



Manajemen Keamanan, Risiko, dan Layanan Teknologi Informasi



Dr. Mario Tulenan Parinsi, S.Kom., M.T.I.
Ray Rivai Anugrah Aer Pelealu, S.Pd., M.Pd.
Renaldy Ryan Guntur Molo, S.Pd.

MANAJEMEN KEAMANAN, RISIKO, DAN LAYANAN TEKNOLOGI INFORMASI

Dr. Mario Tulenan Parinsi, S.Kom., M.T.I
Ray Rivai Anugrah Aer Pelealu, S.Pd., M.Pd
Renaldy Ryan Guntur Molo, S.Pd



Tahta Media Group

UU No 28 tahun 2014 tentang Hak Cipta

Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Pelindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

- i. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
- ii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
- iii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
- iv. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

Hak cipta dilindungi undang-undang

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari Penerbit.

MANAJEMEN KEAMANAN, RISIKO, DAN LAYANAN TEKNOLOGI INFORMASI

Penulis:

Dr. Mario Tulenan Parinsi, S.Kom., M.T.I.
Ray Rivai Anugrah Aer Pelealu, S.Pd., M.Pd
Renaldy Ryan Guntur Molo, S.Pd

Desain Cover:

Tahta Media

Editor:

Tahta Media

Proofreader:

Tahta Media

Ukuran:

viii, 122, uk: 15,5 x 23 cm

ISBN: 978-634-262-289-6

Cetakan Pertama:

Agustus 2026

Hak Cipta 2026, Pada Penulis

Isi diluar tanggung jawab percetakan

Copyright © 2026 by Tahta Media Group

All Right Reserved

PENERBIT TAHTA MEDIA GROUP

Perumahan Mitra Utama Residence 3 Blok A no 1, Sawahan, Tempel,
Kec. Gatak, Kabupaten Sukoharjo, Jawa Tengah 57557

email: tahtaliterasimedia@gmail.com

website: <http://store.tahtamedia.co.id/>

Anggota IKAPI (216/JTE/2021)

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya buku Manajemen Keamanan, Risiko, dan Layanan Teknologi Informasi dapat diselesaikan dengan baik. Buku ini disusun sebagai salah satu upaya untuk memberikan pemahaman yang komprehensif mengenai pengelolaan teknologi informasi yang aman, andal, efektif, dan berkelanjutan di tengah pesatnya perkembangan transformasi digital yang terjadi di berbagai sektor kehidupan.

Perkembangan teknologi informasi telah membawa perubahan besar dalam cara organisasi menjalankan proses bisnis, memberikan layanan, mengelola data, dan berinteraksi dengan pemangku kepentingan. Teknologi digital kini menjadi faktor strategis yang menentukan keberhasilan organisasi dalam meningkatkan efisiensi, produktivitas, inovasi, serta daya saing. Namun, di balik berbagai peluang yang ditawarkan, transformasi digital juga menghadirkan tantangan yang semakin kompleks, terutama terkait keamanan informasi, pengelolaan risiko teknologi, kepatuhan terhadap regulasi, serta penyediaan layanan teknologi informasi yang berkualitas.

Dalam konteks tersebut, organisasi tidak cukup hanya menguasai teknologi, tetapi juga harus mampu mengelola keamanan informasi, risiko teknologi informasi, dan layanan teknologi informasi secara terintegrasi. Ketiga aspek tersebut merupakan fondasi penting dalam membangun tata kelola teknologi informasi yang mampu mendukung pencapaian tujuan organisasi sekaligus menjaga keberlangsungan operasional di tengah lingkungan digital yang dinamis.

Buku ini disusun secara sistematis dan komprehensif dengan mencakup berbagai topik utama yang berkaitan dengan manajemen teknologi informasi. Pembahasan diawali dengan landasan konseptual teknologi informasi dan tata kelola TI, dilanjutkan dengan konsep

keamanan informasi, Sistem Manajemen Keamanan Informasi (Information Security Management System), ancaman dan serangan siber, manajemen risiko teknologi informasi, manajemen layanan teknologi informasi, pengelolaan infrastruktur dan operasional TI, audit dan kepatuhan teknologi informasi, studi kasus implementasi, hingga pembahasan mengenai masa depan keamanan, risiko, dan layanan teknologi informasi.

Materi dalam buku ini mengacu pada berbagai standar, kerangka kerja, dan praktik terbaik internasional, seperti ISO/IEC 27001, ISO 31000, COBIT, ITIL, NIST Cybersecurity Framework, serta berbagai referensi ilmiah terkini yang relevan dengan perkembangan teknologi informasi. Dengan demikian, buku ini tidak hanya memberikan pemahaman teoritis, tetapi juga memberikan gambaran praktis mengenai implementasi keamanan, risiko, dan layanan TI dalam berbagai jenis organisasi.

Buku ini diharapkan dapat menjadi referensi bagi mahasiswa, dosen, peneliti, praktisi teknologi informasi, auditor sistem informasi, manajer teknologi informasi, pengelola keamanan informasi, serta para pengambil kebijakan yang ingin memahami dan mengimplementasikan pengelolaan teknologi informasi secara lebih efektif. Selain itu, buku ini juga diharapkan dapat mendukung kegiatan pembelajaran, penelitian, dan pengembangan kompetensi di bidang keamanan informasi, manajemen risiko, tata kelola TI, dan manajemen layanan teknologi informasi.

Penulis menyadari bahwa buku ini masih memiliki berbagai keterbatasan. Oleh karena itu, kritik, saran, dan masukan yang konstruktif sangat diharapkan untuk penyempurnaan pada edisi berikutnya. Semoga buku ini dapat memberikan manfaat yang luas bagi pengembangan ilmu pengetahuan, peningkatan kompetensi

profesional, serta mendukung terwujudnya organisasi yang aman, tangguh, dan adaptif dalam menghadapi tantangan era digital.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan, inspirasi, dan kontribusi dalam proses penyusunan buku ini. Semoga buku ini dapat menjadi salah satu sumber pengetahuan yang bermanfaat bagi pembaca dalam memahami dan mengelola teknologi informasi secara strategis dan berkelanjutan.

DAFTAR ISI

KATA PENGANTAR	iv
DAFTAR ISI	vii
BAB 1 PENDAHULUAN.....	1
A. Manajemen TI di Era Digital.....	1
B. Transformasi Digital dan Tantangan Keamanan Informasi	4
C. Peran Manajemen Keamanan, Risiko, dan Layanan TI.....	6
D. Tujuan dan Manfaat Manajemen TI.....	8
E. Ruang Lingkup Buku.....	9
Latihan Soal!.....	11
BAB 2 KONSEP DASAR TEKNOLOGI INFORMASI DAN SISTEM INFORMASI.....	17
A. Pengertian Teknologi Informasi	17
B. Komponen Sistem Informasi	19
C. Infrastruktur Teknologi Informasi	22
D. Arsitektur Sistem Informasi.....	23
E. Peran TI dalam Organisasi Modern.....	25
Latihan Soal!.....	26
BAB 3 TATA KELOLA TEKNOLOGI INFORMASI (IT GOVERNANCE).....	32
A. Konsep IT Governance.....	32
B. Prinsip Tata Kelola TI.....	35
C. Kerangka Kerja <i>IT Governance</i>	36
D. Hubungan <i>IT Governance</i> dan Manajemen Risiko	39
E. Implementasi Tata Kelola TI dalam Organisasi	41
Latihan soal!	42
BAB 4 KONSEP DASAR KEAMANAN INFORMASI.....	48
A. Definisi Keamanan Informasi	48
B. Tujuan Keamanan Informasi.....	51

C. Prinsip CIA Triad	53
D. Ancaman dan Kerentanan Sistem Informasi	56
E. Dampak Pelanggaran Keamanan Informasi	57
Latihan Soal!	59
BAB 5 SISTEM MANAJEMEN KEAMANAN INFORMASI (INFORMATION SECURITY MANAGEMENT SYSTEM-ISMS)	65
A. Konsep ISMS	65
B. Standar ISO 27001	68
C. Komponen Sistem Manajemen Keamanan Informasi	70
D. Siklus PDCA dalam ISMS	72
E. Implementasi ISMS dalam Organisasi	75
Latihan Soal!	77
BAB 6 ANCAMAN DAN SERANGAN SIBER	83
A. Jenis Ancaman Keamanan Informasi	83
B. Malware dan Ransomware	86
C. Phishing dan Social Engineering	89
D. Serangan Jaringan (<i>DDoS</i> dan <i>Man-in-the-Middle</i>)	92
E. Strategi Mitigasi Ancaman Siber	94
Latihan Soal!	96
BAB 7 PENUTUP	103
A. Kesimpulan	103
B. Saran	106
DAFTAR PUSTAKA	109
DAFTAR SINGKATAN DAN ISTILAH	113
A. Daftar Singkatan	113
B. Daftar Istilah	117

BAB 1

PENDAHULUAN

A. MANAJEMEN TI DI ERA DIGITAL

Perkembangan teknologi informasi telah mengubah hampir seluruh aspek kehidupan manusia, mulai dari aktivitas ekonomi, pendidikan, kesehatan, pemerintahan, hingga komunikasi sosial. Organisasi modern tidak lagi memandang teknologi informasi hanya sebagai alat pendukung operasional, melainkan sebagai aset strategis yang menentukan daya saing, keberlanjutan bisnis, dan kemampuan inovasi organisasi. Transformasi tersebut ditandai dengan meningkatnya penggunaan *cloud computing*, *big data*, *artificial intelligence*, *Internet of Things (IoT)*, serta berbagai platform digital yang memungkinkan organisasi beroperasi secara lebih efisien dan terintegrasi.

Transformasi digital menjadi fenomena global yang mendorong organisasi untuk melakukan perubahan fundamental dalam proses bisnis, model layanan, serta strategi pengambilan keputusan. Digitalisasi memungkinkan organisasi mengelola informasi secara cepat, akurat, dan real-time sehingga mampu meningkatkan kualitas pelayanan kepada pelanggan maupun masyarakat. Namun, ketergantungan yang semakin tinggi terhadap teknologi informasi juga menghadirkan berbagai risiko baru yang berkaitan dengan keamanan data, privasi informasi, gangguan layanan, hingga ancaman siber yang semakin kompleks (Saeed et al., 2023).

BAB 2

KONSEP DASAR TEKNOLOGI INFORMASI DAN SISTEM INFORMASI

A. PENGERTIAN TEKNOLOGI INFORMASI

Teknologi informasi (TI) merupakan salah satu fondasi utama dalam penyelenggaraan organisasi modern. Perkembangan teknologi digital telah mengubah cara individu, organisasi, dan pemerintah dalam mengelola informasi, mengambil keputusan, serta memberikan layanan kepada masyarakat. Dalam era ekonomi digital, teknologi informasi tidak lagi dipandang sebagai fungsi pendukung (*support function*), melainkan sebagai aset strategis yang menentukan daya saing, inovasi, dan keberlanjutan organisasi.

Secara umum, teknologi informasi dapat didefinisikan sebagai seluruh perangkat keras (*hardware*), perangkat lunak (*software*), jaringan komunikasi, basis data, prosedur, dan sumber daya manusia yang digunakan untuk mengumpulkan, mengolah, menyimpan, mengamankan, dan mendistribusikan informasi guna mendukung berbagai aktivitas organisasi. Menurut Stair dan Reynolds (2023), teknologi informasi merupakan kombinasi teknologi berbasis komputer yang memungkinkan organisasi mengelola data menjadi informasi yang bernilai bagi proses bisnis dan pengambilan keputusan.

BAB 3

TATA KELOLA TEKNOLOGI INFORMASI (*IT GOVERNANCE*)

A. KONSEP IT GOVERNANCE

Perkembangan teknologi informasi yang semakin pesat telah menjadikan teknologi sebagai salah satu aset strategis organisasi. Pada masa lalu, teknologi informasi lebih banyak digunakan sebagai alat pendukung operasional, tetapi saat ini teknologi telah menjadi penggerak utama inovasi, transformasi digital, dan penciptaan nilai organisasi. Ketergantungan yang semakin tinggi terhadap teknologi menyebabkan organisasi harus memastikan bahwa seluruh investasi, kebijakan, dan aktivitas teknologi informasi selaras dengan tujuan bisnis. Kebutuhan inilah yang melahirkan konsep tata kelola teknologi informasi atau *Information Technology Governance (IT Governance)*.

Secara umum, *IT Governance* merupakan bagian integral dari tata kelola organisasi yang berfokus pada kepemimpinan, struktur organisasi, kebijakan, proses, dan mekanisme pengendalian untuk memastikan bahwa teknologi informasi mendukung pencapaian tujuan organisasi secara efektif, efisien, aman, dan berkelanjutan. Menurut De Haes, Van Grembergen, Joshi, dan Huygh (2024), *IT Governance* merupakan sistem yang digunakan oleh organisasi untuk mengarahkan dan mengendalikan pemanfaatan teknologi digital agar

BAB 4

KONSEP DASAR KEAMANAN INFORMASI

A. DEFINISI KEAMANAN INFORMASI

Perkembangan teknologi informasi yang sangat pesat telah membawa perubahan besar dalam cara organisasi mengelola data, menjalankan proses bisnis, dan memberikan layanan kepada pengguna. Hampir seluruh aktivitas organisasi modern bergantung pada sistem informasi yang terhubung melalui jaringan digital. Ketergantungan tersebut menjadikan informasi sebagai salah satu aset paling berharga yang harus dilindungi. Dalam konteks inilah keamanan informasi (*information security*) menjadi disiplin yang sangat penting dalam manajemen teknologi informasi.

Informasi merupakan sumber daya strategis yang memiliki nilai ekonomi, operasional, hukum, dan reputasional bagi organisasi. Data pelanggan, catatan transaksi keuangan, dokumen bisnis, informasi penelitian, hingga data pribadi pegawai merupakan contoh aset informasi yang harus dijaga dari berbagai ancaman. Kehilangan, kebocoran, manipulasi, atau gangguan terhadap informasi dapat menimbulkan dampak yang sangat besar terhadap keberlangsungan organisasi.

Menurut standar International Organization for Standardization dan International Electrotechnical Commission dalam ISO/IEC 27000:2022, keamanan informasi adalah upaya untuk menjaga

BAB 5

SISTEM MANAJEMEN KEAMANAN INFORMASI (INFORMATION SECURITY MANAGEMENT SYSTEM – ISMS)

A. KONSEP ISMS

Transformasi digital telah menyebabkan informasi menjadi salah satu aset paling penting dalam organisasi modern. Aktivitas bisnis, layanan publik, transaksi keuangan, komunikasi organisasi, hingga pengambilan keputusan strategis saat ini sangat bergantung pada pengelolaan informasi yang akurat, aman, dan tersedia setiap saat. Ketergantungan tersebut menyebabkan organisasi menghadapi berbagai risiko yang semakin kompleks, mulai dari kebocoran data, serangan siber, gangguan operasional, hingga pelanggaran regulasi perlindungan data.

Dalam lingkungan digital yang penuh ketidakpastian tersebut, organisasi memerlukan pendekatan yang sistematis dan terstruktur untuk mengelola keamanan informasi. Pendekatan tersebut dikenal sebagai Sistem Manajemen Keamanan Informasi atau *Information Security Management System* (ISMS).

BAB 6

ANCAMAN DAN SERANGAN SIBER

A. JENIS ANCAMAN KEAMANAN INFORMASI

Perkembangan teknologi digital telah membawa manfaat besar bagi organisasi, pemerintah, dan masyarakat. Pemanfaatan teknologi informasi memungkinkan peningkatan efisiensi, produktivitas, inovasi, dan kualitas layanan dalam berbagai sektor. Namun, semakin tingginya ketergantungan terhadap sistem digital juga meningkatkan paparan terhadap berbagai ancaman keamanan informasi. Saat ini, ancaman siber menjadi salah satu risiko utama yang dihadapi organisasi karena dapat mengganggu operasional, menyebabkan kerugian finansial, merusak reputasi, bahkan mengancam keberlangsungan bisnis.

Ancaman keamanan informasi (*information security threats*) dapat didefinisikan sebagai segala kondisi, tindakan, atau peristiwa yang berpotensi mengeksploitasi kerentanan sistem sehingga menyebabkan gangguan terhadap kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Menurut *National Institute of Standards and Technology* (NIST), ancaman dapat berasal dari manusia, proses, teknologi, maupun faktor lingkungan yang mampu menimbulkan dampak negatif terhadap aset informasi organisasi (NIST, 2024).

Dalam lingkungan digital modern, ancaman keamanan informasi berkembang secara dinamis. Pelaku ancaman (*threat actors*) tidak lagi

BAB 7

PENUTUP

A. KESIMPULAN

Transformasi digital telah mengubah paradigma organisasi dalam mengelola proses bisnis, pelayanan, komunikasi, dan pengambilan keputusan. Teknologi informasi tidak lagi dipandang sebagai fungsi pendukung (*support function*), melainkan telah berkembang menjadi aset strategis yang menentukan daya saing, keberlanjutan, dan kemampuan organisasi dalam menciptakan nilai. Perubahan tersebut menuntut organisasi untuk membangun tata kelola teknologi informasi yang tidak hanya berorientasi pada efisiensi operasional, tetapi juga mampu menjamin keamanan informasi, mengelola risiko, serta menyediakan layanan teknologi informasi yang berkualitas.

Buku ini telah menguraikan berbagai konsep, teori, standar, dan praktik terbaik yang menjadi fondasi dalam pengelolaan keamanan, risiko, dan layanan teknologi informasi. Pembahasan diawali dengan pemahaman mengenai konsep dasar teknologi informasi dan sistem informasi sebagai landasan dalam membangun lingkungan digital organisasi. Selanjutnya dibahas tata kelola teknologi informasi (*Information Technology Governance*) yang menekankan pentingnya keselarasan antara strategi bisnis dan strategi teknologi informasi melalui penerapan kerangka kerja seperti *COBIT* dan *ISO/IEC 38500*.

Pada aspek keamanan informasi, buku ini menjelaskan bahwa perlindungan aset informasi merupakan tanggung jawab seluruh organisasi, bukan hanya unit teknologi informasi. Prinsip

DAFTAR PUSTAKA

- Alharbi, F., & Drew, S. (2022). Information security governance in digital transformation: A systematic literature review. *Computers & Security*, 118, 102738.
- Alshaikh, M. (2021). Developing cybersecurity culture to influence employee behavior. *Computers & Security*, 98, 102003.
- AXELOS. (2019). *ITIL foundation: ITIL 4 edition*. TSO.
- De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2024). *Enterprise governance of information technology: Achieving strategic alignment and value* (4th ed.). Springer.
- ENISA. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity.
- Gibson, D. (2024). *Managing risk in information systems* (3rd ed.). Jones & Bartlett Learning.
- Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2022). Cyber security threats and vulnerabilities: A systematic mapping study. *IEEE Access*, 10, 12345–12367.
- International Electrotechnical Commission. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—Information security controls*. IEC.
- International Organization for Standardization. (2018). *ISO 31000:2018 Risk management—Guidelines*. ISO.
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.
- ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.

- ISACA. (2019). *COBIT 2019 framework: Introduction and methodology*. ISACA.
- ISACA. (2022). *CISA review manual 27th edition*. ISACA.
- ISACA. (2023). *CRISC review manual*. ISACA.
- Kim, D., Solomon, M., & Iseminger, D. (2022). *Fundamentals of information systems security* (4th ed.). Jones & Bartlett Learning.
- Kumar, R., Singh, P., & Sharma, A. (2023). Cloud computing adoption for enterprise digital transformation: Opportunities, challenges, and security considerations. *Journal of Cloud Computing*, 12(1), 1–18.
- Laudon, K. C., & Laudon, J. P. (2024). *Management information systems: Managing the digital firm* (18th ed.). Pearson.
- Maiwald, E. (2023). *Network security: A beginner's guide* (4th ed.). McGraw-Hill.
- National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Revision 5)*. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2022). *Risk management framework for information systems and organizations (NIST Special Publication 800-37 Revision 2)*. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce.
- Peltier, T. R. (2022). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Auerbach Publications.

- Rainer, R. K., Prince, B., & Watson, H. J. (2022). *Management information systems* (6th ed.). Wiley.
- Ross, J. W., Beath, C. M., & Mocker, M. (2019). *Designed for digital: How to architect your business for sustained success*. MIT Press.
- Saeed, A., Ahmad, M., Khan, M. A., & Ali, R. (2023). Cybersecurity challenges in digital transformation: A systematic review. *Journal of Information Security and Applications*, 73, 103430.
- Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2022). Variables influencing information security policy compliance: A systematic review. *Information & Computer Security*, 30(2), 185–212.
- Stair, R. M., & Reynolds, G. W. (2023). *Principles of information systems* (15th ed.). Cengage Learning.
- Stallings, W. (2022). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley.
- Stallings, W. (2023). *Network security essentials: Applications and standards* (7th ed.). Pearson.
- Stallings, W., & Brown, L. (2024). *Computer security: Principles and practice* (5th ed.). Pearson.
- Tankard, C. (2022). Advanced persistent threats and cyber resilience in enterprise environments. *Network Security*, 2022(8), 5–12.
- Turban, E., Pollard, C., & Wood, G. (2021). *Information technology for management: Driving digital transformation to increase local and global performance, growth and sustainability* (12th ed.). Wiley.
- Van Grembergen, W., De Haes, S., & Guldentops, E. (2022). *Strategies for information technology governance* (2nd ed.). IGI Global.
- Vrhovec, S. L. R., & Markelj, B. (2024). Human factors and information security awareness in organizations: Current trends and future directions. *Computers & Security*, 137, 103641.

- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.
- Whitman, M. E., & Mattord, H. J. (2023). *Management of information security* (8th ed.). Cengage Learning.
- Yadav, G., & Paul, R. (2023). Cyber resilience in digital enterprises: Challenges and strategic approaches. *Journal of Cyber Security Technology*, 7(3), 221–243.
- Zhou, Y., Li, X., & Wang, H. (2022). Artificial intelligence for cybersecurity: A comprehensive review. *IEEE Access*, 10, 93432–93458.
- Zhou, Z., & Piramuthu, S. (2023). Information security governance and organizational performance: An empirical investigation. *Information Systems Management*, 40(2), 145–162.

DAFTAR SINGKATAN DAN ISTILAH

A. DAFTAR SINGKATAN

Singkatan	Kepanjangan	Keterangan
AI	<i>Artificial Intelligence</i>	Teknologi kecerdasan buatan yang mampu meniru kemampuan berpikir manusia
ALE	<i>Annualized Loss Expectancy</i>	Estimasi kerugian tahunan akibat risiko tertentu
API	<i>Application Programming Interface</i>	Antarmuka yang memungkinkan komunikasi antar aplikasi
ARO	<i>Annual Rate of Occurrence</i>	Frekuensi terjadinya risiko dalam satu tahun
AIOps	<i>Artificial Intelligence for IT Operations</i>	Pemanfaatan AI untuk operasional TI
BYOD	<i>Bring Your Own Device</i>	Kebijakan penggunaan perangkat pribadi dalam lingkungan kerja
CIA	<i>Confidentiality, Integrity, Availability</i>	Tiga prinsip utama keamanan informasi
CIO	<i>Chief Information Officer</i>	Pimpinan yang bertanggung jawab atas strategi TI organisasi
CISO	<i>Chief Information Security Officer</i>	Pimpinan yang bertanggung jawab atas keamanan informasi organisasi

COBIT	<i>Control Objectives for Information and Related Technology</i>	Kerangka tata kelola dan manajemen TI
CPU	<i>Central Processing Unit</i>	Unit pemrosesan utama komputer
CSF	<i>Cybersecurity Framework</i>	Kerangka kerja keamanan siber dari NIST
CSI	<i>Continual Service Improvement</i>	Proses peningkatan layanan TI secara berkelanjutan
DDoS	<i>Distributed Denial of Service</i>	Serangan yang membanjiri sistem dengan lalu lintas berlebih
DNS	<i>Domain Name System</i>	Sistem penerjemah nama domain ke alamat IP
EDR	<i>Endpoint Detection and Response</i>	Sistem deteksi dan respons ancaman pada perangkat pengguna
ERP	<i>Enterprise Resource Planning</i>	Sistem terintegrasi untuk pengelolaan sumber daya perusahaan
GDPR	<i>General Data Protection Regulation</i>	Regulasi perlindungan data Uni Eropa
GRC	<i>Governance, Risk, and Compliance</i>	Pendekatan integrasi tata kelola, risiko, dan kepatuhan
HIPAA	<i>Health Insurance Portability and Accountability Act</i>	Regulasi perlindungan data kesehatan di Amerika Serikat
IDS	<i>Intrusion Detection System</i>	Sistem pendeteksi intrusi jaringan

IEC	<i>International Electrotechnical Commission</i>	Organisasi standar internasional bidang elektroteknik
IoT	<i>Internet of Things</i>	Jaringan perangkat yang saling terhubung melalui internet
IPS	<i>Intrusion Prevention System</i>	Sistem pencegah intrusi jaringan
ISACA	<i>Information Systems Audit and Control Association</i>	Organisasi profesional audit dan tata kelola TI
ISMS	<i>Information Security Management System</i>	Sistem Manajemen Keamanan Informasi
ISO	<i>International Organization for Standardization</i>	Organisasi standar internasional
IT	<i>Information Technology</i>	Teknologi Informasi
IT Governance	<i>Information Technology Governance</i>	Tata Kelola Teknologi Informasi
ITIL	<i>Information Technology Infrastructure Library</i>	Kerangka kerja manajemen layanan TI
ITSM	<i>Information Technology Service Management</i>	Manajemen Layanan Teknologi Informasi
KPI	<i>Key Performance Indicator</i>	Indikator utama pengukuran kinerja
LAN	<i>Local Area Network</i>	Jaringan komputer dalam area terbatas
MFA	<i>Multi-Factor Authentication</i>	Metode autentikasi dengan lebih dari satu faktor verifikasi

NIST	<i>National Institute of Standards and Technology</i>	Lembaga standar dan teknologi Amerika Serikat
NMS	<i>Network Management System</i>	Sistem pengelolaan jaringan
NPM	<i>Network Performance Monitoring</i>	Pemantauan kinerja jaringan
PDCA	<i>Plan-Do-Check-Act</i>	Siklus peningkatan berkelanjutan
PCI DSS	<i>Payment Card Industry Data Security Standard</i>	Standar keamanan industri kartu pembayaran
PaaS	<i>Platform as a Service</i>	Layanan penyedia platform komputasi berbasis cloud
RBAC	<i>Role-Based Access Control</i>	Pengendalian akses berdasarkan peran pengguna
RMF	<i>Risk Management Framework</i>	Kerangka kerja manajemen risiko
SaaS	<i>Software as a Service</i>	Layanan perangkat lunak berbasis cloud
SDM	Sumber Daya Manusia	Individu yang terlibat dalam organisasi
SIEM	<i>Security Information and Event Management</i>	Sistem pengelolaan dan analisis peristiwa keamanan
SLA	<i>Service Level Agreement</i>	Perjanjian tingkat layanan
SOAR	<i>Security Orchestration, Automation, and Response</i>	Platform otomatisasi respons keamanan

SLE	<i>Single Loss Expectancy</i>	Estimasi kerugian akibat satu kejadian risiko
SP	<i>Special Publication</i>	Publikasi khusus NIST
SVS	<i>Service Value System</i>	Sistem penciptaan nilai layanan dalam ITIL 4
TI	Teknologi Informasi	Teknologi yang digunakan untuk mengelola informasi
VPN	<i>Virtual Private Network</i>	Jaringan privat virtual melalui internet
WAN	<i>Wide Area Network</i>	Jaringan komputer dengan cakupan wilayah luas
ZTA	<i>Zero Trust Architecture</i>	Arsitektur keamanan berbasis prinsip verifikasi berkelanjutan

B. DAFTAR ISTILAH

A

Aset Informasi

Segala bentuk informasi, data, perangkat, aplikasi, maupun sumber daya yang memiliki nilai bagi organisasi dan perlu dilindungi.

Ancaman (*Threat*)

Segala kondisi, aktivitas, atau kejadian yang berpotensi menyebabkan kerusakan, kehilangan, atau gangguan terhadap aset informasi.

Audit TI

Proses evaluasi independen terhadap sistem, infrastruktur, proses, dan pengendalian teknologi informasi untuk memastikan efektivitas, keamanan, dan kepatuhan.

Availability

Prinsip keamanan informasi yang memastikan bahwa informasi dan layanan tersedia ketika dibutuhkan oleh pengguna yang berwenang.

B

Blockchain

Teknologi penyimpanan data terdistribusi yang menggunakan rantai blok terenkripsi untuk menjamin integritas dan transparansi data.

Business Continuity

Kemampuan organisasi untuk mempertahankan operasi penting ketika terjadi gangguan atau bencana.

C

Cloud Computing

Model penyediaan sumber daya komputasi melalui internet yang dapat diakses sesuai kebutuhan.

Compliance

Tingkat kesesuaian organisasi terhadap regulasi, standar, kebijakan, dan persyaratan yang berlaku.

Confidentiality

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

Control

Kebijakan, prosedur, teknologi, atau mekanisme yang digunakan untuk mengurangi risiko.

Cyber Resilience

Kemampuan organisasi untuk mengantisipasi, merespons, memulihkan, dan beradaptasi terhadap insiden siber.

Cybersecurity

Upaya melindungi sistem, jaringan, perangkat, dan data dari ancaman serta serangan siber.

D

Data Center

Fasilitas yang digunakan untuk menempatkan server, penyimpanan data, jaringan, dan infrastruktur pendukung teknologi informasi.

Digital Transformation

Proses pemanfaatan teknologi digital untuk mengubah cara organisasi beroperasi dan menciptakan nilai.

E

Edge Computing

Model komputasi yang memproses data lebih dekat ke sumber data dibandingkan pusat data utama.

F

Firewall

Perangkat keras atau perangkat lunak yang berfungsi mengendalikan lalu lintas jaringan berdasarkan aturan keamanan tertentu.

G

Governance

Sistem pengawasan dan pengendalian yang digunakan untuk memastikan pencapaian tujuan organisasi.

I

Incident

Gangguan atau kejadian yang menyebabkan penurunan atau terhentinya kualitas layanan TI.

Information Security

Perlindungan informasi dari akses, penggunaan, pengungkapan, perubahan, atau penghancuran yang tidak sah.

Integrity

Prinsip keamanan informasi yang memastikan bahwa data tetap akurat, lengkap, dan tidak berubah tanpa otorisasi.

K

Kerentanan (*Vulnerability*)

Kelemahan pada sistem, proses, atau sumber daya yang dapat dimanfaatkan oleh ancaman.

M

Malware

Perangkat lunak berbahaya yang dirancang untuk merusak, mencuri, atau mengganggu sistem komputer.

Monitoring

Proses pengawasan dan pengukuran kondisi sistem atau layanan secara berkelanjutan.

P

Phishing

Teknik penipuan yang bertujuan memperoleh informasi sensitif dengan menyamar sebagai pihak terpercaya.

Privacy

Hak individu untuk mengendalikan penggunaan dan pengungkapan data pribadinya.

Q

Quantum Computing

Teknologi komputasi yang memanfaatkan prinsip mekanika kuantum untuk memproses informasi dengan kecepatan sangat tinggi.

R

Ransomware

Jenis malware yang mengenkripsi data korban dan meminta tebusan untuk memulihkannya.

Residual Risk

Risiko yang masih tersisa setelah tindakan pengendalian atau mitigasi diterapkan.

Risk Assessment

Proses identifikasi, analisis, dan evaluasi risiko untuk menentukan tingkat risiko dan prioritas penanganannya.

30. Risk Matrix

Alat analisis yang digunakan untuk mengukur tingkat risiko berdasarkan kemungkinan dan dampak.

Risk Register

Dokumen yang berisi daftar risiko, tingkat risiko, kontrol yang diterapkan, dan status mitigasi risiko.

S

Security Awareness

Tingkat pemahaman dan kesadaran individu terhadap pentingnya keamanan informasi.

Service Desk

Fungsi layanan yang menjadi titik kontak utama antara pengguna dan penyedia layanan TI.

Service Level Agreement (SLA)

Dokumen yang menjelaskan tingkat layanan yang disepakati antara penyedia layanan dan pengguna.

Social Engineering

Teknik manipulasi psikologis yang digunakan untuk memperoleh akses atau informasi secara tidak sah.

T

Tata Kelola TI

Sistem pengelolaan dan pengawasan teknologi informasi yang bertujuan mendukung pencapaian tujuan organisasi.

Threat Intelligence

Informasi yang dikumpulkan dan dianalisis mengenai ancaman siber untuk mendukung pengambilan keputusan keamanan.

V

Virtualisasi

Teknologi yang memungkinkan satu perangkat fisik menjalankan beberapa lingkungan komputasi virtual.

Z

Zero Trust

Pendekatan keamanan yang mengharuskan setiap pengguna, perangkat, dan aplikasi diverifikasi sebelum diberikan akses.

Zero-Day Attack

Serangan yang memanfaatkan kerentanan perangkat lunak yang belum diketahui atau belum memiliki perbaikan resmi

Manajemen Keamanan, Risiko, dan Layanan Teknologi Informasi

Buku ini disusun secara sistematis dan komprehensif dengan mencakup berbagai topik utama yang berkaitan dengan manajemen teknologi informasi. Pembahasan diawali dengan landasan konseptual teknologi informasi dan tata kelola TI, dilanjutkan dengan konsep keamanan informasi, Sistem Manajemen Keamanan Informasi (Information Security Management System), ancaman dan serangan siber, manajemen risiko teknologi informasi, manajemen layanan teknologi informasi, pengelolaan infrastruktur dan operasional TI, audit dan kepatuhan teknologi informasi, studi kasus implementasi, hingga pembahasan mengenai masa depan keamanan, risiko, dan layanan teknologi informasi.

Materi dalam buku ini mengacu pada berbagai standar, kerangka kerja, dan praktik terbaik internasional, seperti ISO/IEC 27001, ISO 31000, COBIT, ITIL, NIST Cybersecurity Framework, serta berbagai referensi ilmiah terkini yang relevan dengan perkembangan teknologi informasi. Dengan demikian, buku ini tidak hanya memberikan pemahaman teoritis, tetapi juga memberikan gambaran praktis mengenai implementasi keamanan, risiko, dan layanan TI dalam berbagai jenis organisasi.

Buku ini diharapkan dapat menjadi referensi bagi mahasiswa, dosen, peneliti, praktisi teknologi informasi, auditor sistem informasi, manajer teknologi informasi, pengelola keamanan informasi, serta para pengambil kebijakan yang ingin memahami dan mengimplementasikan pengelolaan teknologi informasi secara lebih efektif. Selain itu, buku ini juga diharapkan dapat mendukung kegiatan pembelajaran, penelitian, dan pengembangan kompetensi di bidang keamanan informasi, manajemen risiko, tata kelola TI, dan manajemen layanan teknologi informasi.



IKAPI
IKATAN PENERBIT INDONESIA

CV. Tahta Media Group

Sukoharjo, Jawa Tengah

Web : www.tahtamedia.co.id

Ig : tahtamedia group

Telp/WA : +62 896 5427 3996

