

CYBER CORRECTIONAL COMPETENCY: INOVASI PENGUATAN SDM PEMASYARAKATAN DALAM MENGHADAPI KEJAHATAN SIBER DI LEMBAGA PEMASYARAKATAN

Bima Hafizh Ramadhan

Politeknik Imigrasi Pemasyarakatan Indonesia

DOI. <https://doi.org/10.52472/jcm.v3i1.781>

Journal of Correctional
Management
2026, Vol.3 (1) 23 - 30
Politeknik Ilmu Pemasyarakatan

Review
22-05-2026

Accepted
25-06-2026

Abstract

This article develops the concept of Cyber Correctional Competency as a human-resource innovation for strengthening correctional institutions in facing cybercrime and digital-service risks. The study applies a qualitative literature-review and document-analysis approach using Indonesian correctional, personal-data, and electronic-information regulations; government cybersecurity reports; correctional information-system documents; and competency frameworks from ENISA and NIST. The analysis identifies a gap between increasingly digital correctional work and uneven cyber literacy among officers. Six competency pillars are proposed: cyber awareness, data protection, digital evidence, incident response, secure-system use, and correctional cyber intelligence. These competencies are mapped to security, registration, public service, treatment, supervision, and managerial functions. Implementation should use role-based microlearning, case studies, simulations, tabletop exercises, cyber champions, and clear escalation procedures. The main constraints are workload, unequal digital capacity, limited infrastructure, weak incident-reporting culture, inter-unit coordination, and privacy risks. A gradual, contextual, rights-based competency system can improve institutional security, data integrity, accountability, and service resilience.

Keywords : cybersecurity competency; correctional human resources; data protection; cybercrime; digital governance

Abstrak

Artikel ini mengembangkan konsep Cyber Correctional Competency sebagai inovasi manajemen sumber daya manusia untuk memperkuat kesiapan lembaga pemasyarakatan menghadapi kejahatan siber dan risiko layanan digital. Penelitian menggunakan pendekatan kualitatif melalui studi literatur dan analisis dokumen terhadap regulasi pemasyarakatan, perlindungan data pribadi, serta informasi elektronik; laporan keamanan siber pemerintah; dokumen Sistem Database Pemasyarakatan; dan kerangka kompetensi ENISA serta NIST. Hasil analisis menunjukkan adanya kesenjangan antara meningkatnya pekerjaan digital pemasyarakatan dan belum meratanya literasi siber petugas. Enam pilar kompetensi dirumuskan, yaitu cyber awareness, data protection, digital evidence, incident response, secure system, dan correctional cyber intelligence. Kompetensi tersebut dipetakan pada fungsi pengamanan, registrasi, pelayanan publik, pembinaan, pengawasan, dan manajemen. Implementasi disarankan melalui microlearning berbasis peran, studi kasus, simulasi, tabletop exercise, cyber champion, serta SOP eskalasi insiden. Tantangan utama meliputi beban kerja, kesenjangan kemampuan digital, keterbatasan sarana, budaya pelaporan, koordinasi lintas unit, dan risiko privasi. Penguatan kompetensi yang bertahap dan berbasis hak dapat meningkatkan keamanan, integritas data, akuntabilitas, serta ketahanan layanan pemasyarakatan.

Kata kunci : kompetensi siber; SDM pemasyarakatan; perlindungan data; kejahatan siber; tata kelola digital

Pendahuluan

Perkembangan teknologi digital telah mengubah cara organisasi publik berkomunikasi, mengelola data, memberikan layanan, dan mengambil keputusan. Perubahan tersebut juga berlangsung di lingkungan masyarakat. Lembaga masyarakat tidak lagi dapat dipahami hanya sebagai ruang pengamanan dan pembinaan secara fisik, karena sebagian proses kerja telah terhubung dengan sistem informasi, data elektronik, layanan komunikasi, perangkat digital, dan jaringan lintas unit. Situasi ini membawa manfaat berupa efisiensi dan konsolidasi informasi, tetapi sekaligus membuka ruang risiko baru yang tidak seluruhnya dapat dijawab dengan pola pengamanan konvensional.

Dalam praktik masyarakat, risiko digital dapat muncul melalui penyalahgunaan gawai, komunikasi elektronik terlarang, penipuan daring, pemerasan, transaksi digital ilegal, pencurian atau manipulasi data, penyalahgunaan media sosial, serta gangguan terhadap sistem informasi. Ancaman tersebut dapat melibatkan pihak dari dalam maupun luar lembaga dan sering kali memanfaatkan kelemahan manusia, seperti penggunaan kata sandi yang lemah, pembagian akun, kelalaian membuka tautan berbahaya, penggunaan perangkat pribadi untuk pekerjaan dinas, dan keterlambatan melaporkan indikasi insiden. Karena itu, keamanan siber di lingkungan masyarakat tidak dapat dibebankan hanya kepada petugas teknologi informasi.

Undang-Undang Nomor 22 Tahun 2022 tentang Masyarakat menegaskan bahwa fungsi masyarakat meliputi pelayanan, pembinaan, pembimbingan masyarakat, perawatan, pengamanan, dan pengamatan dengan menjunjung penghormatan, perlindungan, serta pemenuhan hak asasi manusia. Seluruh fungsi tersebut membutuhkan data yang akurat dan proses kerja yang dapat dipertanggungjawabkan. Pada saat yang sama, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menempatkan pengelolaan data pribadi sebagai tanggung jawab yang harus dijalankan secara aman. Data warga binaan, keluarga, petugas, kesehatan, pembinaan, remisi, dan integrasi merupakan informasi sensitif yang berisiko menimbulkan kerugian apabila diakses, diubah, atau disebarkan tanpa kewenangan.

Konteks ancaman juga terlihat pada laporan keamanan siber pemerintah. Laporan Tahunan Kamsiber 2024 yang diterbitkan Kominfo-CSIRT menggambarkan adanya trafik anomali, insiden siber, kebutuhan vulnerability assessment dan penetration testing, serta ancaman berbasis berkas berbahaya pada lingkungan instansi pemerintah (Kementerian Komunikasi dan Digital, 2025). Lanskap Keamanan Siber Indonesia 2024 juga menempatkan peningkatan ketahanan siber sebagai kebutuhan penting bagi penyelenggara layanan publik (Badan Siber dan Sandi Negara, 2025). Temuan tersebut memperlihatkan bahwa organisasi pemerintah yang mengelola data dan layanan digital perlu membangun kapasitas manusia yang sejalan dengan perkembangan risiko.

Di lingkungan masyarakat, Sistem Database Masyarakat (SDP) menjadi contoh konkret transformasi kerja berbasis informasi. Sistem tersebut mendukung pengelolaan data warga binaan dan proses kerja antara unit pelaksana teknis, kantor wilayah, dan Direktorat Jenderal Masyarakat. Keberadaan sistem digital meningkatkan kebutuhan terhadap kedisiplinan akun, pengaturan hak akses, validitas input, keamanan perangkat, dan kerahasiaan data. Kegagalan pada salah satu unsur dapat memengaruhi integritas data serta kualitas pelayanan dan pengambilan keputusan.

Permasalahan utama dalam konteks tersebut bukan sekadar kekurangan teknologi, melainkan kesenjangan kompetensi manusia yang mengoperasikan, mengawasi, dan bertanggungjawab teknologi. Kerangka Cyber Correctional Competency dalam artikel ini dikembangkan untuk menjawab kebutuhan tersebut. Konsep ini tidak bertujuan menjadikan seluruh petugas sebagai ahli keamanan siber, melainkan memastikan setiap petugas memiliki kompetensi dasar yang relevan dengan tugasnya, sementara fungsi tertentu memperoleh kemampuan lanjutan untuk pengamanan bukti digital, respons insiden, pengelolaan risiko, dan analisis pola. Artikel ini bertujuan menganalisis kondisi existing SDM masyarakat, merumuskan komponen kompetensi siber yang kontekstual, serta menyusun strategi implementasi yang bertahap, realistis, dan berkelanjutan.

Metode

Artikel ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur dan

analisis dokumen. Pendekatan tersebut dipilih karena tujuan penelitian adalah membangun kerangka konseptual kompetensi, bukan mengukur hubungan antarvariabel secara statistik. Bahan analisis terdiri atas regulasi nasional yang relevan, dokumen dan laporan pemerintah mengenai keamanan siber dan sistem informasi masyarakat, serta kerangka kompetensi keamanan siber yang menjadi rujukan internasional.

Sumber utama yang dianalisis meliputi Undang-Undang Nomor 22 Tahun 2022 tentang Pemasarakan, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Lanskap Keamanan Siber Indonesia 2024, Laporan Tahunan Kamsiber 2024, dokumen Sistem Database Masyarakat, European Cybersecurity Skills Framework dari ENISA, NICE Framework dari NIST, dan kajian mengenai kesenjangan keterampilan keamanan siber. Dokumen-dokumen tersebut dipilih karena mewakili empat dimensi analisis, yaitu mandat masyarakat, tata kelola data, ancaman siber, dan pengembangan kompetensi.

Analisis dilakukan dalam tiga tahap. Pertama, mengidentifikasi aktivitas masyarakat yang bersinggungan dengan data, perangkat, komunikasi, dan sistem elektronik. Kedua, memetakan risiko serta kebutuhan kompetensi pada fungsi pengamanan, registrasi, pelayanan publik, pembinaan, dan manajemen. Ketiga, mensintesis kebutuhan tersebut ke dalam pilar Cyber Correctional Competency serta rancangan strategi pembelajaran dan tata kelola implementasi. Hasil penelitian bersifat konseptual dan dimaksudkan sebagai dasar pengembangan kebijakan, kurikulum, serta penelitian lapangan lanjutan.

Hasil

Hasil analisis menunjukkan bahwa pekerjaan masyarakat semakin bergantung pada data dan perangkat digital, tetapi kompetensi siber belum selalu diposisikan sebagai bagian dari kompetensi inti petugas. Pada fungsi pengamanan, fokus utama masih cenderung berada pada kontrol fisik, ketertiban, lalu lintas orang dan barang, serta pencegahan gangguan keamanan secara langsung. Padahal, penyelundupan perangkat komunikasi, penggunaan akun dan aplikasi pesan, transaksi

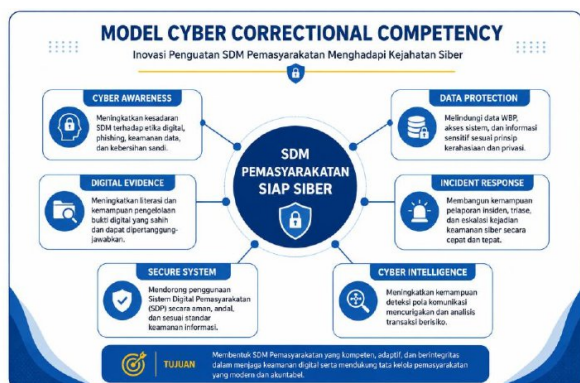
digital, serta koordinasi dengan jaringan luar dapat membentuk pola ancaman yang membutuhkan kemampuan deteksi digital dan pelaporan yang lebih sistematis.

Pada fungsi registrasi dan pengelolaan data, risiko utama berkaitan dengan kebocoran informasi, akses tidak sah, kesalahan atau manipulasi data, dan penggunaan akun yang tidak sesuai kewenangan. Petugas membutuhkan pemahaman tentang klasifikasi informasi, prinsip minimalisasi akses, kerahasiaan, akurasi, validasi, serta tanggung jawab terhadap data pribadi. Pada fungsi pelayanan publik, risiko dapat muncul melalui hoaks, penipuan yang mengatasnamakan lembaga, penyebaran informasi yang tidak terverifikasi, atau pengungkapan data yang tidak semestinya. Sementara itu, fungsi pembinaan membutuhkan literasi etika digital agar teknologi dapat digunakan sebagai sarana edukasi dan reintegrasi, bukan menjadi sumber risiko baru.

Analisis juga menunjukkan perlunya pembagian kompetensi berdasarkan peran. Seluruh petugas memerlukan literasi dasar, seperti pengelolaan kata sandi, pengenalan phishing, kehati-hatian menggunakan media sosial, keamanan perangkat, dan mekanisme pelaporan insiden. Petugas yang menangani registrasi dan data membutuhkan kemampuan perlindungan informasi yang lebih kuat. Petugas pengamanan membutuhkan kompetensi mengenali pola komunikasi atau perangkat mencurigakan. Pejabat struktural membutuhkan pemahaman mengenai manajemen risiko, tata kelola akses, prioritas respons, dan koordinasi lintas unit. Dengan demikian, model kompetensi tidak tepat apabila dibuat seragam tanpa mempertimbangkan fungsi kerja.

Berdasarkan pemetaan tersebut, Cyber Correctional Competency dirumuskan dalam enam pilar. Pertama, cyber awareness, yaitu kesadaran terhadap risiko, etika digital, phishing, penggunaan perangkat, dan kebersihan kata sandi. Kedua, data protection, yaitu kemampuan menjaga data warga binaan, keluarga, petugas, dan informasi sensitif berdasarkan hak akses dan prinsip kerahasiaan. Ketiga, digital evidence, yaitu kemampuan awal mencatat, menjaga, dan melaporkan bukti digital secara benar. Keempat, incident response, yaitu kemampuan mengenali, melakukan triase awal, mengeskalasi, mendokumentasikan, dan mendukung pemulihan insiden. Kelima, secure system, yaitu penggunaan sistem masyarakat

sesuai standar keamanan informasi. Keenam, correctional cyber intelligence, yaitu kemampuan mengenali pola komunikasi, transaksi, atau aktivitas digital yang dapat menjadi peringatan dini.



Gambar 1. Model pilar Cyber Correctional Competency

Rancangan pembelajaran yang muncul dari analisis menekankan metode yang singkat, kontekstual, dan berbasis skenario kerja. Cyber awareness dapat diberikan melalui microlearning dan kuis; perlindungan data melalui studi kasus; digital evidence melalui simulasi penemuan dan pencatatan bukti; incident response melalui tabletop exercise; sedangkan correctional cyber intelligence melalui analisis skenario komunikasi atau transaksi. Output pembelajaran tidak hanya berupa pengetahuan, tetapi kemampuan melakukan tindakan awal yang benar dan mengetahui batas kewenangan sebelum eskalasi kepada unit yang lebih kompeten.

Hambatan implementasi dapat dikelompokkan ke dalam enam area: literasi digital yang tidak merata, beban kerja tinggi, budaya takut melapor, koordinasi lintas unit yang lemah, keterbatasan sarana, dan risiko pelanggaran hak atau privasi. Kesenjangan literasi dapat ditangani melalui pemetaan kemampuan awal dan modul dasar wajib; beban kerja melalui pelatihan per shift dan microlearning; budaya pelaporan melalui mekanisme pelaporan awal yang aman; koordinasi melalui SOP eskalasi dan cyber champion; keterbatasan sarana melalui pemanfaatan learning management system serta materi sederhana; sementara risiko privasi harus dikendalikan melalui prinsip legalitas, proporsionalitas, dan perlindungan data.

Pembahasan

Cyber Correctional Competency menempatkan faktor manusia sebagai lapisan perlindungan pertama dalam tata kelola keamanan digital pemasyarakatan. Pendekatan ini sejalan dengan

realitas bahwa sistem yang baik tetap dapat terganggu ketika pengguna mengabaikan prosedur, membagikan akun, gagal mengenali rekayasa sosial, atau tidak melaporkan anomali. Karena itu, pengembangan kompetensi perlu dimulai dari perubahan kebiasaan kerja. Cyber awareness bukan materi tambahan yang berdiri sendiri, tetapi bagian dari disiplin organisasi sebagaimana kepatuhan terhadap prosedur pengamanan fisik.

Pilar cyber awareness harus dibangun melalui materi yang dekat dengan pekerjaan sehari-hari. Petugas tidak memerlukan istilah teknis yang berlebihan untuk memahami risiko dasar. Skenario seperti menerima pesan yang meminta kata sandi, membuka lampiran yang tidak dikenal, menggunakan jaringan publik, memindahkan data dinas ke perangkat pribadi, atau membagikan tangkapan layar data warga binaan dapat digunakan sebagai konteks pembelajaran. Model microlearning berdurasi singkat dan berulang lebih realistis dibandingkan pelatihan panjang karena petugas bekerja dalam sistem shift dan memiliki beban operasional yang tinggi.

Pilar data protection menjadi penting karena pemasyarakatan mengelola banyak kategori informasi sensitif. Perlindungan data tidak hanya berkaitan dengan mencegah kebocoran, tetapi juga memastikan akses diberikan sesuai tugas, data dimasukkan secara akurat, perubahan dapat ditelusuri, dan informasi tidak digunakan di luar tujuan yang sah. Prinsip ini berkaitan langsung dengan Undang-Undang Nomor 27 Tahun 2022. Dalam praktik, pelatihan dapat menggunakan studi kasus mengenai pembagian akun, permintaan data oleh pihak yang tidak berwenang, penggunaan dokumen melalui aplikasi pesan, atau kebutuhan menghapus informasi yang tidak lagi diperlukan dari perangkat kerja.

Pilar digital evidence diperlukan karena kejadian di lapas dapat menghasilkan temuan berupa perangkat, pesan, tangkapan layar, rekaman transaksi, akun, atau jejak komunikasi. Petugas garis depan tidak harus menjadi pemeriksa forensik, tetapi perlu memahami bahwa bukti digital memiliki karakter mudah berubah dan harus diperlakukan secara hati-hati. Kompetensi dasar meliputi pencatatan kondisi awal, waktu dan tempat penemuan, identitas petugas yang menangani, dokumentasi yang memadai, larangan melakukan perubahan yang tidak perlu, serta eskalasi kepada pihak yang berwenang. Pendekatan

ini membantu menjaga integritas informasi ketika temuan dikembangkan lebih lanjut.

Pilar incident response memperkuat kemampuan organisasi merespons kejadian secara cepat dan terkoordinasi. Insiden dapat berupa akun petugas yang diretas, indikasi kebocoran data, perangkat yang terinfeksi, temuan komunikasi terlarang, atau gangguan pada sistem informasi. Tanpa alur respons yang jelas, petugas dapat saling menunggu, temuan tercecer, atau tindakan awal justru memperbesar dampak. Tabletop exercise dapat digunakan untuk melatih siapa yang mencatat, siapa yang memverifikasi, siapa yang mengisolasi perangkat, siapa yang berkomunikasi dengan pimpinan, dan kapan eskalasi dilakukan.

Pilar secure system menekankan bahwa keamanan tidak hanya ditentukan oleh teknologi yang dipasang, tetapi juga oleh cara sistem digunakan. Sistem Database Masyarakat memberikan manfaat besar dalam konsolidasi data, namun efektivitasnya bergantung pada kedisiplinan pengguna. Pengelolaan akun individu, kontrol akses berbasis peran, pembaruan perangkat, pencadangan, pengamanan koneksi, dan pelaporan gangguan perlu dipahami sebagai bagian dari tata kelola kerja. Petugas harus melihat keamanan sistem sebagai instrumen untuk menjaga kesinambungan layanan, bukan sebagai hambatan administratif.

Pilar correctional cyber intelligence menghubungkan literasi digital dengan fungsi pengamanan dan pengamatan. Dalam konteks masyarakat, pola risiko dapat terlihat dari keterkaitan antara komunikasi, transaksi, identitas, waktu, perangkat, atau jaringan pihak luar. Kompetensi yang dibutuhkan pada level petugas bukan analisis intelijen teknis yang kompleks, melainkan kemampuan mengidentifikasi indikator awal, mendokumentasikan temuan, membandingkan dengan informasi yang tersedia, dan menyampaikannya melalui saluran yang tepat. Pendekatan ini membantu organisasi berpindah dari respons reaktif menuju pencegahan berbasis indikasi.

Kerangka ENISA European Cybersecurity Skills Framework dan NIST NICE Framework dapat menjadi inspirasi untuk mendefinisikan bahasa kompetensi, peran, pengetahuan, dan keterampilan secara lebih sistematis (European Union Agency for Cybersecurity, 2022; National Institute of Standards and Technology, 2024). Namun, adopsinya perlu

disesuaikan dengan karakter masyarakat Indonesia. Petugas lapas, rutan, dan Bapas memiliki fungsi yang berbeda dari profesi keamanan siber murni. Karena itu, desain kurikulum harus memprioritaskan keterampilan yang dapat langsung diterapkan dalam pengamanan, registrasi, pelayanan, pembinaan, pengawasan, dan pengambilan keputusan.

Pengembangan kompetensi juga perlu dibedakan menjadi tingkat dasar, menengah, dan pengampu. Tingkat dasar wajib bagi seluruh pegawai dan mencakup cyber awareness, perlindungan data, serta pelaporan awal. Tingkat menengah ditujukan kepada petugas yang sering menangani data, perangkat, atau kejadian keamanan. Tingkat pengampu dapat diberikan kepada cyber champion di setiap satuan kerja yang berfungsi sebagai penghubung, fasilitator pembelajaran, dan titik koordinasi awal. Cyber champion tidak menggantikan unit teknologi informasi atau aparat penegak hukum, tetapi membantu mempercepat komunikasi dan menjaga keberlanjutan budaya keamanan.

Tantangan terbesar implementasi adalah kesenjangan literasi digital. Kemampuan menggunakan aplikasi tidak selalu identik dengan kemampuan memahami keamanan. Petugas yang terbiasa dengan media sosial dan aplikasi pesan mungkin tetap rentan terhadap rekayasa sosial, penggunaan kata sandi berulang, atau pengelolaan data yang tidak aman. Oleh sebab itu, pemetaan kemampuan awal perlu dilakukan agar materi tidak terlalu sederhana bagi sebagian peserta tetapi juga tidak terlalu teknis bagi peserta lain. Hasil pemetaan dapat menjadi dasar penyusunan modul wajib dan modul lanjutan.

Beban kerja juga menjadi hambatan penting. Pelatihan panjang sulit diterapkan pada organisasi yang harus menjaga layanan dan pengamanan selama dua puluh empat jam. Solusi yang lebih realistis adalah blended learning, microlearning 10-15 menit, pelatihan per shift, kuis berkala, dan simulasi singkat. Materi dapat diberikan dalam siklus berulang agar kompetensi tidak berhenti pada satu kali sosialisasi. Pendekatan ini juga lebih mudah disesuaikan ketika muncul modus baru atau perubahan kebijakan.

Budaya pelaporan insiden perlu mendapatkan perhatian khusus. Dalam organisasi yang kuat secara hierarkis, pegawai dapat menunda pelaporan karena khawatir dianggap melakukan

penetapan cyber champion. Tahap berikutnya berupa simulasi per fungsi, SOP respons insiden, dan penguatan koordinasi. Tahap lanjutan dapat mencakup evaluasi kompetensi, pemanfaatan learning management system, pengembangan materi berbasis kasus nyata yang telah dianonimkan, dan kerja sama dengan lembaga teknis. Strategi bertahap memungkinkan inovasi dijalankan sesuai sumber daya tanpa kehilangan arah strategis.

Evaluasi kompetensi harus dirancang untuk mengukur kemampuan yang benar-benar dibutuhkan di tempat kerja. Penilaian tidak cukup hanya berupa tes pilihan ganda setelah sosialisasi, tetapi dapat dilengkapi dengan simulasi sederhana, observasi kepatuhan prosedur, respons terhadap skenario phishing, kemampuan melakukan eskalasi, dan ketepatan dokumentasi temuan. Hasil evaluasi kemudian digunakan untuk menentukan kebutuhan pelatihan ulang, materi penguatan, serta kebutuhan kompetensi lanjutan pada fungsi tertentu. Pola ini membuat pengembangan SDM menjadi siklus yang berkelanjutan dan dapat disesuaikan dengan perubahan modus ancaman.

Keberhasilan program juga dapat dikaitkan dengan indikator organisasi yang praktis, seperti kepatuhan penggunaan akun individual, kecepatan pelaporan insiden, kelengkapan dokumentasi awal, frekuensi simulasi, dan tindak lanjut terhadap temuan keamanan. Indikator tersebut tidak dimaksudkan untuk memperbanyak beban administratif, melainkan membantu pimpinan melihat apakah budaya keamanan mulai terbentuk. Evaluasi perlu tetap mempertimbangkan konteks satuan kerja agar indikator tidak menimbulkan perilaku formalistik atau mendorong pegawai menyembunyikan kesalahan demi memenuhi target.

Pada akhirnya, nilai utama Cyber Correctional Competency terletak pada integrasinya dengan pekerjaan masyarakat. Kompetensi ini tidak memindahkan fokus lembaga dari pembinaan dan reintegrasi sosial menuju urusan teknologi, tetapi memastikan transformasi digital tidak melemahkan keamanan, akuntabilitas, dan perlindungan hak. Petugas yang lebih siap secara digital dapat menjaga kualitas data, mencegah penyalahgunaan sistem, merespons insiden dengan lebih tepat, serta mendukung layanan dan pembinaan yang semakin bergantung pada teknologi.

dapat diintegrasikan dengan pembinaan pegawai yang sudah berjalan melalui *microlearning*, simulasi per shift, kuis berkala, dan evaluasi berbasis skenario. *Cyber champion* dapat ditetapkan sebagai fasilitator internal untuk memperkuat kesinambungan program, sementara kasus dan modus baru digunakan sebagai bahan pembaruan materi.

Pada tingkat operasional, setiap unit perlu memiliki mekanisme pelaporan yang sederhana, cepat, dan terdokumentasi. Penggunaan akun individual, verifikasi hak akses, pengamanan perangkat, pemisahan data dinas dari perangkat pribadi, serta dokumentasi awal temuan digital harus menjadi kebiasaan kerja. Koordinasi lintas fungsi juga perlu diuji melalui *tabletop exercise* agar alur respons dapat dilaksanakan ketika terjadi insiden nyata.

Penelitian lanjutan perlu menguji kerangka *Cyber Correctional Competency* melalui studi lapangan pada beberapa lapas, rutan, dan Bapas. Penelitian empiris dapat memetakan tingkat literasi siber petugas, menguji efektivitas modul, menilai perubahan perilaku setelah pelatihan, serta mengembangkan indikator kompetensi yang terukur. Pengujian lapangan penting agar kerangka konseptual ini dapat disempurnakan sesuai variasi sumber daya, beban kerja, dan karakter risiko di setiap satuan kerja.

Referensi

- Badan Siber dan Sandi Negara. (2025). *Lanskap Keamanan Siber Indonesia 2024*. BSSN.
- Direktorat Jenderal Pemasyarakatan. (n.d.-a). *Sistem Database Pemasyarakatan: Latar belakang*.
<https://sdp.ditjenpas.go.id/panduan/LatarBelakang.html>
- Direktorat Jenderal Pemasyarakatan. (n.d.-b). *Sistem Database Pemasyarakatan: Maksud dan tujuan*.
<https://sdp.ditjenpas.go.id/panduan/MaksuddanTujuan.html>
- European Union Agency for Cybersecurity. (2022). *European Cybersecurity Skills Framework (ECSF): User manual*. ENISA.
<https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>
- Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Durr, A., & Thiesse, F. (2022). *Towards understanding*

- the skill gap in cybersecurity. arXiv. <https://arxiv.org/abs/2204.13793>
- Kementerian Komunikasi dan Digital. (2025). Laporan Tahunan Kamsiber 2024. Kominfo-CSIRT.
- National Institute of Standards and Technology. (2024). NICE Framework Resource Center. <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>
- Republik Indonesia. (2022a). Undang-Undang Republik Indonesia Nomor 22 Tahun 2022 tentang Pemasarakatan.
- Republik Indonesia. (2022b). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Republik Indonesia. (2024). Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.