SISTEM MANAJEMEN KEAMANAN INFORMASI

ISO/IEC 27001:2022

Panduan Lengkap dan Implementasi

DR. NUNGKY AWANG CHANDRA, S.SI., M.TI.

SISTEM MANAJEMEN KEAMANAN INFORMASI ISO/IEC 27001:2022

Panduan Lengkap dan Implementasi

Dr. Nungky Awang Chandra, S.Si., M.TI.

sada kurnia pustaka

SISTEM MANAJEMEN KEAMANAN INFORMASI ISO/IEC 27001:2022

Panduan Lengkap dan Implementasi

Penulis:

Dr. Nungky Awang Chandra, S.Si., M.TI.

Tata Letak : Lilis Khalisatul Karimah, S.H.
Desain Cover : Asep Nugraha, S.Hum.
Ukuran : UNESCO 15,5 x 23 cm
Halaman : xi, 153
ISBN : 978-634-7522-36-8
Terbit Pada : Maret 2026
Anggota IKAPI : No. 073/BANTEN/2023

PENERBIT PT SADA KURNIA PUSTAKA
Jl. Kramat, Panenjoan Kec. Carenang, Kab. Serang – Banten, 42195
Email : sadapenerbit@gmail.com
Website : sadapenerbit.com & repository.sadapenerbit.com
Telpon/WA : +62 838 1281 8431

KATA PENGANTAR

Perkembangan teknologi digital yang sangat cepat telah menjadikan keamanan informasi sebagai salah satu pilar utama dalam keberlangsungan organisasi modern. Data dan sistem informasi tidak lagi sekadar aset pendukung operasional, melainkan menjadi aset strategis yang menentukan daya saing, reputasi, serta kepercayaan publik terhadap organisasi. Dalam konteks inilah penerapan Sistem Manajemen Keamanan Informasi berbasis standar internasional menjadi kebutuhan yang tidak dapat diabaikan.

Buku yang berjudul **"SISTEM MANAJEMEN KEAMANAN INFORMASI ISO/IEC 27001:2022 Panduan Lengkap dan Implementasi"** ini hadir sebagai kontribusi penting dalam memperkaya literatur profesional di bidang keamanan informasi. Buku ini tidak hanya menjelaskan struktur dan persyaratan standar ISO/IEC 27001:2022 secara sistematis, tetapi juga memberikan pendekatan implementasi yang praktis, aplikatif, dan relevan dengan kebutuhan organisasi saat ini.

Sebagai standar global, ISO/IEC 27001 menuntut pemahaman yang tidak hanya bersifat konseptual, tetapi juga operasional. Penulis buku ini berhasil menyajikan keseimbangan antara landasan teoritis, interpretasi klausul standar, serta praktik implementasi nyata di lingkungan organisasi. Hal ini menjadikan buku ini sangat bermanfaat bagi berbagai kalangan, mulai dari praktisi keamanan informasi, auditor, konsultan, akademisi, hingga pimpinan organisasi yang bertanggung jawab terhadap tata kelola keamanan informasi.

Saya memandang buku ini sebagai referensi yang sangat relevan dan bernilai tinggi, khususnya bagi organisasi yang sedang mempersiapkan implementasi atau sertifikasi ISO/IEC 27001:2022. Penjelasan yang sistematis, disertai contoh dan pendekatan praktis, akan sangat membantu pembaca dalam memahami kompleksitas penerapan Sistem Manajemen Keamanan Informasi secara menyeluruh.

Akhir kata, saya memberikan apresiasi yang setinggi-tingginya kepada penulis atas dedikasi dan kontribusinya dalam menyusun

buku ini. Semoga karya ini dapat menjadi sumber pengetahuan yang bermanfaat, mendorong peningkatan kesadaran keamanan informasi, serta mendukung penerapan praktik terbaik dalam tata kelola keamanan informasi di berbagai sektor.

Semoga buku ini memberikan manfaat luas bagi pengembangan profesionalisme dan peningkatan kualitas pengelolaan keamanan informasi di masa yang akan datang.

Jeffry Yoris ST, M.M
Technical Manager /Lead Auditor ICT
TSI Sertifikasi Internasional
2026

PRAKATA

Puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat, karunia, dan kesempatan yang diberikan sehingga buku yang berjudul **"SISTEM MANAJEMEN KEAMANAN INFORMASI ISO/IEC 27001:2022 Panduan Lengkap dan Implementasi"** ini dapat diselesaikan dengan baik.

Buku ini disusun sebagai referensi komprehensif bagi praktisi, akademisi, auditor, konsultan, regulator, maupun organisasi yang ingin memahami, menerapkan, mengaudit, dan memperoleh sertifikasi ISO/IEC 27001:2022. Materi yang disajikan tidak hanya mencakup konsep dasar dan interpretasi klausul standar, tetapi juga pendekatan implementasi praktis, proses audit, pengelolaan risiko, serta praktik terbaik yang relevan dengan kebutuhan organisasi modern.

Kami menyadari bahwa implementasi Sistem Manajemen Keamanan Informasi bukan sekadar pemenuhan standar, melainkan merupakan bagian integral dari tata kelola organisasi, perlindungan aset informasi, kepatuhan regulasi, serta keberlanjutan operasional. Oleh karena itu, buku ini dirancang untuk memberikan pemahaman yang sistematis sekaligus aplikatif, sehingga dapat digunakan sebagai panduan nyata dalam proses implementasi di lapangan.

Penyusunan buku ini juga mempertimbangkan dinamika regulasi nasional dan praktik internasional, sehingga pembaca dapat memahami keterkaitan antara standar ISO/IEC 27001 dengan konteks tata kelola keamanan informasi di berbagai sektor, termasuk pemerintahan, industri, dan layanan digital.

Kami berharap buku ini dapat menjadi referensi yang bermanfaat dalam memahami konsep dan struktur ISO/IEC 27001:2022, mendukung implementasi Sistem Manajemen Keamanan Informasi, membantu persiapan audit dan sertifikasi, meningkatkan kesadaran dan budaya keamanan informasi, mendukung pengembangan keilmuan dan praktik profesional di bidang keamanan informasi.

Kami menyadari bahwa buku ini masih memiliki keterbatasan. Oleh karena itu, kritik, saran, dan masukan konstruktif dari para pembaca sangat kami harapkan demi penyempurnaan pada edisi berikutnya.

Kami menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan, kontribusi, dan inspirasi dalam penyusunan buku ini.
Ucapan terima kasih kami sampaikan kepada:

- para praktisi keamanan informasi yang telah berbagi pengalaman implementasi di dunia nyata,
- para auditor dan konsultan sistem manajemen yang memberikan wawasan profesional,
- rekan-rekan akademisi yang telah memberikan masukan konseptual dan metodologis,
- institusi dan organisasi yang secara tidak langsung menjadi sumber pembelajaran praktik terbaik,
- keluarga dan rekan sejawat yang memberikan dukungan moral dan motivasi selama proses penulisan.

Tanpa dukungan berbagai pihak tersebut, buku ini tidak akan dapat disusun secara komprehensif seperti yang tersaji saat ini.

Akhir kata, semoga buku ini memberikan manfaat nyata bagi pengembangan tata kelola keamanan informasi yang lebih baik, lebih matang, dan lebih berkelanjutan di berbagai organisasi.

Jakarta, Maret 2026

Penulis

DAFTAR ISI

KATA PENGANTAR ..... **iii**
PRAKATA ..... **v**
DAFTAR ISI ..... **vii**
DAFTAR TABEL ..... **x**
DAFTAR GAMBAR ..... **xi**
BAB 1 PENDAHULUAN, STANDAR, DAN PRINSIP KEAMANAN INFORMASI **1**
A. Latar Belakang 1
B. Standar Keamanan Informasi 7
C. Prinsip Sistem Manajemen Keamanan Informasi 9
D. Tinjauan Keluarga ISO/IEC 27001 10
BAB 2 PENDAHULUAN SISTEM MANAJEMEN KEAMANAN INFORMASI ISO 27001 ..... **12**
A. Pendahuluan 12
B. Sejarah Singkat Perkembangan ISO/IEC 27001 13
C. Struktur Standar ISO 27001 17
D. Siklus PDCA dalam ISO 27001 20
E. Implementasi ISO/IEC 27001 dan Analisis SWOT 24
F. Kepatuhan Hukum dan Regulasi dalam Konteks Indonesia 27
G. Akreditasi dan Sertifikasi ISO/IEC 27001 27
BAB 3 INISIASI DAN PERENCANAAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI **31**
A. Inisiasi Sistem Manajemen Keamanan Informasi 31
B. Perencanaan Penerapan SMKI 40
C. Penetapan Tim Implementasi SMKI 45

BAB 4 KONTEKS ORGANISASI SISTEM MANAJEMEN KEAMANAN INFORMASI 46
A. Pendahuluan 46
B. Identifikasi Kebutuhan dan Harapan Pihak Berkepentingan 51
C. Penetapan Ruang Lingkup SMKI 53
D. Sistem Manajemen Keamanan Informasi (SMKI) 55
BAB 5 KEPEMIMPINAN 56
A. Kepemimpinan dan Komitmen 56
B. Kebijakan SMKI 61
C. Aturan, Tanggungjawab dan Wewenang Organisasi 65
BAB 6 PERENCANAAN 68
A. Tindakan untuk Menghadapi Risiko dan Peluang 68
B. Sasaran Keamanan Informasi dan Pencapaiannya 80
C. Perencanaan Perubahan 82
BAB 7 PENDUKUNG 84
A. Sumber Daya 84
B. Kompetensi 87
C. Kesadaran 90
D. Komunikasi 92
E. Informasi Terdokumentasi 94
BAB 8 *OPERATION* 99
A. Pengendalian dan Perencanaan Operasional 99
B. Penilaian Resiko Keamanan Informasi 101
C. Penanganan Resiko Keamanan Informasi 103
BAB 9 EVALUASI KINERJA 107
A. *Monitoring*, Pengukuran, Analisis dan Evaluasi 107
B. Internal Audit 109
C. Tinjauan Manajemen 114
BAB 10 PERBAIKAN 117
A. Perbaikan Berkesinambungan 117
B. Ketidaksesuaian dan Tindakan Korektif 118
BAB 11 PROSES SERTIFIKASI 124
A. Pemilihan Lembaga Sertifikasi 124
B. Proses Tahapan Audit Eksternal Oleh Lembaga Sertifikasi 130

DAFTAR PUSTAKA **134**
LAMPIRAN RINGKASAN ANNEX A DAN CONTOH SOA **140**
GLOSARIUM **145**
INDEKS **150**
BIOGRAFI PENULIS **153**

DAFTAR TABEL

Tabel 3.1: Rencana Implementasi SMKI 44
Tabel 4.1: Identifikasi Isu Internal yang Berdampak Pada Keamanan Informasi 48
Tabel 4.2: Identifikasi Isu Eksternal yang Berdampak Pada Keamanan Informasi 50
Tabel 4.3: Identifikasi Kebutuhan dan Harapan Pihak Berkepentingan 52
Tabel 4.4: Hubungan Antara Klausul Dan Penentuan Ruang lingkup SMKI 54
Tabel 5.1: Contoh Tanggungjawab dan Wewenang 67
Tabel 6.1: Penilaian Risiko Keamanan Informasi 74
Tabel 6.2: Contoh Penerapan Rencana Tindakan Penanganan Risiko Keamanan Informasi 76
Tabel 6.3: Contoh Sasaran Keamanan Informasi 81
Tabel 6.4: Rencana Perubahan SMKI 82
Tabel 7.1: Identifikasi dan Penetapan Kompetensi Karyawan 88
Tabel 7.2: Evaluasi Penetapan Kompetensi Karyawan 89
Tabel 7.3: Training *Plan* Kompetensi Karyawan 90
Tabel 7.4: Contoh Program *Awareness* SMKI 92
Tabel 7.5: Contoh Rencana Komunikasi SMKI 94
Tabel 7.6: Hirarki atau Struktur Dokumen SMKI 96
Tabel 10.1: Program Perbaikan Berkelanjutan 118
Tabel 10.2: Informasi Umum 121
Tabel 10.3: Analisis Penyebab Utama Metode 5 *Why Analysis* 122
Tabel 10.4: Rencana Tindakan Korektif 122

DAFTAR GAMBAR

Gambar 1. 1: Tiga Pilar CIA.....2
Gambar 1. 2: Hubungan Antara Keamanan Siber dan Domain Keamanan Lainnya Sumber : ISO/IEC 27035 : 2012.....5
Gambar 2. 1: Kerangka Kerja SMKI ISO/IEC 27001 : 2022 Berdasarkan Siklus PDCA 21
Gambar 6.1: Penilaian dan Penangana Risiko Keamanan Informasi .77
Gambar 9.1: Contoh Flow Diagram Tahapan Proses Internal Audit 110

BAB 1
PENDAHULUAN, STANDAR, DAN PRINSIP KEAMANAN INFORMASI

A. Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa banyak manfaat bagi kehidupan modern, namun di sisi lain juga membuka celah bagi berbagai ancaman terhadap keamanan informasi. Data dan sistem digital kini menjadi target utama bagi pelaku kejahatan siber yang memanfaatkan berbagai bentuk serangan seperti *malware*, *ransomware*, *phishing*, SQL *injection*, hingga *Distributed Denial of Service* (DDoS). Serangan-serangan ini dapat menyebabkan kebocoran data, hilangnya akses ke sistem penting, serta kerugian finansial dan reputasi.

Selain dari serangan eksternal, kerentanan (*vulnerability*) dalam sistem informasi baik dari sisi perangkat lunak, perangkat keras, jaringan, maupun perilaku manusia, menjadi titik lemah yang sering dimanfaatkan oleh peretas. Kerentanan ini dapat berasal dari kesalahan konfigurasi, kurangnya pembaruan sistem (*patching*), penggunaan kata sandi yang lemah, atau ketidaksadaran pengguna terhadap praktik keamanan yang baik. Untuk mengatasi risiko tersebut, keamanan informasi menjadi aspek penting yang harus diterapkan secara menyeluruh dan berkelanjutan.

Buku ini tentang tata kelola keamanan informasi untuk para praktisi dan auditor yang digunakan sebagai panduan penerapan dan audit sistem manajemen keamanan informasi. Berdasarkan standar NIST SP 800-12 Rev. 1, keamanan informasi adalah perlindungan terhadap

informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah, dengan tujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Selain standar NIST SP 800-12 Rev.1, ISO/IEC 27001: 2022 juga mendefinisikan keamanan informasi sebagai pemeliharaan kerahasiaan, integritas, dan ketersediaan informasi. Dari dua standard ini menjelaskan bahwa tata kelola keamanan informasi merupakan tindakan perlindungan untuk menjaga kerahasiaan, integritas dan ketersediaan informasi. Adapun 3 pilar keamanan informasi yaitu melindung kerahasiaan (*Confidenciality*), integritas (*Cntegrity*) dan ketersediaan (*Availability)* informasi dapat dilihat pada gambar 1.1. Tiga Pilar CIA

Gambar 1. 1: Tiga Pilar CIA
Sumber: diolah penulis

1. **Kerahasiaan (*Confidentiality*)**
   Kerahasiaan adalah salah satu dari tiga pilar utama dalam keamanan informasi, bersama dengan integritas dan ketersediaan (sering disingkat sebagai prinsip CIA). Kerahasiaan mengacu pada perlindungan informasi agar tidak diakses, dibaca, atau diketahui oleh pihak yang tidak berwenang.

   Tujuan utama dari kerahasiaan adalah menjaga informasi sensitif seperti data pribadi, data keuangan, rahasia dagang, atau

dokumen penting organisasihanya dapat diakses oleh individu atau sistem yang memiliki hak akses yang sah.

Contoh pelanggaran kerahasiaan antara lain:

a. Peretasan yang mencuri data pengguna dari basis data.
b. Pengiriman email berisi informasi rahasia kepada pihak yang salah.
c. Penggunaan *password* yang mudah ditebak sehingga memungkinkan orang lain masuk ke sistem.

Untuk menjaga kerahasiaan, berbagai langkah teknis dan kebijakan dapat diterapkan, seperti:

a. Enkripsi: Mengubah data menjadi format yang tidak bisa dibaca tanpa kunci khusus.
b. Kontrol akses (*access control*): Mengatur siapa yang boleh melihat atau mengubah informasi tertentu.
c. Penggunaan kata sandi yang kuat dan autentikasi dua faktor (2FA).
d. Pelatihan kesadaran keamanan bagi pengguna agar tidak sembarangan membagikan informasi atau klik tautan berbahaya.
e. Penggunaan VPN atau jaringan aman untuk mencegah penyadapan data saat berkomunikasi.

Menjaga kerahasiaan sangat penting, karena pelanggaran terhadap prinsip ini tidak hanya merugikan secara teknis atau ekonomi, tetapi juga bisa berdampak hukum dan reputasi, terutama jika informasi yang bocor adalah data pribadi atau milik pelanggan.

2. Integritas (*Integrity*)

Integritas adalah salah satu komponen utama dalam prinsip CIA (*Confidentiality, Integrity, Availability*) dalam keamanan informasi. Integritas mengacu pada jaminan bahwa data atau informasi tetap akurat, utuh, dan tidak diubah secara tidak sah, baik saat disimpan maupun saat dikirimkan. Hal ini berarti bahwa data harus tetap sesuai dengan kondisi aslinya, tanpa modifikasi, penghapusan, atau penambahan oleh pihak yang tidak berwenang. Setiap perubahan pada data harus dilakukan secara sah, dengan otorisasi yang tepat, dan tercatat secara logis.

Contoh Pelanggaran Integritas:

a. Seorang peretas mengubah nilai transaksi dalam sistem keuangan.

b. *File* penting dimodifikasi oleh virus komputer tanpa sepengetahuan pengguna.
c. Data pasien dalam sistem rumah sakit diubah secara tidak sah, sehingga berdampak pada penanganan medis.

Upaya Menjaga Integritas Informasi:

a. *Hashing*: Menggunakan fungsi hash (seperti SHA-256) untuk mendeteksi perubahan data. Jika data diubah, nilai hash-nya juga akan berubah.
b. Digital *signature* (tanda tangan digital): Digunakan untuk menjamin bahwa data berasal dari sumber yang sah dan tidak dimodifikasi.
c. Kontrol versi dan audit *trail*: Mencatat semua perubahan data dan siapa yang melakukannya.
d. Pengendalian akses: Mencegah pengguna tidak sah mengubah data.
e. Redundansi dan *backup*: Menyediakan salinan data asli jika terjadi kerusakan atau manipulasi.

Menjaga integritas sangat penting untuk mencegah kesalahan pengambilan keputusan, menghindari penipuan, dan memastikan kepercayaan terhadap sistem informasi. Dalam banyak industri seperti keuangan, kesehatan, dan pemerintahan, pelanggaran integritas bisa menyebabkan konsekuensi hukum dan kerugian besar.

3. Ketersediaan (*Availability*)

Ketersediaan adalah salah satu dari tiga pilar utama dalam keamanan informasi, bersama dengan kerahasiaan (*Confidentiality*) dan integritas (*Integrity*). Ketersediaan berarti menjamin bahwa data, sistem, dan layanan informasi selalu dapat diakses dan digunakan oleh pihak yang berwenang ketika dibutuhkan.

Sistem informasi yang memiliki ketersediaan tinggi akan tetap berjalan secara normal dan responsif, bahkan saat terjadi gangguan, beban tinggi, atau serangan. Hal ini sangat penting agar proses bisnis, pelayanan publik, komunikasi, dan operasi lainnya tidak terhenti.

Contoh Pelanggaran Ketersediaan:

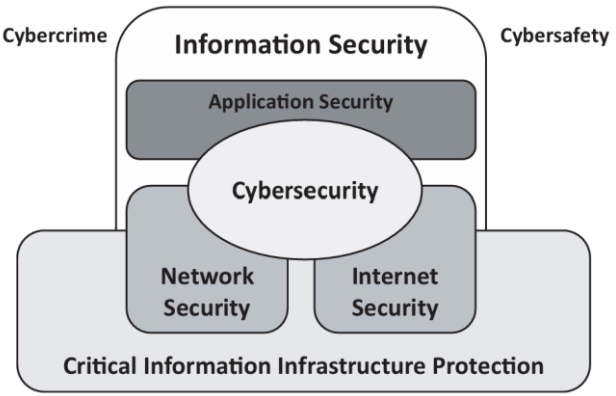
a. Serangan DDoS (*Distributed Denial of Service*) yang membuat situs web tidak bisa diakses.
b. Pemadaman listrik yang menyebabkan server tidak beroperasi.

c. Kerusakan perangkat keras tanpa sistem cadangan.
d. Sistem layanan kesehatan yang tidak bisa diakses saat keadaan darurat.

Langkah untuk Menjaga Ketersediaan:
a. *Backup* data dan sistem secara rutin, agar dapat dipulihkan jika terjadi kerusakan.
b. Redundansi dan *failover*: Menyediakan sistem cadangan atau alternatif (misalnya server *backup*).
c. *Firewall* dan sistem deteksi serangan (IDS/IPS) untuk mencegah serangan yang mengganggu layanan.
d. Pemeliharaan rutin untuk mencegah kerusakan perangkat lunak atau perangkat keras.
e. Monitoring sistem secara *real-time* untuk mendeteksi dan merespons masalah lebih cepat.

Menjaga ketersediaan sangat penting terutama di sektor-sektor yang membutuhkan layanan 24/7 seperti rumah sakit, perbankan, *e-commerce*, dan layanan publik. Jika sistem tidak tersedia saat dibutuhkan, bisa timbul kerugian finansial, hilangnya kepercayaan, hingga risiko terhadap keselamatan manusia.

Adapun hubungan keamanan informasi dengan domain keamanan lainnya menurut ISO/IEC 27035: 2012 dapat ditunjukkan pada gambar 1.2. Hubungan antara keamanan siber dan domain keamanan lainnya.



Gambar 1. 2: Hubungan Antara Keamanan Siber dan Domain Keamanan Lainnya
Sumber : ISO/IEC 27035 : 2012

Dari gambar 1.2. diatas bahwa keamanan informasi meliputi keamanan aplikasi, jaringan, internet yang mendukung dunia maya, termasuk perlindungan terhadap infrastruktur informasi yang kritikal.

Sistem informasi adalah sekumpulan aplikasi, layanan, aset teknologi informasi, atau komponen penanganan informasi lainnya (ISO/IEC 27002 : 2022). Jadi sistem manajemen keamanan informasi merupakan program tata kelola organisasi sistematis yang mencangkup setiap aspek kebijakan melalui kontrol dan prosedur keamanan tertentu. Buku ini membahas tentang penerapan sistem manajemen keamanan informasi berbasis kerangka ISO/IEC 27001 : 2022

Sistem Manajemen Keamanan Informasi (SMKI) atau Information *Security* Management *System* (ISMS) penting karena menyediakan kerangka kerja yang sistematis dan berkelanjutan untuk melindungi aset informasi organisasi dari berbagai ancaman. Berikut adalah alasan utama mengapa SMKI sangat penting :

1. **Melindungi Informasi Sensitif**
   SMKI memastikan bahwa informasi penting seperti data pelanggan, keuangan, dan kekayaan intelektual dilindungi dari:
   a. Akses tidak sah (kerahasiaan),
   b. Perubahan tanpa izin (integritas),
   c. Ketidaksesuaian waktu atau kehilangan (ketersediaan).
2. **Mengurangi Risiko Keamanan**
   Dengan pendekatan manajemen risiko, SMKI:
   a. Mengidentifikasi potensi ancaman dan kerentanannya,
   b. Menetapkan kontrol untuk mengurangi risiko,
   c. Menyiapkan respons terhadap insiden secara proaktif.
3. **Meningkatkan Kepercayaan dan Reputasi**
   Pelanggan dan mitra akan lebih percaya kepada organisasi yang menjaga keamanan informasi mereka dengan standar internasional (seperti ISO/IEC 27001). Ini juga membantu meningkatkan reputasi perusahaan di pasar.
4. **Mendukung Kepatuhan terhadap Regulasi**
   Banyak peraturan seperti:

a. PDP UU No.27 Tahun 2022 tentang perlindungan data pribadi (Indonesia)
b. GDPR (Uni Eropa),
c. PDPA (Malaysia),
d. HIPAA (AS),

Regulasi mengharuskan organisasi menjaga keamanan dan privasi data. SMKI membantu memenuhi persyaratan ini dan menghindari sanksi hukum.

5. **Meminimalkan Dampak Serangan Siber**
   SMKI membantu organisasi:
   a. Mendeteksi insiden lebih cepat,
   b. Menanggapi secara tepat,
   c. Memulihkan operasional dengan lebih efisien, sehingga mengurangi kerugian finansial dan gangguan operasional akibat serangan seperti *ransomware*, *phishing*, dan *malware*.
6. **Meningkatkan Efisiensi Operasional**
   Dengan mendokumentasikan proses, kebijakan, dan prosedur keamanan informasi, SMKI menciptakan kejelasan tanggung jawab dan koordinasi yang lebih baik antar unit.
7. **Mendorong Budaya Keamanan di Organisasi**
   SMKI menekankan pentingnya pelatihan dan kesadaran karyawan terhadap keamanan informasi. Ini membantu menciptakan budaya kerja yang lebih waspada terhadap risiko keamanan.

B. Standar Keamanan Informasi

Berikut adalah beberapa standar keamanan informasi yang paling penting dan banyak digunakan di seluruh dunia. Standar ini membantu organisasi mengelola dan melindungi informasi secara sistematis:

1. **ISO/IEC 27001 (Standar Internasional)**
   a. Fungsi: Memberikan kerangka kerja untuk membangun, menerapkan, menjalankan, memantau, dan meningkatkan Sistem Manajemen Keamanan Informasi.
   b. Fokus utama: Melindungi *kerahasiaan, integritas, dan ketersediaan* informasi.
   c. Mengapa penting: Standar global yang diakui dan sering menjadi dasar sertifikasi keamanan informasi.

2. **ISO/IEC 27002**
   a. Fungsi: Menyediakan panduan praktik terbaik untuk kontrol keamanan informasi.
   b. Isi: Merinci pengendalian keamanan yang disebut dalam ISO/IEC 27001, seperti:
      1) Kontrol akses
      2) Keamanan fisik
      3) Enkripsi
      4) Pengendalian keamanan personel

3. **NIST SP 800 Series (AS)**
   a. Fungsi: Rangkaian dokumen dari *National Institute of Standards and Technology (NIST)*, digunakan oleh institusi pemerintahan dan sektor swasta di AS.
   b. Contoh penting:
      1) NIST SP 800-53: Rekomendasi kontrol keamanan untuk sistem informasi federal.
      2) *NIST Cybersecurity Framework* (CSF): Panduan untuk mengelola risiko siber.

4. **PCI DSS (*Payment Card Industry Data Security Standard*)**
   a. Fungsi: Standar untuk organisasi yang menyimpan, memproses, atau mengirim data kartu kredit.
   b. Tujuan: Melindungi data pemegang kartu dari pencurian atau penipuan.

5. **COBIT (*Control Objectives for Information and Related Technologies*)**
   a. Fungsi: Kerangka kerja untuk tata kelola dan manajemen teknologi informasi.
   b. Fokus: Menjaga keselarasan antara TI dan tujuan bisnis.

6. **GDPR (General Data Protection Regulation – Uni Eropa)**
   a. Fungsi: Bukan standar teknis, tapi regulasi hukum yang mengatur perlindungan data pribadi warga negara Uni Eropa.
   b. Penting untuk organisasi global yang beroperasi di atau memiliki pelanggan dari Eropa.

7. **PDPA (Personal Data Protection *Act* – Malaysia)**
   a. Fungsi: Regulasi yang melindungi data pribadi di Malaysia.
   b. Relevansi: Menuntut organisasi untuk mengambil langkah-langkah keamanan teknis dan organisasi untuk melindungi data pribadi.

C. Prinsip Sistem Manajemen Keamanan Informasi

Berikut adalah prinsip-prinsip utama dari Sistem Manajemen Keamanan Informasi, yang dirancang untuk melindungi informasi organisasi secara menyeluruh dan berkelanjutan:

1. **Kerahasiaan (*Confidentiality*)**
   Informasi hanya dapat diakses oleh pihak yang berwenang.
   a. Mencegah akses tidak sah terhadap data.
   b. Contoh: Autentikasi pengguna, enkripsi data, dan kontrol akses.

2. **Integritas (*Integrity*)**
   Informasi harus akurat, lengkap, dan tidak boleh diubah tanpa izin.
   a. Menjamin bahwa data tidak dimodifikasi, dihapus, atau dirusak secara tidak sah.
   b. Contoh: *Digital signature*, *log audit*, dan *hash* data.

3. **Ketersediaan (*Availability*)**
   Informasi harus tersedia saat dibutuhkan oleh pihak yang berwenang.
   a. Memastikan sistem dan data tetap dapat diakses meski terjadi gangguan atau serangan.
   b. Contoh: *Backup* data, sistem redundan, dan perlindungan terhadap serangan DDoS.

4. **Pendekatan Berbasis Risiko (*Risk-Based Approach*)**
   Fokus pada identifikasi dan penanganan risiko yang paling relevan terhadap aset informasi.
   a. Prioritas diberikan pada area dengan potensi ancaman tertinggi.
   b. Evaluasi risiko dilakukan secara berkala dan sistematis.

5. **Peningkatan Berkelanjutan (*Continuous Improvement*)**
   SMKI harus ditinjau dan diperbarui secara berkala sesuai perubahan ancaman, teknologi, dan kebutuhan organisasi.

a. Diterapkan melalui siklus PDCA (*Plan-Do-Check-Act*).
b. Contoh: Audit internal, tinjauan manajemen, dan tindakan korektif.

6. **Kepatuhan terhadap Regulasi dan Hukum**
   Memastikan bahwa organisasi mematuhi peraturan dan undang-undang yang berlaku terkait perlindungan informasi. Contoh: ISO/IEC 27001, PDPA (Malaysia), GDPR (Uni Eropa).

7. **Tanggung Jawab Manajemen**
   Pimpinan organisasi harus menunjukkan komitmen dan dukungan terhadap keamanan informasi. Termasuk menetapkan kebijakan, menyediakan sumber daya, dan membentuk tim keamanan.

8. **Keterlibatan Karyawan dan Pelatihan**
   Semua pihak dalam organisasi harus diberi pelatihan dan sadar akan pentingnya keamanan informasi. Contoh: Simulasi *phishing*, pelatihan keamanan siber, dan kebijakan penggunaan perangkat.

D. Tinjauan Keluarga ISO/IEC 27001

Keluarga ISO/IEC 27000 adalah serangkaian standar internasional yang dirancang untuk membantu organisasi mengelola keamanan informasi secara sistematis, dengan pusatnya adalah ISO/IEC 27001. Berikut adalah anggota penting dari keluarga ISO/IEC 27000:

1. **ISO/IEC 27000 – Terminologi dan Konsep Dasar**
   a. Menyediakan istilah dan definisi umum yang digunakan di seluruh standar keluarga ISO/IEC 27000.
   b. Berguna untuk memahami konsep dasar seperti "risiko informasi", "kontrol keamanan", dll.

2. **ISO/IEC 27001 – Sistem Manajemen Keamanan Informasi**
   a. Standar inti dalam keluarga ini.
   b. Menetapkan persyaratan untuk membangun, menerapkan, memelihara, dan meningkatkan SMKI.
   c. Cocok untuk sertifikasi.

3. **ISO/IEC 27002 – Panduan Pengendalian Keamanan Informasi**
   a. Memberikan praktik terbaik dan kontrol keamanan yang bisa digunakan untuk mengimplementasikan ISO/IEC 27001.
   b. Berisi kontrol dalam kategori seperti keamanan fisik, kontrol akses, dan keamanan SDM.

4. **ISO/IEC 27005 – Manajemen Risiko Keamanan Informasi**
   a. Memberikan panduan tentang pendekatan manajemen risiko informasi yang mendukung ISO/IEC 27001.
   b. Penting untuk mengidentifikasi, menilai, dan mengelola risiko terhadap aset informasi.

5. **ISO/IEC 27003 – Panduan Implementasi ISO/IEC 27001**
   Memberikan panduan langkah demi langkah untuk mengimplementasikan SMKI berdasarkan ISO/IEC 27001.

6. **ISO/IEC 27004 – Pengukuran dan Evaluasi Keamanan Informasi**
   Menjelaskan cara mengukur efektivitas SMKI, termasuk indikator kinerja dan metrik.

7. **ISO/IEC 27006 – Persyaratan Akreditasi untuk Badan Sertifikasi**
   a. Digunakan oleh badan sertifikasi untuk melakukan audit dan memberikan sertifikasi ISO/IEC 27001.
   b. Menjamin bahwa sertifikasi dilakukan secara profesional dan terakreditasi.

Contoh Lain dalam Keluarga 27000 (berkembang terus):
1. ISO/IEC 27017: Pedoman keamanan *cloud computing*.
2. ISO/IEC 27018: Perlindungan data pribadi di *cloud*.
3. ISO/IEC 27701: Tambahan untuk privasi data (terkait GDPR).
4. ISO/IEC 27019: Untuk industri energi.

BAB 2
PENDAHULUAN SISTEM MANAJEMEN KEAMANAN INFORMASI ISO 27001

A. Pendahuluan

Dalam era transformasi digital dan ekonomi berbasis informasi, informasi telah menjadi salah satu aset paling bernilai bagi organisasi. Informasi tidak lagi hanya berupa dokumen fisik, tetapi mencakup data digital, basis data pelanggan, informasi keuangan, kekayaan intelektual, data penelitian, hingga data pribadi individu. Nilai strategis informasi tersebut menjadikannya sasaran berbagai ancaman keamanan, baik yang bersifat teknis seperti peretasan sistem, maupun non-teknis seperti kebocoran data akibat kelalaian sumber daya manusia. Oleh karena itu, organisasi modern dituntut untuk memiliki pendekatan yang sistematis, terstruktur, dan berkelanjutan dalam melindungi aset informasi yang dimilikinya.

Kerangka kerja ISO merupakan seperangkat kebijakan, prosedur, proses, dan kontrol yang dirancang untuk membantu organisasi dalam mengelola aspek tertentu secara konsisten dan dapat diaudit. Salah satu standar ISO yang memiliki peran strategis dalam konteks keamanan informasi adalah ISO/IEC 27001. Standar ini menetapkan persyaratan untuk membangun, menerapkan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi *atau Information Security Management*

BAB 3
INISIASI DAN PERENCANAAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Inisiasi Sistem Manajemen Keamanan Informasi

Periode akuntansi laporan keuangan BUMDES dimulai pada 1 Januari dan berakhir pada 31 Desember dalam tahun yang bersangkutan. Periode akuntansi hijau BUMDES mengikuti periode akuntansi sektor publik, karena ritme pelaporan dilakukan di akhir sampai dengan awal tahun. Apabila pelaporan dilakukan melebihi 31 Desember di tahun bersangkutan maka penetapan waktu pelaporan tidak melebihi 12 bulan.

Inisiasi Sistem Manajemen Keamanan Informasi (SMKI) adalah proses memulai dan menetapkan kerangka kerja keamanan informasi dalam suatu organisasi. Proses ini mencakup identifikasi ancaman, penilaian risiko, dan penetapan kebijakan serta pengendalian yang sesuai. Inisiasi SMKI bertujuan untuk melindungi aset informasi organisasi dari berbagai ancaman dan risiko, memastikan kerahasiaan, integritas, dan ketersediaan informasi. Adapun tahapan dari inisiasi *system* manajemen keamanan informasi pada sebuah organisasi adalah :

1. **Komitmen Manajemen Puncak**

   Tujuan dari komitmen manajemen adalah untuk mendapatkan dukungan penuh dari pimpinan organisasi. Komitmen manajemen puncak adalah fondasi yang sangat penting dalam keberhasilan

BAB 4
KONTEKS ORGANISASI SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Pendahuluan

ISO/IEC 27001:2022 menempatkan Klausul 4 – *Context of the Organization* sebagai fondasi utama dalam pembangunan dan implementasi *system* manajemen keamanan informasi. Klausul ini menegaskan bahwa keamanan informasi tidak dapat diperlakukan sebagai sistem teknis semata, melainkan harus dipahami sebagai bagian integral dari konteks strategis, bisnis, regulasi, dan lingkungan organisasi. Pendekatan ini menandai pergeseran penting dari paradigma keamanan informasi yang sebelumnya berorientasi pada kontrol teknis menuju pendekatan *risk-based, context-aware*, dan *business-driven*.

Dalam konteks Indonesia, penerapan Klausul 4 menjadi sangat krusial karena organisasi beroperasi dalam lanskap yang kompleks, melibatkan regulasi nasional seperti UU ITE, UU Perlindungan Data Pribadi (UU PDP), Peraturan OJK, Peraturan BSSN, serta tuntutan pasar global yang mengharuskan organisasi mematuhi standar internasional. Oleh karena itu, pemahaman mendalam terhadap konteks organisasi merupakan prasyarat untuk memastikan bahwa SMKI yang dibangun relevan, efektif, dan berkelanjutan.

Klausul 4 terdiri dari empat subklausul utama, yaitu:

1. Pemahaman Konteks Organisasi
2. Identifikasi Kebutuhan dan Harapan Pihak Berkepentingan
3. Penentapan Ruanglingkup SMKI

BAB 5
KEPEMIMPINAN

A. Kepemimpinan dan Komitmen

Klausul 5.1 ISO/IEC 27001:2022 menekankan bahwa keberhasilan Sistem Manajemen Keamanan Informasi sangat ditentukan oleh kepemimpinan dan komitmen manajemen puncak. Standar ini menempatkan keamanan informasi sebagai tanggung jawab strategis organisasi, bukan sekadar fungsi operasional atau teknis yang hanya berada di bawah departemen teknologi informasi. Oleh karena itu, manajemen puncak harus menunjukkan keterlibatan aktif, arah kebijakan yang jelas, serta dukungan nyata terhadap seluruh proses pengelolaan keamanan informasi.

Dalam konteks sistem manajemen, kepemimpinan tidak hanya berarti memberikan persetujuan administratif terhadap dokumen atau kebijakan, tetapi mencakup kemampuan untuk mengarahkan, mengendalikan, dan memastikan bahwa keamanan informasi menjadi bagian integral dari tata kelola organisasi. Manajemen puncak bertanggung jawab untuk memastikan bahwa SMKI dirancang, diterapkan, dipelihara, dan ditingkatkan secara berkelanjutan sesuai dengan tujuan strategis organisasi.

Salah satu aspek utama dari kepemimpinan dalam ISO 27001 adalah akuntabilitas terhadap efektivitas SMKI. Manajemen puncak tidak dapat mendelegasikan tanggung jawab keamanan informasi sepenuhnya kepada staf teknis. Mereka harus memastikan bahwa sistem yang diterapkan benar-benar mampu melindungi kerahasiaan, integritas, dan ketersediaan informasi organisasi. Hal ini menuntut keterlibatan manajemen dalam pengambilan keputusan strategis terkait keamanan

BAB 6
PERENCANAAN

A. Tindakan untuk Menghadapi Risiko dan Peluang

Klausul 6.1 ISO/IEC 27001:2022 mengatur bagaimana organisasi harus merencanakan tindakan untuk mengatasi risiko dan peluang yang berkaitan dengan Sistem Manajemen Keamanan Informasi. Klausul ini menegaskan bahwa penerapan SMKI harus berbasis pada pendekatan manajemen risiko yang sistematis, terstruktur, dan terintegrasi dengan tujuan organisasi.

Dalam konteks sistem manajemen, risiko dipahami sebagai potensi kejadian yang dapat memengaruhi kemampuan organisasi dalam melindungi kerahasiaan, integritas, dan ketersediaan informasi. Sementara itu, peluang dipahami sebagai kondisi yang dapat meningkatkan efektivitas sistem manajemen atau memperkuat perlindungan informasi. Dengan demikian, organisasi tidak hanya berfokus pada pengurangan ancaman, tetapi juga memanfaatkan peluang untuk meningkatkan kinerja keamanan informasi.

Klausul 6.1 berangkat dari pemahaman bahwa setiap organisasi beroperasi dalam lingkungan yang dinamis, di mana perubahan teknologi, proses bisnis, regulasi, dan ancaman siber dapat memengaruhi tingkat risiko keamanan informasi. Oleh karena itu, organisasi harus secara proaktif mengidentifikasi risiko dan peluang, mengevaluasi dampaknya, serta merencanakan tindakan yang tepat untuk mengendalikannya.

Pendekatan ini memastikan bahwa SMKI tidak bersifat reaktif, tetapi mampu mengantisipasi potensi masalah sebelum terjadi. Dengan melakukan perencanaan berbasis risiko, organisasi dapat

BAB 7
PENDUKUNG

A. Sumber Daya

Klausul 7.1 ISO/IEC 27001:2022 menegaskan bahwa organisasi harus menentukan dan menyediakan sumber daya yang diperlukan untuk membangun, menerapkan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi. Klausul ini berada dalam bagian *support* karena berfungsi sebagai fondasi operasional yang memungkinkan seluruh mekanisme SMKI dapat berjalan secara efektif.

Dalam perspektif sistem manajemen, kebijakan dan perencanaan tidak akan menghasilkan dampak nyata tanpa dukungan sumber daya yang memadai. Oleh karena itu, Klausul 7.1 memastikan bahwa organisasi tidak hanya menetapkan tujuan keamanan informasi, tetapi juga menyediakan kapasitas nyata untuk mencapainya. Sumber daya dalam konteks ini tidak terbatas pada aspek finansial, tetapi mencakup seluruh elemen yang memungkinkan sistem keamanan informasi berfungsi secara optimal.

1. Makna Strategis Penyediaan Sumber Daya

Penyediaan sumber daya merupakan bentuk komitmen nyata manajemen terhadap keamanan informasi. Jika organisasi menyatakan bahwa perlindungan informasi merupakan prioritas strategis, maka prioritas tersebut harus tercermin dalam alokasi sumber daya yang memadai. Tanpa dukungan sumber daya, kebijakan keamanan informasi hanya menjadi pernyataan formal tanpa kemampuan implementasi. Dengan menyediakan sumber daya yang cukup, organisasi memastikan bahwa pengendalian keamanan dapat diterapkan secara efektif, risiko dapat dikelola secara sistematis, respons terhadap insiden dapat dilakukan dengan cepat, peningkatan sistem dapat berlangsung berkelanjutan. Dengan kata lain, sumber daya adalah enabler utama keberhasilan SMKI.

BAB 8
OPERATION

A. Pengendalian dan Perencanaan Operasional

Klausul 8.1 ISO/IEC 27001:2022 mengatur bahwa organisasi harus merencanakan, menerapkan, dan mengendalikan proses operasional yang diperlukan untuk memenuhi persyaratan Sistem Manajemen Keamanan Informasi serta melaksanakan tindakan yang telah ditentukan dalam proses manajemen risiko.

Klausul ini merupakan tahap implementasi nyata dari seluruh perencanaan yang telah dilakukan sebelumnya. Jika klausul 4, 5, 6, dan 7 berfokus pada pemahaman konteks, kepemimpinan, perencanaan, serta dukungan sistem, maka klausul 8 berfokus pada bagaimana semua rencana tersebut dijalankan dalam praktik operasional sehari-hari.

Dengan kata lain, klausul 8.1 adalah jembatan antara desain sistem manajemen dan aktivitas operasional. Di sinilah organisasi memastikan bahwa kontrol keamanan benar-benar diterapkan, prosedur dijalankan, dan tindakan pengendalian risiko dilaksanakan secara konsisten.

Perencanaan operasional berarti organisasi harus menentukan bagaimana proses keamanan informasi akan dijalankan. Ini mencakup penentuan aktivitas, metode pelaksanaan, tanggung jawab, serta sumber daya yang diperlukan untuk memastikan bahwa pengendalian keamanan berjalan sesuai rencana. Perencanaan ini harus selaras dengan kebijakan keamanan informasi, hasil penilaian risiko, rencana perlakuan risiko, tujuan keamanan informasi. Tanpa perencanaan operasional yang jelas, kontrol keamanan hanya akan menjadi konsep teoritis tanpa implementasi nyata.

Selain merencanakan, organisasi juga harus mengendalikan pelaksanaan proses operasional. Pengendalian ini bertujuan memastikan

BAB 9
EVALUASI KINERJA

A. *Monitoring*, Pengukuran, Analisis dan Evaluasi

Klausul 9.1 ISO/IEC 27001:2022 mengatur bahwa organisasi harus secara sistematis memantau, mengukur, menganalisis, dan mengevaluasi kinerja Sistem Manajemen Keamanan Informasi. Klausul ini memastikan bahwa organisasi tidak hanya menerapkan kontrol keamanan, tetapi juga menilai apakah kontrol tersebut benar-benar bekerja secara efektif dalam melindungi aset informasi.

Dalam siklus manajemen berbasis risiko, implementasi kontrol keamanan saja tidak cukup. Organisasi harus mengetahui apakah kontrol tersebut berjalan sesuai harapan, apakah risiko benar-benar menurun, dan apakah tujuan keamanan informasi tercapai. Oleh karena itu, organisasi harus menentukan apa yang perlu dipantau dan diukur, bagaimana metode pengukurannya, kapan pemantauan dilakukan, siapa yang bertanggung jawab, serta bagaimana hasilnya dianalisis dan dievaluasi.

Pemantauan dan pengukuran merupakan proses pengumpulan data mengenai kinerja keamanan informasi. Data ini dapat berupa jumlah insiden keamanan, tingkat kepatuhan terhadap kebijakan, efektivitas kontrol teknis, atau kinerja proses operasional. Namun data saja tidak cukup. Organisasi harus menganalisis data tersebut untuk memahami maknanya, kemudian mengevaluasi apakah hasilnya memenuhi target yang ditetapkan.

Klausul ini juga menekankan bahwa organisasi harus memiliki dasar yang jelas dalam menentukan indikator kinerja. Artinya organisasi tidak boleh melakukan pengukuran secara acak, tetapi harus menetapkan indikator yang relevan dengan tujuan keamanan informasi dan risiko yang dihadapi.

BAB 10
PERBAIKAN

A. Perbaikan Berkesinambungan

Klausul 10.1 ISO/IEC 27001:2022 Klausul ini menegaskan bahwa organisasi tidak hanya harus mengimplementasikan dan mengevaluasi SMKI, tetapi juga harus secara aktif melakukan perbaikan berkelanjutan berdasarkan hasil *monitoring*, audit, insiden, dan tinjauan manajemen. Tujuan utamanya perbaikan berkesinambungan ini adalah untuk memastikan sistem tidak stagnan, tetapi terus meningkat sesuai perubahan risiko, teknologi, dan kebutuhan organisasi, meningkatkan efektivitas SMKI, meningkatkan kinerja keamanan informasi, mencegah masalah sebelum terjadi

Klausul 10.1 mengharuskan organisasi secara berkelanjutan meningkatkan kesesuaian, kecukupan, dan efektivitas Sistem Manajemen Keamanan Informasi. Perbaikan berkesinambungan berarti organisasi secara aktif mencari peluang peningkatan, bukan hanya memperbaiki masalah.

Perbaikan dapat berasal dari berbagai sumber, seperti:

1. Hasil audit internal
2. *Monitoring* kinerja keamanan
3. Hasil penilaian risiko
4. Insiden keamanan informasi
5. *Feedback* pihak berkepentingan
6. Tinjauan manajemen
7. Perubahan teknologi atau regulasi

BAB 11
PROSES SERTIFIKASI

A. Pemilihan Lembaga Sertifikasi

Dalam implementasi standar ISO, organisasi yang telah membangun sistem manajemen (misalnya ISO/IEC 27001) perlu menjalani audit sertifikasi oleh pihak independen yang disebut Lembaga sertifikasi (*certification body*). Namun tidak semua badan sertifikasi memiliki kredibilitas yang sama. Oleh karena itu, badan sertifikasi harus diakreditasi oleh lembaga akreditasi resmi untuk menjamin bahwa proses audit dan sertifikasi dilakukan secara kompeten, objektif, dan sesuai standar internasional.

Di Indonesia, sistem ini terhubung dengan kerangka regulasi nasional dan pengakuan internasional. Badan sertifikasi adalah lembaga independen yang melakukan audit kesesuaian terhadap sistem manajemen organisasi dan menerbitkan sertifikat jika organisasi memenuhi persyaratan standar ISO.

Dalam sertifikasi ISO 27001, badan sertifikasi akan melakukan:
1. Audit tahap 1 (kesiapan dokumentasi)
2. Audit tahap 2 (implementasi sistem)
3. Audit surveilans berkala
4. Audit resertifikasi

Badan sertifikasi harus beroperasi sesuai standar internasional ISO/IEC 17021 (standar untuk lembaga sertifikasi sistem manajemen).

Akreditasi adalah proses formal yang menyatakan bahwa badan sertifikasi kompeten untuk melakukan audit dan sertifikasi dalam lingkup tertentu. Akreditasi memastikan bahwa auditor kompeten,

DAFTAR PUSTAKA

Ahmad, A. (2018). Cyber incident response management. Journal of Cyber*security*.

Ahmad, A., Bosua, R., & Scheepers, R. (2015). Protecting organizational competitive advantage. Information Management & Computer *Security*.

AlHogail, A. (2015). Design and validation of information *security* culture framework. Computers in Human Behavior.

Alotaibi, F. (2020). Information *security* management maturity. Information *System*s Journal.

Alshaikh, M. (2020). Developing cyber*security* capability maturity models. Computers & *Security*.Amin, H.E., Samhat, A.E., Chamoun, M., Oueidat, L., Feghali, A.(2024). An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. *Journal of Cybersecurity and Privacy, MDPI,4,* 357-381.

Alshboul, Y. (2019). Information *security* governance frameworks. International Journal of Information *Security*.

Anderson, R. (2020). *Security* Engineering: A Guide to Building Dependable Distributed *System*s (3rd ed.). Wiley.

Bada, M., Sasse, A., & Nurse, J. (2019). Cyber*security* awareness campaigns. Computers & *Security*.

Behl, A. (2017). Cyber*security* and Cyberwar. Oxford University Press.

Behl, A., & Behl, K. (2017). Cyber*security* and Cyberwar.

Bishop, M. (2019). Computer *Security*: Art and Science. Addison-Wesley.

Calder, A. (2022). ISO/IEC 27001:2022 – A Pocket Guide. IT Governance Publishing.

Calder, A., & Moir, S. (2020). Information *Security* Based on ISO 27001. IT Governance Publishing.

Calder, A., & Watkins, S. (2019). IT Governance: An International Guide to Data *Security*. Kogan Page.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2018). The economics of information *security*. Management Science.

Chen, T. (2018). Cyber*security* risk management. IEEE *Security* & Privacy.

Cisco. (2022). Annual Cyber*security* Report.

Colwill, C. (2019). Human f*act*ors in information *security*. Information *Security* Technical Report.

Conti, M., & Kumar, A. (2018). A survey on *security* in IoT. IEEE Communications Surveys.

Crossler, R. (2018). A comprehensive *review* of cyber*security* research. Journal of the Association for Information *System*s.

Da Veiga, A. (2020). Information *security* culture measurement. Computers & *Security*.

Darktrace. (2021). Cyber Threat Report.

Deloitte. (2022). Global Cyber Risk Survey.

Dhillon, G., & Backhouse, J. (2018). Information *security* management in the new millennium. Communications of the ACM.

Dosari, K.A., & Fetais, N.(2023). Risk-Management Framework and Information-*Security Systems* for Small and Medium Enterprises (SMEs): AMeta-Analysis Approach. *Journal of Electronics, MDPI,12,* 3629.

ENISA. (2021). Cyber*security* Threat Landscape.

ENISA. (2022). Threat Landscape Report.

EY. (2022). Global Information *Security* Survey.

Garcia, I.D.S., Mejia, J., Gilabert, T.S.F. (2023). Cyber*security Risk assessment*: A *System*atic Mapping *Review*, Proposal, and Validation. *Journal of Applied Science, MDPI, 13,* 395.

Gartner. (2022). Cyber*security* Strategic Roadmap.

Google. (2022). Threat Analysis Report.

Gordon, L., Loeb, M., & Zhou, L. (2019). Investing in cyber*security*. Journal of Accounting and Public Policy.

Hall, J. (2016). Accounting Information *System*s. Cengage.

Hodson, C.J. (2024). *Cyber Risk Management*. London EC1V3RS United Kingdom: Kogan Page Limited.

Humphreys, E. (2016). Information *security* management standards. Information *Security* Journal.

IBM *Security*. (2023). Cost of Data Breach Report.

ISACA. (2019). COBIT 2019 Framework.

ISACA. (2020). CISM *Review* Manual.

ISACA. (2021). CISA *Review* Manual.

ISF. (2021). Information *Security* Forum Report.

ISO. (2012). ISO/IEC 27035 Information *Security* Incident Management.

ISO. (2013). ISO/IEC 27017 *Cloud Security* Controls.

ISO. (2018). ISO 31000 Risk Management Guidelines.

ISO. (2018). ISO/IEC 27005 Information *Security* Risk Management.

ISO. (2019). ISO/IEC 27701 Privacy Information Management.

ISO. (2022). ISO/IEC 27001:2022 Information *Security* Management *System*s — Requirements.

ISO. (2022). ISO/IEC 27002:2022 Information *Security* Controls.

Karyda, M. (2019). Information *security* policy compliance. Information *System*s Frontiers.

Kaspersky Lab. (2022). Global Cyber*security* Outlook.

Kizza, J. (2019). Guide to Computer Network *Security*. Springer.

KPMG. (2022). Cyber*security* Considerations Report.

Krutz, R., & Vines, R. (2017). The CISSP Prep Guide. Wiley.

Lallie, H. et al. (2021). Cyber *security* in the age of COVID-19. Computers & *Security*.

Landoll, D. (2016). The *Security Risk assessment* Handbook. CRC Press.

Laudon, K., & Laudon, J. (2021). Management Information *System*s. Pearson.

Leirvik, R. (2023). *Understand, Manage, and Measure Cyber Risk : Practical Solution for Creating a Sustainable Cyber Program*. Arlington, VA, USA : Apress.

Maiwald, E. (2019). Network *Security*. McGraw-Hill.

McAfee. (2022). Threat Intelligence Report.

Melaku, H.M.(2023). Context-Based and Adaptive Cyber*security* Risk Management Framework. *Journal of Risks, MDPI,11,* 101.

Microsoft. (2022). Digital Defense Report.

Mitnick, K. (2018). The Art of Invisibility.

Nair, A., & Gresshman, M.R. (2023). *Mastering Information Security Compliance Management*. Birmingham, B3 2PB, UK : Packt Publishing Ltd.

National Cyber *Security* Centre. (2022). Cyber *Security* Annual Report.

NIST. (2020). Cyber*security* Framework.

NIST. (2021). Special Publication 800-53 *Security* Controls.

OECD. (2021). Cyber*security* Policy Framework.

OWASP. (2021). Top 10 Web *Security* Risks.

Palo Alto Networks. (2022). Cyber*security* Threat Report.

Parker, D. (2017). Fighting Computer Crime. Wiley.

Peltier, T. (2016). Information *Security* Risk Analysis. CRC Press.

Peltier, T. (2017). Information *Security* Policies, Procedures, and Standards. CRC Press.

Pfleeger, C., & Pfleeger, S. (2015). *Security* in Computing.

Ponemon Institute. (2022). Global Cyber*security* Benchmark Study.

Posthumus, S., & Von Solms, R. (2015). A framework for the governance of information *security*. Computers & *Security*.

PwC. (2022). Global Digital Trust Insights.

Ransbotham, S., Mitra, S., & Ramsey, J. (2017). Information *security* and firm value. MIS Quarterly.

Ross, R., McEvilley, M., & Oren, J. (2016). *Systems Security* Engineering. NIST.

RSA *Security*. (2022). Fraud and Risk Intelligence Report.

SANS Institute. (2022). Cyber*security* Survey Report.

Schneier, B. (2015). Secrets and Lies. Wiley.

Siponen, M., Mahmood, M., & Pahnila, S. (2017). Employees' adherence to *security* policies. Information & Management.

Smith, R. (2018). Authentication: From Passwords to Public Keys.

Solms, R., & Van Niekerk, J. (2016). From information *security* to cyber *security*. Computers & *Security*.

Sophos. (2022). State of *Ransomware* Report.

Spears, J., & Barki, H. (2016). User participation in information *security* risk management. MIS Quarterly.

Stallings, W. (2017). Effective Cyber*security*. Addison-Wesley.

Stallings, W., & Brown, L. (2018). Computer *Security* Principles and Pr*act*ice.

Stoneburner, G. et al. (2018). Risk Management Guide for IT *System*s.

Symantec. (2022). Internet *Security* Threat Report.

Tipton, H., & Krause, M. (2016). Information *Security* Management Handbook.

Trend Micro. (2022). Cyber Risk Landscape.

Venter, H., & Eloff, J. (2017). Information *security* governance framework. Information *System*s Management.

Verizon. (2023). Data Breach Investigation Report.

Von Solms, B., & Von Solms, R. (2018). Cyber*security* and cyberwar. Information *Security* Journal.

Von Solms, R. (2017). Information *security* governance. Computers & *Security*.

Warkentin, M. (2018). Behavioral information *security* research. MIS Quarterly.

Westerman, G. (2019). Digital risk management. MIT Sloan Management *Review*.

Whitman, M. (2018). Information *security* risk management. Journal of Information Privacy and *Security*.

Whitman, M., & Mattord, H. (2018). Management of Information *Security*.

Whitman, M., & Mattord, H. (2021). Principles of Information *Security*.

Williams, P. (2019). Information *security* governance. Journal of Cyber*security*.

World Economic Forum. (2022). Global Cyber*security* Outlook.

Yang, Y. (2019). Cyber*security* governance model. IEEE *Security* & Privacy.

Zhang, Y. (2018). Information *security* risk modeling. Computers & *Security*.

Zhou, L. (2019). Cyber*security* investment strategies. Journal of Cyber*security*.

LAMPIRAN
RINGKASAN ANNEX A
DAN CONTOH SOA

Berikut adalah Tabel Ringkasan Annex A ISO/IEC 27001:2022 yang berisi 93 kontrol keamanan informasi yang dikelompokkan dalam 4 kategori utama:

1. *Organizational Controls* (37 kontrol)
2. *People Controls* (8 kontrol)
3. *Physical Controls* (14 kontrol)
4. *Technological Controls* (34 kontrol)

Annex A merupakan daftar kontrol referensi yang digunakan dalam proses *risk treatment* (klausul 6.1.3) dan didokumentasikan dalam Statement of Applicability (SoA).

Tabel A.5 *Organizational Controls* (37 Kontrol)

No	Kode	Nama Kontrol
1	A.5.1	Kebijakan keamanan informasi
2	A.5.2	Peran dan tanggung jawab keamanan informasi
3	A.5.3	Pemisahan tugas
4	A.5.4	Tanggung jawab manajemen
5	A.5.5	Kontak dengan otoritas
6	A.5.6	Kontak dengan kelompok kepentingan khusus
7	A.5.7	Intelijen ancaman
8	A.5.8	Keamanan informasi dalam manajemen proyek
9	A.5.9	Inventaris aset informasi
10	A.5.10	Penggunaan aset yang dapat diterima
11	A.5.11	Pengembalian aset
12	A.5.12	Klasifikasi informasi
13	A.5.13	Pelabelan informasi
14	A.5.14	Transfer informasi
15	A.5.15	Kontrol akses

16	A.5.16	Manajemen identitas
17	A.5.17	Informasi autentikasi
18	A.5.18	Hak akses
19	A.5.19	Keamanan dalam hubungan pemasok
20	A.5.20	Penanganan keamanan pemasok dalam kontrak
21	A.5.21	Manajemen keamanan dalam rantai pasok ICT
22	A.5.22	Monitoring dan *review* layanan pemasok
23	A.5.23	Keamanan penggunaan layanan *cloud*
24	A.5.24	Perencanaan dan persiapan manajemen insiden
25	A.5.25	Penilaian dan keputusan insiden
26	A.5.26	Respons insiden
27	A.5.27	Pembelajaran dari insiden
28	A.5.28	Pengumpulan bukti
29	A.5.29	Keamanan informasi selama gangguan
30	A.5.30	Kesiapan TIK untuk kelangsungan bisnis
31	A.5.31	Persyaratan hukum, regulasi, kontrak
32	A.5.32	Hak kekayaan intelektual
33	A.5.33	Perlindungan catatan
34	A.5.34	Privasi dan perlindungan data pribadi
35	A.5.35	*Review* independen keamanan informasi
36	A.5.36	Kepatuhan kebijakan keamanan
37	A.5.37	Prosedur operasional terdokumentasi

Tabel A.6 *People Controls* (8 Kontrol)

No	Kode	Nama Kontrol
1	A.6.1	Screening
2	A.6.2	Syarat kerja
3	A.6.3	Kesadaran keamanan
4	A.6.4	Proses disipliner
5	A.6.5	Tanggung jawab setelah terminasi
6	A.6.6	Perjanjian kerahasiaan
7	A.6.7	Kerja jarak jauh
8	A.6.8	Pelaporan insiden keamanan

Table. A.7 *Physical Controls* (14 Kontrol)

No	Kode	Nama Kontrol
1	A.7.1	Perimeter keamanan fisik
2	A.7.2	Kontrol masuk fisik
3	A.7.3	Keamanan kantor, ruangan, fasilitas
4	A.7.4	Monitoring keamanan fisik
5	A.7.5	Perlindungan terhadap ancaman fisik

6	A.7.6	Area kerja aman
7	A.7.7	Clear desk dan clear screen
8	A.7.8	Penempatan peralatan
9	A.7.9	Keamanan aset di luar lokasi
10	A.7.10	Media penyimpanan
11	A.7.11	Utilitas pendukung
12	A.7.12	Keamanan kabel
13	A.7.13	Pemeliharaan peralatan
14	A.7.14	Pembuangan atau penggunaan kembali peralatan

Tabel A.8 *Technological Controls* (34 Kontrol)

No	Kode	Nama Kontrol
1	A.8.1	Endpoint devices
2	A.8.2	Hak akses istimewa
3	A.8.3	Pembatasan akses informasi
4	A.8.4	Akses kode sumber
5	A.8.5	Autentikasi aman
6	A.8.6	Manajemen kapasitas
7	A.8.7	Perlindungan *malware*
8	A.8.8	Manajemen kerentanan teknis
9	A.8.9	Manajemen konfigurasi
10	A.8.10	Penghapusan informasi
11	A.8.11	Masking data
12	A.8.12	Pencegahan kebocoran data
13	A.8.13	*Backup* informasi
14	A.8.14	Redundansi fasilitas
15	A.8.15	Logging
16	A.8.16	Monitoring aktivitas
17	A.8.17	Sinkronisasi waktu
18	A.8.18	Penggunaan utilitas sistem
19	A.8.19	Instalasi software operasional
20	A.8.20	Keamanan jaringan
21	A.8.21	Keamanan layanan jaringan
22	A.8.22	Segmentasi jaringan
23	A.8.23	Web filtering
24	A.8.24	Penggunaan kriptografi
25	A.8.25	Secure development lifecycle
26	A.8.26	Persyaratan keamanan aplikasi
27	A.8.27	Arsitektur sistem aman
28	A.8.28	Secure coding
29	A.8.29	Pengujian keamanan
30	A.8.30	Outsourced development

31	A.8.31	Pemisahan lingkungan
32	A.8.32	Manajemen perubahan
33	A.8.33	Data uji
34	A.8.34	Audit sistem informasi

Annex A tidak wajib semua diterapkan.
Kontrol dipilih berdasarkan hasil *risk assessment*, kebutuhan bisnis, regulasi, kontrak, teknologi yang digunakan, Kontrol yang dipilih dicatat dalam Statement of Applicability (SoA), Contoh pementaan Annex A kedalam SOA dapat ditunjukan pada tabel 1 berikut.

Tabel 1. Contoh *Statement of Applicability* (SOA)

No	Control ID	Nama Kontrol	Relevan (Y/N)	Justifikasi	Status Implementasi	Referensi Dokumen	Risiko Terkait
1	A.5.1	Kebijakan keamanan informasi	Y	Dibutuhkan untuk governance ISMS	Implemented	ISMS Policy v1.2	Risiko tata kelola
2	A.5.9	Inventaris aset	Y	Aset informasi harus dikendalikan	Implemented	Asset Register SOP	Kehilangan aset
3	A.5.15	Kontrol akses	Y	Mencegah akses tidak sah	Implemented	Access Control Policy	Unauthorized access
4	A.5.23	Keamanan layanan *cloud*	Y	Sistem menggunakan *cloud*	Implemented	*Cloud Security* Policy	Data exposure
5	A.6.3	*Security* awareness	Y	Mengurangi human error	Implemented	Training Record	*Phishing*
6	A.6.7	Remote working	Y	Banyak pekerja remote	Implemented	Remote Work Policy	Endpoint risk
7	A.7.2	Physical entry control	Y	Server room terbatas	Implemented	Physical *Security* SOP	Physical intrusion

8	A.7.7	Clear desk policy	Y	Data sensitif hardcopy	Implemented	Clean Desk Policy	Data leakage
9	A.8.7	*Malware* protection	Y	Perlindungan endpoint	Implemented	Antivirus SOP	*Malware* attack
10	A.8.13	*Backup* informasi	Y	Business continuity	Implemented	*Backup* Procedure	Data loss
11	A.8.24	Kriptografi	Y	Enkripsi data sensitif	Implemented	Crypto Policy	Data breach
12	A.8.32	*Change management*	Y	Kontrol perubahan sistem	Implemented	*Change management* SOP	*System* failure
13	A.8.4	Source code access	N	Tidak ada software development	Not Applicable	—	—
14	A.7.9	Asset offsite	N	Semua aset onsite	Not Applicable	—	—

GLOSARIUM

A

Access Control = Mekanisme pembatasan akses ke sistem atau informasi hanya bagi pihak yang berwenang.
Accountability = Prinsip bahwa setiap aktivitas sistem dapat ditelusuri kepada individu yang bertanggung jawab.
Asset = Segala sesuatu yang memiliki nilai bagi organisasi dan perlu dilindungi, seperti data, perangkat keras, atau layanan.
Asset Inventory = Daftar seluruh aset informasi yang dimiliki organisasi.
Authentication = Proses verifikasi identitas pengguna sebelum diberikan akses.
Authorization = Proses pemberian hak akses kepada pengguna yang telah terautentikasi.
Audit = Pemeriksaan sistematis terhadap penerapan sistem manajemen keamanan informasi.
Audit Trail = Catatan aktivitas sistem yang dapat digunakan untuk pelacakan kejadian.

B

Backup = Proses pembuatan salinan data untuk mencegah kehilangan data.
Baseline *Security* = Standar minimum kontrol keamanan yang harus diterapkan.
Business Continuity = Kemampuan organisasi untuk melanjutkan operasi bisnis saat terjadi gangguan.
Business Continuity *Plan* (BCP) = Rencana untuk menjaga kelangsungan operasional organisasi saat terjadi gangguan.
Business Imp*act* Analysis (BIA) = Analisis dampak gangguan terhadap proses bisnis.

C

CIA Triad = Prinsip dasar keamanan informasi: *Confidentiality*, *Integrity*, *Availability*.
Confidentiality = Perlindungan informasi dari akses tidak sah.
Compliance = Kepatuhan terhadap regulasi, standar, dan kebijakan.
Control = Mekanisme yang digunakan untuk mengurangi risiko keamanan informasi.
Cryptography = Teknik pengamanan informasi menggunakan algoritma matematika.

D

Data Classification = Proses pengelompokan data berdasarkan tingkat sensitivitas.

Data Breach = Insiden keamanan yang menyebabkan kebocoran data.

Data *Integrity* = Jaminan bahwa data tetap akurat dan tidak berubah tanpa izin.

Digital Forensics = Proses investigasi terhadap bukti digital setelah insiden keamanan.

E

Encryption = Teknik mengubah data menjadi kode yang tidak dapat dibaca tanpa kunci.

Endpoint *Security* = Perlindungan perangkat pengguna seperti laptop dan smartphone.

Event Management = Pengelolaan kejadian sistem untuk mendeteksi ancaman keamanan.

F

Firewall = Sistem keamanan jaringan yang mengontrol lalu lintas jaringan.

Forensic Investigation = Investigasi digital untuk mengidentifikasi sumber serangan.

Fraud Detection = Proses mendeteksi aktivitas penipuan dalam sistem informasi.

G

Governance = Kerangka kerja pengelolaan keamanan informasi dalam organisasi.

Gap Analysis = Analisis kesenjangan antara kondisi saat ini dengan standar yang diharapkan.

H

Hash Function = Algoritma kriptografi yang menghasilkan nilai hash unik dari data.

Human F*acto*r = Faktor manusia yang dapat mempengaruhi keamanan informasi.

I

Information Asset = Informasi yang memiliki nilai bagi organisasi.

Information *Security* = Perlindungan informasi dari akses tidak sah, perubahan, atau kerusakan.

Integrity = Jaminan bahwa informasi tetap utuh dan akurat.

ISMS = Sistem manajemen yang digunakan untuk mengelola keamanan informasi secara sistematis.

Incident Management = Proses pengelolaan insiden keamanan informasi.

J

Joint Audit = Audit yang dilakukan oleh lebih dari satu auditor atau lembaga sertifikasi.

K

Key Management = Proses pengelolaan kunci kriptografi.

Knowledge Asset = Pengetahuan organisasi yang memiliki nilai strategis.

L

Least Privilege = Prinsip memberikan hak akses minimum yang diperlukan.

Log Management = Pengelolaan catatan aktivitas sistem.

M

Malware = Perangkat lunak berbahaya yang dirancang untuk merusak sistem.

Monitoring = Proses pemantauan aktivitas sistem secara berkelanjutan.

Mitigation = Tindakan untuk mengurangi dampak risiko.

N

Network *Security* = Perlindungan jaringan komputer dari ancaman.

Nonconformity = Ketidaksesuaian terhadap standar atau prosedur.

O

Operational Control = Pengendalian proses operasional untuk memastikan keamanan informasi.

Outsourcing = Penggunaan pihak ketiga untuk menjalankan aktivitas organisasi.

P

Patch Management = Proses pembaruan sistem untuk memperbaiki kerentanan.

Penetration Testing = Pengujian keamanan sistem dengan simulasi serangan.

Policy = Pernyataan formal mengenai aturan keamanan informasi.

Privacy = Perlindungan terhadap data pribadi.

Q

Quality Assurance = Proses memastikan kualitas sistem atau layanan.

R
Risk = Kombinasi kemungkinan terjadinya ancaman dan dampaknya.
Risk assessment = Proses identifikasi dan evaluasi risiko keamanan informasi.
Risk treatment = Tindakan untuk menangani risiko yang telah diidentifikasi.
Risk Register = Dokumen yang berisi daftar risiko organisasi.

S
***Security* Awareness** = Program untuk meningkatkan kesadaran keamanan informasi.
***Security* Control** = Mekanisme perlindungan terhadap ancaman keamanan.
***Security* Incident** = Kejadian yang dapat mengancam keamanan informasi.
Statement of Applicability (SoA) = Dokumen yang menjelaskan kontrol keamanan yang diterapkan.

T
Threat = Potensi penyebab insiden keamanan informasi.
Third Party Risk = Risiko keamanan dari pihak ketiga.

U
User Access Management = Pengelolaan hak akses pengguna terhadap sistem.

V
Vulnerability = Kelemahan dalam sistem yang dapat dimanfaatkan oleh penyerang.
***Vulnerability* Assessment** = Proses identifikasi kelemahan keamanan sistem.

W
Whitelist = Daftar entitas yang diizinkan untuk mengakses sistem.

X
X.509 Certificate = Sertifikat digital untuk autentikasi jaringan.

Y
Zero-Day *Vulnerability* = Kerentanan keamanan yang belum memiliki patch.

Z

Zero Trust *Security* = Model keamanan yang tidak mempercayai pengguna atau perangkat tanpa verifikasi.

Berisi tentang daftar istilah penting yang ada dalam buku ini.

INDEKS

A
Aset Informasi — 45, 112, 118
Audit Eksternal — 210, 212
Audit Internal — 175–182
Availability — 32, 98
Access Control — 125, 280
Awareness Keamanan Informasi — 134

B
Backup Data — 150, 285
Business Continuity *Plan* (BCP) — 160
Business Imp*act* Analysis (BIA) — 162

C
CIA Triad — 30–32
Confidentiality — 30, 92
Compliance — 45, 210
Control Keamanan Informasi — 270
Cryptography — 290

D
Dokumen ISMS — 140
Disaster *Recovery Plan* (DRP) — 165
Data Breach — 295

E
Evaluasi Risiko — 118
Encryption — 292
External Audit — 210

F
Firewall — 288
Forensic Digital — 300

G
Gap Analysis ISO 27001 — 85
Governance Keamanan Informasi — 70

H

Human Error — 310

I
Information *Security* — 25–30
ISMS (Information *Security* Management *System*) — 35–40
Incident Management — 295
Integrity — 31

J
Joint Audit — 210

K
Kebijakan Keamanan Informasi — 105
Kompetensi SDM — 128
Kontrol Annex A — 260–275

L
Log Management — 286
Least Privilege — 284

M
Monitoring Keamanan Informasi — 190
Manajemen Risiko — 110
Malware — 300

N
Network *Security* — 285
Nonconformity — 230

O
Operational Control — 155

P
Penilaian Risiko — 115
Penanganan Risiko — 120
Penetration Testing — 298
Policy Keamanan Informasi — 105

Q
Quality Management *System* — 50

R
Risk assessment — 115

Risk treatment — 120
Risk Register — 118

S
Security Awareness — 135
Security Incident — 295
Statement of Applicability (SoA) — 270
Surveillance Audit — 215

T
Threat — 112
Third Party Risk — 140

U
User Access Management — 284

V
Vulnerability — 112
Vulnerability Assessment — 296

W
Whitelist — 285

X
X.509 Certificate — 290

Y
Zero-Day *Vulnerability* — 300

Z
Zero Trust *Security* — 305Quotient (EQ) 17

BIOGRAFI PENULIS

Dr. Nungky Awang Chandra, S.Si., M.TI. Nungky Awang Chandra, lahir di Semarang 1973. Penulis selain dosen teknik informatika fasilkom universitas mercubuana, juga berprofesi sebagai auditor sistem manajemen keamanan informasi ISO 27001, ISO22301, ISO 27701, ISO 20000, ISO 42001 yang teregister di BSSN. Penulis merupakan lulusan pendidikan Sarjana S1 jurusan Fisika Komputasi Institut Teknologi Bandung pada tahun 1998. Kemudian pada tahun 2007 melanjutkan pendidikan master dibidang Magister Teknologi Informasi Universitas Indonesia, menyelesaikan studinya pada tahun 2009. Pada tahun 2022 penulis juga menyelesaikan studi S3 di Universitas Indonesia dengan disertasi dan publikasi jurnal bereputasi internasional tentang keamanan siber dan manajemen risiko keamanan siber. Selain itu pada tahun 2023 penulis juga menyelesaikan studi postgraduted cyber *security* di Massachusetts Institute of Technology (MIT).

Penulis memiliki kepakaran dibidang keamanan siber, pengembangan aplikasi, drone. Dan untuk mewujudkan karier sebagai dosen profesional, penulis pun aktif sebagai peneliti dibidang kepakarannya tersebut. Beberapa penelitian yang telah dilakukan didanai oleh internal perguruan tinggi dan juga Kemenristek DIKTI. Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini. Adapun untuk koresponden dengan penulis dapat email ke penulis dengan email: nungkyac707@gmail.com

SISTEM MANAJEMEN KEAMANAN INFORMASI

ISO/IEC 27001:2022

Panduan Lengkap dan Implementasi

Ancaman keamanan siber yang semakin kompleks, kebocoran data, serta tuntutan kepatuhan terhadap berbagai regulasi menjadikan pengelolaan keamanan informasi sebagai kebutuhan strategis bagi setiap organisasi. Buku **"SISTEM MANAJEMEN KEAMANAN INFORMASI ISO/IEC 27001:2022 Panduan Lengkap dan Implementasi"** hadir sebagai referensi komprehensif bagi organisasi yang ingin memahami dan menerapkan standar keamanan informasi secara sistematis dan terstruktur. Buku ini membahas secara mendalam konsep, prinsip, serta tahapan implementasi **ISO/IEC 27001**, yaitu standar internasional yang memberikan kerangka kerja dalam membangun, menerapkan, memantau, dan meningkatkan Sistem Manajemen Keamanan Informasi untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi organisasi. Melalui pendekatan yang praktis dan aplikatif, buku ini menjelaskan bagaimana organisasi dapat memulai penerapan SMKI mulai dari tahap inisiasi, perencanaan, implementasi, monitoring, hingga peningkatan berkelanjutan, termasuk pembentukan tim implementasi, penyusunan kebijakan keamanan informasi, metodologi manajemen risiko, serta pengelolaan dokumen dan kontrol keamanan.

Selain itu, buku ini juga membahas berbagai aspek penting dalam pengelolaan keamanan informasi seperti manajemen risiko, pengelolaan sumber daya, audit internal, tindakan korektif, serta evaluasi efektivitas sistem keamanan informasi. Penjelasan dilengkapi dengan contoh penerapan praktis, tabel, serta pendekatan analisis yang dapat membantu organisasi memahami langkah-langkah implementasi secara lebih sistematis. Penerapan ISO/IEC 27001 tidak hanya membantu organisasi dalam melindungi aset informasi, tetapi juga memberikan berbagai manfaat strategis seperti meningkatkan kepercayaan pelanggan dan mitra bisnis, mendukung kepatuhan terhadap regulasi perlindungan data, meningkatkan efisiensi operasional, serta meminimalkan dampak serangan siber. Buku ini juga menyoroti pentingnya tata kelola keamanan informasi yang baik serta peran lembaga sertifikasi dan regulator dalam memastikan bahwa proses sertifikasi dilakukan oleh badan yang kompeten dan diakui secara nasional maupun internasional.

sada kurnia pustaka

ISBN 978-634-7522-36-8

9 786347 522368