja organisasi serta meninjau kembali temuan audit pada periode sebelumnya dan memverifikasi efektivitas tindakan perbaikan yang telah dilaksanakan (*International Organization for Standardization*, 2022).

Hasil dari pelaksanaan audit *surveilans* ini diharapkan tidak hanya memberikan gambaran praktis bagi PT ABC dalam memetakan dan merencanakan pemenuhan standar keamanan informasi, tetapi juga dapat menjadi referensi akademik dalam kajian keamanan informasi dan audit kepatuhan berbasis ISO/IEC 27001:2022.

## 2. METODE PELAKSANAAN

Pelaksanaan audit *surveilans* ISO/IEC 27001:2022 pada PT ABC diawali dengan penyusunan program audit sebagaimana dipersyaratkan dalam ISO 19011:2018 dan ISO/IEC 17021-1:2015. Program audit disusun sebagai rencana strategis dan komprehensif yang mencakup ruang lingkup, jadwal, metode, serta sumber daya yang diperlukan untuk memastikan audit dapat dilaksanakan secara sistematis dan efektif (*International Organization for Standardization*, 2015) (*International Organization for Standardization*, 2018) . Tujuan utama penyusunan program audit adalah untuk memverifikasi bahwa Sistem Manajemen Keamanan Informasi (SMKI) PT ABC berjalan secara efektif, memenuhi persyaratan pelanggan, mematuhi ketentuan peraturan perundang-undangan yang berlaku, serta selaras dengan standar ISO/IEC 27001:2022. Diagram alir bisa dilihat pada Gambar 1.




**Gambar 1.**
Diagram Alir Pelaksanaan Audit ISO 27001

Audit *surveilans* dilaksanakan selama tiga hari, yaitu pada tanggal 20-22 Agustus 2025, di lingkungan PT ABC. Audit dilakukan oleh dua orang auditor yang dibagi ke dalam dua tim. Pembagian ruang lingkup audit dilakukan per hari untuk memastikan cakupan proses yang memadai. Pada tanggal 20 Agustus 2025, Tim A melakukan audit pada area/departemen *Health Underwriting* dan *Central Processing Health*, sedangkan Tim B mengaudit area *Application Development, Special Project, Helpdesk Support,* dan *People Development.* Pada tanggal 21 Agustus 2025, Tim A mengaudit area *Claim Health, Central Processing General*, dan *Contact Center*, sementara Tim B mengaudit area *General Services* serta *Information System and Technology.* Selanjutnya, pada tanggal 22 Agustus 2025, Tim A mengaudit area *Claim General Motor Vehicle* (MV), *Claim General Non-MV*, dan *Risk Engineering*, sedangkan Tim B melakukan audit pada area *Information System and Technology* serta *Quality Assurance.*

Dalam melaksanakan audit, auditor menerapkan prinsip-prinsip audit sesuai ISO 19011:2018, meliputi integritas, penyajian secara adil, transparansi, kecermatan profesional, kerahasiaan, independensi, serta pendekatan berbasis bukti. Audit diawali dengan pelaksanaan rapat perdana yang melibatkan manajemen puncak, manajemen representatif, kepala departemen, serta personel terkait. Agenda rapat perdana mencakup perkenalan auditor, konfirmasi kerahasiaan informasi, penjelasan tujuan dan proses audit, metode dan kriteria audit, klasifikasi temuan audit, mekanisme pelaporan, serta ruang lingkup dan rencana audit (*International Organization for Standardization*, 2018).

Metodologi audit yang digunakan dalam penelitian ini meliputi wawancara dengan *auditee*, telaah dokumen (termasuk manual SMKI, prosedur setiap departemen, sasaran keamanan informasi, *statement of applicability*, serta dokumen risiko dan peluang, pengambilan sampel bukti, dan observasi lapangan. Kriteria audit mencakup persyaratan ISO/IEC 27001:2022, peraturan perundang-undangan yang berlaku, persyaratan pelanggan, serta prosedur dan dokumen internal pada masing-masing departemen (*United Registrar of Systems*, 2024).

Temuan audit diklasifikasikan oleh lembaga sertifikasi *United Registrar of Systems* (URS) ke dalam dua kategori utama, yaitu *Concern* yang mencakup *Non-Conformity* (temuan mayor) dan *Discrepancy* (temuan minor), serta *Comment* yang mencakup *Potential Non-Compliance (PNC)* dan *Opportunity for Improvement* (OFI) (*United Registrar of Systems*, 2024).

Sebagai bagian dari evaluasi, auditor melakukan penelaahan terhadap *Statement of Applicability* (SoA) sebagai dokumen wajib dalam SMKI berdasarkan ISO/IEC 27001:2022 (*International Organization for Standardization*, 2022). SoA memuat keputusan organisasi terkait kontrol *Annex* A yang diterapkan maupun tidak diterapkan, beserta justifikasinya. PT ABC memberikan justifikasi atas beberapa kontrol yang dinyatakan tidak berlaku, antara lain kontrol A.5.23 terkait keamanan informasi untuk layanan *cloud* karena pengelolaan pusat data masih dilakukan secara *on-premises*, kontrol A.7.9 terkait keamanan aset di luar lokasi karena tidak terdapat aset di luar pusat data, serta beberapa kontrol pada *Annex* 8 yang berkaitan dengan hak akses istimewa, akses ke *source code,* persyaratan keamanan aplikasi, dan *secure coding* karena tidak terdapat aktivitas pengembangan aplikasi

## 3. HASIL DAN PEMBAHASAN

Pada lembaga sertifikasi *United Registrar of Systems* (URS), format dan struktur laporan audit *surveilans* disusun berdasarkan pengelompokan kontrol dalam ISO/IEC 27001:2022. Jika ISO 27001 memberi tahu organisasi apa yang harus dilakukan (persyaratan), maka ISO 27002 menjelaskan bagaimana cara melakukannya secara teknis.

Dokumen ISO 27002 ini memberikan detail mendalam untuk setiap kontrol keamanan yang ada di lampiran A (Annex A) ISO 27001. Setiap kontrol dievaluasi dengan mengacu pada bukti objektif yang tersedia serta penetapan Person in Charge (PIC) sebagai bentuk akuntabilitas penerapan Sistem Manajemen Keamanan Informasi (SMKI) (*International Organization for Standardization*, 2022).

### 3.1. Kontrol Organisasi

Evaluasi terhadap tiga puluh tujuh kontrol organisasi seperti pada Tabel 1 menunjukkan bahwa PT ABC telah memiliki kerangka kebijakan dan tata kelola keamanan informasi yang terdokumentasi dengan baik. Kebijakan keamanan informasi, peran dan tanggung jawab, pemisahan tugas, serta tanggung jawab manajemen didukung oleh dokumen formal seperti kebijakan internal, struktur organisasi, deskripsi jabatan, dan peraturan perusahaan. Hubungan dengan pihak berwenang dan kelompok kepentingan khusus juga telah diatur melalui mekanisme komunikasi internal dan eksternal yang terdokumentasi.

Selain itu, pengelolaan aset informasi, klasifikasi dan pelabelan informasi, serta pengendalian akses fisik dan logis terhadap pusat data telah diterapkan secara konsisten. Pengelolaan insiden keamanan informasi, termasuk kesiapan respons, pembelajaran dari insiden, serta pengumpulan bukti, didukung oleh prosedur operasional dan instruksi kerja yang relevan. Kontrol terkait layanan cloud (A 5.23) dinyatakan tidak berlaku karena seluruh pengelolaan pusat data masih dilakukan secara *on-premises*.

**Tabel 1.**
Evaluasi terhadap Kontrol Organisasi

| | |
|---|---|
| A 5.1 | *Policies for information security* |
| *Evidence* | - Kebijakan mutu dan keamanan informasi.<br>- Peraturan internal terkait dengan kebijakan mutu dan keamanan informasi sesuai dengan Surat Keputusan Direksi tentang Standar Penerbitan Peraturan Internal. |
| A 5.2 | *Information security roles and responsibilities* |
| *Evidence* | - Struktur organisasi<br>- Deskripsi pekerjaan. |
| A 5.3 | *Segregation of duties* |
| *Evidence* | - Pedoman mutu dan keamanan informasi.<br>- Struktur organisasi, deskripsi jabatan, tugas dan tanggung jawab. |
| A 5.4 | *Management responsibilities* |
| *Evidence* | - Peraturan Perusahaan<br>- Pedoman Etika dan Perilaku<br>- Kontrak kerja<br>- Pernyataan Kerahasiaan |
| A 5.5 | *Contact with authorities* |
| *Evidence* | - Surat Keputusan Direksi tentang Tabel Komunikasi Internal dan Eksternal serta Adendumnya.<br>- Rekaman pelaksanaan komunikasi internal dan eksternal. |
| A 5.6 | *Contact with special interest groups* |
| *Evidence* | - Surat Keputusan Direksi tentang Tabel Komunikasi Internal dan Eksternal serta Adendumnya.<br>- Rekaman pelaksanaan komunikasi internal dan eksternal. |
| A 5.7 | *Threat intelligence* |
| *Evidence* | Instruksi kerja untuk *Threat Intelligence report*. |

**Tabel 1. (Lanjutan)**
Evaluasi terhadap Kontrol Organisasi

| | |
|---|---|
| A 5.8 | *Information security in project management* |
| *Evidence* | - SOP pemeliharaan dan perbaikan sarana dan prasarana.<br>- SOP Infrastruktur.<br>- Instruksi kerja pemeliharaan dan perbaikan infrastruktur di *data center*.<br>- Pernyataan kerahasiaan. |
| A 5.9 | *Inventory of information and other associated assets* |
| *Evidence* | - SOP *fixed assets*<br>- SOP infrastruktur<br>- Daftar lisensi data center.<br>- Daftar asset hardware data center.<br>- Daftar dokumen.<br>- Daftar rekaman. |
| A 5.10 | *Acceptable use of information and other associated assets* |
| *Evidence* | - SOP Fixed assets<br>- SOP Infrastruktur |
| A 5.11 | *Return of assets* |
| *Evidence* | SOP Infrastruktur. |
| A 5.12 | *Classification of information* |
| *Evidence* | Instruksi kerja klasifikasi dan pelabelan informasi dalam ruang lingkup infrastruktur *data center.* |
| A 5.13 | *Labelling of information* |
| *Evidence* | Instruksi kerja klasifikasi dan pelabelan informasi dalam ruang lingkup infrastruktur *data center.* |
| A 5.14 | *Information transfer* |
| *Evidence* | - SOP penerbitan dan pengendalian dokumen internal.<br>- Instruksi kerja klasifikasi dan pelabelan informasi dalam ruang lingkup infrastruktur *data center*.<br>- Petunjuk kerja proses *backup* menggunakan *tape backup* LTO. |
| A 5.15 | *Access control* |
| *Evidence* | Instruksi kerja pengaturan akses untuk ruangan dan aset *data center*. |
| A 5.16 | *Identity management* |
| *Evidence* | Instruksi kerja pengaturan akses untuk ruangan dan aset *data center*. |
| A 5.17 | *Authentication information* |
| *Evidence* | Instruksi kerja pengaturan akses untuk ruangan dan aset *data center*. |
| A 5.18 | *Access rights* |
| *Evidence* | Instruksi kerja pengaturan akses untuk ruangan dan aset *data center*. |
| A 5.19 | *Information security in supplier relationships* |
| *Evidence* | - SOP pemesanan cetakan dan barang.<br>- SOP seleksi dan evaluasi vendor.<br>- Insturksi kerja pemilihan buyer dan vendor departemen infrastruktur.<br>- Surat pernyataan kerahasiaan atau perjanjian kerja sama. |

**Tabel 1. (Lanjutan)**
Evaluasi terhadap Kontrol Organisasi

| | |
|---|---|
| A 5.20 | *Addressing information security within supplier agreements* |
| *Evidence* | - SOP pemesanan cetakan dan barang.<br>- SOP seleksi dan evaluasi vendor.<br>- Instruksi kerja pemilihan buyer dan vendor departemen infrastruktur.<br>- Surat pernyataan kerahasiaan atau perjanjian kerja sama. |
| A 5.21 | *Managing information security in the ICT supply chain* |
| *Evidence* | Surat pernyataan kerahasiaan/perjanjian kerja sama. |
| A 5.22 | *Monitoring, review and change management of supplier services* |
| *Evidence* | - SOP seleksi dan evaluasi vendor.<br>- Instruksi kerja pemilihan *buyer* dan vendor departemen infrastruktur. |
| A 5.23 | *Information security for use of cloud services* |
| *Evidence* | *Not applicable.* |
| A 5.24 | *Information security incident management planning and preparation* |
| *Evidence* | - SOP investigasi insiden keamanan infrastruktur *data center*.<br>- Petunjuk kerja panduan penggunaan IT *information system*. |
| A 5.25 | *Assessment and decision on information security events* |
| *Evidence* | - SOP investigasi insiden keamanan infrastruktur data center.<br>- Petunjuk kerja panduan penggunaan IT *information system*. |
| A 5.26 | *Response to information security incidents* |
| *Evidence* | - SOP investigasi insiden keamanan infrastruktur data center.<br>- Petunjuk kerja panduan penggunaan IT *information system*. |
| A 5.27 | *Learning from information security incidents* |
| *Evidence* | - SOP investigasi insiden keamanan infrastruktur data center.<br>- Petunjuk kerja panduan penggunaan IT *information system*. |
| A 5.28 | *Collection of evidence* |
| *Evidence* | Petunjuk kerja panduan penggunaan IT *information system*. |
| A 5.29 | *Information security during disruption* |
| *Evidence* | - Pedoman *business continuity plan* (BCP) *Data Center*.<br>- Instruksi kerja pelaksanaan proses *disaster recovery*. |
| A 5.30 | *ICT readiness for business continuity* |
| *Evidence* | - *Schedule of DRP testing*<br>- *DRP testing result.* |
| A 5.31 | *Legal, statutory, regulatory and contractual requirements* |
| *Evidence* | - Daftar peraturan eksternal.<br>- SOP manajemen kepatuhan. |
| A 5.32 | *Intellectual property rights* |
| *Evidence* | - SOP manajemen kepatuhan.<br>- Memorandum anti pembajakan. |
| A 5.33 | *Protection of records* |
| *Evidence* | - Instruksi kerja pengendalian operasional *data center*.<br>- Petunjuk kerja proses *backup* menggunakan *tape backup* LTO. |

**Tabel 1. (Lanjutan)**
Evaluasi terhadap Kontrol Organisasi

| | |
|---|---|
| A 5.34 | *Privacy and protection of PII* |
| *Evidence* | - Pedoman etika dan perilaku.<br>- Pedoman perlindungan konsumen dan Masyarakat. |
| A 5.35 | *Independent review of information security* |
| *Evidence* | Laporan audit internal. |
| A 5.36 | *Compliance with policies, rules and standards for information security* |
| *Evidence* | Laporan audit internal. |
| A 5.37 | *Documented operating procedures* |
| *Evidence* | - Daftar induk dokumen internal Perusahaan.<br>- *Edocument*. |

## 3.2. Kontrol Sumber Daya Manusia

Delapan kontrol sumber daya manusia dievaluasi seperti dapat dilihat pada Tabel 2 dan menunjukkan bahwa aspek keamanan informasi telah terintegrasi dalam siklus pengelolaan SDM, mulai dari proses rekrutmen, penetapan syarat dan ketentuan kerja, hingga pemutusan hubungan kerja. Program kesadaran dan pelatihan keamanan informasi dilaksanakan secara berkala, serta mekanisme pelaporan insiden keamanan informasi telah tersedia dan terdokumentasi.

**Tabel 2.**
Evaluasi terhadap Kontrol Sumber Daya Manusia

| | |
|---|---|
| A 6.1 | *Screening* |
| *Evidence* | - SOP *recruitment*<br>- *Application form*.<br>- Deskripsi jabatan. |
| A 6.2 | *Terms and conditions of employment* |
| *Evidence* | - Pedoman etika dan perilaku.<br>- Perjanjian kerja. |
| A 6.3 | I*nformation security awareness, education and training* |
| *Evidence* | - *Awareness training*.<br>- SOP *learning and development program*.<br>- Surat Keputusan direksi tentang table komunikasi internal dan eksternal. |
| A 6.4 | *Disciplinary process* |
| *Evidence* | - Peraturan Perusahaan.<br>- Sosialisasi pedoman etika dan perilaku. |
| A 6.5 | *Responsibilities after termination or change of employment* |
| *Evidence* | - Pedoman etika dan perilaku.<br>- Surat pernyataan. |
| A 6.6 | *Confidentiality or non-disclosure agreements* |
| *Evidence* | - Pedoman etika dan perilaku.<br>- Surat pernyataan. |
| A 6.7 | *Remote working* |
| *Evidence* | - Peraturan Perusahaan<br>- SOP Remote Working |

**Tabel 2. (Lanjutan)**
Evaluasi terhadap Kontrol Sumber Daya Manusia

| | |
|---|---|
| A 6.8 | *Information security event reporting* |
| *Evidence* | - SOP Investigasi insiden keamanan infrastruktur *data center*.<br>- Petunjuk kerja panduan penggunaan IT *information system*. |

### 3.3. Kontrol Fisik

Empat belas kontrol fisik difokuskan pada perlindungan pusat data dari ancaman fisik dan lingkungan (seperti pada Tabel 3). Hasil audit menunjukkan bahwa perimeter keamanan fisik, pengendalian akses, pemantauan melalui CCTV, pengelolaan utilitas pendukung telah diterapkan secara memadai. Beberapa kontrol, seperti keamanan aset di luar lokasi (A.7.9), dinyatakan tidak berlaku karena seluruh aset kritikal berada di dalam lingkungan pusat data.

**Tabel 3.**
Evaluasi terhadap Kontrol Fisik

| | |
|---|---|
| A 7.1 | *Physical security perimeters* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 7.2 | *Physical entry* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 7.3 | *Securing offices, rooms and facilities* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 7.4 | *Physical security monitoring* |
| *Evidence* | - Instruksi kerja monitoring CCTV Data Center.<br>- CCTV monitoring *report.* |
| A 7.5 | *Protecting against physical and environmental threats* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 7.6 | *Working in secure areas* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 7.7 | *Clear desk and clear screen* |
| *Evidence* | *- Memorandum of clear desk and clear screen policy.*<br>*- poster clear desk and clear screen.* |
| A 7.8 | *Equipment siting and protection* |
| *Evidence* | - SOP pemeliharaan dan perbaikan sarana dan prasarana.<br>- SOP *fixed assets*.<br>- SOP *infrastructure.* |
| A 7.9 | *Security of assets off-premises* |
| *Evidence* | *Not applicable* |
| A 7.10 | *Storage media* |
| *Evidence* | Instruksi kerja penanganan media yang dapat dipindahkan dari data center. |
| A 7.11 | *Supporting utilities* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 7.12 | *Cabling security* |
| *Evidence* | - Instruksi kerja klasifikasi dan pelabelan informasi dalam ruang lingkup infrastruktur data center.<br>- Instruksi kerja pengendalian operasional data center. |

**Tabel 3. (Lanjutan)**
Evaluasi terhadap Kontrol Fisik

| | |
|---|---|
| A 7.13 | *Equipment maintenance* |
| *Evidence* | - SOP Pemeliharaan dan perbaikan sarana dan prasarana.<br>- Instruksi kerja pengendalian operasional data center. |
| A 7.14 | *Secure disposal or re-use of equipment* |
| *Evidence* | - Instruksi kerja penanganan media yang dapat dipindahkan dari data center.<br>- SOP *fixed assets*.<br>- SOP i*nfrastructure.* |

## 3.4. Kontrol Teknologi

Sebanyak tiga puluh empat kontrol teknologi dievaluasi seperti pada Tabel 4 untuk memastikan perlindungan terhadap sistem informasi dan infrastruktur TI. Penerapan pengamanan *endpoint*, pengelolaan kerentanan teknis, *hardening system*, pencadangan data, pemantauan aktivitas, serta pengamanan jaringan menunjukkan tingkat kesesuaian yang baik terhadap persyaratan ISO/IEC 27001:2022. Kontrol yang berkaitan dengan pengembangan aplikasi dan *secure coding* dinyatakan tidak berlaku karena tidak terdapat aktivitas pengembangan perangkat lunak internal.

**Tabel 4.**
Evaluasi terhadap Kontrol Fisik

| | |
|---|---|
| A 8.1 | *User endpoint devices* |
| *Evidence* | *Implementation of using trend micro (antivirus end user).* |
| A 8.2 | *Privileged access rights* |
| *Evidence* | *No Applicable* |
| A 8.3 | *Information access restriction* |
| *Evidence* | *Access control matrix information system technology division.* |
| A 8.4 | *Access to source code* |
| *Evidence* | *No Applicable* |
| A 8.5 | *Secure authentication* |
| *Evidence* | Instruksi kerja pengaturan akses untuk ruangan dan aset data center. |
| A 8.6 | *Capacity management* |
| *Evidence* | Instruksi kerja monitoring server. |
| A 8.7 | *Protection against malware* |
| *Evidence* | - SOP pengujian dan pemeliharaan keamanan aplikasi.<br>- Instruksi kerja penanganan risiko virus dan turunannya. |
| A 8.8 | *Management of technical vulnerabilities* |
| *Evidence* | Instruksi kerja penanganan kerentanan teknis data center dengan *hardening.* |
| A 8.9 | *Configuration management* |
| *Evidence* | - Instruksi kerja penanganan kerentanan teknis data center dengan *hardening*.<br>- Laporan *hardening server* dan *router.* |
| A 8.10 | *Information deletion* |
| *Evidence* | Instruksi kerja penanganan media yang dapat dipindahkan dari data center. |
| A 8.11 | *Data masking* |
| *Evidence* | Instruksi kerja data *masking non-production*. |

**Tabel 4. (Lanjutan)**
Evaluasi terhadap Kontrol Fisik

| | |
|---|---|
| A 8.12 | *Data leakage prevention* |
| *Evidence* | Instruksi kerja *data masking non-production*. |
| A 8.13 | *Information backup* |
| *Evidence* | Petunjuk kerja proses backup menggunakan *tape backup* LTO. |
| A 8.14 | *Redundancy of information processing facilities* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 8.15 | *Logging* |
| *Evidence* | - Instruksi kerja monitoring *server.*<br>- Program IT *information system.*<br>- Laporan monitoring *server*. |
| A 8.16 | *Monitoring activities* |
| *Evidence* | - Instruksi kerja monitoring *server.*<br>- Laporan monitoring *server.* |
| A 8.17 | *Clock synchronization* |
| *Evidence* | Instruksi kerja pengaturan akses untuk ruangan dan asset data center. |
| A 8.18 | *Use of privileged utility programs* |
| *Evidence* | Instruksi kerja pengaturan akses untuk ruangan dan asset data center. |
| A 8.19 | *Installation of software on operational systems* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 8.20 | *Networks security* |
| *Evidence* | - Instruksi kerja pengendalian operasional data center.<br>- SOP pengujian dan pemeliharaan keamanan aplikasi. |
| A 8.21 | *Security of network services* |
| *Evidence* | - SOP pengujian dan pemeliharaan keamanan aplikasi.<br>- Instruksi kerja penanganan risiko virus dan turunannya. |
| A 8.22 | *Segregation of networks* |
| *Evidence* | Topologi jaringan. |
| A 8.23 | *Web filtering* |
| *Evidence* | - Implementasi penggunaan *trend micro*.<br>- SOP *remote working.* |
| A 8.24 | *Use of cryptography* |
| *Evidence* | Instruksi kerja standarisasi enkripsi. |
| A 8.25 | *Secure development life cycle* |
| *Evidence* | - SOP seleksi dan evaluasi vendor.<br>- Surat pernyataan kerahasiaan atau perjanjian kerja sama. |
| A 8.26 | *Application security requirements* |
| *Evidence* | *Not applicable.* |
| A 8.27 | *Secure system architecture and engineering principles* |
| *Evidence* | Instuksi kerja pemeliharaan dan perbaikan infrastruktur data center. |

**Tabel 4. (Lanjutan)**
Evaluasi terhadap Kontrol Fisik

| | |
|---|---|
| A 8.28 | *Secure coding* |
| *Evidence* | *Not applicable.* |
| A 8.29 | *Security testing in development and acceptance* |
| *Evidence* | - SOP pengujian dan pemeliharaan keamanan aplikasi.<br>- Instruksi kerja pengendalian operasional data center.<br>- SOP pemeliharaan dan perbaikan sarana dan prasarana. |
| A 8.30 | *Outsourced development* |
| *Evidence* | - SOP Seleksi dan evaluasi vendor.<br>- Instruksi kerja pemeliharaan dan perbaikan infrastruktur di data center. |
| A 8.31 | *Separation of development, test and production environments* |
| *Evidence* | Instruksi kerja pengaturan akses untuk ruangan dan asset data center. |
| A 8.32 | *Change management* |
| *Evidence* | Instruksi kerja pengendalian operasional data center. |
| A 8.33 | *Test information* |
| *Evidence* | SOP Pengujian dan pemeliharaan keamanan aplikasi. |
| A 8.34 | *Protection of information systems during audit testing* |
| *Evidence* | - Pedoman etika dan perilaku.<br>- Perjanjian kerja sama.<br>- SOP audit atas system manajemen mutu dan keamanan informasi. |

Selain evaluasi kontrol *Annex* A, auditor juga melakukan peninjauan terhadap temuan audit tahun 2024. Hasil peninjauan menunjukkan bahwa PT ABC telah menindaklanjuti seluruh temuan tersebut melalui tindakan korektif yang sesuai, sehingga tidak ditemukan temuan ketidaksesuaian pada audit surveilans tahun berjalan.

Secara keseluruhan, hasil audit *surveilans* menunjukkan bahwa penerapan kontrol keamanan informasi pada pusat data internal PT ABC telah sesuai dengan *Statement of Applicability* dan persyaratan ISO/IEC 27001:2022. Temuan yang diidentifikasi bersifat Opportunity for Improvement (OFI) dan ditujukan untuk meningkatkan kematangan serta efektivitas SMKI secara berkelanjutan.

### 3.5. Dokumentasi dan Catatan

Seluruh informasi direkam dan didokumentasikan dengan baik sesuai dengan prosedur pengendalian dokumen dan prosedur pengendalian rekaman organisasi.

### 3.6. Audit Internal dan Tindakan Perbaikan

Audit internal dilaksanakan sekali dalam setahun untuk menilai kepatuhan terhadap standar ISO/IEC 27001:2022. Temuan audit menjadi dasar bagi *continuous improvement* pada sistem manajemen keamanan informasi. Temuan dalam internal audit dibahas dalam rapat tinjauan manajemen secara periodik setiap tahun.

## 4. KESIMPULAN DAN SARAN

Penelitian ini bertujuan untuk mengevaluasi efektivitas *Statement of Applicability* (SoA) melalui pelaksanaan audit *surveilans* ISO/IEC 27001:2022 pada infrastruktur pusat data internal PT ABC. Hasil audit *surveilans* menunjukkan bahwa ruang lingkup Sistem

Manajemen Keamanan Informasi (SMKI) telah didefinisikan secara jelas dan mencerminkan aktivitas serta layanan utama organisasi.

Audit *surveilans* mencakup seluruh proses dan unit kerja yang relevan dengan pengelolaan pusat data internal. Evaluasi dilakukan menggunakan pendekatan berbasis risiko dan didukung oleh bukti objektif yang memadai. Seluruh persyaratan ISO/IEC 27001:2022, regulasi yang berlaku, serta persyaratan internal organisasi telah dipenuhi. Implementasi kontrol *Annex* A terbukti selaras dengan SoA, dan kontrol yang dinyatakan tidak berlaku telah disertai justifikasi yang dapat diterima.

Hasil audit menunjukkan bahwa SMKI PT ABC berjalan secara efektif, didukung oleh manajemen risiko yang terdokumentasi dengan baik, tingkat kesadaran karyawan yang memadai, serta komitmen manajemen puncak dalam penyediaan sumber daya, pemantauan kinerja, dan pelaksanaan tinjauan manajemen. Selama audit, tidak ditemukan ketidaksesuaian baik kategori *Non-Conformity* maupun *Discrepancy*. Namun demikian, tiga *Opportunities for Improvement* (OFI) dicatat sebagai masukan untuk peningkatan kematangan SMKI.

Dengan demikian, hasil penelitian ini menegaskan bahwa audit *surveilans* berperan penting dalam memvalidasi kesesuaian dan efektivitas SoA serta mendukung keberlanjutan sertifikasi ISO/IEC 27001:2022. Berdasarkan hasil audit, kelanjutan sertifikasi ISO/IEC 27001:2022 bagi PT. ABC direkomendasikan.

Berdasarkan hasil evaluasi, beberapa rekomendasi yang dapat dipertimbangkan adalah sebagai berikut:

1. Penyelenggaraan pelatihan keamanan siber dan *Generative AI* secara berkala untuk meningkatkan kesadaran dan kompetensi karyawan.
2. Penetapan peran *Key Custodian* guna memperkuat pengelolaan kunci kriptografi.
3. Pelaksanaan pengujian teknis keamanan menggunakan metodologi OSSTMM [5] sebagai pelengkap evaluasi berbasis audit kepatuhan.

## 4. DAFTAR PUSTAKA

*1.* International Organization for Standardization. (2015). ISO/IEC 17021-1:2015 – Conformity assessment: *Requirements for bodies providing audit and certification of management systems.*
*2.* International Organization for Standardization. (2018). ISO 19011:2018 – *Guidelines for auditing management systems.*
*3.* International Organization for Standardization. (2022). ISO/IEC 27001:2022 – *Information security, cybersecurity and privacy protection: Information security management systems.*
4. International Organization for Standardization. (2022). ISO/IEC 27002:2022 – *Information security, cybersecurity and privacy protection: Information security controls.*
5. Otoritas Jasa Keuangan Republik Indonesia. (2024). Peraturan Otoritas Jasa Keuangan Nomor 36 Tahun 2024 tentang Perubahan atas Peraturan Otoritas Jasa Keuangan Nomor 69/POJK.05/2016 tentang Penyelenggaraan Usaha Perusahaan Asuransi, Perusahaan Asuransi Syariah, Perusahaan Reasuransi, dan Perusahaan Reasuransi Syariah. Jakarta: OJK.
6. United Registrar of Systems. (2024). BM-10: Auditor Field Manual. London: URS.