e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Adoption of Cyber Security Maturity Framework for Data Protection in Higher Education

Raden Mochammad Fazri [1)]
[1)]*Study Program of Informatics, Faculty of Industrial Technology, Universitas Islam Indonesia*
Email: [1)] radenmochammadfazry25@gmail.com

How to Cite :
Fazri. R, M. (2026). Adoption of Cyber Security Maturity Framework for Data Protection in Higher Education. Jurnal Media Computer Science, 5(1)

ARTICLE HISTORY
Received [15 Juli 2025]
Revised [20 Januari 2026]
Accepted [25 Januari 2026]

KEYWORDS
Wireshark, Windump, Network Security Monitoring.

This is an open access article under the CC–BY-SA license

ABSTRAK

Keamanan informasi menjadi prioritas utama di lingkungan pendidikan tinggi akibat meningkatnya risiko ancaman siber. Badan Siber dan Sandi Negara (BSSN) mengembangkan Cyber Security Maturity (CSM) versi 1.10 sebagai instrumen pengukuran kematangan keamanan siber yang mencakup lima domain utama: Tata Kelola, Identifikasi, Proteksi, Deteksi, dan Respon. Penelitian ini bertujuan mengkaji penerapan CSM BSSN pada perguruan tinggi di Indonesia serta mengidentifikasi tantangan penerapan akibat keterbatasan sumber daya manusia (SDM) IT dan dukungan dana. Metode penelitian yang digunakan adalah kualitatif deskriptif dengan pendekatan analisis tematik. Teknik pengumpulan data dilakukan melalui wawancara mendalam kepada informan kunci di salah satu perguruan tinggi swasta besar di Indonesia (disamarkan sebagai Universitas Alpha), serta studi literatur dari artikel ilmiah terkait penerapan berbagai framework keamanan informasi seperti Indeks KAMI, ISO 27001:2013, NIST, dan COBIT di perguruan tinggi. Hasil kajian menunjukkan bahwa keterbatasan SDM IT dan dukungan dana menjadi tantangan utama dalam implementasi CSM BSSN, khususnya pada domain Tata Kelola, Proteksi, dan Respon. Penelitian ini memberikan rekomendasi praktis bagi perguruan tinggi dalam mengadopsi CSM BSSN, termasuk strategi optimalisasi SDM dan pengelolaan pendanaan.

ABSTRACT

Information security has become a top priority in higher education environments due to the increasing risks of cyber threats. The National Cyber and Crypto Agency (BSSN) developed Cyber Security Maturity (CSM) version 1.10 as an instrument for assessing cybersecurity maturity, covering five main domains: Governance, Identification, Protection, Detection, and Response. This study aims to explore the implementation of CSM BSSN in Indonesian higher education institutions and identify implementation challenges due to limited IT human resources and funding support. The research employs a qualitative descriptive methodology with a thematic analysis approach. Data collection techniques include in-depth interviews with key informants at one of the Private Universites in Indonesia (disguised as Alpha University) and literature studies from scholarly articles on the implementation of various information security frameworks such as Indeks KAMI, ISO 27001:2013, NIST, and COBIT in higher education. The findings indicate that limitations in IT human resources and funding are the main challenges in implementing CSM BSSN, particularly in the Governance, Protection, and Response domains. This study provides practical recommendations for higher education institutions to adopt CSM BSSN, including strategies for optimizing IT human resources and funding management.

PENDAHULUAN

Indonesia tercatat sebagai salah satu pengguna internet terbesar di dunia. Mengutip laporan *We Are Social* 2022, jumlah pengguna internet di Indonesia mencapai sekitar 204,7 juta (penetrasi 73,3% populasi) pada Januari 2022 (Hiras Simorangkir et al., 2024). Perkembangan teknologi informasi di sektor pendidikan tinggi pun semakin pesat, apalagi ketika pandemi COVID-19 melanda, perguruan tinggi terpaksa beralih sepenuhnya ke pembelajaran digital dan platform *e-learning* (Tan et al., 2024). Dampak dari transformasi digital ini adalah meningkatnya ancaman serangan siber yang menyasar institusi pendidikan. BSSN (Badan Siber dan Sandi Negara) melaporkan bahwa sepanjang tahun 2021 terdapat lebih dari 1,65 miliar anomali serangan siber di Indonesia, dan sektor akademik menjadi target tertinggi sekitar 37,77% dari total insiden. Serangan siber pada perguruan tinggi dapat mengakibatkan kerugian finansial yang sangat besar – mencakup biaya pemulihan data, investasi pada teknologi keamanan baru, konsultasi hukum, hingga potensi kompensasi pada pihak ketiga (Cost of a Data Breach Report 2020 Contents, 2020). Serta kerugian non-materiil berupa kerusakan reputasi institusi (Bada & Nurse, 2019). Ketika perguruan tinggi gagal menjaga keamanan informasi, kepercayaan publik menurun yang berimbas pada penurunan pendaftar mahasiswa baru dan kemungkinan hilangnya kerjasama dengan mitra. Lebih jauh lagi, insiden keamanan informasi dapat menyebabkan hilangnya data penting akademik maupun administratif, yang butuh waktu dan tenaga besar untuk dipulihkan. Oleh karena itu, institusi pendidikan tinggi perlu meningkatkan kesiapan dan langkah mitigasi untuk melindungi aset informasi berharga mereka serta memastikan kelangsungan operasional.

Menanggapi kondisi tersebut, Badan Siber dan Sandi Negara telah mengembangkan instrumen penilaian keamanan siber bernama *Cyber Security Maturity* (CSM) BSSN versi 1.10. Instrumen CSM BSSN ini berfungsi untuk mengukur tingkat kematangan pengelolaan keamanan siber suatu organisasi melalui lima domain utama, serta mengidentifikasi kesenjangan (*gap*) antara kondisi tata kelola keamanan siber saat ini dengan kondisi ideal. Output dari penilaian CSM adalah nilai tingkat maturitas keamanan siber organisasi beserta laporan rekomendasi perbaikan. Instrumen CSM BSSN telah mulai diterapkan di berbagai instansi pemerintah, namun penerapannya dalam lingkungan perguruan tinggi hingga kini masih belum banyak didokumentasikan secara luas. Oleh karena itu, penelitian ini bertujuan untuk mengukur tingkat kematangan keamanan informasi di sebuah institusi perguruan tinggi menggunakan tools CSM BSSN v1.10, mengidentifikasi gap dan tantangan implementasinya pada kondisi SDM TI yang terbatas, serta merumuskan strategi adopsi CSM BSSN v1.10 yang relevan dan adaptif berdasarkan hasil evaluasi tersebut.

LANDASAN TEORI

Keamanan Informasi di Perguruan Tinggi

Keamanan informasi di era digital telah menjadi perhatian global maupun nasional (Budiyanto & Mabruri, 2025). Sektor pendidikan tinggi tidak luput dari ancaman siber; serangan terhadap perguruan tinggi semakin meningkat seiring meningkatnya ketergantungan pada infrastruktur TI dan internet. Studi terbaru menunjukkan lonjakan insiden siber yang signifikan di universitas secara global (Singh Lallie et al., 2025). Di berbagai negara, institusi pendidikan tinggi telah menghadapi sejumlah kasus *data breach* yang mengekspos data sensitif civitas akademika, termasuk insiden besar seperti serangan terhadap Penn State University, serangan SQL injection di Malaysia, hingga pencurian data ribuan mahasiswa dan staff Universitas (Othman 2023). Penerapan pembelajaran jarak jauh selama pandemi juga berkontribusi membuka celah keamanan baru pada sistem perguruan tinggi (Alexei et al., 2021). Sayangnya, kesadaran keamanan siber di kalangan civitas akademik relatif masih rendah; survei di Batam menunjukkan mayoritas mahasiswa memiliki praktik keamanan yang lemah (Tan et al., 2024) dan kurangnya literasi keamanan data di perguruan tinggi

menjadi tantangan tersendiri (Awang et al., 2024). Padahal, data di lingkungan kampus, mulai dari data pribadi mahasiswa/dosen hingga hasil penelitian tergolong *critical assets* yang rentan disalahgunakan jika bocor (Oguta, 2020). Pemerintah Indonesia telah mengesahkan Undang-Undang Perlindungan Data Pribadi tahun 2022, yang meningkatkan urgensi perguruan tinggi untuk memperkuat keamanan data mereka agar mematuhi regulasi (Diba Tanzilla et al., 2023). Tanpa pengelolaan keamanan informasi yang memadai, perguruan tinggi berisiko menghadapi denda regulasi maupun kehilangan kepercayaan publik.

Menganalisis Peran Framework dan Gap Analysis dalam Evaluasi Keamanan Siber

Berbagai kerangka kerja (*framework*) dan standar telah dikembangkan untuk menilai dan meningkatkan keamanan informasi organisasi. Di Indonesia, BSSN sebelumnya memperkenalkan Indeks KAMI (Keamanan Informasi) sebagai alat evaluasi tingkat kesiapan keamanan informasi yang telah diimplementasikan di instansi pemerintah dan beberapa kampus (Anas et al., 2021; Syaeful Bahry & Sugiantoro, 2024). Indeks KAMI mengevaluasi aspek tata kelola keamanan berdasarkan standar ISO/IEC 27001 dan peraturan pemerintah, namun fokusnya lebih pada kepatuhan (*compliance*). Adapun CSM BSSN v1.10 dirancang untuk mengukur *maturity level* keamanan siber secara lebih komprehensif. CSM BSSN mengadopsi praktik terbaik dari berbagai standar global seperti *NIST Cybersecurity Framework* dan ISO/IEC 27001 – yang menggarisbawahi fungsi identifikasi, proteksi, deteksi, respons, dan pemulihan dalam keamanan siber (Almuhammadi & Alsaleh, 2017; Yehezikha Beatrix Natasya Ully, 2023). Pada CSM v1.10, lima domain penilaian mencakup: (1) Tata kelola keamanan informasi, (2) Manajemen risiko keamanan informasi, (3) Keamanan SDM, (4) Pengelolaan aset informasi, dan (5) Teknologi & operasional keamanan. Masing-masing domain dievaluasi tingkat kematangannya dari level dasar hingga optimal. Penilaian maturitas semacam ini sejalan dengan pendekatan kerangka NIST yang menilai kapabilitas *Identify, Protect, Detect, Respond,* dan *Recover* (Almuhammadi & Alsaleh, 2017). Gap analysis digunakan dalam kerangka CSM untuk membandingkan kondisi aktual terhadap kerangka ideal, sehingga dapat diidentifikasi area yang perlu ditingkatkan (Rasmussen et al., 2018).

Mengidentifikasi Tantangan dan GAP dalam Adopsi Keamanan Informasi di Perguruan Tinggi

Beberapa penelitian terdahulu terkait keamanan informasi di perguruan tinggi memberikan gambaran tantangan yang dihadapi. Isnaini dan (Isnaini & Suhartono, 2022) mengevaluasi penerapan prinsip dasar keamanan informasi di sebuah universitas menggunakan COBIT 5, dan menemukan belum terpenuhinya sebagian besar kontrol secara optimal karena keterbatasan sumber daya dan dukungan. (Suwito et al., 2016) menganalisis tingkat maturitas keamanan TI di lingkungan perguruan tinggi dan melaporkan bahwa kapabilitas deteksi insiden dan respons masih rendah dibanding aspek kebijakan. (Mantra et al., 2020) melalui penilaian kerentanan web di beberapa universitas di Indonesia juga mengindikasikan tingkat maturitas keamanan teknis yang bervariasi dan perlunya peningkatan pada prosedur proteksi. Selain itu, hasil studi (Suryono, 2023) atas penilaian mandiri SMKI (Sistem Manajemen Keamanan Informasi) pada instansi pemerintah memberikan indikasi bahwa keberadaan SOP dan organisasi khusus keamanan (seperti *CSIRT*) sangat membantu peningkatan kematangan. Agar keamanan informasi efektif, ia harus terintegrasi dengan proses bisnis dan layanan inti perguruan tinggi. Penelitian (Astuti et al., 2024) mengungkap tantangan tata kelola data pada integrasi sistem nasional PDDIKTI, menekankan perlunya kebijakan dan standar keamanan yang konsisten antar perguruan tinggi. Demikian pula, (Wibowo et al., 2021) mencatat pentingnya identifikasi permasalahan dan intervensi dalam sinkronisasi data pendidikan tinggi agar terjamin keamanannya. Dari berbagai tinjauan pustaka di atas, dapat dilihat bahwa adopsi kerangka keamanan (seperti CSM BSSN) di perguruan tinggi perlu mempertimbangkan aspek kesadaran pengguna, keterbatasan SDM, serta penyesuaian dengan regulasi dan proses bisnis institusi. Penelitian ini akan berkontribusi mengisi gap kajian dengan memfokuskan pada strategi adopsi CSM BSSN di perguruan tinggi, khususnya dalam kondisi sumber daya yang terbatas.

METODE PENELITIAN

Pendekatan penelitian yang digunakan adalah kualitatif deskriptif. Penelitian dilakukan sebagai studi kasus pada sebuah universitas di Indonesia yang dipilih secara purposif karena karakteristik keterbatasan SDM TI. Fokus penelitian ini adalah menganalisis tingkat kematangan keamanan informasi perguruan tinggi tersebut dan strategi adopsi kerangka CSM BSSN dalam konteks keterbatasan SDM.

Pengumpulan Data: Data primer diperoleh melalui wawancara semi-terstruktur dengan para pemangku kepentingan keamanan informasi di universitas, antara lain pejabat pengelola tata kelola TI, manajer risiko & compliance, dan tim *Computer Security Incident Response Team* (CSIRT) universitas. Wawancara semi-terstruktur dipilih agar peneliti dapat menggali informasi mendalam sekaligus mempertahankan fokus pada topik yang diteliti (Alshenqeeti, 2014). Data sekunder diperoleh dari telaah dokumen kebijakan keamanan informasi kampus, laporan audit TI terdahulu, serta studi literatur yang relevan untuk keperluan triangulasi.

Analisis Data: transkrip wawancara dianalisis menggunakan teknik *thematic analysis* untuk menemukan tema-tema kunci terkait tantangan dan kebutuhan dalam penerapan keamanan informasi (Braun & Clarke, 2006). Proses analisis tematik meliputi: membaca berulang transkrip, *coding* pernyataan penting, pengelompokan *coding* menjadi tema, dan penarikan kesimpulan. Beberapa tema yang diantisipasi meliputi: kesadaran & budaya keamanan, kapasitas SDM, kebijakan & kepatuhan, serta aspek teknis operasional keamanan. Keabsahan data dijaga dengan metode triangulasi sumber, yaitu membandingkan hasil wawancara dengan data penilaian CSM dan temuan studi terdahulu. Misalnya, apabila dari wawancara teridentifikasi rendahnya frekuensi audit keamanan, hal ini ditriangulasi dengan dokumen audit kampus serta dibandingkan dengan temuan penelitian lain terkait hal serupa (misalnya studi Isnaini & Suhartono (2022) tentang evaluasi keamanan di universitas lain). Dengan triangulasi dan *cross-check* tersebut, diharapkan interpretasi hasil menjadi lebih valid dan dapat diandalkan.

HASIL DAN PEMBAHASAN

Pada bagian ini disajikan hasil penelitian dan pembahasannya. Temuan utama dari wawancara mendalam dengan informan kunci dan studi literatur dirangkum pada Tabel 1. Tabel ini memperlihatkan perbandingan antara data primer (hasil wawancara) dan data sekunder (temuan dari literatur) untuk setiap domain keamanan siber yang dianalisis. Setelah tabel, uraian detail disampaikan guna membahas hasil tersebut secara kualitatif sesuai domain CSM, tanpa penilaian numerik, melainkan berfokus pada insight dari wawancara dan kesesuaiannya dengan referensi studi terdahulu.

Tabel 1. Rekapitulasi Hasil Wawancara dan Studi Literatur Penerapan Keamanan Informasi di Universitas Alpha dan Perguruan Tinggi Lainnya

No	Narasumber	Domain CSM	Pertanyaan	Data Primer (Wawancara)	Data Sekunder (Literatur)
1	Kepala Bidang Administrasi & Manajemen Proyek	1. Tata Kelola	Apakah keamanan informasi telah menjadi bagian penting dari strategi institusi?	Dibentuknya tim Governance Risk & Compliance dan penetapan keamanan informasi dalam strategi kampus.	Pada Universitas X dibentuk sebuah direktorat khusus untuk keamanan informasi.
2	Kepala Bidang Administrasi &	2. Tata Kelola	Bagaimana alokasi sumber daya	Sudah ditetapkan, ada pengalokasian	Pada Universitas X terkendala

	Manajemen Proyek		(SDM/dana) untuk keamanan informasi?	dana untuk keamanan informasi, tetapi jumlahnya masih terbatas dan perlu optimalisasi.	pada personel yang terbatas, terutama dalam operasional dan monitoring keamanan informasi.
3	Kepala Bidang Administrasi & Manajemen Proyek	3. Adopsi CSM	Apakah Anda mengetahui tools CSM BSSN v1.10?	Sudah mengetahui, namun secara detail memang baru diperkenalkan kepada unit terkait.	Pada Universitas Y sudah mengetahui dan melakukan asesmen dengan CSM BSSN.
4	Kepala Bidang Administrasi & Manajemen Proyek	4. Adopsi CSM	Apakah institusi pernah mempertimbangkan atau menggunakan tools CSM BSSN v1.10?	Iya, karena banyaknya aplikasi yang sudah dibangun internal, CSM digunakan sebagai instrumen monitoring keamanan.	Pada Universitas Y sudah selalu melakukan evaluasi dengan framework nasional.
5	Kepala Bidang Administrasi & Manajemen Proyek	5. Kesiapan Institusi	Menurut Anda, apakah perguruan tinggi mampu mencapai level kematangan CSM yang optimal?	Tentunya iya, karena sudah menjadi goals institusi. Namun ada kendala sumber daya dan komitmen implementasi.	Pada Universitas Y sudah cukup bagus dalam penerapan framework, tapi ada gap pada tata kelola dan SDM.
6	Kepala Bidang Administrasi & Manajemen Proyek	6. Kesiapan Institusi	Apa bentuk dukungan manajerial yang dibutuhkan agar keamanan informasi berjalan optimal?	Dukungannya merupakan pembentukan tim khusus untuk keamanan dan perumusan kebijakan formal oleh pimpinan.	Pada Universitas Z sudah menerapkan framework nasional dan didukung pimpinan universitas.
7	Project Manager Governance Risk & Compliance	7. Tata Kelola	Apakah kebijakan keamanan informasi formal sudah tersedia dan berjalan?	Sudah tersedia, dan untuk versi pertama sudah diimplementasikan, sedang dikembangkan menjadi IT Policy v2.	Pada Universitas Z kebijakan keamanan informasi sudah tersedia namun butuh pembaruan.
8	Project Manager Governance Risk & Compliance	8. Tata Kelola	Apakah terdapat struktur tanggung jawab yang jelas dalam keamanan informasi?	Sudah ada, dibentuknya tim core merupakan penanda komitmen organisasi pada keamanan informasi.	Pada Universitas Z belum ada struktur organisasi khusus, hanya peran tambahan pada unit TI.
9	Project Manager Governance Risk & Compliance	9. Identifikasi	Apakah seluruh aset digital institusi telah didata dan dikelola secara formal?	Belum seluruh, namun sudah ada pendataan aset dan inventarisasi, dengan rencana	Pada Universitas X proses inventarisasi dan klasifikasi aset sudah mulai

				penguatan.	diterapkan.
10	Project Manager CSIRT-SOC	10. Identifikasi	Apakah Universitas secara rutin melakukan penilaian risiko keamanan informasi?	Kalau rutin belum, namun pernah dilakukan pada saat asesmen besar.	Pada Universitas Y sudah secara rutin dilakukan audit risiko berbasis framework nasional.
11	Project Manager CSIRT-SOC	11. Proteksi	Apa saja sistem proteksi TI yang digunakan saat ini (firewall, antivirus, endpoint)?	untuk sistem proteksinya menggunakan firewall di level publik yang sudah terintegrasi dengan IDS IPS, Malware protection, Url Protection, DNS filtering, disisi LAN juga menggunakan firewall yang sama, di sisi website menggunakan WAV,	Pada Universitas X dan Y sudah menerapkan firewall, IDS/IPS, dan segmentasi jaringan; namun proteksi endpoint masih jadi tantangan umum akibat keterbatasan pembiayaan.
12	Project Manager CSIRT-SOC	12. Proteksi	Apakah backup data dilakukan secara otomatis dan terdokumentasi?	sudah otomatis dan terdokumentasi.	Di banyak universitas, pelatihan awareness baru dilakukan tahunan atau saat ada insiden besar.
13	Project Manager CSIRT-SOC	13. Deteksi	Bagaimana proses deteksi dini dan monitoring insiden dilakukan?	sudah ada, penerapannya di firewall	Pada universitas Z dan beberapa kampus lain, SOC/SIEM diterapkan namun operasi 24/7 sulit tercapai tanpa SDM dan anggaran memadai.
14	Project Manager CSIRT-SOC	14. Deteksi	Bagaimana tata kelola log dan pelaporan insiden?	Log insiden dikumpulkan secara terpusat, namun analisis log dan eskalasi insiden kadang terlambat karena SDM terbatas dan volume data tinggi.	Banyak kampus telah punya sistem log terpusat, tetapi analisis dan pelaporan insiden lambat jika tak ada dukungan staff dan tools yang memadai.
15	Project Manager CSIRT-SOC	15. Respon	Apakah ada prosedur dan tim khusus penanganan insiden?	Sudah ada tim CSIRT, namun masih dalam tahap penguatan.	Universitas X dan Y juga sudah membentuk CSIRT;

				Prosedur respons sudah disusun, tetapi update dan sosialisasi perlu ditingkatkan.	pembaruan prosedur & latihan respons jadi tantangan serupa.
16	Project Manager CSIRT-SOC	16. Respon	Apa kendala utama dalam respons insiden?	personel siaga terbatas, update pengetahuan belum merata, dan dana penanganan insiden masih kurang.	Studi literatur menyoroti kendala sama di banyak PT: keterbatasan tim, keterbatasan dana untuk latihan dan recovery.

Tabel 1 di atas menggambarkan secara ringkas temuan utama dari wawancara dan studi literatur pada berbagai domain keamanan siber. Berikutnya, hasil-hasil tersebut dibahas secara mendalam per domain untuk memahami bagaimana kerangka CSM BSSN telah diadopsi dan diterapkan di lingkungan perguruan tinggi yang diteliti, serta bagaimana kondisinya dibandingkan dengan temuan studi lain.

Tata Kelola Keamanan Informasi dan Sumber Daya

Dari aspek tata kelola, informan mengonfirmasi bahwa keamanan informasi telah menjadi prioritas strategis di institusi. Hal ini ditandai dengan pembentukan tim khusus *Governance, Risk & Compliance (GRC)* di Biro Sistem Informasi sebagai penanggung jawab inisiatif keamanan siber. Keberadaan tim GRC menunjukkan adanya komitmen manajemen terhadap keamanan informasi, sejalan dengan temuan pada literatur bahwa perguruan tinggi lain (misalnya Universitas X) membentuk unit setara direktorat TIK untuk fokus pada keamanan dan sistem informasi institusi. Kebijakan keamanan informasi formal juga sudah tersedia dan telah disosialisasikan kepada civitas akademika. Informan GRC menjelaskan bahwa institusi bahkan tengah menyempurnakan kebijakan tersebut ke versi kedua, yang menandakan evaluasi dan perbaikan berkelanjutan. Sebaliknya, studi terdahulu di Universitas Z menunjukkan kebijakan keamanan informasi yang dimiliki masih pada tataran kerangka dasar dan belum komprehensif, menyorot perbedaan tingkat kematangan kebijakan antar institusi.

Struktur tata kelola keamanan informasi di institusi studi kasus ini relatif jelas. Selain tim GRC, sudah ditetapkan struktur tanggung jawab yang mencakup pembagian peran untuk pengelolaan keamanan (termasuk adanya tim CSIRT-SOC). Informan menyebut pembentukan *core team* GRC sebagai penambahan struktur penting seiring meningkatnya kebutuhan keamanan pada berbagai sistem. Literatur mendukung pentingnya kejelasan struktur ini; Universitas Z, misalnya, dilaporkan belum memiliki struktur organisasi keamanan informasi yang jelas, sehingga tanggung jawab keamanan tersebar dan kurang efektif. Dengan demikian, institusi yang diteliti berada selangkah lebih maju dalam aspek tata kelola dengan adanya tim dan struktur formal.

Dari segi sumber daya, institusi telah mengalokasikan SDM dan dana khusus untuk keamanan informasi. Informan mencatat adanya alokasi anggaran, contohnya untuk pembelian perangkat lunak/alat keamanan yang mendukung penerapan kerangka CSM. Ini menunjukkan dukungan manajerial dalam bentuk penyediaan resource bagi inisiatif keamanan siber. Sebagai perbandingan, sebuah studi pada Universitas X mengindikasikan kendala kekurangan personel khusus keamanan serta ketiadaan sejumlah prosedur penting (seperti prosedur *backup*, pengelolaan akses, penghancuran data). Kondisi tersebut merefleksikan kurangnya dukungan sumber daya dan kontrol di Universitas X. Sementara itu, institusi kita tampak lebih siap karena telah menyiapkan tim dan anggaran meski tentu peningkatan kapasitas SDM terus diperlukan. Temuan ini menegaskan bahwa

tata kelola yang kuat mencakup kebijakan, struktur organisasi yang jelas, dan alokasi sumber daya memadai merupakan fondasi penting bagi keamanan informasi di perguruan tinggi.

Adopsi Kerangka CSM BSSN dan Kesiapan Institusi

Dalam hal adopsi kerangka CSM BSSN, informan menyatakan telah mengetahui keberadaan *tools* CSM versi 1.10 yang disediakan BSSN. Meskipun pemahaman detail teknis atas *tools* tersebut terbatas pada sebagian pihak (karena penanganannya dipercayakan pada tim khusus), kesadaran akan kerangka CSM ini sudah ada di institusi. Bahkan, institusi mendapat dorongan dari BSSN melalui program kemitraan untuk mengadopsi CSM di perguruan tinggi. Langkah proaktif ini sejalan dengan praktik di beberapa perguruan tinggi lain. Misalnya, literatur menyebut bahwa Universitas Y telah mengenal dan mulai menggunakan *tool* CSM BSSN untuk menilai kematangan keamanan siber mereka.

Institusi studi kasus mempertimbangkan penerapan CSM seiring meningkatnya jumlah aplikasi yang dikembangkan dan kesadaran akan kerentanan keamanan pada aplikasi tersebut. Informan menjelaskan bahwa fokus terhadap keamanan informasi mulai ditingkatkan, terutama untuk memastikan aplikasi-aplikasi internal aman dari ancaman. Hal ini beriringan dengan upaya BSSN yang melibatkan perguruan tinggi dalam pilot project penerapan CSM. Berdasarkan literatur, Universitas Y sudah rutin melakukan evaluasi kematangan keamanan siber menggunakan CSM dan terus meningkatkan hasil evaluasinya. Ini menunjukkan bahwa adopsi CSM di perguruan tinggi lain telah memberikan hasil positif berupa pemantauan kematangan secara berkala. Institusi studi kasus berada pada tahap awal yang menjanjikan, dengan adanya niat dan beberapa langkah awal menuju implementasi kerangka CSM.

Terkait kesiapan institusi untuk adopsi penuh CSM, informan meyakini bahwa kampus mampu mengadopsi kerangka ini secara menyeluruh. Pihak manajemen telah menetapkan standar keamanan berbasis kerangka kerja sebagai *goal* jangka panjang. Artinya, integrasi CSM ke dalam proses manajemen keamanan informasi akan terus ditingkatkan secara bertahap. Temuan ini diperkuat oleh literatur yang menunjukkan Universitas Y berhasil mencapai tingkat kematangan keamanan yang cukup baik, walau belum optimal di semua aspek. Hal tersebut mengindikasikan bahwa dengan komitmen berkelanjutan, peningkatan kematangan keamanan siber dapat dicapai dari waktu ke waktu. Institusi yang diteliti berada di jalur yang benar dengan memiliki rencana dan target jelas untuk standarisasi keamanan melalui CSM.

Dukungan manajerial merupakan faktor krusial dalam kesuksesan adopsi kerangka keamanan. Informan menekankan perlunya dukungan pimpinan berupa pembentukan tim khusus untuk implementasi CSM dan penguatan budaya keamanan di semua lapisan (pengembang aplikasi, tim infrastruktur jaringan, dsb.). Jadi, bukan hanya satuan keamanan yang terlibat, tetapi seluruh tim TI didorong mengintegrasikan aspek keamanan dalam pekerjaan sehari-hari. Hal ini sejalan dengan rekomendasi pada literatur: sebuah studi di Universitas Z menemukan bahwa meskipun framework keamanan telah mulai diterapkan, ketiadaan dukungan manajerial (misalnya belum adanya kebijakan formal berbasis standar internasional) menjadi penghambat. Oleh karena itu, langkah institusi studi kasus membentuk tim khusus dan merumuskan kebijakan menunjukkan dukungan manajerial yang tepat, yang diyakini akan memperlancar adopsi penuh kerangka CSM ke depannya.

Manajemen Risiko Keamanan Informasi dan Kepatuhan Standar

Aspek identifikasi dan manajemen risiko di perguruan tinggi ini menunjukkan kemajuan parsial. Dari wawancara terungkap bahwa pendataan dan klasifikasi aset digital institusi sudah mulai dilakukan, mencakup aset fisik dan digital. Namun, upaya ini belum mencakup seluruh aset secara lengkap dan masih perlu penyempurnaan. Situasi serupa ditemukan pada studi Universitas X, di mana inventarisasi aset digital baru dilakukan sebagian dan beberapa aset penting belum terkelola dengan baik. Kekurangan dalam pendataan aset dapat berdampak pada terlewatnya

perlindungan untuk aset-aset tertentu. Oleh karena itu, meski institusi sudah berada di arah yang benar dengan melakukan inventarisasi, diperlukan kesinambungan agar seluruh aset informasi teridentifikasi dan terklasifikasi sesuai tingkat kritikalnya.

Praktik penilaian risiko keamanan informasi di institusi ini belum teragendakan secara rutin. Informan GRC menyebut bahwa formalisasi manajemen risiko baru dilakukan sekali (tahun 2023) dan belum menjadi proses tahunan. Hal ini menunjukkan bahwa siklus manajemen risiko masih ad-hoc dan perlu ditingkatkan frekuensinya. Berbeda dengan itu, Universitas Y dilaporkan telah menjalankan penilaian risiko secara rutin dan terjadwal. Pelaksanaan rutin ini mencerminkan kedewasaan lebih tinggi dalam proaktif mengidentifikasi risiko dan menangani celah keamanan sebelum insiden terjadi. Dengan kata lain, institusi studi kasus perlu mengadopsi pola serupa agar evaluasi risiko menjadi bagian integral dari tata kelola keamanan informasi tiap periode (misalnya tahunan atau per semester).

Terkait audit keamanan TI, institusi menggunakan kerangka CSM sebagai acuan standar dalam prosedur audit internal. Hal ini berarti aspek-aspek CSM dijadikan panduan checklist saat melakukan audit keamanan terhadap sistem dan infrastruktur yang ada. Meskipun demikian, implementasi audit berbasis kerangka ini diakui belum optimal penuh; fokus audit masih pada area-area yang dianggap paling kritis. Di Universitas X, berdasarkan literatur, telah dilakukan audit keamanan TI dengan mengacu standar nasional semacam CSM, meski kedalaman dan cakupan audit mungkin terbatas oleh sumber daya. Ini menunjukkan bahwa baik institusi studi kasus maupun beberapa perguruan tinggi lain sudah mengadopsi standar kerangka nasional dalam audit, namun tantangannya adalah memastikan audit mencakup seluruh domain dan dilakukan secara mendalam.

Tantangan dalam audit dan pengendalian risiko terutama terletak pada kurangnya kesadaran (*security awareness*) di kalangan pengguna dan pengelola sistem. Informan menekankan bahwa tanpa awareness, banyak risiko tidak akan terbaca atau ditangani sampai insiden terjadi. Ini ditambah dengan keterbatasan sumber daya (baik jumlah maupun kompetensi personel) yang dapat menghambat proses audit dan mitigasi risiko. Temuan ini konsisten dengan laporan dari Universitas Y, di mana kurangnya prosedur formal dan kesadaran pengguna disebut sebagai hambatan utama dalam manajemen risiko. Implikasinya, untuk meningkatkan efektivitas manajemen risiko, institusi perlu berinvestasi dalam program peningkatan kesadaran keamanan (misalnya pelatihan rutin bagi staf/pengguna) dan memperjelas prosedur formal sehingga semua pihak tahu langkah yang harus diambil dalam pengelolaan risiko dan insiden.

Pada aspek kepatuhan terhadap standar/kerangka kerja eksternal, institusi telah mengadopsi referensi dari standar internasional (seperti ISO 27001, COBIT, NIST) dalam praktik keamanannya, meskipun secara parsial. Informan menyatakan tidak semua kontrol dalam standar tersebut diimplementasikan, tetapi kerangka terkenal itu digunakan sebagai panduan umum. Hal ini positif karena menunjukkan keterbukaan institusi terhadap *best practices* global. Sebagai contoh, literatur mencatat Universitas Y mengacu pada NIST SP 800-30 dalam penerapan manajemen risiko keamanan informasi mereka. Dengan demikian, langkah institusi studi kasus yang mengadopsi bagian relevan dari ISO/NIST/COBIT mencerminkan upaya menuju kepatuhan standar, yang pada gilirannya dapat mempermudah integrasi kerangka CSM (yang pada dasarnya selaras dengan standar keamanan umum). Kedepannya, konsistensi dalam menerapkan standar ini akan membantu institusi membangun sistem keamanan informasi yang *compliant* dan diakui baik secara nasional maupun internasional.

Implementasi Teknis: Proteksi, Deteksi, dan Respon Insiden

Dari sisi teknis operasional, institusi telah menerapkan berbagai kontrol proteksi untuk melindungi aset informasi. Berdasarkan wawancara dengan tim CSIRT-SOC, di lingkungan jaringan kampus sudah dipasang perangkat *firewall* di level gateway publik yang memiliki fitur terintegrasi seperti *Intrusion Detection/Prevention System (IDS/IPS)*, anti-malware, filter URL, dan filter DNS. Bahkan di jaringan internal (LAN) digunakan firewall serupa untuk segmentasi, dan untuk aplikasi web

diterapkan *Web Application Firewall (WAF)* guna melindungi layanan web kampus. Konfigurasi berlapis ini menunjukkan keseriusan dalam proteksi infrastruktur dan aplikasi. Sebagai perbandingan, studi di Universitas X mengungkap bahwa detail kontrol keamanan jaringan belum dijelaskan secara lengkap, namun perguruan tinggi tersebut telah melakukan upaya perlindungan di sisi aplikasi melalui pengujian keamanan dan penutupan kerentanan (patching). Dibanding kasus tersebut, institusi yang diteliti tampaknya lebih komprehensif dalam menerapkan kontrol proteksi, mencakup jaringan hingga aplikasi.

Mekanisme proteksi data melalui *backup* juga sudah diimplementasikan dengan baik. Informan menyebut *backup* data di sistem institusi telah berjalan otomatis dan terdokumentasi. Artinya, ada prosedur baku untuk pencadangan data secara terjadwal dan pencatatan hasil *backup*. Hal ini sangat penting untuk menjamin ketersediaan data apabila terjadi insiden seperti kegagalan sistem atau serangan *ransomware*. Kondisi ini berbanding terbalik dengan temuan di Universitas U, di mana proses *backup* masih manual dan tidak terdokumentasi sehingga rawan menimbulkan kehilangan data. Dengan sudah otomatisnya proses *backup*, institusi studi kasus menunjukkan kematangan lebih tinggi dalam manajemen kontinuitas layanan.

Pada aspek deteksi ancaman dan insiden, institusi telah memiliki sistem deteksi *intrusion* (IDS/IPS) yang terintegrasi dengan firewall. Penerapan IDS/IPS pada firewall memungkinkan traffic berbahaya dikenali dan dihentikan secara real-time sebelum menembus jaringan lebih dalam. Literasi dari Universitas A mendukung pentingnya hal ini, dimana kampus tersebut menggunakan *IDS* (disebut *StartaGuard* dalam studi) secara terpusat untuk memantau trafik jaringan dan mendeteksi ancaman. Selain itu, pemantauan log sistem di institusi studi kasus dilaksanakan dengan gabungan cara manual dan otomatis. Beberapa log (mungkin untuk sistem kritis) sudah terkumpul ke sistem monitoring terpusat, sementara log lain masih diperiksa manual oleh administrator. Tentunya target ke depan adalah mengintegrasikan log secara penuh agar Security Information and Event Management (SIEM) lebih optimal. Sebagai pembanding, Universitas A sudah menjalankan monitoring log terpusat dengan platform khusus, yang memungkinkan deteksi anomali lebih cepat. Maka, langkah institusi untuk mulai menerapkan sistem terpusat patut dilanjutkan hingga seluruh komponen keamanan *termonitor* secara terintegrasi.

Dalam hal respon insiden, institusi telah memiliki *Standard Operating Procedure* (SOP) penanganan insiden keamanan informasi. SOP tersebut, misalnya, menetapkan bahwa insiden harus ditindaklanjuti dalam jangka waktu tertentu (informan menyebut *1x24 jam* sebagai waktu respons awal). Keberadaan SOP menandakan bahwa institusi sudah mempunyai kerangka kerja operasional untuk menangani insiden, meskipun efektivitasnya bergantung pada kepatuhan dan kecepatan tim saat insiden nyata terjadi. Studi di Universitas U menunjukkan bahwa meski SOP insiden tersedia, pelaksanaannya belum optimal – artinya memiliki prosedur saja tidak cukup tanpa simulasi dan evaluasi. Institusi studi kasus tampaknya menyadari hal ini, terlihat dari upaya mereka melakukan simulasi tanggap insiden tiap tahun. Simulasi tersebut berfungsi sebagai latihan bagi tim keamanan (CSIRT) untuk menguji kesiapan prosedur dan koordinasi dalam menangani skenario insiden. Beberapa perguruan tinggi lain juga dilaporkan mengadakan pelatihan keamanan seperti *penetration testing* sebagai bagian dari program tanggap insiden. Ini menunjukkan bahwa latihan praktis secara periodik merupakan komponen penting dalam membangun kapabilitas respon insiden yang tangguh.

Keberadaan CSIRT-SOC di institusi memberikan keuntungan tersendiri dalam koordinasi keamanan. Informan menjelaskan bahwa CSIRT berperan meningkatkan kesiapan dengan mengadakan pelatihan keterampilan untuk tim dan menjalankan proteksi-proteksi yang ada secara optimal. Meskipun literatur khusus tentang kesiapan CSIRT di perguruan tinggi belum banyak, diketahui bahwa beberapa kampus telah membentuk CSIRT yang diberi mandat jelas untuk pencegahan dan penanggulangan insiden siber. Dalam kasus institusi ini, CSIRT yang terstruktur menandai kematangan organisasional yang lebih tinggi: ada tim terlatih yang siap merespons insiden sesuai prosedur. Hal ini merupakan adopsi baik dari model kerangka CSM pada domain

respon, di mana keberlangsungan tim tanggap insiden (CSIRT) dan mekanisme umpan balik pasca-insiden menjadi indikator penting kematangan.

Integrasi Temuan dan Implikasi

Menilik seluruh temuan di atas, dapat dilihat bahwa upaya adopsi kerangka CSM BSSN di lingkungan perguruan tinggi studi kasus berlangsung dengan pendekatan bertahap dan kualitatif. Tanpa melibatkan skor numerik, analisis menunjukkan area mana yang sudah kuat dan mana yang perlu ditingkatkan. Secara umum, aspek tata kelola dan dukungan manajerial di institusi tersebut tergolong baik karena tersedianya kebijakan formal, tim khusus (GRC dan CSIRT), serta alokasi sumber daya menunjukkan pondasi yang kokoh. Hal ini selaras dengan literatur yang menekankan pentingnya komitmen manajemen dan struktur organisasi dalam penerapan keamanan informasi di sektor pendidikan tinggi.

Di sisi lain, aspek operasional teknis (identifikasi aset, proteksi, deteksi, respon) juga telah diimplementasikan, namun beberapa hal masih perlu penguatan. Inventarisasi aset dan penilaian risiko misalnya, perlu dijalankan lebih rutin dan menyeluruh agar kerangka manajemen risiko berjalan efektif. Penerapan kontrol proteksi dan deteksi sudah cukup maju dengan teknologi firewall terintegrasi dan *logging* terpusat parsial, yang sebaiknya terus ditingkatkan menjadi sepenuhnya terintegrasi. SOP insiden yang ada perlu terus diuji melalui simulasi agar saat terjadi insiden nyata, tim dapat merespons sesuai prosedur dengan sigap.

Studi literatur pembanding memberikan konteks bahwa perguruan tinggi lain menghadapi tantangan serupa, terutama dalam hal awareness dan dukungan manajemen. Beberapa universitas telah lebih dulu menerapkan evaluasi kematangan (seperti Universitas Y dengan CSM rutin tahunannya), sementara yang lain masih berada di tahap awal. Institusi studi kasus dapat mengambil pelajaran dari praktik terbaik (best practices) di tempat lain, misalnya pentingnya penjadwalan rutin risk assessment dan penggunaan platform SIEM untuk monitoring yang lebih baik. Sebaliknya, institusi ini juga bisa menjadi contoh bagi yang lain dalam hal komitmen pimpinan dan pembentukan organisasi keamanan (tim GRC dan CSIRT yang aktif).

Secara keseluruhan, tanpa penyebutan skor numerik, analisis kualitatif ini menegaskan bahwa kerangka CSM BSSN dapat diadopsi di perguruan tinggi dengan menyesuaikannya pada konteks dan kemampuan masing-masing. Keberhasilan awal tampak pada aspek tata kelola dan beberapa kontrol teknis, sedangkan aspek-aspek lain membutuhkan peningkatan berkelanjutan. Pembahasan ini diharapkan dapat membantu institusi pendidikan tinggi lain dan pemangku kebijakan untuk memahami faktor-faktor kunci (seperti kebijakan, sumber daya, awareness, dan latihan insiden) dalam mengamankan informasi kampus, sekaligus mendorong penggunaan kerangka nasional (CSM BSSN) sebagai panduan peningkatan maturitas keamanan siber secara non-kuantitatif dan berkelanjutan.

KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini mengkaji adopsi kerangka Cyber Security Maturity (CSM) BSSN v1.10 di sebuah perguruan tinggi yang memiliki keterbatasan SDM TI dan dana secara kualitatif. Berdasarkan wawancara mendalam dan studi literatur institusi yang diteliti menunjukkan bahwa aspek tata kelola dan kontrol keamanan dasar telah terbentuk dengan baik. Namun demikian, ditemukan tantangan signifikan terutama dalam aspek identifikasi risiko dan deteksi insiden siber.

Tantangan ini terutama disebabkan oleh keterbatasan jumlah dan kapasitas tenaga ahli keamanan siber, implementasi teknologi monitoring yang belum optimal, serta praktik manajemen risiko yang belum rutin. Selain itu, rendahnya kesadaran keamanan siber di kalangan pengguna, kurangnya pelatihan rutin bagi SDM TI, serta perlunya pembaruan kebijakan dan prosedur agar

sesuai dengan standar terkini menjadi isu penting yang perlu ditangani agar adopsi CSM BSSN berjalan efektif dan berkelanjutan.

Saran

Untuk meningkatkan kematangan keamanan informasi dan berhasil mengadopsi CSM BSSN v1.10, perguruan tinggi perlu menerapkan strategi berkelanjutan. Pertama, meningkatkan kompetensi dan kesadaran keamanan siber pada seluruh lapisan, mengadakan pelatihan teknis bagi staf TI dan program edukasi awareness bagi dosen/mahasiswa secara rutin. Kedua, memperkuat tata kelola dengan meninjau dan menyempurnakan kebijakan keamanan informasi, serta memastikan kepatuhan melalui audit internal yang terjadwal. Ketiga, mengoptimalkan pemanfaatan teknologi keamanan sesuai kapasitas, misalnya menggunakan alat otomasi untuk pemantauan log dan sistem deteksi serangan guna mengimbangi keterbatasan SDM. Keempat, menjalin kolaborasi dengan lembaga eksternal (BSSN, konsultan keamanan) untuk pendampingan, asesmen berkala, dan bantuan penanganan insiden jika diperlukan. Terakhir, mengintegrasikan manajemen risiko ke dalam proses operasional dan melakukan evaluasi maturitas secara periodik. Dengan menerapkan rekomendasi strategi di atas, perguruan tinggi diharapkan dapat meningkatkan tingkat maturitas keamanan informasinya secara bertahap sehingga lebih siap menghadapi ancaman siber, meskipun memiliki keterbatasan sumber daya internal.

DAFTAR PUSTAKA

Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model For Nist Cyber Security Framework. 51–62. Https://Doi.Org/10.5121/Csit.2017.70305

Alshenqeeti, H. (2014). Interviewing As A Data Collection Method: A Critical Review. English Linguistics Research, 3(1). Https://Doi.Org/10.5430/Elr.V3n1p39

Anas, A. S., Utami, I. G. A. S. D. G., Maulachela, A. B., & Juliansyah, A. (2021). Kami Index As An Evaluation Of Academic Information System Security At Xyz University. Matrix : Jurnal Manajemen Teknologi Dan Informatika, 11(2), 55–62. Https://Doi.Org/10.31940/Matrix.V11i2.2447

Alexei, A., Alexei, A., Arina, A., & Anatolie, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. Article In International Journal Of Scientific & Technology Research. Www.Ijstr.Org

Astuti, H. M., Wibowo, R. P., & Herdiyanti, A. (2024). Towards The National Higher Education Database In Indonesia: Challenges To Data Governance Implementation From The Perspective Of A Public University. Procedia Computer Science, 234, 1322–1331. Https://Doi.Org/10.1016/J.Procs.2024.03.130

Awang, H., Benlahcene, A., & Mansor, N. S. (2024). Data Security Knowledge Among Students Of Public Universities: A Fundamental Competency For Success In The Education 5.0 Era. In Preconceptions Of Policies, Strategies, And Challenges In Education 5.0 (Pp. 17–32). Igi Global. Https://Doi.Org/10.4018/979-8-3693-3041-8.Ch002

Bada, M., & Nurse, J. R. C. (2019). The Social And Psychological Impact Of Cyberattacks. In Emerging Cyber Threats And Cognitive Vulnerabilities (Pp. 73–92). Elsevier. Https://Doi.Org/10.1016/B978-0-12-816203-3.00004-6

Braun, V., & Clarke, V. (2006). Using Thematic Analysis In Psychology. Qualitative Research In Psychology, 3(2), 77–101. Https://Doi.Org/10.1191/1478088706qp063oa

Budiyanto, D., & Mabruri, M. (2025). Pentingnya Keamanan Siber Dalam Era Digital: Tinjauan Global Dan Kondisi Di Indonesia. Prosiding Seminar Nasional Sains Dan Teknologi Seri Iii Fakultas Sains Dan Teknologi, 2(1).

Cost Of A Data Breach Report 2020 Contents. (N.D.). Retrieved April 24, 2025, From Https://Www.Ibm.Com/Security/Digital-Assets/Cost-Data-Breach-Report/1cost%20of%20a%20data%20breach%20report%202020.Pdf

Diba Tanzilla, F., Hanita, M., & Widiawan, B. (2023). Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law. International Journal Of Progressive Sciences And Technologies (Ijpsat, 40(2), 164–170.

Hiras Simorangkir, A., Josias, A., & Runturambi, S. (2024). Budaya & Masyarakat Digital Dalam Ketahanan Siber Di Indonesia: Sebuah Adaptasi Dari Pendekatan Capacity Maturity Model (Cmm). Https://Doi.Org/10.38035/Jmpis.V5i4

Isnaini, K. N., & Suhartono, D. (2022). Evaluation Of Basic Principles Of Information Security At University Using Cobit 5. Matrik : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer, 21(2), 317–326. Https://Doi.Org/10.30812/Matrik.V21i2.1311

Mantra, I., Rahman, A. A., & Saragih, H. (2020). Maturity Framework Analysis Iso 27001: 2013 On Indonesian Higher Education. In International Journal Of Engineering & Technology (Vol. 9, Issue 2). Www.Sciencepubco.Com/Index.Php/Ijet

Othman, Z. (2023). Sustainability Of Higher Education Institutions: Case Study On Cyber Attacks. Global Business Management Review, 15. Https://Doi.Org/10.32890/Gbmr2023.15.1.2

Oguta, S. (2020). Security Of Critical Data In Universities. In International Journal Of Creative Research Thoughts (Vol. 8, Issue 9). Www.Ijcrt.Org

Prastowo, S. L., & Sudiana, D. (2024). Recommendations For A Framework For Handling Security Incidents Of Electronic-Based Government Systems (Spbe) Using The Iso/Iec 27035: 2023 Standard. Jinav: Journal Of Information And Visualization, 5(1), 107–114. Https://Doi.Org/10.35877/454ri.Jinav2747

Purwanti, L., Widyaningrum, R., & Melinda, S. A. (2020). Analisis Penggunaan Media Power Point Dalam Pembelajaran Jarak Jauh Pada Materi Animalia Kelas Viii. Journal Of Biology Education, 3(2), 157. Https://Doi.Org/10.21043/Jobe.V3i2.8446

Rasmussen, J., Natsiavas, P., Votis, K., Moschou, K., Campegiani, P., Coppolino, L., Cano, I., Marí, D., Faiella, G., Stan, O., Abdelrahman, O., Nalin, M., Baroni, I., Voss-Knude, M., Vella, V. A., Grivas, E., Mesaritakis, C., Dumortier, J., Petersen, J., … Koutkias, V. (2018). Gap Analysis For Information Security In Interoperable Solutions At A Systemic Level: The Konfido Approach. Ifmbe Proceedings, 66, 75–79. Https://Doi.Org/10.1007/978-981-10-7419-6_13

Singh Lallie, H., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing Cyber Attacks And Cyber Security Vulnerabilities In The University Sector. Https://Doi.Org/10.3390/Computers

Suryono, I. (2023). Evaluasi Penilaian Mandiri Penerapan Smki Di Salah Satu Lingkungan K/L. In Jurnal Penelitian Ilmu Komputer Issn : Xxxx-Xxxx (Vol. 1, Issue 1). Https://Mypublikasi.Com/

Suwito, M. H., Matsumoto, S., Kawamoto, J., Gollmann, D., & Sakurai, K. (2016). An Analysis Of It Assessment Security Maturity In Higher Education Institution. Lecture Notes In Electrical Engineering, 376, 701–713. Https://Doi.Org/10.1007/978-981-10-0557-2_69

Syaeful Bahry, M., & Sugiantoro, B. (2024). Evaluasi Tingkat Keamanan Indeks Kami (Studi Kasus : Universitas X) (Vol. 7, Issue 2).

Tan, T., Sama, H., Wibowo, T., Wijaya, G., & Aboagye, O. E. (2024). Kesadaran Keamanan Siber Pada Kalangan Mahasiswa Universitas Di Kota Batam Cybersecurity Awareness Among University Students In Batam City. Jurnal Teknologi Dan Informasi (Jati), 14. Https://Doi.Org/10.34010/Jati.V14i2

Taufan Anwar, M., Aryanti, U., Wijana, M., & Atmoko, D. (2024). Mitigasi Risiko Keamanan Informasi Menggunakan Sni Iso/Iec 27001:2013 Berbasis Manajemen Risiko Octave Allegro Di Perguruan Tinggi : Studi Kasus Perguruan Tinggi X. Insani Informatics For Educators And Professionals: Journal Of Informatics, 9(1), 73–83.

Thenabadu, M. (2022). Ijriss) |Volume Vi, Issue Vi. In International Journal Of Research And Innovation In Social Science. Www.Rsisinternational.Org

Tusriyanto, Sulaeman, Moh. M., & Nurcholidah, L. (2023). Optimising Organisational Performance Through Human Resource Management Strategy And Technology Integration To Enhance Innovation. Technology And Society Perspectives (Tacit), 1(3). Https://Doi.Org/10.61100/Tacit.V1i3.81

Whitman, M. E., & Mattord, H. J. (2022). Information Security. Www.Cengage.Com/Highered

Wibowo, R. P., Nurkasanah, I., Hendrawan, R. A., Yuhana, U. L., Wibisono, A., Lestari, N. A., & Zehroh, S. A. (2021). Problem Identification And Intervention In The Higher Education Data Synchronization System In Indonesia. Procedia Computer Science, 197, 484–494. Https://Doi.Org/10.1016/J.Procs.2021.12.165

Widyasuri, A., Priambodo, D. F., Ajhari, A. A., & Sunaringtyas, S. U. (2024). Security Analysis Of Audit Tools. International Conference On Computer, Control, Informatics And Its Applications, Ic3ina, 2024, 405–410. Https://Doi.Org/10.1109/Ic3ina64086.2024.10732702

Yehezikha Beatrix Natasya Ully. (2023, July). Cyber Security Maturity Tool. Https://Pluto.Poltekssn.Ac.Id/. Https://Pluto.Poltekssn.Ac.Id/Research/Cyber-Security-Maturity-Tool/