Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 1, Januari 2025
http://doi.org/10.33395/remik.v9i1.14302
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Peran Risk Communication dan Risk Training dalam Mendukung Manajemen Risiko Cyber Security

[1]*Fitriya Mawadah Warohmah, [2] Ilham
[1,2] Universitas Islam Negeri Sunan Ampel
Surabaya, Indonesia

[1]09020622027@student.uinsby.ac.id, [2] ilham@uinsa.ac.id

*Penulis Korespondensi
Diajukan : 06/12/2024
Diterima : 15/12/2024
Dipublikasi : 06/01/2025

ABSTRAK
Penelitian ini bertujuan untuk menganalisis peran *Risk Communication* dan *Risk Training* dalam mendukung manajemen risiko, khususnya dalam konteks keamanan siber. Populasi penelitian mencakup literatur yang relevan terkait manajemen risiko, komunikasi risiko, dan pelatihan risiko dalam organisasi, termasuk jurnal ilmiah, laporan teknis, dan studi kasus. Teknik pengambilan sampel dilakukan dengan *purposive sampling*, berfokus pada sumber-sumber yang membahas topik keamanan siber dan strategi mitigasi risiko. Metode penelitian menggunakan pendekatan studi pustaka dengan analisis kualitatif untuk mengidentifikasi hubungan antara *Risk Communication, Risk Training*, dan efektivitas sistem manajemen risiko. Hasil penelitian menunjukkan bahwa *Risk Communication* yang efektif memainkan peran penting dalam memastikan informasi terkait risiko, langkah mitigasi, dan ancaman yang mungkin terjadi dapat disampaikan kepada seluruh pemangku kepentingan organisasi, mulai dari staf operasional hingga manajemen puncak. Hal ini mempercepat respons terhadap ancaman, menciptakan pemahaman kolektif, dan meminimalkan dampak ketidaksiapan organisasi dalam menghadapi serangan siber. Sementara itu, *Risk Training* dirancang untuk membekali karyawan dengan keterampilan praktis, seperti mengenali, menilai, dan merespons ancaman siber, melalui pendekatan simulasi dan studi kasus nyata. Pelatihan yang berkelanjutan memastikan karyawan tetap tanggap terhadap ancaman yang terus berkembang. Kesimpulannya, integrasi antara *Risk Communication* dan *Risk Training* menghasilkan sinergi yang memperkuat manajemen risiko organisasi secara keseluruhan. Dengan adaptasi terhadap perkembangan teknologi dan ancaman siber yang terus berubah, organisasi dapat meningkatkan kesiapan, ketahanan, serta keberlanjutan operasi mereka, sekaligus melindungi aset penting dari dampak ancaman siber.

Kata Kunci: Keamanan Siber, Manajemen Risiko, *Risk Communication*, *Risk Training*

I. PENDAHULUAN

Dalam era digital yang semakin maju, risiko terhadap keamanan siber telah menjadi perhatian utama bagi banyak organisasi. Teknologi yang berkembang pesat memberikan keuntungan besar, namun juga meningkatkan kerentanan terhadap ancaman yang kompleks dan beragam. Berbagai serangan siber, seperti *phishing*, *malware*, dan serangan DDoS (*Distributed Denial of Service*), dapat merusak integritas data, mengganggu operasi bisnis, dan merugikan reputasi perusahaan (Barafort et al., 2019). Oleh karena itu, pengelolaan risiko yang tepat melalui pendekatan proaktif, seperti *risk*

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 1, Januari 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i1.14302 p-ISSN : 2541-1332

training dan *risk communication*, menjadi sangat penting untuk menjaga kelangsungan operasi organisasi (Abrams & Greenhawt, 2020).

Risk training adalah proses memberikan pengetahuan dan keterampilan kepada karyawan agar mereka mampu mengidentifikasi, menilai, dan mengelola risiko yang mungkin terjadi. Pelatihan ini mencakup berbagai topik, mulai dari pengenalan ancaman siber hingga metode pencegahan dan mitigasi risiko (Kure et al., 2018). Tujuan utama dari *risk training* adalah memastikan setiap individu dalam organisasi memiliki pemahaman yang mendalam tentang potensi ancaman serta mampu mengambil tindakan yang tepat dalam menghadapi situasi berisiko. Dengan pelatihan yang efektif, organisasi dapat membangun pertahanan yang lebih kuat terhadap berbagai ancaman (Hamir, 2021).

Namun, pelatihan saja tidak cukup jika tidak diimbangi dengan komunikasi risiko yang baik. *Risk communication* adalah proses menyampaikan informasi tentang risiko kepada semua pemangku kepentingan dalam organisasi. Informasi ini mencakup penjelasan tentang potensi risiko, dampak yang mungkin terjadi, dan langkah-langkah mitigasi yang harus diambil (Abrams & Greenhawt, 2020). Komunikasi risiko yang efektif memastikan bahwa semua anggota organisasi, dari manajemen hingga staf operasional, memiliki pemahaman yang sama mengenai ancaman yang dihadapi dan langkah-langkah yang perlu diambil untuk mengelolanya (Demek et al., 2018).

Dalam konteks keamanan siber, *risk communication* sering kali menjadi tantangan karena sifat ancaman yang terus berubah. Organisasi harus mampu beradaptasi dengan cepat terhadap perkembangan ancaman baru, dan ini memerlukan alur komunikasi yang jelas dan terstruktur. Tanpa komunikasi yang baik, tindakan mitigasi yang diambil mungkin tidak akan berjalan efektif, dan ini dapat meningkatkan kemungkinan terjadinya insiden yang merugikan (Adebisi et al., 2021).

Kombinasi antara pelatihan risiko dan komunikasi risiko merupakan fondasi penting dalam menciptakan lingkungan kerja yang aman dan sadar akan risiko. Kedua elemen ini saling melengkapi: *risk training* memberikan pengetahuan dasar kepada karyawan, sementara *risk communication* memastikan bahwa informasi penting disebarluaskan dengan cara yang tepat kepada semua pihak terkait. Dalam lingkungan bisnis yang dinamis, koordinasi antara pelatihan dan komunikasi menjadi kunci untuk menciptakan ketahanan terhadap ancaman siber (Kure et al., 2018).

Saat sebuah organisasi menghadapi ancaman baru, *risk training* dapat memberikan panduan tentang langkah-langkah praktis untuk mencegah atau mengurangi dampaknya. Namun, tanpa komunikasi yang jelas mengenai ancaman tersebut, staf mungkin tidak menyadari urgensi situasi atau tanggung jawab mereka dalam menangani risiko. Oleh karena itu, keberhasilan strategi manajemen risiko sangat bergantung pada seberapa baik informasi tersebut disampaikan dan dipahami di seluruh tingkatan organisasi.

Selain itu, komunikasi risiko yang efektif juga menciptakan budaya transparansi dalam organisasi. Karyawan merasa lebih terlibat ketika mereka dilibatkan dalam diskusi mengenai risiko dan diberikan akses terhadap informasi yang relevan. Hal ini dapat meningkatkan rasa tanggung jawab individu dan kolektif dalam menjaga keamanan data dan sistem. Dengan komunikasi yang baik, setiap karyawan dapat menjadi bagian dari solusi dalam menghadapi ancaman siber.

Pelatihan risiko yang berkelanjutan juga sangat penting mengingat bahwa ancaman siber tidak statis, melainkan terus berkembang. Organisasi perlu memperbarui program pelatihan mereka secara berkala untuk mengatasi ancaman terbaru dan menyesuaikan metode mitigasi yang digunakan. Pelatihan yang sudah usang atau tidak relevan lagi dapat memberikan rasa aman yang palsu dan membuat organisasi lebih rentan terhadap serangan baru (Hamir, 2021).

Pada akhirnya, sinergi antara *risk training* dan *risk communication* memberikan landasan yang kuat bagi manajemen risiko organisasi. Melalui pelatihan yang efektif dan komunikasi yang transparan, organisasi dapat membangun kesadaran risiko yang menyeluruh, meningkatkan kesiapan dalam menghadapi ancaman, dan memastikan bahwa semua anggota tim memiliki pengetahuan dan alat yang mereka butuhkan untuk melindungi aset penting organisasi (Barafort et al., 2019; Kure et al., 2018).

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 1, Januari 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i1.14302 p-ISSN : 2541-1332

II. STUDI LITERATUR

Penelitian Terdahulu

Manajemen risiko merupakan disiplin yang sangat penting dalam organisasi modern, terutama di era digital yang dipenuhi oleh ancaman siber. Risiko dalam konteks ini adalah kemungkinan peristiwa yang dapat berdampak negatif terhadap organisasi, termasuk kerusakan pada aset fisik, gangguan operasional, atau kehilangan data, (Barafort et al., 2019). Oleh karena itu, pelatihan risiko (*risk training*) dan komunikasi risiko (*risk communication*) telah menjadi elemen inti dari strategi manajemen risiko yang efektif. Kedua konsep ini tidak hanya fokus pada identifikasi dan mitigasi risiko, tetapi juga memastikan bahwa semua pihak dalam organisasi memahami dan siap menangani ancaman yang ada. Terdapat beberapa langkah dalam menentukan manajemen resiko, (Hamir, 2021) sebagai berikut:

Langkah 1 - Lingkup, Konteks, dan Kriteria

Langkah pertama adalah menetapkan konteks internal dan eksternal organisasi, ruang lingkup manajemen risiko, tujuan, keputusan yang perlu dibuat, jangka waktu, dan sumber daya. Konteks ini mencakup pemahaman terhadap lingkungan internal dan eksternal organisasi. Selain itu, organisasi juga perlu mengembangkan kriteria risiko yang akan digunakan.

Langkah 2 - Penilaian Risiko

Penilaian risiko mencakup tiga langkah:

- Identifikasi Risiko: Proses untuk menemukan, mengenali, dan mendeskripsikan risiko.
- Analisis Risiko: Mempertimbangkan secara rinci ketidakpastian, sumber risiko, konsekuensi, kemungkinan kejadian, skenario, dan efektivitas kontrol.
- Evaluasi Risiko: Membandingkan hasil analisis risiko dengan kriteria risiko yang ditetapkan pada langkah pertama.

Langkah 3 - Penanganan Risiko

Penanganan risiko adalah proses untuk memodifikasi risiko. Langkah ini bertujuan untuk memilih dan menerapkan opsi-opsi yang dapat mengatasi risiko tersebut.

Langkah 4 - Pemantauan dan Peninjauan

Pada tahap ini, organisasi memantau dan meninjau efektivitas rencana penanganan risiko, strategi, dan sistem manajemen yang telah diterapkan untuk mengelola risiko secara efektif.

Langkah 5 - Komunikasi dan Konsultasi

Tujuan dari langkah ini adalah membantu para pemangku kepentingan memahami risiko, dasar pengambilan keputusan, dan alasan mengapa tindakan tertentu diperlukan.

Langkah 6 - Pencatatan dan Pelaporan

Langkah ini bertujuan untuk meningkatkan aktivitas manajemen risiko serta memfasilitasi interaksi dengan pemangku kepentingan dan pihak yang bertanggung jawab dalam kegiatan manajemen risiko.

Pelatihan risiko dan komunikasi risiko tidak dapat berjalan secara terpisah dalam pengelolaan risiko IT siber, (Kure et al., 2018). Keduanya saling melengkapi dan bersama-sama membentuk sistem manajemen risiko yang holistik. Pelatihan memberikan landasan pengetahuan teknis, sementara komunikasi risiko memastikan bahwa informasi terbaru tentang ancaman disampaikan dengan tepat waktu dan dipahami oleh semua anggota organisasi.

III. METODE

Metode penelitian yang digunakan dalam penelitian ini adalah **studi pustaka** yang merujuk pada jurnal-jurnal sebelumnya. Dalam penelitian ini, beberapa langkah dilakukan untuk mengkaji

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 1, Januari 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i1.14302 p-ISSN : 2541-1332

peran *Risk Communication* dan *Risk Training* dalam manajemen risiko, khususnya di konteks keamanan siber. Langkah-langkah tersebut adalah sebagai berikut:

Langkah 1 – Mencari sumber data sekunder

Mencari dan mengidentifikasi jurnal, buku, laporan penelitian, dan literatur lain yang relevan dengan *Risk Communication*, *Risk Training*, dan manajemen risiko, khususnya yang berkaitan dengan keamanan siber di organisasi.

Langkah 2 – Melakukan literatur review

Melakukan kajian pustaka secara mendalam untuk memahami konsep-konsep utama terkait komunikasi risiko dan pelatihan risiko. Literatur yang dibaca mencakup teori-teori manajemen risiko, studi kasus dari organisasi lain, dan praktik terbaik yang terkait dengan mitigasi risiko.

Langkah 3 – Mengelompokkan sumber pustaka sesuai kebutuhan

Mengelompokkan sumber pustaka berdasarkan tema atau topik yang relevan, misalnya: kelompok *Risk Communication*, kelompok *Risk Training*, dan manajemen risiko. Hal ini memudahkan dalam menganalisis dan menyusun laporan.

Langkah 4 – Mengambil sumber data pustaka

Mengambil informasi dari jurnal dan literatur yang telah dikelompokkan. Data yang relevan digunakan untuk menyusun argumen dan mendukung analisis tentang bagaimana *Risk Communication* dan *Risk Training* diterapkan dalam organisasi.

Langkah 5 – Pelaporan

Menyusun laporan akhir yang memaparkan hasil penelitian dari studi pustaka tersebut. Laporan ini menjelaskan bagaimana *Risk Communication* dan *Risk Training* mendukung manajemen risiko dalam organisasi, dengan fokus pada penerapan di konteks keamanan siber.

IV. HASIL DAN PEMBAHASAN

Program Risk Training

Tujuan: Program *Risk Training* ini bertujuan untuk membekali karyawan dengan keterampilan dan pengetahuan yang diperlukan untuk mengenali, menilai, dan merespons ancaman risiko, terutama terkait dengan keamanan siber. Melalui pelatihan ini, karyawan akan mampu menerapkan praktik keamanan terbaik dan memahami peran mereka dalam menjaga integritas sistem dan data organisasi.

Sasaran: Karyawan dari berbagai level, terutama yang terlibat langsung dalam operasional IT, keamanan siber, serta staf lain yang berinteraksi dengan data sensitif.

Durasi Pelatihan : 3 Hari (6 Jam per Hari)

Metode Pelatihan:

Hari 1: Sesi tatap muka dengan penjelasan teori (ancaman siber, mitigasi risiko, penilaian risiko).

Hari 2: Sesi simulasi ancaman siber (*cyber attack simulation*) dan respons insiden.

Hari 3: Ujian atau tes simulasi, *workshop* penyusunan kebijakan mitigasi, dan penutupan.

Agenda Risk Training

Tabel 1. Agenda Risk Training

Hari	Topik	Deskripsi	Durasi
Hari 1	**Pengantar Risiko dan Ancaman Siber**	- Pengenalan tentang konsep risiko. - Penjelasan tentang ancaman siber utama: *Phishing*, malware, DDoS, dan *social engineering*.	3 Jam
	Penilaian Risiko	- Teknik mengidentifikasi risiko di lingkungan organisasi. - Cara menilai dampak dan kemungkinan risiko.	3 Jam
Hari 2	**Simulasi Ancaman Siber**	- Simulasi serangan siber pada jaringan organisasi (*cyber attack simulation*). - Praktik langsung penanganan insiden siber.	4 Jam

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 1, Januari 2025
http://doi.org/10.33395/remik.v9i1.14302
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Hari	Topik	Deskripsi	Durasi
	Mitigasi Risiko	- Pengenalan dan penerapan kontrol keamanan: penggunaan *firewall*, enkripsi data, sistem autentikasi, serta pemantauan aktivitas jaringan.	2 Jam
Hari 3	**Ujian atau Tes Simulasi**	- Ujian tertulis atau simulasi respons terhadap ancaman.	2 Jam
	Workshop Penyusunan Kebijakan Mitigasi	- Penyusunan kebijakan mitigasi berdasarkan ancaman yang dihadapi oleh organisasi. - Diskusi dan kolaborasi antara peserta mengenai strategi keamanan terbaik.	3 Jam
	Penutupan dan Evaluasi	- Diskusi terbuka mengenai hasil pelatihan. - Evaluasi program pelatihan melalui survei peserta.	1 Jam

***Materi Pelatihan**:*

Pengantar Risiko dan Ancaman Siber
- Definisi risiko siber.
- Jenis-jenis ancaman siber (misalnya: *Phishing*, malware, ransomware, serangan *zero-day*).
- Dampak ancaman terhadap organisasi.

Penilaian Risiko
- Identifikasi aset berharga organisasi.
- Teknik penilaian risiko: Analisis dampak dan probabilitas.
- Matriks risiko: Penggunaan untuk menentukan prioritas penanganan risiko.

Mitigasi Risiko
- Strategi mitigasi: Pengendalian preventif, detektif, dan korektif.
- Penerapan teknologi keamanan: *Firewall*, enkripsi, dan *Intrusion Detection System* (IDS).
- Penggunaan autentikasi ganda (MFA) dan kebijakan kata sandi yang aman.

Simulasi Ancaman Siber
- Praktik simulasi serangan DDoS.
- Latihan *phishing* email dan bagaimana mengenalinya.
- Tanggapan terhadap ancaman: Mengisolasi sistem yang terinfeksi dan langkah-langkah pemulihan.

Kebijakan dan Prosedur Respons Insiden
- Proses laporan insiden.
- Alur komunikasi selama insiden siber.
- Tindakan segera untuk mitigasi kerusakan akibat serangan siber.

Evaluasi dan Feedback
- Penilaian keterampilan melalui simulasi atau ujian.
- Umpan balik dari peserta untuk meningkatkan program pelatihan.

Program Risk Communication

Tujuan: Tujuan dari *Risk Communication* ini adalah memastikan bahwa informasi mengenai ancaman, risiko, dan langkah-langkah mitigasi disampaikan dengan jelas dan tepat waktu kepada semua pemangku kepentingan, termasuk manajemen, karyawan, dan pihak eksternal yang relevan. Program ini bertujuan untuk menciptakan kesadaran bersama dan mendukung respons yang cepat dan efektif terhadap risiko yang mungkin terjadi, terutama dalam konteks keamanan siber.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 1, Januari 2025
http://doi.org/10.33395/remik.v9i1.14302
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Sasaran: Seluruh karyawan, mulai dari staf teknis hingga manajemen, serta pemangku kepentingan eksternal seperti mitra bisnis dan vendor yang terkait dengan operasional organisasi.
Saluran Komunikasi:

- **Email dan Buletin Internal**: Saluran utama untuk menyampaikan informasi risiko terbaru dan pembaruan terkait ancaman.
- **Intranet dan Portal Keamanan**: Platform yang menyediakan akses ke kebijakan keamanan, prosedur tanggap darurat, serta pembaruan rutin mengenai risiko.
- **Rapat Reguler (*Townhall* dan *Divisional Meetings*)**: Pertemuan berkala untuk membahas risiko terkini dan respons organisasi terhadap ancaman.
- **Media Sosial Internal/Platform Kolaborasi**: Sistem komunikasi cepat seperti Slack, Microsoft Teams, atau platform lainnya untuk mempercepat distribusi informasi risiko. **Pelatihan dan Webinar**: Sesi berkala untuk membahas ancaman siber terbaru, perubahan dalam kebijakan, dan peningkatan risiko.

Tabel 2. Agenda Risk Communication

Komponen	Deskripsi	Frekuensi
Email Risiko Rutin	Pengiriman email rutin yang berisi pembaruan mengenai ancaman siber terbaru dan langkah mitigasi.	Mingguan/Bulanan
Peringatan Risiko Mendesak	Email atau notifikasi khusus ketika ada ancaman serius yang membutuhkan perhatian segera.	Sesuai kebutuhan
Portal Informasi Risiko	Penyediaan portal di intranet untuk akses ke informasi risiko, panduan keamanan, dan laporan insiden.	Terus-menerus
Rapat Risiko Bulanan	Pertemuan rutin antara tim manajemen risiko dan tim TI untuk membahas ancaman terkini.	Bulanan
Webinar dan Pelatihan Online	Sesi online yang membahas ancaman baru, kebijakan keamanan, atau studi kasus insiden risiko.	Triwulan
Laporan Risiko Terpadu	Laporan risiko yang didistribusikan kepada manajemen puncak untuk menilai tingkat risiko keseluruhan.	Triwulan/Per-Kejadian
Sistem Pelaporan Insiden	Saluran resmi bagi karyawan untuk melaporkan potensi risiko atau insiden yang mencurigakan.	Sesuai kebutuhan

Elemen Risk Communication

1. **Kejelasan Pesan**:
   Pesan yang dikomunikasikan harus jelas, singkat, dan mudah dipahami oleh semua pihak, termasuk karyawan non-teknis. Ini penting untuk memastikan bahwa semua orang dapat mengambil tindakan yang sesuai ketika menghadapi risiko.
2. **Aksesibilitas Informasi**:
   Semua informasi terkait risiko harus tersedia dan mudah diakses oleh karyawan, termasuk kebijakan keamanan, prosedur mitigasi, dan langkah-langkah tanggap darurat. Portal intranet khusus atau aplikasi internal harus digunakan untuk mendistribusikan informasi risiko.
3. **Keteraturan Komunikasi**:
   Komunikasi risiko harus dilakukan secara teratur. Pembaruan rutin mengenai ancaman, pembaruan kebijakan, dan laporan insiden harus dikomunikasikan melalui email atau rapat rutin. Ini memastikan bahwa karyawan selalu terinformasi tentang risiko terbaru.
4. **Penyebaran Informasi Risiko Mendesak**:

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 1, Januari 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i1.14302 p-ISSN : 2541-1332

Jika ada ancaman serius seperti serangan siber yang sedang berlangsung atau kerentanan baru yang ditemukan, peringatan harus segera dikirimkan melalui email, platform kolaborasi, atau aplikasi komunikasi cepat. Informasi ini harus mencakup langkah-langkah mitigasi segera yang perlu diambil.

5. **Koordinasi Antar Tim**:
   Komunikasi risiko harus melibatkan berbagai departemen, termasuk TI, manajemen risiko, dan operasional. Rapat koordinasi rutin akan membantu memastikan bahwa semua pihak terkait memahami risiko yang sedang dihadapi dan bagaimana mereka berkontribusi dalam mitigasi risiko tersebut.
6. **Tanggapan terhadap Insiden**:
   Setiap karyawan harus mengetahui saluran pelaporan insiden dan prosedur respons ketika risiko terjadi. Komunikasi tentang insiden yang sedang terjadi, termasuk penilaian risiko dan langkah-langkah pemulihan, harus dilakukan secara cepat dan jelas.
7. **Pendidikan Berkelanjutan**:
   Komunikasi risiko juga melibatkan edukasi berkelanjutan melalui pelatihan dan webinar yang memberikan informasi tentang ancaman terbaru, teknologi keamanan baru, dan perubahan kebijakan risiko. Ini memastikan bahwa karyawan selalu mengikuti perkembangan terbaru dalam keamanan siber.

V. KESIMPULAN

Risk Communication dan *Risk Training* merupakan elemen kunci dalam mendukung manajemen risiko, terutama di bidang keamanan siber. *Risk Communication* sangat penting untuk memastikan bahwa informasi mengenai risiko, ancaman, dan langkah-langkah mitigasi disampaikan secara efektif kepada seluruh pemangku kepentingan di organisasi. Dengan komunikasi yang jelas dan terstruktur, karyawan dapat lebih memahami risiko yang dihadapi dan bertindak sesuai dengan prosedur mitigasi yang telah ditetapkan. Sementara itu, *Risk Training* berperan dalam membekali karyawan dengan keterampilan yang diperlukan untuk mengenali dan merespons ancaman siber. Pelatihan yang berkelanjutan membantu meningkatkan kesadaran karyawan terhadap ancaman yang terus berkembang, sekaligus memperkuat kemampuan mereka dalam menangani insiden keamanan. Integrasi yang baik antara *Risk Communication* dan *Risk Training* memungkinkan organisasi menjadi lebih tangguh dalam menghadapi risiko dan mengurangi dampak negatif dari ancaman yang mungkin terjadi. Dengan penerapan yang konsisten, organisasi dapat meningkatkan kesiapan dan respons mereka terhadap risiko, terutama dalam era digital yang semakin kompleks. Selain itu, penelitian dapat difokuskan pada pengembangan kerangka kerja komprehensif yang mengintegrasikan *Risk Communication* dan *Risk Training* dengan teknologi berbasis kecerdasan buatan (*Artificial Intelligence*) untuk deteksi dini dan respons cepat terhadap ancaman siber.

VI. REFERENSI

Abrams, E. M., & Greenhawt, M. (2020). Risk communications during Covid-19. *The Journal of Allergy and Clinical Immunology*, *8*(6), 1791–1794.

Adebisi, Y. A., Rabe, A., & Lucero-Prisno, D. E. (2021). Risk communication and community engagement strategies for COVID-19 in 13 African countries. *Health Promotion Perspectives*, *11*(2), 137–147. https://doi.org/10.34172/hpp.2021.18

Ahmad, B. M., Ahmed, S. M., & Sylvanus, D. E. (2023). Enhancing Phishing Awareness Strategy Through Embedded Learning Tools: A Simulation Approach. *Archives of Advanced Engineering Science*, *XX*(December), 1–14. https://doi.org/10.47852/bonviewaaes32021392

Barafort, B., Mesquida, A. L., & Mas, A. (2019). ISO 31000-Based Integrated Risk Management Process Assessment Model for IT Organizations. Journal of Software: Evolution and Process, 31(1). https://doi.org/10.1002/smr.1984

Baranoff, E., Brockett, P. L., & Kahane, Y. (2009). *Risk Management for Enterprises and Individuals*. Flat World Knowledge, L.L.C.

Bensaada, I., & Taghezout, N. (2019). An enterprise risk management system for SMEs: Innovative design paradigm and risk representation model. *Small Enterprise Research*, 26(2), 179–206. https://doi.org/10.1080/13215906.2019.1624190

Crane, L., Gantz, G., Isaacs, S., Jose, D., & Sharp, R. (2013). *Introduction to Risk Management: Understanding Agricultural Risk* (2nd ed.). Extension Risk Management Education and Risk Management Agency. http://www.extensionrme.org/pubs/IntroductionToRiskManagement.pdf

Demek, K. C., Raschke, R. L., Janvrin, D. J., & Dilla, W. N. (2018). Do organizations use a formalized risk management process to address social media risk? *International Journal of Accounting Information Systems*, 28, 31–44. https://doi.org/10.1016/j.accinf.2017.12.004

Duong, L. (2009). Influence of risk management in operations of small-medium enterprises and micro companies: A case study for Viope Solutions Ltd. *Arcada University of Applied Sciences*.

Hamir, H. (2021). An Analysis of Risk Management Processes and Comparison with ISO31000:2018. *Asian Journal of Research in Business and Management*, *December 2021*. https://doi.org/10.55057/ajrbm.2021.3.4.3

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, *8*(6). https://doi.org/10.3390/app8060898

Technical Committee ISO/TC 262. (2018). ISO 31000:2018(en) Risk management — Guidelines. International Organization for Standardization. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Xu, Y. (2020). A review of cyber security risks of power systems: from static to dynamic false data attacks. *Protection and Control of Modern Power Systems*, *5*(1). https://doi.org/10.1186/s41601-020-00164-w

Verbano, C., & Venturini, K. (2013). Managing Risks In SMEs: A Literature Review And Research Agenda. Journal of Technology Management and Innovation, 8(3), 186–197. https://doi.org/10.4067/s0718-27242013000400017

Zoghi, F. S. (2017). Risk Management Practices And SMEs: An Empirical Study On Turkish SMEs. International Journal of Trade, Economics and Finance, 8(2), 123–127. https://doi.org/10.18178/ijtef.2017.8.2.550