MANAJEMEN RISIKO KEAMANAN INFORMASI ISO/IEC 27005 : 2022

Penulis:
Dr. Nungky Awang Chandra, S.Si., M.TI.
Siti Maesaroh, S.Kom., M.T.I.
Mohamad Yusuf, S.Kom., M.C.S
Diva Alifta Chandra, B.Eng., M.Sc.

MANAJEMEN RISIKO KEAMANAN INFORMASI ISO/IEC 27005 : 2022

Dr. Nungky Awang Chandra, S.Si., M.TI.
Siti Maesaroh, S.Kom., M.T.I.
Mohamad Yusuf, S.Kom., M.C.S.
Diva Alifta Chandra, B.Eng., M.Sc.

sada kurnia pustaka

MANAJEMEN RISIKO KEAMANAN INFORMASI ISO/IEC 27005 : 2022

Penulis:
Dr. Nungky Awang Chandra, S.Si., M.TI.
Siti Maesaroh, S.Kom., M.T.I.
Mohamad Yusuf, S.Kom., M.C.S.
Diva Alifta Chandra, B.Eng., M.Sc.

Tata Letak : Lilis Khalisatul Karimah
Desain Cover : Asep Nugraha
Ukuran : UNESCO 15,5 x 23 cm
Halaman : xiv, 183
ISBN : 978-634-7522-60-3
Terbit Pada : Mei 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

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga buku yang berjudul **"Manajemen Risiko Keamanan Informasi ISO/IEC 27005 : 2022"** ini dapat diselesaikan dengan baik. Buku ini disusun sebagai upaya untuk memberikan pemahaman yang komprehensif mengenai konsep, metodologi, serta praktik terbaik dalam pengelolaan risiko keamanan informasi.

Perkembangan teknologi informasi yang sangat pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan dan kegiatan organisasi. Digitalisasi sistem informasi, penggunaan layanan *cloud*, integrasi perangkat *Internet of Things* (IoT), serta pemanfaatan kecerdasan buatan (Artificial *Intelligence*) telah meningkatkan efisiensi dan produktivitas organisasi. Namun di sisi lain, perkembangan tersebut juga menghadirkan berbagai tantangan baru dalam keamanan informasi.

Ancaman siber seperti kebocoran data, serangan *ransomware*, pencurian identitas digital, serta gangguan terhadap sistem informasi menjadi risiko yang semakin nyata bagi organisasi di berbagai sektor. Oleh karena itu, organisasi perlu menerapkan pendekatan yang sistematis dalam mengelola risiko keamanan informasi agar dapat melindungi aset informasi yang dimiliki serta menjaga keberlangsungan operasional organisasi.

Standar ISO/IEC 27005 : 2022 memberikan kerangka kerja yang komprehensif dalam pengelolaan risiko keamanan informasi. Standar ini melengkapi implementasi sistem manajemen keamanan informasi (SMKI) berbasis ISO/IEC 27001, dengan menyediakan metodologi yang sistematis untuk melakukan identifikasi, analisis, evaluasi, serta penanganan risiko keamanan informasi.

Buku ini disusun untuk memberikan pemahaman yang lebih mendalam mengenai penerapan manajemen risiko keamanan informasi berdasarkan standar internasional tersebut. Pembahasan

dalam buku ini mencakup konsep dasar keamanan informasi, kerangka kerja standar ISO/IEC 27000, metode analisis risiko, implementasi kontrol keamanan berdasarkan ISO/IEC 27002, serta berbagai teknik analisis risiko modern seperti *vulnerability* assessment, penetration testing, dan *threat intelligence*.

Selain itu, buku ini juga membahas berbagai perkembangan terbaru dalam keamanan siber, termasuk risiko keamanan yang berkaitan dengan teknologi modern seperti *cloud computing*, artificial *intelligence*, *Internet of Things*, serta potensi risiko keamanan di era komputasi kuantum. Dengan demikian, buku ini diharapkan dapat memberikan perspektif yang lebih luas mengenai tantangan keamanan informasi di masa depan.

Penulis menyadari bahwa buku ini masih memiliki berbagai keterbatasan. Oleh karena itu, kritik dan saran yang konstruktif dari para pembaca sangat diharapkan untuk penyempurnaan buku ini di masa yang akan datang.

Akhir kata, penulis berharap buku ini dapat memberikan manfaat bagi para praktisi keamanan informasi, auditor sistem informasi, manajer risiko, akademisi, serta mahasiswa yang ingin memahami konsep dan implementasi manajemen risiko keamanan informasi secara lebih mendalam.

Semoga buku ini dapat menjadi salah satu referensi yang bermanfaat dalam meningkatkan kesadaran dan kemampuan organisasi dalam mengelola risiko keamanan informasi.

Penulis

PRAKATA

Perkembangan teknologi informasi dalam beberapa dekade terakhir telah membawa perubahan yang sangat signifikan dalam berbagai sektor kehidupan, baik di bidang pemerintahan, industri, pendidikan, maupun layanan publik. Digitalisasi proses bisnis, penggunaan sistem informasi berbasis *cloud*, serta meningkatnya konektivitas jaringan global telah memberikan berbagai kemudahan dalam pengelolaan informasi dan pengambilan keputusan.

Namun demikian, kemajuan teknologi tersebut juga diiringi dengan meningkatnya risiko keamanan informasi. Ancaman siber seperti kebocoran data, serangan *malware*, *ransomware*, hingga pencurian informasi sensitif menjadi tantangan serius bagi organisasi modern. Berbagai insiden keamanan informasi yang terjadi di berbagai negara menunjukkan bahwa risiko siber dapat menimbulkan dampak yang sangat besar terhadap stabilitas operasional organisasi serta kepercayaan publik.

Dalam menghadapi tantangan tersebut, organisasi memerlukan pendekatan yang sistematis dalam mengelola risiko keamanan informasi. Salah satu standar internasional yang banyak digunakan dalam pengelolaan risiko keamanan informasi adalah ISO/IEC 27005, yang merupakan bagian dari keluarga standar ISO/IEC 27000. Standar ini memberikan panduan yang komprehensif mengenai proses identifikasi, analisis, evaluasi, serta penanganan risiko keamanan informasi sebagai bagian dari implementasi Sistem Manajemen Keamanan Informasi (SMKI).

Buku ini disusun dengan tujuan untuk memberikan pemahaman yang komprehensif mengenai konsep dan praktik manajemen risiko keamanan informasi berbasis ISO/IEC 27005 : 2022. Pembahasan dalam buku ini tidak hanya mencakup konsep teoritis, tetapi juga dilengkapi dengan contoh implementasi praktis, studi kasus, serta berbagai template yang dapat digunakan dalam proses manajemen risiko.

Selain membahas kerangka standar internasional seperti ISO/IEC 27001, ISO/IEC 27002, dan ISO/IEC 27005, buku ini juga mengintegrasikan berbagai pendekatan modern dalam analisis risiko keamanan informasi, termasuk penggunaan Common *Vulnerability Scoring System* (CVSS), *threat intelligence*, *vulnerability* assessment, dan penetration testing. Buku ini juga menyoroti perkembangan risiko keamanan siber yang berkaitan dengan teknologi modern seperti *cloud computing*, *Internet of Things* (IoT), *Artificial Intelligence*, serta potensi risiko keamanan pada era komputasi kuantum.

Penulis berharap buku ini dapat menjadi referensi yang bermanfaat bagi para praktisi keamanan informasi, auditor sistem informasi, manajer risiko, akademisi, serta mahasiswa yang memiliki minat dalam bidang keamanan informasi dan manajemen risiko siber.

Penulis menyadari bahwa penyusunan buku ini tidak lepas dari berbagai keterbatasan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari para pembaca demi penyempurnaan buku ini di masa mendatang.

Akhir kata, penulis berharap buku ini dapat memberikan kontribusi dalam meningkatkan pemahaman mengenai pentingnya manajemen risiko keamanan informasi serta mendorong penerapan praktik keamanan informasi yang lebih baik dalam berbagai organisasi.

Jakarta, 2026

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

A. Latar Belakang Keamanan Informasi

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan besar dalam cara organisasi menjalankan operasional bisnisnya. Digitalisasi proses bisnis, penggunaan sistem informasi berbasis *cloud*, serta integrasi jaringan global telah memungkinkan organisasi untuk meningkatkan efisiensi, produktivitas, dan inovasi. Namun di sisi lain, ketergantungan yang semakin tinggi terhadap teknologi informasi juga meningkatkan risiko terhadap keamanan informasi.

Informasi saat ini telah menjadi salah satu aset paling berharga bagi organisasi. Data pelanggan, data keuangan, rahasia dagang, hingga informasi strategis perusahaan menjadi elemen penting yang harus dilindungi agar tidak disalahgunakan oleh pihak yang tidak berwenang. Dalam konteks ini, keamanan informasi tidak hanya berkaitan dengan perlindungan teknologi, tetapi juga mencakup aspek manajemen, kebijakan, prosedur, serta kesadaran sumber daya manusia.

Keamanan informasi secara umum bertujuan untuk melindungi tiga prinsip utama yang dikenal sebagai CIA *Triad*, yaitu *Confidentiality* (kerahasiaan), *Integrity* (keutuhan), dan *Availability* (ketersediaan). Kerahasiaan memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang, integritas memastikan bahwa informasi tidak diubah secara tidak sah, sedangkan ketersediaan menjamin bahwa informasi dapat diakses saat dibutuhkan oleh pengguna yang berhak.

Dalam praktiknya, organisasi menghadapi berbagai tantangan dalam menjaga keamanan informasi. Serangan siber semakin kompleks dan berkembang seiring dengan kemajuan teknologi. Pelaku kejahatan

siber menggunakan berbagai teknik seperti *malware*, *ransomware*, *phishing*, dan eksploitasi kerentanan sistem untuk mendapatkan akses ilegal ke sistem informasi organisasi.

Selain ancaman eksternal, risiko keamanan informasi juga dapat berasal dari faktor internal seperti kesalahan manusia, kurangnya kontrol keamanan, atau kelemahan dalam pengelolaan sistem informasi. Oleh karena itu, organisasi perlu mengembangkan pendekatan yang sistematis dan terstruktur untuk mengidentifikasi, menganalisis, serta mengelola risiko keamanan informasi secara efektif.

Salah satu pendekatan yang banyak digunakan secara internasional adalah penerapan *system* manajemen keamanan informasi (SMKI) yang mengacu pada standar ISO/IEC 27001. Dalam kerangka SMKI tersebut, manajemen risiko menjadi komponen utama yang membantu organisasi dalam menentukan prioritas pengendalian keamanan informasi berdasarkan tingkat risiko yang dihadapi.

Standar ISO/IEC 27005:2022 hadir sebagai panduan khusus yang menjelaskan proses manajemen risiko keamanan informasi secara komprehensif. Standar ini memberikan kerangka kerja sistematis bagi organisasi untuk mengidentifikasi ancaman, menganalisis kerentanan, mengevaluasi dampak risiko, serta menentukan strategi pengendalian yang tepat.

Dengan demikian, pemahaman terhadap konsep dan implementasi manajemen risiko keamanan informasi menjadi sangat penting bagi organisasi dalam menghadapi tantangan keamanan siber di era digital saat ini.

B. Ancaman dan Dampak Siber Global

Seiring dengan meningkatnya penggunaan teknologi digital dalam berbagai sektor industri, ancaman siber juga mengalami peningkatan yang signifikan baik dari sisi jumlah maupun kompleksitas. Serangan siber tidak lagi hanya menargetkan perusahaan teknologi, tetapi juga berbagai sektor lainnya seperti sektor keuangan, kesehatan, pemerintahan, energi, dan infrastruktur kritis.

Lanskap ancaman siber global menunjukkan eskalasi yang konsisten. Verizon DBIR 2025 melaporkan bahwa *ransomware* hadir dalam 44% *breach* dan meningkat 37% dibanding tahun sebelumnya,

sementara eksploitasi kerentanan sebagai initial *attack* vector juga naik 34%, terutama pada perangkat perimeter dan VPN. IBM melaporkan rata-rata biaya global kebocoran data pada 2025 sebesar USD 4,4 juta, sedangkan *phishing* tetap menjadi vektor *breach* yang paling umum. Di sisi lain, World Economic Forum 2025 menyoroti bahwa 66% organisasi memperkirakan AI akan menjadi faktor paling berpengaruh terhadap keamanan siber, tetapi hanya 37% yang memiliki proses untuk menilai keamanan alat AI sebelum digunakan.

Temuan-temuan tersebut memperlihatkan bahwa ancaman siber modern tidak hanya berasal dari *malware* tradisional, tetapi juga dari kelemahan tata kelola, integrasi pihak ketiga, ketidaksiapan organisasi terhadap AI, dan kompleksitas lingkungan digital yang semakin terhubung. ENISA *Threat* Landscape 2024 menekankan bahwa periode 2023–2024 ditandai eskalasi geopolitik, peningkatan kompleksitas ancaman, dan kebutuhan prioritisasi tindakan mitigasi yang lebih tajam. Karena itu, organisasi memerlukan pendekatan sistematis yang tidak hanya reaktif terhadap insiden, tetapi mampu mengidentifikasi risiko lebih awal, menilai tingkat paparannya, dan menentukan kontrol yang proporsional.

Bedasarkan Jenis ancaman siber global saat ini mencakup berbagai bentuk serangan, antara lain *malware*, *ransomware*, *phishing*, *distributed denial-of-service* (DDoS), *data breach*, serta eksploitasi kerentanan sistem. Serangan *ransomware* misalnya, telah menjadi salah satu ancaman terbesar bagi organisasi di seluruh dunia. Dalam serangan ini, penyerang mengenkripsi data korban dan meminta tebusan agar data tersebut dapat dipulihkan kembali.

Selain itu, serangan *phishing* juga menjadi metode yang sering digunakan oleh penyerang untuk memperoleh kredensial pengguna. Melalui teknik rekayasa sosial, penyerang dapat mengelabui pengguna untuk memberikan informasi sensitif seperti *username*, *password*, atau data finansial.

Dampak dari serangan siber terhadap organisasi dapat sangat signifikan. Dampak tersebut tidak hanya berupa kerugian finansial akibat kehilangan data atau gangguan operasional, tetapi juga dapat merusak reputasi organisasi serta menurunkan kepercayaan pelanggan. Dalam beberapa kasus, kebocoran data juga dapat menyebabkan konsekuensi

hukum dan regulasi bagi organisasi yang tidak mampu melindungi informasi pribadi pengguna.

Selain kerugian finansial langsung, insiden keamanan informasi juga dapat menyebabkan gangguan terhadap keberlangsungan bisnis. Serangan terhadap sistem informasi dapat menghentikan operasional organisasi, mengganggu layanan kepada pelanggan, serta menimbulkan kerugian ekonomi yang besar.

Oleh karena itu, organisasi perlu mengembangkan strategi keamanan informasi yang komprehensif untuk mengantisipasi berbagai ancaman siber yang terus berkembang. Salah satu pendekatan yang efektif adalah dengan menerapkan manajemen risiko keamanan informasi yang terstruktur dan berbasis standar internasional

C. Manfaat Manajemen Risiko Keamanan Informasi (MRKI)

Manajemen risiko merupakan proses sistematis yang digunakan untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang dapat mempengaruhi pencapaian tujuan organisasi. Dalam konteks keamanan informasi, manajemen risiko berfokus pada perlindungan aset informasi dari berbagai ancaman yang dapat menyebabkan kerugian bagi organisasi.

Pendekatan manajemen risiko memungkinkan organisasi untuk memahami secara lebih baik potensi risiko yang dihadapi serta menentukan prioritas pengendalian yang paling efektif. Dengan melakukan analisis risiko, organisasi dapat mengidentifikasi aset informasi yang paling kritis, mengetahui potensi ancaman yang dapat menyerang sistem informasi, serta mengevaluasi tingkat kerentanan yang dimiliki.

Salah satu manfaat utama dari penerapan manajemen risiko keamanan informasi adalah membantu organisasi dalam mengalokasikan sumber daya secara lebih efektif. Tidak semua risiko memiliki tingkat dampak yang sama, sehingga organisasi perlu memprioritaskan pengendalian pada risiko yang memiliki tingkat keparahan tertinggi.

Selain itu, manajemen risiko juga membantu organisasi dalam meningkatkan kesiapsiagaan terhadap insiden keamanan informasi. Dengan memahami potensi risiko yang ada, organisasi dapat merancang

kebijakan keamanan, prosedur mitigasi, serta mekanisme respons insiden yang lebih efektif.

Pendekatan manajemen risiko juga mendukung pengambilan keputusan berbasis data. Manajemen dapat menggunakan hasil analisis risiko sebagai dasar dalam menentukan strategi keamanan informasi yang sesuai dengan kebutuhan organisasi.

Dalam konteks tata kelola teknologi informasi, manajemen risiko keamanan informasi juga menjadi bagian penting dari praktik tatakelola teknologi informasi. Penerapan manajemen risiko yang efektif dapat membantu organisasi dalam meningkatkan ketahanan sistem informasi serta memastikan bahwa keamanan informasi menjadi bagian integral dari strategi bisnis organisasi.

D. Peran ISO/IEC 27005 dalam Kerangka SMKI

ISO/IEC 27005 merupakan standar internasional yang memberikan panduan mengenai manajemen risiko keamanan informasi. Standar ini dirancang untuk mendukung implementasi sistem manajemen keamanan informasi sebagaimana yang ditetapkan dalam ISO/IEC 27001.

ISO/IEC 27005 menyediakan kerangka kerja sistematis yang membantu organisasi dalam mengidentifikasi, menganalisis, dan mengelola risiko keamanan informasi secara terstruktur. Standar ini tidak menetapkan metode perhitungan risiko tertentu, tetapi memberikan fleksibilitas bagi organisasi untuk memilih metode analisis risiko yang sesuai dengan kebutuhan dan karakteristik organisasinya.

Dalam kerangka SMKI, proses manajemen risiko biasanya mencakup beberapa tahapan utama, yaitu penetapan konteks risiko, identifikasi risiko, analisis risiko, evaluasi risiko, serta penanganan risiko. Proses ini dilakukan secara berkelanjutan untuk memastikan bahwa risiko keamanan informasi selalu berada dalam tingkat yang dapat diterima oleh organisasi.

ISO/IEC 27005 juga menekankan pentingnya komunikasi risiko serta pemantauan dan peninjauan risiko secara berkala. Dengan demikian, manajemen risiko keamanan informasi tidak hanya menjadi aktivitas satu kali, tetapi merupakan proses yang berkelanjutan dalam siklus peningkatan berkelanjutan (*continuous improvement*).

Penerapan ISO/IEC 27005 membantu organisasi dalam mengintegrasikan manajemen risiko ke dalam sistem manajemen keamanan informasi secara menyeluruh. Hal ini memungkinkan organisasi untuk meningkatkan efektivitas pengendalian keamanan serta memastikan bahwa risiko keamanan informasi dikelola secara proaktif.

E. Tujuan, Ruang Lingkup dan Metodologi

ISO/IEC 27005 Buku ini disusun dengan tujuan untuk memberikan pemahaman komprehensif mengenai konsep dan implementasi manajemen risiko keamanan informasi berdasarkan standar ISO/IEC 27005:2022. Buku ini diharapkan dapat menjadi referensi bagi akademisi, praktisi keamanan informasi, auditor, serta mahasiswa yang mempelajari bidang keamanan siber dan manajemen risiko.
Secara khusus, buku ini bertujuan untuk:

1. Menjelaskan konsep dasar keamanan informasi dan manajemen risiko.
2. Menguraikan kerangka kerja manajemen risiko keamanan informasi berdasarkan ISO/IEC 27005.
3. Menyajikan metode analisis risiko yang dapat digunakan dalam pengelolaan keamanan informasi.
4. Memberikan contoh penerapan manajemen risiko keamanan informasi dalam organisasi.
5. Menjelaskan hubungan antara ISO/IEC 27005 dengan standar keamanan informasi lainnya seperti ISO/IEC 27001 dan ISO/IEC 27002.

Ruang lingkup pembahasan dalam buku ini mencakup teori dasar keamanan informasi, konsep manajemen risiko, proses *risk assessment*, *risk treatment*, serta implementasi kontrol keamanan informasi dalam organisasi. Selain itu, buku ini juga membahas berbagai metode dan teknik yang dapat digunakan untuk melakukan analisis risiko keamanan informasi.

Metodologi penulisan buku ini menggunakan pendekatan studi literatur dan analisis standar internasional yang relevan dengan manajemen risiko keamanan informasi. Sumber utama yang digunakan dalam penyusunan buku ini adalah standar ISO/IEC 27005:2022, serta

berbagai referensi ilmiah dan publikasi akademik yang membahas keamanan informasi dan manajemen risiko.

Penulisan buku ini mengacu pada standar dan kerangka kerja lain yang berkaitan dengan keamanan informasi, seperti ISO/IEC 27001, ISO/IEC 27002, serta berbagai kerangka kerja manajemen risiko yang digunakan dalam praktik industri. Pendekatan analitis digunakan untuk menjelaskan konsep-konsep utama dalam manajemen risiko keamanan informasi, sedangkan pendekatan deskriptif digunakan untuk menggambarkan proses implementasi standar ISO/IEC 27005 dalam organisasi.

Dalam beberapa bagian, buku ini juga menyajikan contoh kasus dan ilustrasi praktis untuk membantu pembaca memahami penerapan konsep manajemen risiko dalam situasi nyata. Dengan pendekatan tersebut, diharapkan buku ini dapat memberikan pemahaman yang tidak hanya bersifat teoritis tetapi juga aplikatif.

BAB 2
KONSEP DASAR KEAMANAN INFORMASI

A. Definisi Keamanan Informasi

Keamanan informasi merupakan aspek penting dalam pengelolaan sistem informasi modern. Seiring dengan meningkatnya ketergantungan organisasi terhadap teknologi informasi dan komunikasi, perlindungan terhadap informasi menjadi kebutuhan yang sangat krusial. Informasi tidak hanya berfungsi sebagai alat pendukung operasional, tetapi juga menjadi aset strategis yang memiliki nilai ekonomi, hukum, dan reputasi bagi organisasi.

Secara umum, keamanan informasi dapat didefinisikan sebagai upaya melindungi informasi dari akses, penggunaan, pengungkapan, perubahan, atau penghancuran yang tidak sah. Tujuan utama dari keamanan informasi adalah memastikan bahwa informasi tetap terlindungi sepanjang siklus hidupnya, mulai dari proses penciptaan, penyimpanan, pengolahan, transmisi, hingga penghapusan.

Standar internasional ISO/IEC 27000 mendefinisikan keamanan informasi sebagai perlindungan terhadap informasi guna memastikan kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi. Ketiga elemen tersebut dikenal sebagai fondasi utama keamanan informasi dan sering disebut sebagai CIA *Triad*.

Dalam praktiknya, keamanan informasi tidak hanya mencakup perlindungan terhadap data digital, tetapi juga mencakup perlindungan terhadap dokumen fisik, sistem informasi, jaringan komputer, perangkat keras, serta sumber daya manusia yang terlibat dalam pengelolaan

informasi. Oleh karena itu, keamanan informasi harus dipandang sebagai kombinasi antara teknologi, proses, kebijakan organisasi, dan kesadaran pengguna.

Pendekatan keamanan informasi modern juga menekankan pentingnya manajemen risiko. Organisasi diharapkan mampu mengidentifikasi berbagai risiko yang dapat mempengaruhi keamanan informasi serta menentukan langkah mitigasi yang tepat untuk mengurangi potensi kerugian akibat insiden keamanan.

Dengan demikian, keamanan informasi tidak hanya berfungsi sebagai mekanisme perlindungan teknis, tetapi juga merupakan bagian dari tata kelola organisasi yang bertujuan menjaga keberlangsungan bisnis serta melindungi kepentingan berbagai pemangku kepentingan.

B. Prinsip CIA *Triad*

Prinsip CIA *Triad* merupakan model fundamental dalam keamanan informasi yang menjelaskan tiga prinsip utama yang harus dijaga dalam pengelolaan informasi. Model ini digunakan secara luas dalam berbagai standar keamanan informasi, termasuk ISO/IEC 27001 dan ISO/IEC 27005. Konsep CIA *Triad* dapat ditunjukkan pada gambar 2.1 Prinsip CIA *Triad*

Gambar 2. 1: Prinsip CIA *Triad*
Sumber: Diolah Penulis

1. ***Confidentiality* (Kerahasiaan)**
   Confidentiality mengacu pada perlindungan informasi agar hanya dapat diakses oleh pihak yang memiliki otorisasi. Tujuan dari prinsip

ini adalah mencegah pengungkapan informasi kepada pihak yang tidak berhak.

Contoh penerapan *confidentiality* antara lain:

a. Penggunaan sistem autentikasi dan otorisasi
b. Enkripsi data
c. Kontrol akses berbasis peran (*role-based access control*)
d. Kebijakan klasifikasi informasi

Dalam organisasi, informasi sering diklasifikasikan berdasarkan tingkat sensitivitasnya, seperti publik, internal, rahasia, dan sangat rahasia. Pengendalian akses terhadap informasi dilakukan berdasarkan klasifikasi tersebut.

2. *Integrity* (Keutuhan)

Integrity berkaitan dengan menjaga keakuratan dan konsistensi informasi sepanjang siklus hidupnya. Informasi harus terlindungi dari perubahan yang tidak sah baik secara sengaja maupun tidak sengaja.

Pengendalian yang digunakan untuk menjaga integritas informasi meliputi:

a. Penggunaan *hash function*
b. Digital signature
c. Mekanisme kontrol perubahan (*change management*)
d. Sistem *logging* dan audit

Integritas informasi sangat penting terutama dalam sistem yang berkaitan dengan transaksi keuangan, rekam medis, atau data kritis lainnya.

3. *Availability* (Ketersediaan)

Availability memastikan bahwa informasi dan sistem informasi dapat diakses oleh pengguna yang berwenang ketika dibutuhkan. Gangguan terhadap ketersediaan sistem dapat menyebabkan terhentinya operasional organisasi.

Beberapa mekanisme untuk menjaga ketersediaan sistem antara lain:

a. Sistem *backup* dan *recovery*
b. Redundansi sistem

c. *Load balancing*
d. *Disaster recovery plan*

Ketiga prinsip dalam CIA *Triad* saling terkait dan harus dijaga secara seimbang. Terlalu fokus pada salah satu aspek tanpa memperhatikan aspek lainnya dapat menyebabkan ketidakseimbangan dalam sistem keamanan informasi.

C. Prinsip Tambahan Keamanan Informasi

Struktur Selain CIA *Triad*, konsep keamanan informasi modern juga mencakup beberapa prinsip tambahan yang bertujuan memperkuat perlindungan terhadap informasi.

1. *Authenticity*

Authenticity berkaitan dengan kemampuan sistem untuk memastikan bahwa identitas pengguna, perangkat, atau sistem yang berinteraksi dengan sistem informasi adalah benar dan dapat dipercaya.

Teknologi yang digunakan untuk memastikan autentikasi antara lain:

a. *Password*
b. *Multi-factor authentication*
c. Biometrik
d. Sertifikat digital

2. *Accountability*

Accountability mengacu pada kemampuan sistem untuk mencatat dan melacak aktivitas pengguna sehingga setiap tindakan dapat dipertanggungjawabkan.

Penerapan *accountability* biasanya melibatkan:

a. Audit *trail*
b. Sistem *logging*
c. *Monitoring* aktivitas pengguna

Prinsip ini sangat penting dalam investigasi insiden keamanan informasi.

3. Non-repudiation

Non-repudiation memastikan bahwa suatu pihak tidak dapat menyangkal tindakan yang telah dilakukan dalam sistem informasi.

Teknologi yang digunakan untuk mendukung *non-repudiation* meliputi:

a. *Digital signature*
b. *Timestamping*
c. *Cryptographic evidence*

Prinsip ini sering digunakan dalam transaksi elektronik dan sistem keuangan digital.

4. *Reliability*

Reliability berkaitan dengan kemampuan sistem untuk beroperasi secara konsisten dan dapat dipercaya dalam jangka waktu tertentu. Sistem yang reliabel mampu memberikan layanan secara stabil tanpa mengalami gangguan yang signifikan.

Reliability biasanya dicapai melalui:

a. Desain sistem yang robust
b. *Monitoring* performa *system*
c. Pemeliharaan sistem secara berkala

D. Aset Informasi dalam Organisasi

Dalam konteks keamanan informasi, aset merupakan segala sesuatu yang memiliki nilai bagi organisasi dan perlu dilindungi. Aset informasi tidak hanya terbatas pada data digital, tetapi juga mencakup berbagai komponen lain yang mendukung pengelolaan informasi. Aset informasi dapat dikategorikan menjadi beberapa jenis, antara lain:

1. Aset Data

Aset data mencakup seluruh informasi yang disimpan, diproses, atau ditransmisikan oleh organisasi, seperti *database* pelanggan, data transaksi, dokumen bisnis, dan laporan keuangan.

2. Aset Perangkat Keras

Perangkat keras merupakan komponen fisik yang digunakan dalam pengolahan informasi, seperti server, komputer, perangkat jaringan, perangkat penyimpanan

3. Aset Perangkat Lunak

Perangkat lunak mencakup berbagai aplikasi dan sistem operasi yang digunakan untuk mengelola informasi.

4. **Aset Jaringan**
   Aset jaringan meliputi infrastruktur komunikasi yang menghubungkan berbagai sistem informasi dalam organisasi.
5. **Aset Sumber Daya Manusia**
   Sumber daya manusia juga merupakan bagian penting dari aset informasi karena pengguna sistem memiliki akses terhadap informasi organisasi.

Identifikasi aset informasi merupakan langkah penting dalam proses manajemen risiko keamanan informasi. Dengan mengetahui aset yang dimiliki, organisasi dapat menentukan prioritas perlindungan terhadap aset yang paling kritis. Adapun contoh dalam mengklasifikasikan aset informasi dapat ditunjukan pada tabel 2.1.

Tabel 2. 1: Contoh Klasifikasi Aset Informasi

Kategori Aset	Contoh Aset	Nilai bagi Organisasi	Potensi Risiko
Data / Informasi	*Database* pelanggan, laporan keuangan, dokumen kontrak	Sangat tinggi	Kebocoran data, manipulasi informasi
Perangkat Keras	Server, komputer, *router*, *firewall*	Tinggi	Kerusakan perangkat, pencurian
Perangkat Lunak	Sistem ERP, aplikasi web, sistem operasi	Tinggi	Eksploitasi kerentanan *software*
Jaringan	Infrastruktur LAN/WAN, VPN, internet *gateway*	Tinggi	Serangan jaringan, DDoS
Layanan TI	Email server, *cloud service*, *database service*	Tinggi	Gangguan layanan
Sumber Daya Manusia	Administrator sistem, staf IT, pengguna	Sangat tinggi	*Insider threat, human error*
Dokumen Fisik	Arsip kontrak, dokumen hukum	Sedang	Kehilangan dokumen

Sumber: Diolah Penulis

E. Ancaman dan Kerentanan Sistem Informasi

Ancaman keamanan informasi dapat berasal dari berbagai sumber, baik internal maupun eksternal. Ancaman tersebut dapat berupa tindakan yang disengaja maupun kejadian yang tidak disengaja. Beberapa jenis ancaman yang umum terjadi antara lain *malware*, *ransomware*, *phishing*, serangan DDoS, *insider threat*, kegagalan *system*, jenis ancaman global ini dapat ditunjukan pada tabel 2.2

Tabel 2. 2: Jenis Ancaman Serangan Siber

Jenis Ancaman	Deskripsi	Contoh Dampak
Malware	Program berbahaya yang dirancang untuk merusak sistem	Kerusakan data, pencurian informasi
Ransomware	*Malware* yang mengenkripsi data korban dan meminta tebusan	Sistem tidak dapat diakses
Phishing	Teknik rekayasa sosial untuk mencuri kredensial pengguna	Pencurian akun
DDoS *Attack*	Serangan yang membanjiri server dengan trafik	Layanan tidak tersedia
Insider threat	Ancaman dari dalam organisasi	Kebocoran data internal
SQL Injection	Serangan pada aplikasi web melalui *database*	Manipulasi *database*
Man-in-the-Middle Attack	Penyadapan komunikasi antara dua pihak	Pencurian informasi sensitif
Zero-Day Exploit	Eksploitasi kerentanan yang belum diketahui vendor	Kompromi sistem

Sumber: Diolah Penulis

Kerentanan merupakan kelemahan dalam sistem informasi yang dapat dimanfaatkan oleh ancaman untuk menyebabkan kerusakan atau gangguan terhadap sistem. Contoh kerentanan antara lain konfigurasi sistem yang tidak aman, perangkat lunak yang tidak diperbarui, kebijakan keamanan yang lemah, kurangnya pelatihan keamanan bagi pengguna.

Hubungan antara aset, ancaman, dan kerentanan merupakan dasar dalam analisis risiko keamanan informasi, dapat ditunjukan pada gambar 2.2.

Gambar 2. 2: Konsep *Asset–Threat–Vulnerability* (ATV)
Sumber: Diolah Penulis

F. Dampak Insiden Keamanan Informasi

Insiden keamanan informasi dapat menimbulkan berbagai dampak bagi organisasi. Dampak tersebut dapat bersifat finansial, operasional, hukum, maupun reputasional.

1. **Dampak Finansial**
   Kerugian finansial dapat terjadi akibat kehilangan data, gangguan operasional, biaya pemulihan sistem, serta pembayaran denda akibat pelanggaran regulasi.

2. **Dampak Operasional**
   Insiden keamanan dapat menyebabkan gangguan terhadap layanan organisasi, sehingga aktivitas bisnis tidak dapat berjalan dengan normal.
3. **Dampak Hukum**
   Organisasi yang gagal melindungi data pelanggan dapat menghadapi konsekuensi hukum serta sanksi dari regulator.

4. Dampak Reputasi

Reputasi organisasi dapat menurun akibat kebocoran data atau kegagalan dalam menjaga keamanan informasi.

Dalam beberapa kasus, dampak reputasi dapat lebih besar dibandingkan kerugian finansial langsung karena hilangnya kepercayaan pelanggan dapat mempengaruhi keberlangsungan bisnis dalam jangka panjang. Oleh karena itu, organisasi perlu menerapkan strategi keamanan informasi yang komprehensif serta mengintegrasikan manajemen risiko ke dalam sistem manajemen keamanan informasi.

Konsep dasar keamanan informasi merupakan fondasi penting dalam memahami manajemen risiko keamanan informasi. Prinsip CIA *Triad* memberikan kerangka dasar perlindungan informasi, sedangkan prinsip tambahan seperti *authenticity*, *accountability*, *non-repudiation*, dan *reliability* memperkuat sistem keamanan secara menyeluruh.

Identifikasi aset informasi, analisis ancaman, serta pemahaman terhadap kerentanan sistem menjadi langkah awal dalam proses manajemen risiko keamanan informasi. Dengan memahami hubungan antara aset, ancaman, dan kerentanan, organisasi dapat melakukan analisis risiko secara lebih sistematis.

Pembahasan pada bab berikutnya akan menguraikan kerangka kerja standar internasional keamanan informasi serta peran ISO/IEC 27005 dalam mendukung implementasi manajemen risiko keamanan informasi dalam organisasi.

BAB 3
KERANGKA STANDAR INTERNASIONAL KEAMANAN INFORMASI

A. Keluarga Standar ISO/IEC 27000

Seiring dengan meningkatnya ketergantungan organisasi terhadap teknologi informasi, kebutuhan akan standar internasional dalam pengelolaan keamanan informasi menjadi semakin penting. Standar internasional memberikan kerangka kerja yang sistematis bagi organisasi untuk mengelola risiko keamanan informasi secara konsisten dan terstruktur.

Salah satu keluarga standar yang paling banyak digunakan dalam bidang keamanan informasi adalah ISO/IEC 27000 series. Keluarga standar ini dikembangkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC) sebagai panduan global dalam pengelolaan keamanan informasi.

Seri standar ISO/IEC 27000 mencakup berbagai aspek keamanan informasi, mulai dari sistem manajemen keamanan informasi, kontrol keamanan, manajemen risiko, hingga manajemen insiden keamanan.

Tujuan utama dari keluarga standar ini adalah membantu organisasi dalam:

1. Melindungi kerahasiaan informasi
2. Menjaga integritas data
3. Memastikan ketersediaan informasi
4. Mengelola risiko keamanan secara sistematis

BAB 4
KONSEP DASAR MANAJEMEN RISIKO

A. Definisi Risiko

Dalam konteks organisasi modern yang semakin bergantung pada teknologi informasi, risiko merupakan faktor yang tidak dapat dihindari. Setiap aktivitas bisnis, penggunaan teknologi, maupun pengelolaan informasi selalu memiliki potensi ketidakpastian yang dapat mempengaruhi pencapaian tujuan organisasi. Oleh karena itu, pemahaman terhadap konsep risiko menjadi hal yang sangat penting dalam pengelolaan sistem informasi dan keamanan organisasi.

Secara umum, risiko dapat didefinisikan sebagai kemungkinan terjadinya suatu peristiwa yang dapat memberikan dampak terhadap pencapaian tujuan organisasi. Dalam standar ISO 31000, risiko didefinisikan sebagai *effect of uncertainty on objectives*. Definisi ini menekankan bahwa risiko berkaitan dengan ketidakpastian yang dapat mempengaruhi pencapaian tujuan organisasi baik secara positif maupun negatif.

Dalam konteks keamanan informasi, risiko biasanya berkaitan dengan potensi kerugian yang timbul akibat ancaman terhadap aset informasi organisasi. Risiko keamanan informasi muncul ketika suatu ancaman memanfaatkan kerentanan yang terdapat pada sistem informasi sehingga menimbulkan dampak terhadap kerahasiaan, integritas, atau ketersediaan informasi.

Sebagai contoh, sebuah organisasi yang menyimpan data pelanggan dalam sistem *database* memiliki risiko kebocoran data jika

BAB 5
STRUKTUR ISO/IEC 27005:2022

A. Evolusi ISO/IEC 27005

Perkembangan teknologi informasi yang pesat serta meningkatnya kompleksitas ancaman siber mendorong kebutuhan akan pendekatan yang lebih sistematis dalam mengelola risiko keamanan informasi. Salah satu standar internasional yang dikembangkan untuk memenuhi kebutuhan tersebut adalah ISO/IEC 27005, yang secara khusus memberikan panduan mengenai manajemen risiko keamanan informasi.

ISO/IEC 27005 merupakan bagian dari keluarga standar ISO/IEC 27000 series, yang berfokus pada pengelolaan keamanan informasi melalui pendekatan sistem manajemen keamanan informasi (SMKI). Standar ini dirancang untuk mendukung implementasi ISO/IEC 27001 dengan memberikan metodologi yang lebih rinci dalam proses identifikasi, analisis, evaluasi, dan penanganan risiko keamanan informasi.

Sejak pertama kali diperkenalkan, standar ISO/IEC 27005 telah mengalami beberapa kali pembaruan untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan organisasi. Versi pertama standar ini diterbitkan pada tahun 2008, sebagai panduan awal dalam penerapan manajemen risiko keamanan informasi. Versi ini menekankan pentingnya pendekatan berbasis risiko dalam pengelolaan keamanan informasi serta memberikan kerangka dasar untuk proses *risk assessment* dan *risk treatment*.

Pada tahun 2011, standar ini diperbarui untuk meningkatkan keselarasan dengan perkembangan standar keamanan informasi lainnya

BAB 6
KONTEKS MANAJEMEN RISIKO

A. Penetapan Ruang Lingkup Organisasi

Dalam proses manajemen risiko keamanan informasi, langkah pertama yang harus dilakukan oleh organisasi adalah *establishing the context* atau penetapan konteks risiko. Tahap ini merupakan fondasi bagi seluruh proses manajemen risiko karena menentukan ruang lingkup, tujuan, serta pendekatan yang akan digunakan dalam analisis risiko.

Menurut ISO/IEC 27005, *establishing the contex*t bertujuan untuk memastikan bahwa proses manajemen risiko dilakukan sesuai dengan kondisi organisasi, kebutuhan bisnis, serta lingkungan operasional yang dihadapi. Tanpa penetapan konteks yang jelas, proses analisis risiko dapat menjadi tidak relevan atau tidak mencerminkan kondisi sebenarnya dari organisasi.

Penetapan konteks mencakup beberapa aspek penting, antara lain:

1. Konteks organisasi
2. Konteks bisnis
3. Konteks teknologi informasi
4. Konteks regulasi
5. Konteks ancaman keamanan

Konteks organisasi berkaitan dengan karakteristik internal organisasi seperti struktur organisasi, proses bisnis, budaya organisasi, serta kebijakan yang berlaku. Faktor-faktor ini mempengaruhi bagaimana organisasi mengelola risiko keamanan informasi.

Sebagai contoh, organisasi yang bergerak di sektor perbankan biasanya memiliki tingkat regulasi yang lebih ketat dibandingkan organisasi di sektor lain. Oleh karena itu, pendekatan manajemen risiko

BAB 7
IDENTIFIKASI RISIKO KEAMANAN INFORMASI

A. Konsep Identifikasi Risiko

Identifikasi risiko merupakan tahap awal dalam proses *risk assessment* yang bertujuan untuk menemukan dan mendokumentasikan berbagai sumber risiko yang dapat mempengaruhi aset informasi organisasi. Tahap ini sangat penting karena kualitas hasil analisis risiko sangat bergantung pada kemampuan organisasi dalam mengidentifikasi potensi ancaman secara komprehensif.

Dalam konteks keamanan informasi, identifikasi risiko dilakukan dengan memahami hubungan antara aset informasi, ancaman, dan kerentanan yang dapat menyebabkan terjadinya insiden keamanan informasi. Proses ini biasanya dilakukan melalui berbagai teknik seperti *brainstorming*, wawancara dengan pemangku kepentingan, analisis dokumentasi sistem, serta penggunaan basis data ancaman siber global.

Tujuan utama dari identifikasi risiko adalah untuk menghasilkan daftar risiko potensial yang dapat dianalisis lebih lanjut pada tahap berikutnya dalam proses manajemen risiko.

B. Diagram Proses Identifikasi Risiko

Proses identifikasi risiko biasanya dimulai dengan memahami konteks organisasi, kemudian dilanjutkan dengan identifikasi aset, ancaman, dan kerentanan yang terkait dengan sistem informasi organisasi. Tahapan dalam proses identifikasi risiko meliputi:

BAB 8
ANALISIS RISIKO KEAMANAN INFORMASI

A. Metode Analisis Risiko

Analisis risiko merupakan tahap penting dalam proses manajemen risiko keamanan informasi. Setelah risiko diidentifikasi pada tahap sebelumnya, organisasi perlu melakukan analisis untuk memahami tingkat risiko yang dihadapi. Analisis risiko bertujuan untuk menentukan kemungkinan terjadinya suatu risiko serta dampak yang ditimbulkan terhadap organisasi.

Dalam kerangka ISO/IEC 27005, analisis risiko dilakukan untuk menentukan tingkat risiko yang berkaitan dengan setiap skenario risiko yang telah diidentifikasi. Hasil dari proses analisis ini kemudian digunakan untuk menentukan prioritas penanganan risiko pada tahap evaluasi risiko.

Secara umum, terdapat tiga pendekatan utama dalam analisis risiko, yaitu metode kualitatif, kuantitatif, dan semi-kuantitatif.

1. Metode Kualitatif

Metode kualitatif merupakan pendekatan analisis risiko yang menggunakan deskripsi verbal atau kategori tertentu untuk menilai tingkat risiko. Pendekatan ini biasanya menggunakan skala seperti rendah, sedang, dan tinggi untuk menggambarkan kemungkinan terjadinya risiko dan dampak yang ditimbulkan.

Metode kualitatif sering digunakan dalam organisasi karena relatif mudah diterapkan dan tidak memerlukan data numerik yang kompleks. Penilaian biasanya dilakukan melalui diskusi dengan para

BAB 9
EVALUASI RISIKO KEAMANAN INFORMASI

A. Konsep Evaluasi Risiko

Evaluasi risiko merupakan tahap lanjutan setelah proses analisis risiko dalam kerangka manajemen risiko keamanan informasi. Tujuan utama evaluasi risiko adalah menentukan apakah tingkat risiko yang telah dihitung dapat diterima oleh organisasi atau memerlukan tindakan mitigasi lebih lanjut.

Dalam konteks ISO/IEC 27005, evaluasi risiko dilakukan dengan membandingkan tingkat risiko yang dihasilkan dari proses analisis dengan *risk criteria* yang telah ditetapkan sebelumnya. *Risk criteria* biasanya ditentukan berdasarkan kebijakan organisasi, toleransi risiko, serta persyaratan regulasi yang berlaku.

Hasil evaluasi risiko biasanya menghasilkan tiga kemungkinan keputusan, yaitu:

1. Risiko dapat diterima *(risk acceptance)*
2. Risiko harus dikurangi *(risk mitigation)*
3. Risiko harus dihindari *(risk avoidance)*

Proses evaluasi risiko sangat penting karena membantu organisasi dalam menentukan prioritas pengelolaan risiko serta memastikan bahwa sumber daya keamanan informasi digunakan secara efektif.

Risk ranking merupakan proses pengurutan tingkat risiko berdasarkan hasil analisis risiko yang telah dilakukan sebelumnya.

BAB 10
RISK TREATMENT
(PENANGANAN RISIKO)

A. Strategi Penanganan Risiko

Risk treatment merupakan tahap dalam proses manajemen risiko yang bertujuan untuk menentukan tindakan yang diperlukan dalam menangani risiko yang telah dianalisis dan dievaluasi. Pada tahap ini, organisasi memilih strategi yang paling sesuai untuk mengurangi atau mengelola risiko yang dihadapi.

Dalam kerangka ISO/IEC 27005, *risk treatment* melibatkan proses pemilihan dan penerapan kontrol keamanan yang tepat untuk mengurangi kemungkinan terjadinya risiko atau meminimalkan dampaknya terhadap organisasi.

Terdapat beberapa strategi umum dalam penanganan risiko keamanan informasi, yaitu:

1. *Risk mitigation*
2. *Risk avoidance*
3. *Risk transfer*
4. *Risk acceptance*

Pemilihan strategi tersebut bergantung pada tingkat risiko, toleransi risiko organisasi, serta biaya yang diperlukan untuk melakukan mitigasi.

1. Risk Mitigation

BAB 11
IMPLEMENTASI KONTROL KEAMANAN

A. Jenis Kontrol Keamanan

Kontrol keamanan merupakan mekanisme yang dirancang untuk melindungi sistem informasi dari berbagai ancaman keamanan. Dalam kerangka manajemen risiko keamanan informasi, kontrol keamanan diterapkan sebagai bagian dari proses *risk treatment* untuk mengurangi kemungkinan terjadinya risiko maupun dampak yang ditimbulkannya.

Menurut berbagai standar keamanan informasi seperti ISO/IEC 27001 dan ISO/IEC 27002, kontrol keamanan dapat diklasifikasikan ke dalam tiga kategori utama, yaitu *administrative controls, technical controls*, dan *physical controls*. Ketiga jenis kontrol ini saling melengkapi dalam membentuk sistem perlindungan keamanan informasi yang komprehensif.

1. Administrative Controls

Administrative controls merupakan kebijakan, prosedur, dan praktik manajemen yang dirancang untuk mengatur bagaimana sistem keamanan informasi dikelola dalam organisasi. Kontrol ini biasanya berkaitan dengan tata kelola keamanan informasi serta pengelolaan sumber daya manusia.

Administrative controls berfungsi sebagai fondasi dalam implementasi keamanan informasi karena mengatur perilaku pengguna serta prosedur operasional organisasi.

Contoh administrative *control*s antara lain:

a. Kebijakan keamanan informasi

BAB 12
KOMUNIKASI DAN KONSULTASI RISIKO

A. Komunikasi Risiko kepada *Stakeholder*

Komunikasi risiko merupakan salah satu elemen penting dalam proses manajemen risiko keamanan informasi. Dalam kerangka ISO/IEC 27005, komunikasi risiko bertujuan untuk memastikan bahwa informasi mengenai risiko keamanan informasi dapat dipahami oleh seluruh pemangku kepentingan yang terkait dengan pengelolaan sistem informasi organisasi.

Proses komunikasi risiko melibatkan pertukaran informasi antara berbagai pihak yang memiliki kepentingan terhadap keamanan informasi, seperti manajemen organisasi, tim teknologi informasi, auditor, regulator, serta pengguna sistem. Komunikasi yang efektif memungkinkan organisasi untuk meningkatkan kesadaran terhadap risiko serta memastikan bahwa keputusan yang diambil dalam pengelolaan risiko didasarkan pada informasi yang akurat.

Komunikasi risiko tidak hanya dilakukan setelah proses analisis risiko selesai, tetapi juga dilakukan sepanjang siklus manajemen risiko. Informasi mengenai risiko harus dikomunikasikan secara transparan agar seluruh pihak yang terlibat dapat memahami tingkat risiko yang dihadapi serta langkah-langkah yang diperlukan untuk mengurangi risiko tersebut.

1. Tujuan Komunikasi Risiko

Beberapa tujuan utama komunikasi risiko dalam organisasi antara lain:

BAB 13
RISK MONITORING DAN *REVIEW*

A. *Monitoring* Risiko

Monitoring risiko merupakan proses pemantauan berkelanjutan terhadap kondisi risiko keamanan informasi dalam organisasi. Dalam kerangka manajemen risiko keamanan informasi, *monitoring* bertujuan untuk memastikan bahwa risiko yang telah diidentifikasi dan dianalisis tetap berada dalam batas toleransi yang telah ditetapkan oleh organisasi.

Lingkungan teknologi informasi dan ancaman siber terus berkembang dengan sangat cepat. Oleh karena itu, risiko keamanan informasi tidak bersifat statis, melainkan dapat berubah seiring waktu. *Monitoring* risiko memungkinkan organisasi untuk mendeteksi perubahan kondisi risiko secara dini sehingga tindakan mitigasi dapat segera dilakukan.

Dalam standar ISO/IEC 27005, *monitoring* risiko merupakan bagian penting dari siklus manajemen risiko yang berkelanjutan. Proses *monitoring* memastikan bahwa kontrol keamanan yang telah diterapkan tetap efektif dalam melindungi aset informasi organisasi.

1. Tujuan *Monitoring* Risiko

Monitoring risiko memiliki beberapa tujuan utama, antara lain:

a. Memastikan bahwa kontrol keamanan berfungsi secara efektif
b. Mendeteksi perubahan kondisi risiko dalam organisasi
c. Mengidentifikasi ancaman baru yang muncul
d. Memastikan kepatuhan terhadap kebijakan keamanan informasi

BAB 14
STUDI KASUS MANAJEMEN RISIKO KEAMANAN INFORMASI

A. Studi Kasus Organisasi Pemerintah

Organisasi pemerintah memiliki tanggung jawab besar dalam melindungi informasi publik serta data sensitif masyarakat. Sistem informasi yang digunakan oleh instansi pemerintah biasanya mencakup layanan administrasi publik, sistem pengelolaan data kependudukan, serta sistem layanan digital pemerintahan.

Dalam beberapa tahun terakhir, sektor pemerintahan menjadi salah satu target utama serangan siber. Hal ini disebabkan oleh tingginya nilai informasi yang dimiliki oleh instansi pemerintah, seperti data identitas penduduk, informasi keuangan negara, serta dokumen kebijakan strategis.

Studi kasus ini menggambarkan penerapan manajemen risiko keamanan informasi pada sebuah instansi pemerintah yang mengelola sistem layanan administrasi kependudukan berbasis web.

1. Asset Inventory

Langkah pertama dalam manajemen risiko adalah mengidentifikasi aset informasi yang dimiliki organisasi.

BAB 15
TOOLS DAN TEKNIK ANALISIS RISIKO

A. *Risk assessment Tools*

Risk assessment tools merupakan perangkat atau metode yang digunakan untuk membantu organisasi dalam melakukan proses analisis risiko keamanan informasi secara sistematis. *Tools* ini membantu organisasi dalam mengidentifikasi aset informasi, menganalisis ancaman, menilai kerentanan sistem, serta menentukan tingkat risiko yang dihadapi.

Dalam praktik manajemen risiko keamanan informasi, penggunaan tools analisis risiko sangat penting karena organisasi modern memiliki infrastruktur teknologi informasi yang kompleks. Tanpa dukungan alat analisis yang memadai, proses identifikasi dan evaluasi risiko akan menjadi sulit dilakukan secara efektif.

Risk assessment tools biasanya digunakan untuk mendukung beberapa tahapan utama dalam manajemen risiko, yaitu:

1. Identifikasi aset informasi
2. Identifikasi ancaman dan kerentanan
3. Analisis tingkat risiko
4. Penyusunan *risk register*

Risk assessment tools dapat diklasifikasikan ke dalam beberapa kategori utama, antara lain:

BAB 16
TREN RISIKO SIBER MODERN: MASA DEPAN MANAJEMEN RISIKO KEAMANAN INFORMASI

Perkembangan teknologi digital telah mengubah lanskap keamanan informasi secara signifikan. Transformasi digital yang melibatkan teknologi seperti *Artificial Intelligence* (AI), *cloud computing*, *Internet of Things* (IoT), serta integrasi rantai pasok digital telah menciptakan peluang baru bagi organisasi untuk meningkatkan efisiensi operasional. Namun demikian, teknologi tersebut juga menghadirkan tantangan baru dalam pengelolaan risiko keamanan informasi.

Ancaman siber modern menjadi semakin kompleks dan terorganisir. Penyerang tidak lagi hanya memanfaatkan kerentanan teknis, tetapi juga menggunakan teknik rekayasa sosial, eksploitasi sistem *cloud*, serta serangan terhadap rantai pasok digital. Oleh karena itu, organisasi perlu mengembangkan pendekatan manajemen risiko keamanan informasi yang adaptif dan proaktif.

Bab ini membahas beberapa tren utama risiko siber modern yang berpotensi mempengaruhi masa depan pengelolaan keamanan informasi, yaitu risiko yang berkaitan dengan AI, *cloud computing*, IoT, serta *supply chain cyber risk*.

BAB 17
KESIMPULAN DAN REKOMENDASI

Manajemen risiko keamanan informasi merupakan komponen fundamental dalam melindungi aset informasi organisasi dari berbagai ancaman siber yang terus berkembang. Seiring dengan meningkatnya ketergantungan organisasi terhadap teknologi informasi, pengelolaan risiko keamanan informasi menjadi semakin penting untuk memastikan keberlangsungan operasional organisasi serta menjaga kepercayaan *stakeholder*.

Standar ISO/IEC 27005 memberikan kerangka kerja yang sistematis dalam mengidentifikasi, menganalisis, mengevaluasi, dan mengelola risiko keamanan informasi. Melalui pendekatan berbasis risiko ini, organisasi dapat memahami berbagai ancaman yang dihadapi serta menentukan strategi mitigasi yang tepat.

Bab ini menyajikan kesimpulan dari konsep-konsep utama yang telah dibahas dalam buku ini serta memberikan rekomendasi bagi organisasi dalam mengimplementasikan manajemen risiko keamanan informasi secara efektif.

A. Ringkasan Konsep Utama

Buku ini membahas berbagai konsep dan praktik dalam manajemen risiko keamanan informasi yang mengacu pada standar internasional ISO/IEC 27005. Konsep utama yang dibahas mencakup prinsip dasar keamanan informasi, kerangka kerja manajemen risiko, serta penerapan kontrol keamanan dalam organisasi.

LAMPIRAN

Lampiran berikut berisi template praktis yang dapat digunakan langsung oleh organisasi dalam implementasi manajemen risiko keamanan informasi berbasis ISO/IEC 27005. Template ini mencakup *Risk Register*, *Risk assessment* Worksheet, *Risk Matrix*, Mapping Risiko ke kontrol ISO 27002, *Risk treatment* Plan, *Risk* Heatmap, Statement of Applicability, serta Audit *Checklist* ISO/IEC 27001.

LAMPIRAN A — Template *Risk Register* ISO/IEC 27005

Risk Register merupakan dokumen utama dalam manajemen risiko keamanan informasi yang berfungsi untuk mencatat seluruh risiko yang telah diidentifikasi, dianalisis, serta dievaluasi oleh organisasi. Dokumen ini membantu organisasi dalam memonitor perkembangan risiko serta memastikan bahwa tindakan mitigasi dilakukan secara sistematis. *Risk Register* biasanya mencakup informasi mengenai aset informasi, ancaman, kerentanan, tingkat risiko, serta rencana mitigasi risiko.

Tabel L.A.1 Template *Risk Register*

No	*Asset*	*Threat*	*Vulnerability*	L × I = Score	*Risk* Level	*Control*	*Risk* Owner
1	*Database* pelanggan	Data *breach*	Weak access *control*	5 × 5 = 25	Critical	*Encryption*	IT *Security*
2	Web server	SQL injection	Input validation lemah	4 × 5 = 20	Critical	WAF	DevOps
3	Email server	*Phishing*	Kurang *awareness*	4 × 3 = 12	High	Training	HR

Risk Register harus diperbarui secara berkala untuk mencerminkan perubahan kondisi risiko dalam organisasi. Dalam Lampiran F disajikan contoh *Risk Register* lengkap dengan 20 baris risiko yang berbeda.

LAMPIRAN B — Contoh *Risk assessment Worksheet*

Risk assessment Worksheet digunakan untuk mendokumentasi-kan proses analisis risiko secara lebih rinci. *Worksheet* ini biasanya digunakan oleh tim keamanan informasi dalam melakukan penilaian risiko terhadap aset informasi organisasi.

Tabel L.B.1 *Risk assessment Worksheet*

Asset	***Asset* Value**	***Threat***	***Vulnerability***	***Likelihood***	***Impact***	***Risk* Score**
Database pelanggan	5	Data theft	Weak *encryption*	4	5	20
Web portal	4	SQL injection	Poor input validation	4	5	20
Laptop pegawai	3	*Malware*	No endpoint *security*	3	3	9

Risk Score biasanya dihitung menggunakan rumus :

Risk Score = Likelihood × Impact.

Worksheet ini membantu organisasi dalam melakukan analisis risiko secara sistematis.

LAMPIRAN C — Contoh *Risk Matrix*

Risk Matrix merupakan alat visual yang digunakan untuk mengklasifikasikan tingkat risiko berdasarkan kombinasi antara kemungkinan terjadinya ancaman *(likelihood)* dan dampak yang ditimbulkan *(impact).*

Tabel L.C.1 *Risk Matrix* (5×5)

Impact / Likelihood	**1**	**2**	**3**	**4**	**5**
5	*Medium*	*High*	*High*	*Critical*	*Critical*
4	*Medium*	*Medium*	*High*	*High*	*Critical*
3	*Low*	*Medium*	*Medium*	*High*	*High*
2	*Low*	*Low*	*Medium*	*Medium*	*High*

1	*Low*	*Low*	*Low*	*Medium*	*Medium*

Tabel L.C.2 Kategori Risiko

Risk Score	***Risk Level***
1–4	*Low*
5–9	*Medium*
10–16	*High*
17–25	*Critical*

Risk Matrix membantu organisasi dalam menentukan prioritas penanganan risiko.

LAMPIRAN D — *Mapping* Risiko ke ISO/IEC 27002:2022 *Controls*

Standar ISO/IEC 27002:2022 menyediakan panduan implementasi kontrol keamanan yang dapat digunakan organisasi untuk mengurangi risiko keamanan informasi. Mapping risiko ke kontrol ISO 27002 membantu organisasi dalam menentukan kontrol keamanan yang sesuai untuk mengurangi risiko yang dihadapi.

Tabel L.D.1 Contoh Mapping Risiko ke Kontrol ISO 27002

Risiko	**Kontrol ISO 27002**	**Deskripsi Kontrol**
Data *breach*	Access *control*	Pengaturan hak akses pengguna
Malware	Protection against *malware*	Implementasi antivirus
Phishing	*Security awareness*	Pelatihan keamanan pengguna
Data loss	*Backup*	Pencadangan data secara berkala
Unauthorized access	Secure authentication	Implementasi MFA

Mapping ini biasanya digunakan dalam penyusunan dokumen *Statement of Applicability (SoA)* dalam implementasi ISO/IEC 27001.

LAMPIRAN E — Contoh *Risk treatment Plan*

Risk treatment Plan merupakan dokumen yang menjelaskan tindakan mitigasi risiko yang akan dilakukan oleh organisasi. Dokumen ini disusun setelah proses evaluasi risiko selesai dilakukan.

Risk treatment Plan biasanya mencakup informasi mengenai risiko yang harus ditangani, kontrol keamanan yang akan diterapkan, serta jadwal implementasi.

Tabel L.E.1 Template *Risk treatment Plan*

No	Risiko	*Risk* Level	Kontrol Keamanan	Penanggung Jawab	Target Waktu
1	Data *breach database*	Critical	Enkripsi *database*	IT *Security*	3 bulan
2	SQL injection	Critical	Web Application *Firewall*	DevOps	2 bulan
3	*Phishing attack*	High	*Security awareness* training	HR	1 bulan
4	*Malware* infection	Medium	Endpoint protection	IT Operations	2 bulan

Risk treatment Plan membantu organisasi dalam memastikan bahwa mitigasi risiko dilakukan secara terstruktur dan terkoordinasi.

LAMPIRAN F — Contoh *Risk Register*

Risk Register berikut digunakan untuk mencatat seluruh risiko keamanan informasi yang diidentifikasi dalam sebuah organisasi beserta tindakan mitigasinya. Tabel ini merupakan contoh praktis penerapan template *Risk Register* pada Lampiran A. Untuk keterbacaan, *register* disajikan dalam dua tabel yang saling melengkapi dan dihubungkan oleh kolom Nomor risiko.

Tabel L.F.1 *Risk Register* — Identifikasi & Penilaian Risiko

No	*Asset*	*Threat*	*Vulnerability*	L×I=Score	Level
1	*Database* pelanggan	Data *breach*	Weak access *control*	5×5=25	Critical
2	Web server	SQL injection	Input validation lemah	4×5=20	Critical
3	Email server	*Phishing*	Kurang *awareness*	4×3=12	High
4	Laptop karyawan	*Malware*	Antivirus tidak update	3×3=9	Medium
5	*Cloud* storage	Data leakage	Misconfiguration	4×5=20	Critical
6	VPN *gateway*	Brute force	*Password* lemah	3×4=12	High
7	Source code repo	*Insider threat*	Privilege tinggi	3×4=12	High
8	*Backup* server	Data loss	*Backup* tidak dienkripsi	3×4=12	High
9	Network infra	DDoS	*Firewall* tidak optimal	4×4=16	High
10	*Database* HR	Data theft	Weak authentication	3×5=15	High
11	IoT device	Botnet	Firmware lama	3×3=9	Medium
12	ERP *system*	*Unauthorized access*	IAM lemah	3×4=12	High
13	Mobile app	Credential theft	Enkripsi lemah	4×4=16	High
14	Data center	Physical intrusion	Akses fisik lemah	2×5=10	High
15	Email *system*	Spam *attack*	Filtering lemah	3×3=9	Medium
16	Web API	API abuse	No rate limiting	4×4=16	High
17	Payment *system*	Fraud	Validasi transaksi lemah	4×5=20	Critical
18	Network router	Config *attack*	Default credential	3×4=12	High

19	File server	Data loss	*Backup* gagal	2×4=8	Medium
20	SaaS app	Account takeover	*Password* policy lemah	3×4=12	High

Tabel L.F.2 *Risk Register* — Penanganan Risiko

No	***Asset***	***Control***	***Risk* Owner**
1	*Database* pelanggan	*Encryption*	IT *Security*
2	Web server	WAF	DevOps
3	Email server	Training	HR
4	Laptop karyawan	Endpoint *security*	IT
5	*Cloud* storage	Access *control*	*Cloud* Admin
6	VPN *gateway*	MFA	Network Team
7	Source code repo	Role-*based* access *control*	DevOps
8	*Backup* server	*Encryption*	IT *Security*
9	Network infra	Network *monitoring*	Network Team
10	*Database* HR	MFA	IT *Security*
11	IoT device	Firmware update	IT
12	ERP *system*	Identity & Access Mgmt	IT *Security*
13	Mobile app	Secure authentication	DevOps
14	Data center	CCTV *monitoring*	Facilities
15	Email *system*	Email *security gateway*	IT
16	Web API	API *gateway*	DevOps
17	Payment *system*	Fraud detection	Finance IT
18	Network router	Hardening	Network Admin
19	File server	*Backup monitoring*	IT
20	SaaS app	MFA	*Security* Team

LAMPIRAN G — *Risk Heatmap* Organisasi

Risk Heatmap digunakan untuk memvisualisasikan tingkat risiko organisasi berdasarkan kombinasi *Likelihood* dan *Impact*. Visualisasi ini membantu manajemen memahami prioritas risiko secara cepat.

Tabel L.G.1 *Risk Heatmap*

Impact / Likelihood	**1**	**2**	**3**	**4**	**5**
5	Medium	High	High	Critical	Critical
4	Medium	Medium	High	High	Critical
3	Low	Medium	Medium	High	High
2	Low	Low	Medium	Medium	High
1	Low	Low	Low	Medium	Medium

Tabel L.G.2 *Interpretasi Heatmap*

Warna Risiko	**Kategori**
Hijau	*Low Risk*
Kuning	*Medium Risk*
Oranye	*High Risk*
Merah	*Critical Risk*

Heatmap membantu manajemen memahami prioritas risiko organisasi secara visual.

LAMPIRAN H — *Template Statement of Applicability (SoA)*

Statement of Applicability (SoA) merupakan dokumen penting dalam implementasi ISO/IEC 27001 yang mencantumkan kontrol keamanan yang dipilih berdasarkan hasil *risk assessment*.

Tabel L.H.1 Template *SoA*

***Control* ID**	***Control* Name**	**Applicable**	**Justification**	**Implementation Status**
A.5.1	Information *security* policy	Yes	Mendukung kebijakan keamanan	Implemented

A.5.15	Access *control*	Yes	Mengurangi *Unauthorized access*	Implemented
A.6.3	*Security awareness* training	Yes	Mengurangi *phishing risk*	Implemented
A.7.4	Physical *security monitoring*	Yes	Melindungi data center	Planned
A.8.5	Secure authentication	Yes	Mengurangi account takeover	Implemented
A.8.7	Protection against *malware*	Yes	Mengurangi *malware* infection	Implemented
A.8.13	*Backup*	Yes	Mencegah data loss	Implemented
A.8.24	Cryptography	Yes	Perlindungan data sensitif	Planned

SoA menjadi dokumen utama yang diperiksa auditor dalam sertifikasi ISO/IEC 27001.

LAMPIRAN I — *Template Audit Checklist ISO/IEC 27001*

Audit *checklist* ISO/IEC 27001 merupakan alat bantu untuk melakukan internal audit terhadap implementasi Sistem Manajemen Keamanan Informasi (SMKI). *Checklist* ini membantu organisasi mengevaluasi tingkat kepatuhan terhadap persyaratan standar ISO/IEC 27001:2022.

Tabel L.I.1 Template *Audit Checklist ISO/IEC 27001*

Klausul	Persyaratan	Status	Bukti / Catatan
4.1	Konteks organisasi terkait keamanan informasi telah diidentifikasi	Compliant	Dokumen Konteks Organisasi

4.2	Pihak berkepentingan (*stakeholder*s) telah diidentifikasi	Compliant	*Stakeholder Register*
4.3	Ruang lingkup SMKI telah ditetapkan	Compliant	*Scope* Statement
5.1	Komitmen kepemimpinan terhadap SMKI dapat dibuktikan	Compliant	Risalah rapat manajemen
5.2	Kebijakan keamanan informasi telah ditetapkan dan dikomunikasikan	Compliant	Information *Security* Policy
5.3	Peran, tanggung jawab, dan otoritas telah ditetapkan	Compliant	RACI *Matrix*
6.1	*Risk assessment* dilakukan secara berkala	Compliant	*Risk assessment* Report
6.2	Tujuan keamanan informasi telah ditetapkan	Compliant	Information *Security* Objectives
7.2	Kompetensi personel keamanan informasi terdokumentasi	Partial	Training Record
7.3	*Awareness* program keamanan informasi telah dilaksanakan	Compliant	*Awareness* Training Log
8.1	Operasi pengelolaan risiko keamanan terkendali	Compliant	*Risk treatment* Plan
8.2	*Risk assessment* dilakukan pada interval terencana	Compliant	*Risk Register* Update

9.1	*Monitoring* dan pengukuran keamanan informasi dilakukan	Compliant	KPI Dashboard
9.2	Internal audit SMKI dilaksanakan secara berkala	Compliant	Internal Audit Report
9.3	Tinjauan manajemen SMKI dilakukan secara berkala	Partial	*Management* Review Minutes
10.1	Continual improvement diterapkan dalam SMKI	Compliant	Improvement Plan
10.2	Ketidaksesuaian dan tindakan korektif dikelola	Compliant	CAPA Log

Hasil audit *checklist* menjadi dasar dalam menentukan area perbaikan SMKI dan persiapan sertifikasi ISO/IEC 27001.

DAFTAR PUSTAKA

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

Badan Siber dan Sandi Negara. (2021). Pedoman Manajemen Risiko Keamanan Siber. BSSN.

BSI Group. (2015). ISO/IEC 27017:2015 Information technology — *Security* techniques — Code of practice for information *security control*s *based* on ISO/IEC 27002 for *cloud service*s. International Organization for Standardization.

BSI Group. (2018). ISO 31000:2018 *Risk management* — Guidelines. International Organization for Standardization.

BSI Group. (2018). ISO/IEC 27000:2018 Information technology — *Security* techniques — Information *security management system*s — *Overview* and vocabulary. International Organization for Standardization.

BSI Group. (2019). ISO/IEC 27018:2019 Information technology — *Security* techniques — Code of practice for protection of personally identifiable information (PII) in public *cloud*s. International Organization for Standardization.

BSI Group. (2022). ISO/IEC 27001:2022 Information *security*, cyber*security* and privacy protection — Information *security management system*s — Requirements. International Organization for Standardization.

BSI Group. (2022). ISO/IEC 27002:2022 Information *security*, cyber*security* and privacy protection — Information *security control*s. International Organization for Standardization.

BSI Group. (2022). ISO/IEC 27005:2022 Information *security*, cyber*security* and privacy protection — Guidance on managing information *security risk*s. International Organization for Standardization.

BSI Group. (2023). ISO/IEC 27035-1:2023 Information technology — Information *security* incident *management* — Part 1: Principles and process. International Organization for Standardization.

Calder, A., & Watkins, S. (2019). IT *Governance*: An International Guide to Data *Security* and ISO 27001/ISO 27002 (7th ed.). Kogan Page.

ENISA. (2022). *Threat* Landscape Report. European Union Agency for Cyber*security*.

ISACA. (2019). COBIT 2019 Framework: *Governance* and *Management* Objectives. ISACA.

NIST. (2012). NIST Special Publication 800-30 Rev. 1: Guide for Conducting *Risk assessment*s. National Institute of Standards and Technology.

NIST. (2018). Framework for Improving Critical Infrastructure Cyber*security*, Version 1.1. National Institute of Standards and Technology.

NIST. (2020). NIST Special Publication 800-37 Rev. 2: *Risk Management* Framework for Information *System*s and Organizations. National Institute of Standards and Technology.

NIST. (2024). Post-Quantum Cryptography Standardization. National Institute of Standards and Technology.

Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

World Economic Forum. (2024). Global Cyber*security* Outlook 2024. WEF.

GLOSARIUM

A

Access Control

Mekanisme pengamanan yang digunakan untuk mengatur dan membatasi akses pengguna terhadap sistem, aplikasi, atau data berdasarkan hak akses yang dimiliki.

Annual Loss Expectancy (ALE)

Estimasi total kerugian finansial tahunan yang dapat terjadi akibat suatu risiko, dihitung dengan rumus ALE = SLE × ARO.

Annual Rate of Occurrence (ARO)

Frekuensi rata-rata terjadinya suatu insiden keamanan dalam satu tahun.

Artificial Intelligence (AI)

Teknologi yang memungkinkan sistem komputer untuk meniru kemampuan kognitif manusia seperti pembelajaran, analisis data, dan pengambilan keputusan.

Asset (Aset Informasi)

Segala sesuatu yang memiliki nilai bagi organisasi dan perlu dilindungi, seperti data, perangkat keras, perangkat lunak, jaringan, serta sumber daya manusia.

Attack Surface

Keseluruhan titik atau area dalam sistem informasi yang dapat menjadi target serangan oleh pihak yang tidak berwenang.

Audit

Proses pemeriksaan sistematis dan independen untuk mengevaluasi efektivitas penerapan sistem manajemen keamanan informasi.

Availability (Ketersediaan)

Prinsip keamanan informasi yang memastikan bahwa sistem dan data dapat diakses oleh pengguna yang berwenang ketika dibutuhkan.

B

Backup

Salinan data atau sistem yang dibuat untuk pemulihan jika terjadi kehilangan atau kerusakan data.

Brainstorming

Teknik diskusi kelompok yang digunakan untuk mengidentifikasi berbagai potensi risiko keamanan informasi.

Brute Force Attack

Serangan yang dilakukan dengan mencoba berbagai kombinasi kata sandi secara otomatis hingga ditemukan kombinasi yang benar.

C

CIA Triad

Model dasar keamanan informasi yang terdiri dari tiga prinsip utama: Confidentiality, Integrity, dan Availability.

Cloud Computing

Model penyediaan layanan komputasi melalui internet, mencakup penyimpanan, server, basis data, dan perangkat lunak.

Common Vulnerability Scoring System (CVSS)

Standar yang digunakan untuk menilai tingkat keparahan kerentanan keamanan pada sistem informasi.

Confidentiality (Kerahasiaan)

Prinsip keamanan informasi yang memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang.

Control (Pengendalian)

Langkah atau mekanisme yang diterapkan untuk mengurangi risiko keamanan informasi, dapat berupa kebijakan, prosedur, maupun teknologi.

Cybersecurity

Upaya perlindungan sistem komputer, jaringan, dan data dari serangan digital atau ancaman siber.

D

Data Breach

Insiden keamanan yang mengakibatkan informasi sensitif diakses, dicuri, atau diungkapkan tanpa izin.

Detective Control

Jenis pengendalian keamanan yang berfungsi untuk mendeteksi terjadinya insiden, contohnya intrusion detection system.

DDoS Attack (Distributed Denial of Service)

Serangan yang membanjiri server atau jaringan dengan trafik berlebih sehingga layanan tidak dapat diakses oleh pengguna sah.

E

Encryption (Enkripsi)

Proses mengubah informasi menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai.

Exploit

Teknik atau kode yang digunakan oleh penyerang untuk memanfaatkan kerentanan dalam sistem.

F

Firewall

Sistem keamanan jaringan yang digunakan untuk memantau dan mengontrol lalu lintas jaringan berdasarkan aturan keamanan tertentu.

H

Hash Function

Fungsi matematika yang mengubah data menjadi nilai tetap (hash) yang digunakan untuk verifikasi integritas data.

I

Identity and Access Management (IAM)

Kerangka kerja kebijakan dan teknologi untuk mengelola identitas digital dan hak akses pengguna terhadap sistem.

Impact (Dampak)

Tingkat kerugian atau gangguan yang ditimbulkan oleh terjadinya suatu insiden keamanan informasi.

Incident Response

Proses terstruktur untuk menangani dan memitigasi insiden keamanan informasi dengan tujuan mengurangi dampak.

Information Security

Perlindungan informasi dari akses tidak sah, perubahan, gangguan, atau kerusakan untuk menjamin kerahasiaan, integritas, dan ketersediaannya.

Information Security Management System (ISMS)

Kerangka kerja manajemen yang digunakan organisasi untuk mengelola keamanan informasi secara sistematis sesuai ISO/IEC 27001.

Insider threat

Ancaman keamanan yang berasal dari individu di dalam organisasi yang memiliki akses sah ke sistem.

Integrity (Integritas)
Prinsip keamanan informasi yang memastikan bahwa data tidak diubah atau dimodifikasi tanpa izin.
Internet of Things (IoT)
Jaringan perangkat fisik yang terhubung ke internet dan dapat saling berkomunikasi serta bertukar data.
ISO/IEC 27001
Standar internasional yang menetapkan persyaratan untuk membangun, menerapkan, memelihara, dan meningkatkan ISMS.
ISO/IEC 27002
Standar internasional yang menyediakan panduan implementasi kontrol keamanan informasi.
ISO/IEC 27005
Standar internasional yang menyediakan panduan manajemen risiko keamanan informasi sebagai pelengkap ISO/IEC 27001.
ISO 31000
Standar internasional kerangka kerja umum manajemen risiko yang dapat diterapkan pada berbagai jenis risiko organisasi.

L
Likelihood (Kemungkinan)
Ukuran kemungkinan terjadinya suatu ancaman atau insiden keamanan dalam periode waktu tertentu.

M
Malware
Perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem komputer.
Multi-Factor Authentication (MFA)
Mekanisme autentikasi yang memerlukan lebih dari satu faktor verifikasi sebelum memberikan akses ke sistem.

N
NIST Cybersecurity Framework
Kerangka kerja keamanan siber yang dikembangkan oleh National Institute of Standards and Technology Amerika Serikat.

P

Penetration Testing

Metode pengujian keamanan yang mensimulasikan serangan terhadap sistem untuk mengidentifikasi kerentanan.

Phishing

Teknik penipuan yang digunakan untuk memperoleh informasi sensitif seperti password atau data keuangan dengan menyamar sebagai entitas terpercaya.

Preventive Control

Jenis pengendalian keamanan yang berfungsi mencegah terjadinya insiden, contohnya firewall dan autentikasi.

Q

Quantum Computing

Paradigma komputasi yang memanfaatkan prinsip mekanika kuantum, berpotensi mengubah keamanan kriptografi konvensional.

R

Ransomware

Jenis malware yang mengenkripsi data korban dan meminta tebusan untuk mengembalikan akses data.

Risk (Risiko)

Kombinasi antara kemungkinan terjadinya suatu ancaman dan dampak yang ditimbulkannya terhadap organisasi.

Risk Acceptance

Keputusan organisasi untuk menerima suatu risiko tanpa melakukan tindakan mitigasi tambahan.

Risk Analysis

Proses analisis untuk menentukan tingkat kemungkinan dan dampak dari suatu risiko keamanan informasi.

Risk assessment

Proses menyeluruh yang mencakup identifikasi, analisis, dan evaluasi risiko keamanan informasi.

Risk Avoidance

Strategi penanganan risiko dengan menghilangkan aktivitas atau aset yang menjadi sumber risiko.

Risk Criteria
Kriteria yang digunakan organisasi untuk menilai signifikansi suatu risiko serta menentukan keputusan penerimaan atau mitigasi.
Risk Evaluation
Proses membandingkan tingkat risiko hasil analisis dengan risk criteria untuk menentukan tindakan yang diperlukan.
Risk Heatmap
Visualisasi grafis tingkat risiko organisasi berdasarkan kombinasi likelihood dan impact.
Risk Identification
Tahap awal manajemen risiko untuk menemukan dan mendokumentasikan sumber-sumber risiko keamanan informasi.
Risk Matrix
Tabel yang menggambarkan tingkat risiko sebagai kombinasi nilai likelihood dan impact.
Risk Mitigation
Strategi penanganan risiko dengan menerapkan kontrol untuk mengurangi tingkat risiko sampai batas yang dapat diterima.
Risk Owner
Pihak yang ditunjuk untuk bertanggung jawab dalam mengelola dan memantau suatu risiko tertentu.
Risk Register
Dokumen yang mencatat seluruh risiko yang diidentifikasi dalam organisasi beserta tingkat risiko dan tindakan mitigasinya.
Risk Score
Nilai numerik yang menggambarkan tingkat risiko, biasanya dihitung dari Likelihood × Impact.
Risk Transfer
Strategi penanganan risiko dengan memindahkan tanggung jawab risiko kepada pihak ketiga seperti penyedia asuransi.
Risk treatment
Langkah-langkah yang diambil untuk mengurangi, menghindari, mentransfer, atau menerima risiko keamanan informasi.

S

Security Awareness

Tingkat kesadaran pengguna terhadap praktik keamanan informasi yang baik dalam organisasi.

Security Control

Langkah atau mekanisme yang diterapkan untuk melindungi sistem informasi dari ancaman keamanan.

Security Incident

Peristiwa yang dapat mengganggu kerahasiaan, integritas, atau ketersediaan sistem informasi.

Single Loss Expectancy (SLE)

Estimasi kerugian finansial dari satu kali terjadinya insiden, dihitung dari Asset Value × Exposure Factor.

Social Engineering

Teknik manipulasi psikologis untuk membuat korban menyerahkan informasi sensitif atau melakukan tindakan tertentu.

Statement of Applicability (SoA)

Dokumen dalam ISO/IEC 27001 yang berisi daftar kontrol keamanan yang diterapkan organisasi berdasarkan hasil analisis risiko.

STRIDE

Model threat modeling yang mengkategorikan ancaman menjadi Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, dan Elevation of Privilege.

Supply Chain Attack

Serangan siber yang menargetkan pemasok atau mitra teknologi sebagai jalur masuk ke organisasi target.

T

Threat (Ancaman)

Potensi penyebab insiden yang dapat merusak atau mengganggu sistem informasi.

Threat Intelligence

Informasi yang dianalisis mengenai ancaman keamanan siber untuk membantu organisasi dalam mendeteksi dan mencegah serangan.

Threat Modeling

Pendekatan sistematis untuk mengidentifikasi ancaman terhadap sistem informasi sejak tahap perancangan.

V

Vulnerability (Kerentanan)

Kelemahan dalam sistem informasi yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan.

Vulnerability Assessment

Proses identifikasi dan evaluasi kerentanan keamanan dalam sistem informasi.

Vulnerability Scanning

Teknik otomatis untuk memindai sistem dan menemukan kerentanan yang sudah diketahui.

W

Web Application Firewall (WAF)

Solusi keamanan yang melindungi aplikasi web dari berbagai serangan seperti SQL injection dan cross-site scripting.

Z

Zero-Day Exploit

Eksploitasi terhadap kerentanan yang belum diketahui atau belum diperbaiki oleh vendor.

Zero Trust Architecture

Model keamanan yang mengharuskan verifikasi identitas secara terus-menerus sebelum memberikan akses ke sistem atau data.

INDEKS

BIOGRAFI PENULIS

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

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 te*register* 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 Infomasi Universitas Indonesia, menyelesaikan studinya pada tahun 2009. Pada tahun 2022 penulis juga menyelesikan 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 menyelasaikan studi postgraduted cyber *security* di Massachusetts Institute of Technology (MIT).

Penulis memiliki kepakaran dibidang keamanan siber, pengembangann 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

Siti Maesaroh, S.Kom., M.T.I.

Ketertarikan penulis terhadap ilmu komputer dimulai pada tahun 2010 silam. Hal tersebut membuat penulis memilih untuk masuk ke Sekolah Perguruan Tinggi Di bidang Sistem Informasi. Setelah lulus S1, 2 tahun kemudian, penulis menyelesaikan studi S2 di prodi Teknik Informatika Program Pasca Sarjana Universitas Raharja. Penulis memiliki kepakaran dibidang *Web Technology dan Data Science.* Dan untuk mewujudkan karir 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. Dengan tujuan mengembangkan solusi perangkat lunak inovatif yang memecahkan tantangan bisnis dengan menggunakan keterampilan pemrograman dan pengetahuan teknologi terkini. Terus meningkatkan kemampuan teknis dan kepemimpinan melalui pengalaman praktis dan pembelajaran berkelanjutan. Email Penulis: mays41946@gmail.com.

Mohamad Yusuf, S.Kom., M.C.S.

Penulis dilahirkan di Jakarta pada tanggal 7 September 1976. Pendidikan S1 diselesaikan pada tahun 2001 di Universitas Budi Luhur Jurusan Teknik Informatika. Selanjutnya, pendidikan S2 di Preston University Islamabad Pakistan dan saat ini sedang menyelesaikan S3 di Universiti Malaysia Kelantan pada bidang Data Science. Penulis adalah Dosen Tetap Universitas Mercu Buana Jakarta. Buku populer yang telah dihasilkan adalah Pemrograman Mobile dengan Flutter, Pemrograman Java, Aplikasi Mobile Teori dan Praktek, Teknik 2D/3D Blender Untuk Pemula hingga Ahli, Bahasa Pemrograman Python dan Pembelajaran Mesin dan Kecerdasan Buatan Teori dan Aplikasi Praktis. Selain itu juga telah menulis buku tentang Tata Kelola Teknologi Informasi. Untuk menghubungi penulis di email: mhd.yusuf@mercubuana.ac.id.

Diva Alifta Chandra, B.Eng,. M.Sc.

Diva Alifta Chandra lahir di Purwokerto pada tahun 2001. Ia merupakan seorang auditor sistem manajemen keamanan informasi yang tersertifikasi ISO 27001 dan ISO 27701 dari lembaga internasional IRCA (United Kingdom) dan PECB (Canada). Penulis menyelesaikan pendidikan sarjana (S1) di bidang Biomedical Engineering dari University of Technology Malaysia (UTM), kemudian melanjutkan studi pascasarjana dan meraih gelar Master of Data Science dari University of Malaya (UM) dengan disertasi yang berfokus pada Algorithmic Social *Computing*. Selain berkarier sebagai auditor, penulis juga aktif berprofesi sebagai Penetration Tester dan SOC Analyst. Dengan kepakaran di bidang keamanan siber dan ilmu data, penulis berkomitmen untuk mengembangkan karier sebagai dosen dan peneliti profesional. Penulis secara aktif meneliti serta menulis artikel ilmiah seputar social *computing*, dengan harapan dapat memberikan kontribusi nyata bagi kemajuan bangsa dan negara. Untuk korespondensi, penulis dapat dihubungi melalui email: divaac56@gmail.com

MANAJEMEN RISIKO KEAMANAN INFORMASI ISO/IEC 27005 : 2022

Di era ketika data telah menjadi aset paling berharga sekaligus paling rentan, ransomware melumpuhkan organisasi dalam hitungan jam, kebocoran data menggerus kepercayaan publik, dan serangan rantai pasok digital menjatuhkan korporasi raksasa hanya dari satu titik lemah. Pertanyaannya bukan lagi "apakah" sebuah organisasi akan diserang, tetapi "kapan" dan "seberapa siap" mereka menghadapinya. Buku ini hadir sebagai panduan komprehensif berbasis standar internasional ISO/IEC 27005:2022 yang memandu pembaca menapaki seluruh siklus manajemen risiko keamanan informasi dari penetapan konteks, identifikasi ancaman dan kerentanan, analisis serta evaluasi risiko, hingga penerapan kontrol keamanan dan pemantauan berkelanjutan. Tidak berhenti pada teori, buku ini menyajikan studi kasus pada organisasi pemerintah, perusahaan teknologi, dan industri finansial; sembilan template praktis siap pakai (*Risk Register, Risk Matrix, Risk Treatment Plan, SoA, Audit Checklist*, dan lainnya); serta integrasi dengan teknik modern seperti CVSS, *threat intelligence, vulnerability assessment, dan penetration testing*.

Tujuh belas bab disusun secara progresif: dari fondasi konseptual (CIA Triad, keluarga ISO/IEC 27000, kerangka ISO 31000), inti standar ISO/IEC 27005:2022, implementasi kontrol dan tata kelola, studi kasus serta tools analisis, hingga pemetaan tren risiko siber masa depan mencakup AI dalam *cybersecurity, cloud security, IoT, supply chain risk*, dan ancaman komputasi kuantum terhadap kriptografi modern. Praktisi keamanan informasi dan CISO, auditor sistem informasi dan SMKI, manajer risiko serta profesional GRC, akademisi dan mahasiswa bidang keamanan informasi, hingga pimpinan organisasi di sektor publik maupun swasta yang ingin memahami bagaimana keamanan informasi terhubung dengan strategi bisnis dan keberlangsungan organisasi.

Manajemen risiko keamanan informasi bukanlah proyek dengan titik selesai, melainkan disiplin berkelanjutan. Buku ini ditulis sebagai kompas yang dapat dipegang setiap kali organisasi menghadapi pertanyaan sulit: apakah kita cukup aman, apa yang harus dilindungi terlebih dahulu, dan bagaimana kita memutuskan mengajak pembaca melangkah dari reaktif menjadi proaktif, dari sekadar mematuhi standar menjadi membangun ketahanan siber yang sejati.

sada kurnia pustaka

ISBN 978-634-7522-40-3
9 786347 522603