Literatur Review

Nama : Septya Kurnia Azzahra

NPM : 227006516065

Mata Kuliah : Metodologi Penelitian/ R.02

Dosen : Nur Hayati

NO.	CITE	JUDUL	SUMBER DATA	METODE	HASIL
Luar Negeri					
1	Schneller, L., Porter, C. N., & Wakefield, A. (2022). Implementing converged Security risk management: drivers, barriers, and facilitators. Security Journal, 36(2), 333–349. https://doi.org/10.	Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators	Penelitian ini menggunakan data primer yang dikumpulkan melalui wawancara semi-terstruktur dengan delapan profesional keamanan senior dari Eropa, Australasia, dan Timur Tengah. Peserta mewakili berbagai spesialisasi keamanan termasuk keamanan TI, keamanan fisik, dan kelangsungan bisnis di sektor swasta dan pemerintah, dengan pengalaman di bidang logistik, energi, keamanan siber, teknologi informasi, otomotif, dan pertahanan nasional.	• Metode yang digunakan dalam penelitian ini mencakup wawancara semi-terstruktur dengan delapan profesional keamanan senior, yang dilakukan secara daring melalui platform Skype dan Zoom antara Februari dan Maret 2020. Penelitian ini juga memanfaatkan literatur dan studi yang ada tentang konvergensi, termasuk penelitian	• Hasil penelitian menyoroti pentingnya pelatihan dan pendidikan, serta soft skills, dalam upaya pendekatan konvergensi yang efektif. Penelitian tersebut juga menemukan bahwa kurangnya definisi tunggal atau pemahaman tentang konvergensi mengaburkan temuan, dan bahwa pendekatan konvergensi yang cocok untuk semua orang mungkin tidak efektif atau bahkan tidak memungkinkan. Studi tersebut menemukan bahwa merekrut orang dengan keahlian yang tepat dianggap sangat penting, dan bahwa kepemimpinan upaya konvergensi dapat didasarkan

	1057/s41284-022-00341-6			ASIS Foundation dan Laporan Risiko Global 2016 dari Forum Ekonomi Dunia. • Penelitian ini menggunakan pendekatan kualitatif, dengan wawancara mendalam yang dilakukan dengan delapan profesional keamanan perusahaan senior, dan data dianalisis menggunakan pendekatan tematik, dengan mengidentifikasi pendorong, hambatan, dan fasilitator konvergensi keamanan.	pada budaya, kepribadian, hubungan, atau bahkan kebetulan. • Hasil penelitian menunjukkan bahwa pendorong konvergensi keamanan meliputi serangan siber, penipuan, dan reputasi organisasi, sedangkan hambatannya meliputi peran organisasi tradisional, kurangnya kepercayaan, dan faktor pribadi individu, dan fasilitatornya meliputi keterampilan pribadi yang diinginkan, konseptualisasi keamanan dan manajemen risiko, dan struktur organisasi yang efektif. • Hasil penelitian menyoroti pentingnya soft skills yang kuat, satu pandangan tentang risiko, dan pendekatan organisasi kolaboratif dalam mempromosikan manajemen keamanan konvergen. Studi tersebut juga menemukan bahwa pendidikan dan pelatihan sangat penting untuk membentuk keterampilan bisnis dan komunikasi yang penting bagi praktisi keamanan.

2	Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security, 105*, 102239. https://doi.org/10.1016/j.cose.2021.102239	Cyber-threat perception and risk management in the Swedish financial sector	• Survei kuantitatif terhadap 42 peserta dari sektor keuangan Swedia. • Wawancara mendalam dengan 5 pimpinan konferensi kerja sama dalam simulasi krisis nasional sektor keuangan. • Data dikumpulkan selama dan setelah latihan manajemen krisis nasional FSPOS pada tahun 2018.	Penelitian ini menggunakan metode campuran (mixed methods) yang terdiri dari: • Survei kuesioner yang dikembangkan dari penelitian sebelumnya untuk mengukur kebutuhan informasi dalam membentuk Common Operational Picture (COP) dan tingkat Cyber Situational Awareness (CSA). • Wawancara semi-terstruktur untuk mendalami persepsi ancaman siber dan tantangan dalam pembentukan	• Sektor keuangan Swedia memiliki pemahaman yang tinggi terhadap krisis, namun belum sistematis dalam mengelola informasi terkait aktor ancaman jangka panjang. • Ancaman siber dipersepsikan sebagai risiko besar terhadap infrastruktur teknis, layanan IT, dan reputasi organisasi. • Terdapat keinginan kuat untuk membangun common operational picture (COP) sebagai sarana berbagi informasi situasional antarorganisasi. • Integrasi personel TI ke dalam tim manajemen krisis direkomendasikan untuk memperkuat manajemen risiko siber.

				CSA pada tingkat industri.	
3	Temitope, A. O., Adedayo, L. Y., & Kareem, B. (2023). *Cybersecurity Risk Management in Agile Development: Protecting Data and System*. *International Journal of Science and Research Archive*, 8(1), 988–994. https://doi.org/10.30574/ijsra.2023.8.1.0188	Cybersecurity Risk Management in Agile Development: Protecting Data and System	• Studi literatur komprehensif dari berbagai sumber terkait keamanan siber dalam pengembangan Agile • Laporan industri dari Cybersecurity Ventures dan CISO Magazine • Studi kasus pelanggaran keamanan (Capital One 2019, Target 2013) • Standar keamanan internasional seperti ISO/IEC 27001	• Analisis deskriptif terhadap integrasi praktik keamanan dalam pengembangan Agile • Penilaian risiko dilakukan melalui Continuous Risk Assessment, Threat Modeling dan User Story Analysis • Pendekatan DevSecOps sebagai kerangka mitigasi risiko siber dalam Agile	• Diidentifikasi lima risiko utama: data breaches, insider threats, third-party vulnerabilities, insecure coding, dan kurangnya security testing • 72% tim Agile tidak memiliki proses penilaian keamanan formal yang terintegrasi ke dalam alur kerja mereka • Strategi mitigasi mencakup: Penerapan DevSecOps, Otomatisasi pengujian keamanan dan Pelatihan keamanan berkelanjutan • Budaya sadar keamanan dibangun melalui komunikasi terbuka, kebijakan yang jelas, dan pengangkatan “security champions” • Studi kasus (Capital One & Target) menunjukkan efektivitas integrasi keamanan ke dalam proses Agile
4	Wang, Z., & Liu, X. (2022). *Cyber security of railway cyber-physical system (CPS) – A risk*	Cyber security of railway cyber-physical system (CPS) – A risk	• Studi kasus retrospektif terhadap sistem Advanced Train Control System (ATCS) yang digunakan di	• Penelitian ini mengembangkan dan mengusulkan metodologi manajemen	• Sistem ATCS memiliki kerentanan serius akibat penggunaan radio 900 MHz tanpa enkripsi, yang telah dimanfaatkan oleh komunitas

	management methodology. Communications in Transportation Research, 2, 100078. https://doi.org/10.1016/j.commtr.2022.100078	management methodology	banyak perusahaan kereta api barang di Amerika Serikat. • Data teknis ATCS dikumpulkan dari dokumentasi sistem, pengamatan terhadap praktik industri, dan simulasi berbasis model. • Simulasi penyerangan DoS menggunakan perangkat lunak khusus berbasis Python dan NetworkX.	risiko siber khusus untuk sistem kereta CPS (rail-CPS), dengan pendekatan iteratif berbasis NIST framework. • Metodologi mencakup tahapan: 1. Identifikasi ancaman dari komponen fisik ke komponen siber 2. Dekonstruksi teknis untuk model alur serangan dan interaksi siber-fisik 3. Analisis konsekuensi melalui pemodelan simulasi (contoh: penundaan kereta akibat DoS) 4. Strategi mitigasi dan solusi pemulihan,	eavesdropper selama lebih dari 15 tahun. • Ancaman spoofing Blue Block berpotensi menembus mekanisme fail-safe sistem vital dan menyebabkan pengaktifan sinyal yang membahayakan. • Simulasi DoS menunjukkan bahwa satu jam serangan DoS dapat menyebabkan penundaan kumulatif 24,9 jam kereta dan waktu pemulihan 8,6 jam pada jalur tunggal. • Mitigasi vital threat mencakup penguatan verifikasi administratif dan prosedur voice communication, serta peningkatan aturan operasional. • Mitigasi teknis mencakup transisi ke teknologi komunikasi baru (misal 5G, Wi-Fi mesh), backup menggunakan fiber optik atau jaringan lokal, serta penggunaan sistem cadangan seperti PTC atau GSM-R.

				serta perulangan proses (looping) • Pendekatan studi kasus dilakukan pada sistem CTC-ATCS, dengan dua ancaman: • Ancaman vital seperti serangan spoofing terhadap sistem Blue Block • Ancaman non-vital seperti serangan DoS pada saluran komunikasi radio ATCS	
5	Salin, H., & Lundgren, M. (2022). *Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams*. *Journal of Cybersecurity and Privacy*, 2(2), 276–291. https://doi.org/10.3390/jcp2020015	Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams	• Studi literatur terhadap 15 artikel pada database: IEEE Xplore, ACM Digital Library, Google Scholar. • Survei terhadap 145 pengembang perangkat lunak dari 8 organisasi di Swedia (industri konsultan, finansial, pemerintahan).	• Literature review berbasis 5 tantangan utama dari Oueslati et al. (2015): C1: Software Development Life Cycle C2: Incremental Development C3: Security Assurance C4: Awareness and	• Dihasilkan framework manajemen risiko keamanan siber untuk proyek agile dengan 5 langkah utama: 1. Risk Collection: identifikasi risiko harian saat daily stand-up. 2. Risk Refinement**:** evaluasi risiko lanjutan saat backlog refinement. 3. Risk Mitigation: penerapan mitigasi risiko dalam sprint. 4. Knowledge Transfer: dokumentasi pembelajaran saat retrospective.

				Collaboration C5: Security Management • Survei dengan 10 pernyataan berbasis skala Likert untuk menilai sikap terhadap solusi keamanan siber di lingkungan agile. • Analisis integrasi solusi menjadi kerangka kerja 5 langkah.	5. Escalation: pelaporan risiko ke manajemen secara iteratif. • Framework bersifat ringan, fleksibel, cocok dengan prinsip agile. • Survei menunjukkan mayoritas responden mendukung penerapan framework ini, terutama dari yang berpengalaman dalam keamanan siber dan manajemen risiko.
NO.	**CITE**	**JUDUL**	**SUMBER DATA**	**METODE**	**HASIL**
Dalam Negeri					
1	Mahendra, V., & Soewito, B. (2023). *Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber*. Techno.com, 22(3), 527–538. https://doi.org/10.33633/tc.v22i3.8491	Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber	• Observasi terhadap aplikasi di lingkungan Kementerian PUPR • Wawancara dan kuesioner kepada 33 pegawai dari total 63 target • Tinjauan dokumen internal seperti dokumen keamanan, proses bisnis, dan kebijakan aplikasi	• Penelitian dilakukan dalam beberapa tahap: • Pengumpulan data awal melalui observasi, kuesioner, dan dokumen • Penilaian kondisi saat ini terhadap keamanan aplikasi • Mitigasi kerentanan	• Identifikasi kondisi saat ini menghasilkan skor rata-rata 2,77, sementara skor kondisi yang diinginkan adalah 3,00, menandakan ada kesenjangan 0,23. • Ditemukan 32 rekomendasi yang dibagi berdasarkan fungsi keamanan: • Identify (9), Protect (11), Detect (3), Respond (5), Recover (4) • Prioritas rencana aksi terbagi menjadi:

				(khususnya SQL Injection) • Pemetaan kerangka kerja CIS Controls ke dalam kerangka kerja NIST Cybersecurity • Identifikasi kondisi saat ini dan yang diinginkan • Analisis kesenjangan dan pemberian rekomendasi • Penyusunan rencana aksi dengan prioritas (tinggi, sedang, rendah) Framework yang digunakan: • NIST CSF: Identify, Protect, Detect, Respond, Recover • CIS Controls v8: 18 kontrol	• 14 isu prioritas tinggi, 18 sedang, 0 rendah • Setelah mitigasi, tidak ditemukan lagi kerentanan tinggi (contohnya SQL Injection berhasil ditangani). • Kesimpulan: gabungan kerangka kerja NIST CSF dan CIS Controls dinilai efektif dalam membantu pengukuran kematangan keamanan siber dan pembuatan strategi manajemen risiko yang lebih terarah di lingkungan Kementerian PUPR.

				utama dan 153 sub-kontrol	
2	Tan, T., & Soewito, B. (2022). *Manajemen Risiko Serangan Siber Menggunakan Framework NIST Cybersecurity di Universitas ZXC*. *Journal of Information System, Applied, Management, Accounting and Research*, 6(2), 411–422. https://doi.org/10.52362/jisamar.v6i2.781	Manajemen Risiko Serangan Siber Menggunakan Framework NIST Cybersecurity di Universitas ZXC	• Pengumpulan data melalui observasi lapangan dan wawancara staf TI • Penilaian teknis pada 39 sistem berbasis web dengan tools Nessus • Referensi kebijakan dan standar keamanan menggunakan kerangka NIST CSF	• Penelitian dilakukan melalui pendekatan studi kasus dan analisis risiko • Tahapan utama meliputi: identifikasi sistem penting, pemindaian kerentanan, evaluasi keamanan saat ini, serta penyusunan profil keamanan target • Framework NIST digunakan sebagai dasar penilaian dan perencanaan perbaikan keamanan	• Ditemukan 7 sistem dengan risiko tinggi, 8 sistem risiko sedang, 24 risiko rendah • Rata-rata tingkat kematangan keamanan siber saat ini hanya 1,33 dari skala 3 (Partially Achieved) • Rekomendasi peningkatan keamanan untuk mencapai target profil Largely Achieved (2/3) Hasil dari penilaian menunjukan hasil kondisi keamanan siber di lingkungan Universitas ZXC masih belum mencapai standar yang direkomendasikanDari hasil penelitian ini, penulis memberikan rekomendasi control menggunakan Framework NIST Cybersecurity untuk meningkatkan keamanan siber pada sistem layanan web dan situs web.

3	Julianto, A. S., Hikmah, I. R., & Yasa, R. N. (2024). *Cyber-Risk Management Menggunakan NIST Cybersecurity*	Cyber-Risk Management Menggunakan NIST Cybersecurity Framework (CSF)	• Studi kasus pada Instansi XYZ yang bergerak di bidang komunikasi, persandian, dan statistik.	• Menggunakan kerangka kerja:
				  • NIST Cybersecurity
					• Dihasilkan 111 risiko:
					  ○ 35 kategori tinggi
					  ○ 63 sedang
					  ○ 13 rendah
					• Risiko dikategorikan dalam 5 skenario utama: serangan logis,

	Framework (CSF) dan COBIT 2019 pada Instansi XYZ. Jurnal Info Kripto, 18(2), 41–47.	dan COBIT 2019 pada Instansi XYZ	• Observasi, wawancara, dan analisis dokumen internal (Risk Register, kebijakan TI). • Identifikasi atas 28 aset, 17 ancaman, dan 13 kerentanan. • Penilaian risiko menghasilkan 111 risiko.	Framework (CSF) • COBIT 2019 • Proses terdiri dari 6 tahap utama: 1. Prioritize and Scope – Menentukan ruang lingkup, aset, dan tujuan strategis 2. Orient – Identifikasi aset, ancaman, dan kerentanan 3. Create a Current Profile – Penilaian kondisi saat ini menggunakan subkategori NIST CSF dan kapabilitas COBIT 4. Conduct Risk Assessment – Penilaian risiko dengan pendekatan NIST SP 800-30	insiden perangkat keras, kegagalan perangkat lunak, masalah SDM, dan manajemen data. • Instansi XYZ menetapkan target 20 subkategori NIST CSF untuk ditingkatkan ke level kapabilitas 3. • Disusun 12 program kerja berdasarkan Work Products (WP) dan Generic Work Products (GWP) dari COBIT 2019 untuk mitigasi risiko. • Rekomendasi aktivitas meliputi: o Penetapan kebijakan dan SOP keamanan o Perencanaan dan pelaporan SMKI o Penilaian risiko periodik o Dokumentasi kasus bisnis keamanan informasi • kombinasi NIST CSF dan COBIT 2019 efektif dalam mengelola risiko keamanan siber sektor pemerintahan berbasis elektronik (SPBE).

				5. Create a Target Profile – Menentukan target level keamanan berdasarkan kapabilitas (level 3) 6. Determine, Analyze, and Prioritize Gaps – Penyusunan program kerja berbasis rekomendasi kontrol	
4	Destrianto, F. R., Nelmiawati, & Sitorus, M. A. R. (2017). *Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE*. Jurnal Integrasi, 9(1), 35–47.	Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE	• Studi kasus pada Sistem Informasi Akademik (SIA) Politeknik Negeri Batam • Pengumpulan data melalui observasi dan uji keamanan website berdasarkan standar OWASP • Analisis terhadap aset-aset informasi, jenis ancaman, dan	• Menggunakan metode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) • Tiga fase utama: 1. Identifikasi aset dan ancaman 2. Analisis kerentanan dan pengujian keamanan	• Teridentifikasi 4 kategori ancaman utama: 1. Authentication: cookie replay, sniffing, dictionary attack 2. Cryptography: encryption cracking 3. Session Management: session hijacking, replay, MITM attacks 4. Configuration Management: clickjacking

			kerentanan keamanan sistem	(authentication, session management, cryptography, configuration) 3. Manajemen risiko seperti strategi perlindungan dan rencana mitigasi • Pengujian keamanan mengacu pada standar OWASP, termasuk serangan seperti SQL injection, XSS, sniffing, dan MITM (man-in-the-middle)	• Disusun strategi mitigasi risiko termasuk: • Penerapan SSL certificate untuk enkripsi • Penggunaan flag httpOnly untuk cookie • Penerapan protokol aman (HTTPS, VPN, SSH) • Pembatasan multiple login dan pengelolaan sesi • Disusun dokumen manajemen risiko sebagai panduan penguatan keamanan dan pengendalian risiko pada sistem SIA • metode OCTAVE mampu memberikan pendekatan sistematik dalam mengidentifikasi, menganalisis, dan mengelola risiko ancaman terhadap aplikasi website berbasis akademik.
5	Mulianingsih, F., Fajar, & Suharyati. (2025). *Manajemen Risiko Digital: Strategi Keamanan Siber untuk Mitigasi Ancaman di Era Revolusi Industri 4.0*. *Indonesian Research*	Manajemen Risiko Digital: Strategi Keamanan Siber untuk Mitigasi Ancaman di Era Revolusi Industri 4.0	Data diperoleh dari literatur akademik dan industri antara tahun 2019 hingga 2024, termasuk jurnal internasional (IEEE, ACM, ScienceDirect, Scopus), laporan industri (NIST, Cisco, IBM, Gartner,	Penelitian ini menggunakan metode deskriptif kualitatif melalui pendekatan penelitian kepustakaan**.** Tujuannya adalah untuk mengkaji strategi mitigasi risiko digital	• Menghasilkan kerangka 5 dimensi strategi utama**:** 1) Intelijen Ancaman Proaktif 2) Keamanan-sejak-Desain 3) Infrastruktur Berfokus Ketahanan 4) Keamanan Berpusat Manusia

	Journal on Education, 5(2), 888–898. https://irje.org/index.php/irje		WEF), serta standar regulasi (ISO/IEC, NIS2 Directive).	yang efektif di era Industri 4.0 dengan menyintesis berbagai perspektif dari literatur terkini.	5) Tata Kelola Kolaboratif • Penekanan pada integrasi aspek teknologi, manusia, organisasi, dan tata kelola untuk menghadapi ancaman cyber-physical di era Industri 4.0.