Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro dan Informatika
Volume 3, Nomor 2, Maret 2025
e-ISSN: 3031-349X; p-ISSN: 3031-500X, Hal. 27-39
DOI: https://doi.org/10.61132/jupiter.v3i2.780
Available Online at: https://journal.aritekin.or.id/index.php/Jupiter

Strategi Manajemen Risiko Teknologi Informasi Berbasis Studi Literatur

Sri Fuji Muliati[1*], Fidi Supriadi[2], Dani Indra Junaedi[3]
[1,2,3]Universitas Sebelas April, Indonesia

Alamat: Jl. Angkrek Situ No.19, Sumedang, Jawa Barat 45323, tepl/(0261)210223,Indonesia
**Korespondensi penulis: a22100130@mhs.stmik-sumedang.ac.id*

Abstract. *The increasing reliance on information technology (IT) across various sectors has led to the growing importance of managing IT risks effectively. Information technology systems are prone to a variety of risks, including cybersecurity threats, system failures, and human errors. These risks can have severe consequences, such as financial loss, data breaches, and operational disruptions. To address these challenges, organizations must adopt comprehensive risk management strategies. This literature-based study explores various approaches and frameworks for managing IT risks, such as ISO 27001, NIST, and OCTAVE, by reviewing existing research and methodologies. The study aims to identify best practices, challenges, and trends in the field of IT risk management, offering insights into how organizations can improve their risk management strategies to enhance the resilience of their IT systems. Through this literature review, the paper highlights the importance of a systematic approach to IT risk management and provides recommendations for organizations seeking to mitigate risks and safeguard their technological.*

Keywords*: ISO 27001, IT Security, MRTI, NIST, OCTAVE.*

Abstrak. Ketergantungan yang semakin besar pada teknologi informasi (TI) di berbagai sektor telah meningkatkan pentingnya pengelolaan risiko TI secara efektif. Sistem teknologi informasi rentan terhadap berbagai risiko, termasuk ancaman keamanan siber, kegagalan sistem, dan kesalahan manusia. Risiko- risiko ini dapat memiliki dampak yang serius, seperti kerugian finansial, pelanggaran data, dan gangguan operasional. Untuk mengatasi tantangan ini, organisasi harus mengadopsi strategi manajemen risiko yang komprehensif. Studi berbasis literatur ini mengeksplorasi berbagai pendekatan dan kerangka kerja dalam mengelola risiko TI, seperti ISO 27001, NIST, dan OCTAVE, dengan meninjau penelitian dan metodologi yang ada. Studi ini bertujuan untuk mengidentifikasi praktik terbaik, tantangan, dan tren dalam bidang manajemen risiko TI, serta memberikan wawasan tentang bagaimana organisasi dapat meningkatkan strategi manajemen risikonya untuk meningkatkan ketahanan sistem TI. Melalui tinjauan literatur ini, makalah ini menyoroti pentingnya pendekatan sistematis dalam manajemen risiko TI dan memberikan rekomendasi bagi organisasi yang ingin mengurangi risiko dan melindungi aset teknologi.

Kata kunci: ISO 27001, Keamanan TI, MRTI, NIST, OCTAVE.

1. LATAR BELAKANG

Seiring dengan meningkatnya ketergantungan pada teknologi, kompleksitas risiko yang dihadapi juga semakin besar. Tidak hanya serangan dari pihak luar yang semakin canggih, seperti serangan ransomware dan malware, tetapi juga potensi risiko yang datang dari kelemahan internal organisasi, seperti kesalahan konfigurasi sistem, kelalaian dalam pengelolaan data, atau kurangnya kesadaran keamanan di kalangan pengguna (Kesehatan et al., 2024). Risiko ini dapat menyebabkan kerugian yang signifikan bagi organisasi, baik dalam bentuk kerugian finansial, reputasi, maupun gangguan operasional yang dapat menghambat kelangsungan bisnis (Kuncoro et al., 2023; Sinaga & Rochmoeljati, 2024).

Received Februari 13, 2025; Revised Februari 27, 2025; Accepted Maret 12, 2025; Published Maret 15, 2025

Strategi Manajemen Risiko Teknologi Informasi (MRTI) berfokus pada identifikasi, evaluasi, dan mitigasi risiko yang berkaitan dengan penggunaan TI. Dengan adanya strategi ini, organisasi dapat meminimalkan potensi ancaman dan memitigasi dampaknya. Proses ini melibatkan berbagai langkah penting, mulai dari penilaian risiko yang berkelanjutan, pengembangan kebijakan dan prosedur pengamanan, hingga pelatihan dan kesadaran keamanan bagi semua pemangku kepentingan. Penerapan MRTI yang efektif memerlukan pendekatan yang komprehensif dan disesuaikan dengan kebutuhan serta karakteristik risiko yang dihadapi oleh setiap organisasi (Ariyanto, 2024).

Penelitian mengenai MRTI berbasis studi literatur bertujuan untuk mengidentifikasi berbagai pendekatan dan strategi yang telah diterapkan oleh organisasi dalam mengelola risiko TI. Dalam kajian literatur, berbagai framework dan model manajemen risiko sering dijadikan rujukan, seperti ISO 27001, NIST, dan OCTAVE. Studi literatur ini juga menggali metodologi yang digunakan dalam penilaian risiko, baik yang berbasis kuantitatif maupun kualitatif. Dengan memanfaatkan hasil-hasil penelitian terdahulu, studi literatur ini dapat memberikan wawasan yang lebih dalam mengenai praktik terbaik yang dapat diadopsi oleh organisasi untuk meningkatkan ketahanan sistem informasi terhadap risiko yang ada. Melalui pendekatan ini, diharapkan dapat ditemukan berbagai temuan yang berguna untuk merumuskan rekomendasi bagi pengelolaan risiko TI yang lebih efektif dan efisien (Setiawan et al., 2021).

Dengan memanfaatkan hasil-hasil penelitian terdahulu, studi literatur ini dapat memberikan wawasan yang lebih dalam mengenai praktik terbaik yang dapat diadopsi oleh organisasi untuk meningkatkan ketahanan sistem informasi terhadap risiko yang ada. Melalui pendekatan ini, diharapkan dapat ditemukan berbagai temuan yang berguna untuk merumuskan rekomendasi bagi pengelolaan risiko TI yang lebih efektif dan efisien. Selain itu, penelitian ini juga dapat memberikan kontribusi terhadap pengembangan kebijakan dan standar yang lebih baik dalam manajemen risiko TI, guna memastikan bahwa organisasi dapat bertahan dan berkembang meskipun menghadapi ancaman yang semakin kompleks (Evinia & Sitokdana, 2023).

2. KAJIAN TEORITIS

Kajian teoretis dalam pengelolaan risiko teknologi informasi (TI) mencakup beberapa teori dan pendekatan yang relevan. Berikut adalah dua poin utama:

Teori Manajemen Risiko Umum dan Keamanan Informasi:

Kajian ini mengidentifikasi teori-teori yang mendasari manajemen risiko, termasuk teori manajemen risiko umum dan teori keamanan informasi. Tujuannya adalah untuk

memberikan pemahaman yang lebih mendalam mengenai konsep-konsep dasar dalam manajemen risiko TI (MRTI).

Perbandingan Pendekatan dan Model:

Penelitian ini juga membandingkan berbagai pendekatan dalam pengelolaan risiko TI, seperti standar internasional ISO 27001, framework NIST, dan OCTAVE. Setiap model dianalisis untuk menilai kelebihan, kekurangan, serta implementasi praktisnya dalam konteks pengelolaan risiko TI.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur atau literature review untuk mengeksplorasi, menganalisis, dan menyintesis informasi yang tersedia dalam bidang manajemen risiko teknologi informasi (MRTI). Studi literatur ini bertujuan untuk mengidentifikasi dan menilai berbagai teori, model, serta strategi yang telah dikembangkan dan diterapkan dalam pengelolaan risiko TI (Atmojo & Manuputty, 2020).

Tahap selanjutnya adalah pencarian literatur yang relevan, yang mencakup artikel jurnal, buku, laporan penelitian, dan dokumen resmi dari lembaga atau organisasi internasional. Pencarian literatur dilakukan melalui berbagai basis data akademik, seperti Google Scholar, Scopus, Springer, dan IEEE Xplore, yang dikenal memiliki kualitas sumber yang tinggi dalam bidang ini. Proses pencarian dilakukan dengan menggunakan kata kunci yang spesifik, seperti "manajemen risiko teknologi informasi", "strategi pengelolaan risiko TI", "ISO 27001", "NIST framework", dan lainnya, untuk memastikan hasil pencarian yang relevan (Fahlepi et al., 2023). Kriteria pemilihan sumber literatur meliputi:

1) Publikasi yang terbit dalam 5-10 tahun terakhir, untuk memastikan informasi yang digunakan bersifat up-to-date dan mencerminkan perkembangan terbaru dalam bidang MRTI.
2) Sumber yang kredibel dan diakui dalam bidang manajemen risiko dan teknologi informasi, seperti jurnal internasional yang bereputasi, buku teks dari penerbit terkemuka, serta laporan dan pedoman dari lembaga-lembaga yang memiliki otoritas, seperti ISO, NIST, dan organisasi terkait lainnya.
3) Relevansi literatur dengan topik penelitian, yang berkaitan dengan pendekatan, metode, dan strategi dalam MRTI, dengan fokus pada pengelolaan risiko TI di berbagai sektor.

Setelah literatur yang relevan ditemukan, tahap selanjutnya adalah menganalisis dan menyintesis informasi dari berbagai sumber. Proses analisis ini dilakukan secara sistematis dan mencakup beberapa langkah penting(Hom et al., 2020), yaitu:

1) Identifikasi Teori dan Konsep Utama

   Pada tahap ini, peneliti akan menyaring teori-teori utama yang mendasari manajemen risiko TI. Beberapa teori yang akan diidentifikasi meliputi teori manajemen risiko umum, teori keamanan informasi, teori sistem, dan pendekatan berbasis risiko lainnya yang digunakan dalam konteks TI. Hal ini bertujuan untuk memberikan pemahaman yang lebih mendalam mengenai dasar-dasar konsep yang ada dalam MRTI.

2) Perbandingan Pendekatan dan Model:

   Selanjutnya, penelitian akan membandingkan berbagai pendekatan yang ada dalam pengelolaan risiko TI. Ini termasuk standar internasional seperti ISO 27001, framework NIST (National Institute of Standards and Technology), dan OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Setiap model akan dianalisis untuk menilai kelebihan, kekurangan, serta implementasi praktis dari setiap pendekatan dalam konteks pengelolaan risiko TI. Perbandingan ini penting untuk mengetahui sejauh mana masing-masing model bisa diadaptasi dan diimplementasikan sesuai dengan kebutuhan organisasi.

3) Tren dan Tantangan dalam MRTI:

   Tahap berikutnya adalah menyusun temuan terkait dengan tantangan yang dihadapi oleh organisasi dalam menerapkan MRTI. Tren terbaru dalam pengelolaan risiko TI juga akan diidentifikasi, termasuk tantangan-tantangan baru yang muncul akibat perkembangan teknologi, seperti ancaman dari teknologi baru (misalnya kecerdasan buatan, IoT, dan blockchain), serta peningkatan serangan siber yang semakin kompleks. Selain itu, faktor- faktor eksternal, seperti regulasi pemerintah dan standar industri, juga akan dibahas untuk melihat bagaimana hal ini mempengaruhi penerapan strategi MRTI dalam organisasi.

Setelah analisis dilakukan, hasil dari berbagai literatur yang telah dipelajari akan disintesis untuk mengidentifikasi kesamaan dan perbedaan di antara berbagai pendekatan yang ada. Peneliti juga akan menggali temuan-temuan yang relevan dan merumuskan kesimpulan serta rekomendasi yang dapat berguna bagi organisasi dalam mengelola risiko TI secara lebih efektif dan efisien. Melalui sintesis ini, penelitian bertujuan untuk memberikan kontribusi bagi pengembangan strategi manajemen risiko TI yang lebih adaptif dan responsif terhadap ancaman yang semakin berkembang (Ramadhintia & Bisma, 2021).

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil studi literatur yang dilakukan, berbagai pendekatan dan strategi telah diidentifikasi dalam mengelola risiko teknologi informasi (TI) . Di bawah ini disajikan hasil yang diperoleh terkait dengan berbagai model manajemen risiko TI yang digunakan oleh organisasi serta tantangan dalam penerapannya. Berbagai model dan kerangka kerja yang diterapkan dalam pengelolaan risiko TI, berdasarkan studi literatur, di antaranya adalah:

1) ISO/IEC 27001

Kerangka kerja yang berfokus pada keamanan informasi melalui pendekatan sistem manajemen keamanan informasi (ISMS). Model ini mengutamakan perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi.

a. Kelebihan:
   a) Pendekatan yang sistematis dan terstruktur, memungkinkan organisasi untuk mengidentifikasi dan mengelola risiko dengan cara yang berkelanjutan.
   b) Diakui secara internasional, sehingga meningkatkan kepercayaan stakeholder.

b. Kekurangan:
   a) Membutuhkan biaya implementasi yang tinggi, termasuk pelatihan dan audit.
   b) Sulit diakses oleh organisasi kecil yang memiliki keterbatasan sumber daya.

c. Penerapan:

Banyak digunakan oleh perusahaan besar, terutama yang beroperasi di sektor keuangan, perbankan, dan kesehatan, yang memiliki persyaratan ketat terhadap keamanan data.

d. Kompleksitas Implementasi:

ISO/IEC 27001 membutuhkan dokumentasi yang rinci dan pengawasan yang ketat terhadap semua proses manajemen keamanan informasi. Proses audit yang dilakukan secara berkala memastikan kepatuhan terhadap standar ini, namun juga menambah beban administratif organisasi.

e. Konteks Global:

Standar ini sangat relevan untuk organisasi yang beroperasi di lingkungan internasional karena membantu memastikan kesesuaian dengan peraturan lintas negara seperti GDPR di Uni Eropa.

2) NIST (National Institute of Standards and Technology)

Model ini berfokus pada keamanan siber dan menyediakan panduan komprehensif untuk mitigasi risiko serta pemulihan dari insiden TI.

a. Kelebihan:
    a) Menawarkan fleksibilitas dalam adaptasi, memungkinkan organisasi untuk merespons ancaman yang berkembang, seperti ransomware dan serangan phishing.
    b) Memiliki dokumentasi teknis yang mendalam dan panduan implementasi yang praktis.
b. Kekurangan:
    a) Memerlukan tingkat pemahaman teknis yang tinggi, sehingga sulit diimplementasikan oleh organisasi dengan sumber daya manusia yang terbatas.
    b) Tidak semua elemen dalam framework dapat diterapkan tanpa penyesuaian.
c. Penerapan:

    Sangat efektif untuk sektor yang rentan terhadap ancaman siber, seperti energi, transportasi, dan manufaktur.
d. Kapasitas Penyesuaian:

    NIST menawarkan fleksibilitas dalam penyesuaian terhadap kebutuhan organisasi. Misalnya, Framework Cybersecurity NIST mencakup lima fungsi inti: Identifikasi, Proteksi, Deteksi, Respons, dan Pemulihan. Fungsi-fungsi ini memandu organisasi dalam membangun strategi komprehensif terhadap risiko TI.
e. Kelebihan Terkait Skalabilitas:

    Pendekatan modular dari NIST memungkinkan penerapan bertahap sesuai prioritas risiko, sehingga cocok untuk berbagai skala organisasi.

3) OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation):

Menekankan penilaian risiko berbasis aset dan ancaman kritis terhadap aset tersebut.

a. Kelebihan:
    a) Cocok untuk organisasi kecil atau menengah dengan sumber daya terbatas.
    b) Fleksibilitas dalam mengidentifikasi risiko spesifik pada aset yang paling kritis.
b. Kekurangan:
    a) Kurang adaptif terhadap ancaman yang terus berubah.
    b) Fokusnya terbatas pada aset dan tidak selalu mencakup ancaman yang lebih luas.

c. Penerapan:

Sering digunakan oleh organisasi dengan struktur TI yang lebih sederhana, seperti lembaga pendidikan atau bisnis kecil.

d. Pendekatan Berbasis Risiko Prioritas:

OCTAVE mengidentifikasi aset-aset yang paling kritis untuk organisasi dan memberikan perhatian khusus pada perlindungan aset tersebut. Hal ini membuat OCTAVE menjadi pilihan populer di organisasi dengan anggaran terbatas atau kebutuhan spesifik.

e. Keterbatasan Perkembangan:

OCTAVE kurang responsif terhadap ancaman dinamis seperti serangan berbasis AI atau otomatisasi malware, yang saat ini menjadi tren utama di lanskap keamanan siber.

Berikut adalah tabel yang menunjukkan ringkasan penerapan masing-masing model dan kerangka kerja dalam mengelola risiko TI:

Tabel 1

Model/Kerangka Kerja	Fokus Utama	Kelebihan	Kekurangan
ISO/IEC 27001	Keamanan informasi dan sistem manajemen keamanan	Pendekatan sistematis, standar internasional yang diakui	Biaya implementasi yang tinggi, membutuhkan sumber daya besar
NIST	Keamanan siber dan manajemen risiko TI	Komprehensif, berfokus pada ketahanan dan respons terhadap ancaman	Memerlukan adaptasi terhadap kebutuhan spesifik organisasi
OCTAVE	Penilaian risiko berbasis aset dan ancaman kritis	Pendekatan berbasis aset, cocok untuk organisasi dengan sumber daya terbatas	Kurang fleksibel dalam menghadapi ancaman yang terus berkembang

Table 1. Kerang Kerja

Selain kelebihan dan kekurangan masing-masing model, studi literatur juga mengidentifikasi beberapa tantangan umum yang dihadapi organisasi dalam menerapkan MRTI:

a. Perkembangan Ancaman yang Cepat

Ancaman siber terus berkembang, terutama dengan meningkatnya penggunaan teknologi baru seperti kecerdasan buatan, IoT, dan cloud computing.

b. Keterbatasan Sumber Daya:

Organisasi kecil sering kali tidak memiliki anggaran atau tenaga kerja yang cukup untuk mengadopsi model yang kompleks seperti ISO/IEC 27001.

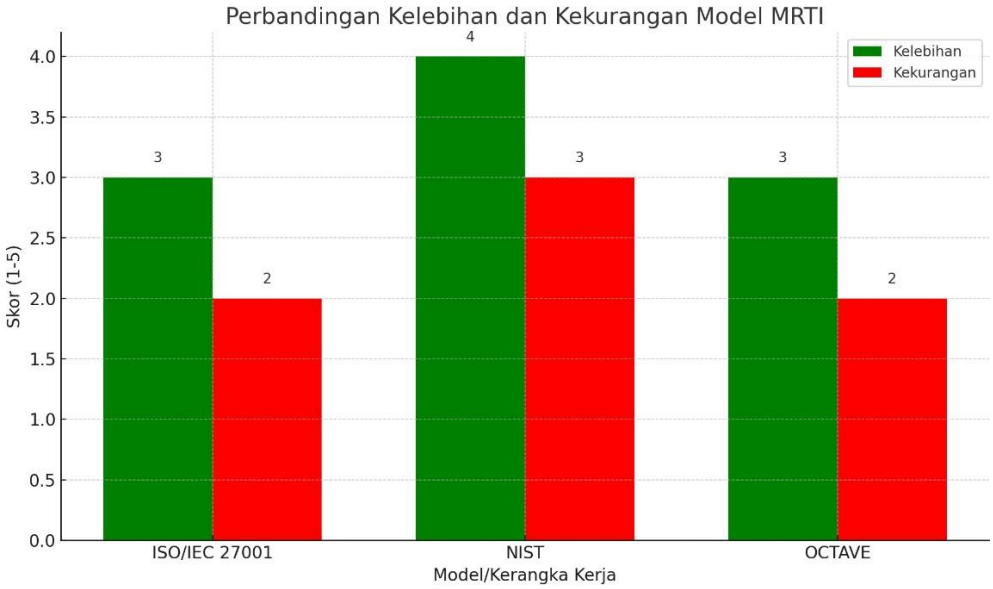
c. Kesadaran Stakeholder yang Rendah:

Implementasi MRTI memerlukan dukungan penuh dari manajemen puncak hingga staf operasional. Rendahnya pemahaman tentang pentingnya pengelolaan risiko sering kali menjadi hambatan.

Berdasarkan hasil analisis, penggunaan kerangka kerja seperti ISO 27001 dan NIST terbukti memberikan pendekatan yang komprehensif dalam mengelola risiko TI.

a. ISO 27001, sebagai standar internasional untuk sistem manajemen keamanan informasi (ISMS), banyak diterapkan oleh organisasi besar untuk melindungi data sensitif dan memastikan kepatuhan terhadap regulasi keamanan informasi. Model ini menawarkan pendekatan yang terstruktur dengan penekanan pada pengelolaan risiko yang berkelanjutan. Namun, implementasinya membutuhkan sumber daya yang signifikan, terutama untuk pelatihan dan audit berkal.
b. NIST, dengan panduan terperinci untuk keamanan siber, menawarkan pendekatan yang lebih teknis dan berfokus pada ancaman yang berkembang, seperti serangan ransomware dan kebocoran data. Pendekatan ini memungkinkan organisasi untuk lebih responsif terhadap ancaman siber dan merencanakan pemulihan dengan lebih baik. Akan tetapi, penerapan NIST memerlukan pemahaman mendalam tentang teknik keamanan dan mungkin tidak mudah diimplementasikan oleh organisasi yang lebih kecil atau yang memiliki keterbatasan sumber daya.
c. OCTAVE, dengan pendekatan berbasis aset, memberikan solusi yang lebih fleksibel dan dapat diadaptasi oleh berbagai jenis organisasi. Model ini memungkinkan organisasi untuk menilai dan memitigasi risiko yang spesifik pada aset yang paling kritis. Meski begitu, OCTAVE tidak cukup responsif terhadap perubahan ancaman yang cepat, yang menjadi tantangan utama dalam menghadapi risiko yang terus berkembang.

Grafik yang menunjukkan perbandingan antara kelebihan dan kekurangan dari tiga model manajemen risiko teknologi informasi (MRTI) yang sering diterapkan oleh organisasi, yaitu ISO/IEC 27001, NIST, dan OCTAVE.



Gambar 1. Grafik Perbandingan

a. ISO/IEC 27001

Memiliki kelebihan dalam memberikan pendekatan sistematis dan merupakan standar internasional yang diakui. Namun, biaya implementasi yang tinggi dan kebutuhan sumber daya yang besar menjadi tantangan utama.

b. NIST

Menawarkan pendekatan yang komprehensif dan berfokus pada ketahanan terhadap ancaman, seperti serangan ransomware. Namun, model ini memerlukan pemahaman teknis yang mendalam dan adaptasi yang lebih sulit bagi organisasi dengan sumber daya terbatas.

c. OCTAVE

Memiliki kelebihan dalam memberikan pendekatan berbasis aset yang fleksibel dan cocok untuk organisasi dengan sumber daya terbatas. Namun, kurang responsif terhadap ancaman yang terus berkembang, sehingga menjadi kelemahan utama.

Dalam Peningkatan Ancaman Cyber berdasarkan laporan terbaru, serangan ransomware meningkat secara eksponensial dalam lima tahun terakhir. Serangan ini tidak hanya menargetkan perusahaan besar tetapi juga organisasi kecil yang tidak memiliki pertahanan memadai. Perkembangan teknologi baru adopsi teknologi seperti Internet of Things (IoT), kecerdasan buatan (AI), dan blockchain membawa tantangan baru dalam manajemen risiko TI.

a. IoT meningkatkan jumlah perangkat yang terhubung, memperbesar area serangan.
b. AI memberikan keuntungan signifikan dalam analisis ancaman tetapi juga

meningkatkan kompleksitas ancaman, karena pelaku kejahatan menggunakan AI untuk otomatisasi serangan.

Dengan peraturan dan kepatuhan yang semakin ketat regulasi seperti GDPR, HIPAA, dan CCPA semakin menekan organisasi untuk mematuhi standar keamanan tinggi, terutama dalam melindungi data pelanggan. Berdasarkan data dari studi literatur, berikut adalah distribusi penggunaan model MRTI dalam berbagai sektor industri:

Tabel 2. Data Pengguna MRTI

Sektor Industri	ISO/IEC 27001	NIST	OCTAVE
Keuangan	75%	60%	30%
Pemerintahan	65%	80%	25%
Pendidikan	50%	40%	60%
Kesehatan	70%	55%	35%
Teknologi	80%	75%	45%

Data ini menunjukkan bahwa setiap sektor memiliki preferensi terhadap model MRTI tertentu sesuai dengan kebutuhan, skala, dan tantangan yang dihadapinya. Pemilihan model yang tepat, atau kombinasi dari beberapa model, sangat penting untuk mencapai pengelolaan risiko yang optimal dalam menghadapi lanskap ancaman yang terus berkembang.

a. Sektor Keuangan

Sektor keuangan menunjukkan dominasi penerapan ISO/IEC 27001 dengan tingkat penggunaan sebesar 75%, diikuti oleh NIST sebesar 60%, dan OCTAVE sebesar 30%. Hal ini mencerminkan fokus sektor keuangan pada standar internasional untuk menjaga kepatuhan terhadap regulasi ketat seperti PCI DSS (Payment Card Industry Data Security Standard). ISO/IEC 27001 memberikan struktur sistematis dalam mengelola keamanan data sensitif, seperti informasi keuangan dan transaksi pelanggan. NIST digunakan untuk meningkatkan keamanan siber dalam menghadapi ancaman seperti penipuan digital dan ransomware, sementara OCTAVE lebih jarang digunakan karena fokusnya yang terbatas pada aset tertentu.

b. Sektor Pemerintahan

Sektor pemerintahan cenderung lebih banyak menggunakan NIST (80%) dibandingkan ISO/IEC 27001 (65%) dan OCTAVE (25%). Dominasi NIST disebabkan oleh panduannya yang dirancang untuk sektor publik, terutama di Amerika Serikat, yang memerlukan pedoman teknis untuk perlindungan data nasional dan keamanan siber. ISO/IEC 27001 juga cukup banyak diterapkan untuk memastikan kepatuhan pada standar internasional, terutama di negara- negara yang memiliki hubungan kerja sama

global. OCTAVE digunakan secara minimal karena kompleksitas kebutuhan sektor pemerintahan sering kali melampaui cakupan model ini.

c. Sektor Pendidikan

Dalam sektor pendidikan, OCTAVE memiliki penerapan tertinggi sebesar 60%, mengungguli ISO/IEC 27001 (50%) dan NIST (40%). Hal ini karena banyak institusi pendidikan menghadapi keterbatasan anggaran dan memilih pendekatan berbasis aset yang lebih hemat biaya. OCTAVE membantu institusi untuk melindungi aset penting seperti data mahasiswa dan riset akademik. Meskipun demikian, ISO/IEC 27001 dan NIST juga digunakan, terutama oleh institusi besar yang memiliki kemampuan untuk menerapkan pendekatan yang lebih komprehensif.

d. Sektor Kesehatan

Sektor kesehatan lebih banyak mengadopsi ISO/IEC 27001 (70%) dibandingkan NIST (55%) dan OCTAVE (35%). ISO/IEC 27001 memberikan kerangka kerja untuk melindungi informasi pasien, yang sangat penting dalam kepatuhan terhadap regulasi seperti HIPAA (Health Insurance Portability and Accountability Act). NIST digunakan untuk menangani ancaman siber, terutama serangan ransomware yang sering menyasar data medis. OCTAVE kurang populer di sektor ini karena kurangnya fleksibilitas dalam menangani ancaman yang terus berkembang.

e. Sektor Teknologi

Sektor teknologi menunjukkan penggunaan yang merata pada ketiga model, dengan ISO/IEC 27001 sebesar 80%, NIST sebesar 75%, dan OCTAVE sebesar 45%. Organisasi teknologi sering menghadapi ancaman yang sangat dinamis dan membutuhkan kombinasi pendekatan yang beragam. ISO/IEC 27001 digunakan untuk menciptakan sistem manajemen keamanan informasi yang komprehensif, sementara NIST memberikan panduan teknis untuk menangani ancaman canggih. OCTAVE digunakan untuk mengelola risiko pada aset tertentu, seperti data pelanggan atau perangkat keras kritis.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil studi literatur mengenai Strategi Manajemen Risiko Teknologi Informasi (MRTI), dapat disimpulkan bahwa penerapan strategi MRTI yang efektif sangat penting bagi organisasi untuk mengelola berbagai risiko yang timbul akibat pemanfaatan teknologi informasi. Tiga model utama yang banyak digunakan, yaitu ISO/IEC 27001, NIST,

dan OCTAVE, menawarkan pendekatan yang berbeda namun saling melengkapi dalam pengelolaan risiko TI. ISO/IEC 27001 fokus pada sistem manajemen keamanan informasi yang terstruktur, NIST menawarkan pedoman yang lebih spesifik pada keamanan siber, sementara OCTAVE lebih berfokus pada penilaian berbasis aset dan ancaman kritis.

Meskipun masing-masing model memiliki kelebihan, tantangan terbesar yang dihadapi oleh organisasi adalah perkembangan ancaman yang cepat, keterbatasan sumber daya, dan rendahnya kesadaran stakeholder tentang pentingnya pengelolaan risiko TI yang sistematis. Oleh karena itu, keberhasilan penerapan MRTI bergantung pada kemampuan organisasi untuk memilih model yang sesuai dengan kebutuhan spesifik, serta mengalokasikan sumber daya yang cukup untuk mendukung implementasinya.

Pentingnya kolaborasi antara manajemen puncak dan seluruh pihak terkait dalam organisasi menjadi faktor kunci agar strategi MRTI dapat berjalan efektif. Pendidikan dan pelatihan yang berkelanjutan mengenai risiko TI, serta pembaruan kebijakan yang konsisten, juga menjadi elemen penting dalam memperkuat ketahanan organisasi terhadap ancaman TI yang terus berkembang.

Organisasi disarankan untuk memilih dan menerapkan kerangka kerja manajemen risiko TI yang sesuai, seperti ISO/IEC 27001, NIST, atau OCTAVE, berdasarkan kebutuhan dan kapasitasnya. Peningkatan kesadaran dan kompetensi stakeholder melalui pelatihan rutin sangat penting untuk memastikan keterlibatan semua pihak. Selain itu, alokasikan sumber daya yang memadai untuk keamanan TI, termasuk investasi dalam perangkat lunak, infrastruktur, dan pelatihan. Penilaian risiko secara berkala perlu dilakukan untuk mengantisipasi ancaman yang terus berkembang. Kolaborasi antar departemen harus diperkuat untuk mendukung implementasi MRTI, dan organisasi juga perlu menyiapkan serta menguji rencana pemulihan bencana untuk memastikan kesiapan menghadapi risiko yang tidak terduga.

DAFTAR REFERENSI

Ariyanto, S. (2024). Analisis framing model Robert N. Entman tentang serangan ransomware pada PT Bank Syariah Indonesia Tbk. *Jurnal CommLine, 9*(1), 59–77.

Ash Siddiqi, H. I., Darwiyanto, E., & Priyadi, Y. (2023). IT risk management analysis on Bank XYZ e-banking service system using ISO 31000. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika), 8*(1), 211–217. https://doi.org/10.29100/jipi.v8i1.3325

Atmojo, S. A., & Manuputty, A. D. (2020). Analisis manajemen risiko teknologi informasi menggunakan ISO 31000 pada aplikasi AHO Office. *Jurnal MDP, 7*(3). http://jurnal.mdp.ac.id

Evinia, E., & Sitokdana, M. N. N. (2023). Risk management based IT analysis using ISO 31000 (Case Study: PT Bawen Mediatama). *Journal of Information Systems and Informatics, 5*(1), 380–390. https://doi.org/10.51519/journalisi.v5i1.420

Fahlepi, R., Fronita, M., Saputra, E., Luthfi Hamzah, M., Marsal, A., Daulay, S., Islam Negeri Sultan Syarif Kasim Riau, U., & Tinggi Teknologi Pekanbaru, S. (2023). Analisis manajemen risiko IT pada sistem informasi akademik menggunakan ISO 31000. *Jurnal Sains Komputer & Informatika (J-SAKTI, 7*(2)).

Hidayat, R., & Suryani, D. (2022). Implementasi manajemen risiko TI pada pengelolaan data mahasiswa di universitas. *Jurnal Teknik Informatika, 15*(3), 113–122.

Hom, J., Anong, B., Rii, K. B., Choi, L. K., & Zelina, K. (2020). The OCTAVE Allegro method in risk management assessment of educational institutions. *Aptisi Transactions on Technopreneurship (ATT), 2*(2), 167–179. https://att.aptisi.or.id/index.php/att/article/view/103

Kesehatan, P., Kepentingan Majduddin, P., & Kunang, Y. N. (2024). Analisis kritis atas tantangan dan strategi manajemen risiko teknologi informasi di Rumah Sakit Ernaldi Bahar: Panduan praktis untuk. *Journal of Information Technology and Society, 2*(1). https://jits.unmuhbabel.ac.id/

Kuncoro, S. D., Ghaisan, R. A., Zaky, M. U., Wulansari, A., & Artikel, S. (2023). Manajemen risiko pada teknologi informasi: Studi kasus pada perusahaan jasa. *Jurnal Ilmiah Sain dan Teknologi, 1*(3).

Ramadhintia, R., & Bisma, R. (2021). Analisis manajemen risiko aplikasi ujian online dengan metode OCTAVE Allegro pada lembaga pendidikan. *Jurnal Sistem dan Teknologi Informasi, 6*(2). http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

Rokhimin, R., & Akbar, M. (2023). Penerapan ISO 31000 pada manajemen risiko TI di perusahaan distribusi barang. *Jurnal Ilmu Komputer dan Sistem Informasi, 8*(2), 215–225.

Sartika, D., & Subagja, F. (2023). Manajemen risiko IT untuk mengurangi risiko operasional pada aplikasi perbankan. *Jurnal Manajemen Sistem Informasi, 12*(2), 99–109.

Setiawan, I., Sekarini, A. R., Waluyo, R., & Afiana, F. N. (2021). Manajemen risiko sistem informasi menggunakan ISO 31000 dan standar pengendalian ISO/EIC 27001 di Tripio Purwokerto. *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, 20*(2), 389–396. https://doi.org/10.30812/matrik.v20i2.1093

Sinaga, B., & Rochmoeljati, R. (2024). Analisis manajemen risiko aset teknologi informasi dan pemeliharaan aset menggunakan quantitative risk analysis WH-TGR. *Industri, 27*(1). http://univ45sby.ac.id/ejournal/index.php/industri/index

Wahyuningsih, S. D., & Hidayah, N. (2023). Evaluasi penerapan manajemen risiko TI pada sistem informasi rumah sakit. *Jurnal Teknologi dan Sistem Informasi, 9*(1), 85–94.