Edukatif: Jurnal Ilmu Pendidikan
Volume 7 Nomor 2 April 2025 Halaman 463 - 479
https://edukatif.org/index.php/edukatif/index

Keamanan Learning Management System Perguruan Tinggi dengan Standard ISO/IEC 27002:2022

Saepudin[1], Khidhir Akbar Ghofar[2], Hendra Wibiksana[3], Adib[4], Tarsinah[5], Ai Nurhayati[6]✉
Universitas Teknologi Bandung, Indonesia[1,2,3,4,5,6]
e-mail : saepudinst@gmail.com[1], khidhirakbarghofar@sttbandung.ac.id[2], hendrawibiksana@utb-univ.ac.id[3], adib@utb-univ.ac.id[4], tarsinahsumarni@utb-univ.ac.id[5], ain38375@gmail.com[6]

Abstrak

Learning Management System (LMS) adalah platform digital yang diterapkan di sektor pendidikan dan pelatihan korporat untuk mengelola, menyimpan, dan mendistribusikan materi pembelajaran online. LMS menyimpan data sensitif, seperti informasi pribadi pengguna, hasil evaluasi, dan materi pembelajaran sehingga LMS memiliki permasalahan yang rentan terhadap risiko keamanan dari ancaman internal maupun eksternal sehingga perlu penerapan standar keamanan yang solid. Penelitian ini bertujuan untuk mengevaluasi penerapan standard keamanan ISO/IEC 27002:2022 pada sistem LMS untuk melindungi data pengguna serta menjaga integritas dan kepercayaan terhadap sistem. Metode yang diterapkan dalam penelitian ini, yakni metode evaluasi penerapan standard keamanan ISO/IEC 27002:2022. Metode ini memberikan panduan kendali keamanan yang komprehensif untuk memastikan kepatuhan terhadap regulasi perlindungan data serta mitigasi risiko keamanan. Berdasarkan analisis dan penerapan standar ini, penelitian ini memberikan rekomendasi bagi pengelola LMS. Rekomendasi ini diterapkan agar dapat meningkatkan ketahanan sistem dalam menghadapi ancaman keamanan informasi yang semakin kompleks. Rekomendasi ini juga termasuk dengan langkah-langkah tambahan yang disesuaikan dengan kebutuhan spesifik organisasi. Rekomendasi untuk LMS perguruan tinggi XYZ adalah membuat beberapa SOP terkait keamanan sistem. Dampak dari penerapan SOP yang direkomendasikan ini dapat meningkatkan keamanan LMS pada perguruan tinggi XYZ.
Kata Kunci: ISO/IEC 27002, Learning Management System, keamanan sistem informasi

Abstract

Learning Management System (LMS) is a digital platform implemented in the corporate education and training sector to manage, store, and distribute online learning materials. LMS stores sensitive data, such as user personal information, evaluation results, and learning materials so LMS making it vulnerable to security risks from internal and external threats, so it is necessary to implement solid security standards. This study aims to evaluate the implementation of the ISO/IEC 27002:2022 security standard on the LMS system to protect user data and maintain integrity and trust in the system. The method applied in this study is the evaluation method for the implementation of the ISO/IEC 27002:2022 security standard. This method provides comprehensive security control guidelines to ensure compliance with data protection regulations and mitigate security risks. Based on the analysis and implementation of this standard, this study provides recommendations for LMS managers. These recommendations are implemented to increase system resilience in the face of increasingly complex information security threats. These recommendations also include additional steps tailored to the specific needs of the organization. The recommendation for the XYZ College LMS is to create several SOPs related to system security. The impact of implementing this recommended SOP can improve LMS security at XYZ College.
Keywords: *ISO/IEC 27002, Learning Management System information security*

✉ Corresponding author :
Email : ain38375@gmail.com
DOI : https://doi.org/10.31004/edukatif.v7i2.7775
ISSN 2656-8063 (Media Cetak)
ISSN 2656-8071 (Media Online)

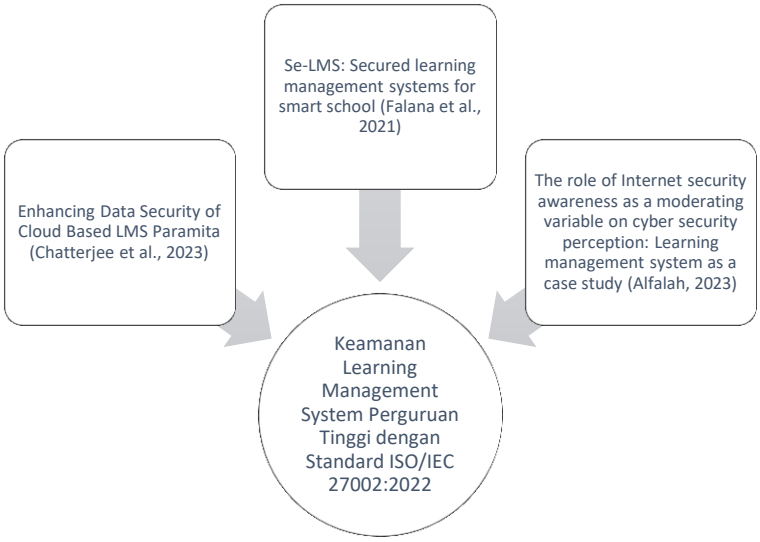
DOI : https://doi.org/10.31004/edukatif.v7i2.7775

PENDAHULUAN

Learning Management System (LMS) merupakan sebuah *platform* yang didesain dalam rangka mempermudah proses kegiatan pembelajaran dan pelatihan melalui daring (Bradley, 2020). LMS dimanfaatkan untuk mengelola, mendistribusikan, dan melacak proses belajar mengajar, baik di institusi pendidikan maupun di perusahaan yang membutuhkan pelatihan karyawan (Nassif et al., 2021). LMS dapat mengakomodasi berbagai bentuk konten, seperti modul *e-learning*, materi pembelajaran interaktif, video, dan kuis untuk mempermudah pelajar dan mahasiswa dalam memahami setiap isi materi yang disampaikan (Egorov et al., 2021).

LMS biasanya terintegrasi dengan berbagai macam alat teknologi, baik integrasi dengan sistem pengukuran kinerja ataupun analitik pembelajaran dalam rangka memaksimalkan tingkat keterlibatan dan efektivitas pembelajaran (Avcı & Ergün, 2022). Secara teknis dan keamanan, LMS harus memenuhi standard tertentu termasuk perlindungan data pengguna yang sesuai dengan peraturan privasi. Keamanan ini sangat penting karena LMS mengelola data pribadi dari banyak pengguna (Chatterjee et al., 2023). Meskipun LMS menawarkan berbagai macam kemudahan untuk akses dan fleksibilitas, sistem ini juga dapat membawa risiko keamanan data yang signifikan (Abdymanapov et al., 2021). LMS banyak menyimpan beraneka macam informasi sensitif, seperti data pribadi pengguna, kinerja akademis, materi kursus, dan informasi yang dilindungi oleh hak kekayaan intelektual (Akacha & Awad, 2023).

State of the art dari penelitian ini tampak pada Gambar 1.



Gambar 1. *State of the Art*

Makalah Chatterjee membahas mengenai ancaman penggunaan LMS yang berbasis *cloud*, serta model dan teknik keamanan kriptografi serta steganografi untuk mengatasi masalah ancaman tersebut (Chatterjee et al., 2023). Ada juga informasi tentang jenis kerentanan keamanan atau operasi pada data *cloud*, dan juga cara mengatasinya menggunakan berbagai jenis algoritma (Akinade et al., 2025). Untuk melindungi berbagai pengguna LMS seperti siswa, instruktur, dan otoritas pengawas, makalah Falana mengusulkan autentikasi multifaktor dan manajemen identitas untuk mengamankan LMS (Falana et al., 2021). Peneliti terdahulu lainnya, yaitu Alfalah menyelidiki pengaruh berbagai dimensi persepsi keamanan siber terhadap sikap mahasiswa mengenai pemakaian sistem manajemen pembelajaran (LMS) dan sejauh mana hubungan ini dapat ditengahi oleh kesadaran keamanan internet (Alfalah, 2023). Perbedaan penelitian yang dilakukan sekarang dibandingkan dengan ketiga peneliti terdahulu tersebut adalah terletak pada penggunaan standard keamanan *Learning Management System* Perguruan Tinggi dengan Standard ISO/IEC 27002:2022. Kebaruan dari

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

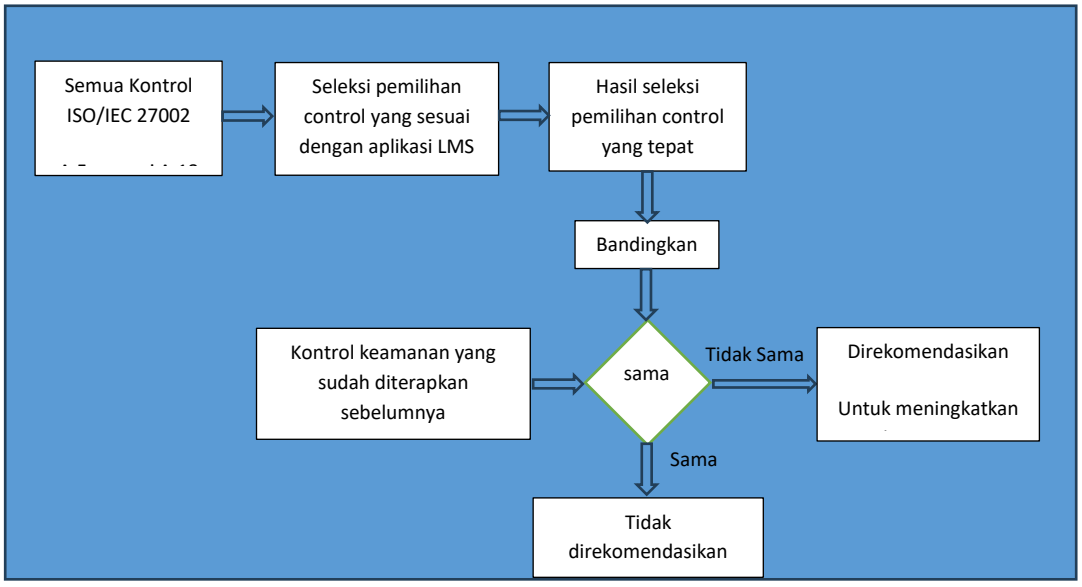
penelitian ini terletak pada upaya dan evaluasi penerapan standard keamanan *Learning Management System* Perguruan Tinggi dengan Standard ISO/IEC 27002:2022.

Penelitian ini penting untuk dilakukan karena LMS menyimpan data yang sensitif, seperti informasi pribadi pengguna, hasil evaluasi, dan materi pembelajaran. LMS memiliki kerentanan terhadap risiko keamanan baik ancaman dari dalam maupun dari luar. Risiko-risiko ini membuat pentingnya penerapan standard keamanan yang kuat dan terpadu.

METODE

Metode yang diterapkan dalam penelitian ini, yakni metode evaluasi penerapan standard ISO/IEC 27002:2022. Standard ini berfungsi dalam melindungi informasi serta menjamin kepatuhan terhadap peraturan perlindungan data yang berlaku (Suorsa & Helo, 2024). Mengadopsi standard ini dapat mempermudah organisasi pengguna LMS dalam menerapkan tahapan keamanan secara sistematis, melindungi data pengguna, dan membangun kepercayaan terhadap sistem pembelajaran yang dikelola. Aplikasi yang ada dalam modul sistem informasi akademik, atau disingkat menjadi LMS (*Learning Management System*), dipergunakan untuk mempermudah dosen dalam proses kegiatan belajar dan mengajar baik unuk kondisi belajar daring maupun belajar luring.

Learning Mangement System adalah salah satu aplikasi yang dibuat untuk proses pembelajaran secara daring dimana ada beberapa kegiatan pengguna baik mahasiswa, dosen maupun admin. Kendali keamanan yang ada di ISO/IEC 27002 meliputi total kendali keamanan yang wajib diterapkan dalam sebuah organisasi. Subjek dari penelitian ini adalah pengguna LMS, yaitu: mahasiswa, dosen, admin dan pengendali keamanan. Tempat penelitian ini dilakukan di Perguruan Tinggi XYZ yang ada di daerah Jawa Barat. Lama penelitian ini selama hampir satu tahun, yaitu pada tahun 2024. Proses validasi data penelitian ini menggunakan metode *content validation* dan triangulasi data.



Gambar 2. *Flowchart* Penelitian

Bagan alir penelitian ini tampak pada Gambar 2. Proses langkah-langkah penelitian ini dimulai dengan cara pendataan semua kendali ISO/IEC 27002, kemudian pemilihan kendali yang sesuai dengan aplikasi LMS. Setelah itu hasil pemilihan kendali yang tepat dibandingkan dengan kendali keamanan yang sudah diterapkan sebelumnya. Apabila hasil perbandingannya sama, maka tidak perlu direkomendasikan. Namun,

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

apabila hasil perbandingannya berbeda, maka perlu dibuat usulan rekomendasi untuk meningkatkan keamanan LMS. Kendali keamanan harus dipilih secara tepat dalam rangka mengamankan aplikasi *Learning Management System* ini. Adapun pemilihan kendali ini dapat dilihat secara satu persatu mulai dari A.5 sampai dengan A.18. Setelah itu dilakukan pemilihan kendali yang tepat yang dapat dilihat dalam diagram Gambar 2.

HASIL DAN PEMBAHASAN

Keamanan sistem informasi adalah aspek penting untuk melindungi data sensitif dan menjaga integritas serta kerahasiaan informasi yang diproses dalam suatu organisasi (Prathiba et al., 2024). Dengan semakin berkembangnya teknologi, ancaman terhadap sistem informasi juga semakin kompleks, mulai dari serangan ancaman siber hingga terjadinya kebocoran data yang dapat merugikan organisasi serta individu pengguna (Villalón-Fonseca, 2022). Oleh sebab itu, setiap organisasi perlu untuk memiliki kebijakan keamanan secara komprehensif seperti penggunaan *firewall*, enkripsi data, serta pembaharuan perangkat lunak secara berkala untuk menangkal ancaman siber tersebut (Zafir et al., 2024).

Tabel 1. Kendali Keamanan ISO/IEC 27002:2022

No.	Kendali	Keterangan
A.5	Kebijakan Keamanan Informasi	Menetapkan kebijakan yang mendukung tujuan keamanan informasi organisasi.
A.6	Organisasi Keamanan Informasi	Menyusun struktur organisasi yang mengelola keamanan informasi, termasuk tanggung jawab individu atau tim.
A.7	Keamanan Sumber Daya Manusia	Meliputi pengelolaan keamanan dalam perekrutan, pelatihan, dan setelah berakhirnya hubungan kerja.
A.8	Pengelolaan Aset	Identifikasi dan perlindungan aset informasi, termasuk perangkat keras, perangkat lunak, dan data sensitif.
A.9	Kontrol Akses	Pengaturan hak akses sistem dan data berdasarkan peran dan kebutuhan, termasuk autentikasi dan otorisasi.
A.10	Enkripsi	Penggunaan enkripsi untuk melindungi kerahasiaan dan integritas data saat disimpan atau dikirimkan.
A.11	Keamanan Fisik dan Lingkungan	Perlindungan terhadap perangkat keras dan infrastruktur fisik yang mendukung sistem informasi.
A.12	Operasi Keamanan	Pemantauan dan pengelolaan sistem untuk menjaga operasional yang aman, serta penanganan insiden keamanan.
A.13	Keamanan Komunikasi	Mengamankan komunikasi informasi, baik internal maupun eksternal, agar tetap terlindungi dari ancaman.
A.14	Pengembangan dan Pemeliharaan Sistem	Memastikan keamanan diterapkan dalam tahap pengembangan perangkat lunak dan pemeliharaan sistem.
A.15	Pengelolaan Hubungan Pihak Ketiga	Mengatur keamanan informasi yang melibatkan pihak ketiga, termasuk vendor dan kontraktor.
A.16	Manajemen Insiden Keamanan Informasi	Prosedur untuk mendeteksi, merespons, dan mengatasi insiden yang mengancam keamanan informasi.
A.17	Aspek Keamanan dalam Manajemen Kontinuitas Bisnis	Menjamin keberlanjutan operasi dengan menjaga keamanan informasi selama situasi darurat atau gangguan.
A.18	Kepatuhan	Memastikan organisasi mematuhi semua hukum, peraturan, dan persyaratan terkait keamanan informasi.

Beberapa kendali keamanan dalam ISO/IEC 27002:2022 dapat dilihat pada Tabel 1. ISO/IEC 27002:2022 adalah standard internasional yang mengatur kebijakan dan kendali keamanan informasi, meliputi

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

pengelolaan akses, keamanan fisik, serta pengelolaan risiko dan insiden. Penerapan standar ini memberikan dasar pijakan yang kuat bagi organisasi dalam mengelola risiko dan menjaga keberlanjutan operasional dalam menghadapi ancaman siber yang terus berkembang pesat. Setelah didapatkan kendali-kendali keamanan yang tepat, hasil dari pemilihan yang ada kaitannya dengan sistem informasi pada *Learning Management System* ini maka selanjutnya dibandingkan terhadap keamanan yang sudah diterapkan sebelumnya. Kendali keamanan ISO/IEC 27002:2013 yang dipilih tampak pada Tabel 2.

Tabel 2. Kendali Keamanan ISO/IEC 27002:2013 yang Dipilih

No.	Kendali	Keterangan	Pemilihan kendali	
			Ya	Tidak
A.5	Kebijakan Keamanan Informasi	Menetapkan kebijakan yang mendukung tujuan keamanan informasi organisasi.		Tidak
A.6	Organisasi Keamanan Informasi	Menyusun struktur organisasi yang mengelola keamanan informasi, termasuk tanggung jawab individu atau tim.		Tidak
A.7	Keamanan Sumber Daya Manusia	Meliputi pengelolaan keamanan dalam perekrutan, pelatihan, dan setelah berakhirnya hubungan kerja.		Tidak
A.8	Pengelolaan Aset	Identifikasi dan perlindungan aset informasi, termasuk perangkat keras, perangkat lunak, dan data sensitif.		Tidak
A.9	Kontrol Akses	Pengaturan hak akses sistem dan data berdasarkan peran dan kebutuhan, termasuk autentikasi dan otorisasi.	Ya	
A.10	Enkripsi	Penggunaan enkripsi untuk melindungi kerahasiaan dan integritas data saat disimpan atau dikirimkan.	Ya	
A.11	Keamanan Fisik dan Lingkungan	Perlindungan terhadap perangkat keras dan infrastruktur fisik yang mendukung sistem informasi.		Tidak
A.12	Operasi Keamanan	Pemantauan dan pengelolaan sistem untuk menjaga operasional yang aman, serta penanganan insiden keamanan.	Ya	
A.13	Keamanan Komunikasi	Mengamankan komunikasi informasi, baik internal maupun eksternal, agar tetap terlindungi dari ancaman.	ya	
A.14	Pengembangan dan Pemeliharaan Sistem	Memastikan keamanan diterapkan dalam tahap pengembangan perangkat lunak dan pemeliharaan sistem.	Ya	
A.15	Pengelolaan Hubungan Pihak Ketiga	Mengatur keamanan informasi yang melibatkan pihak ketiga, termasuk vendor dan kontraktor.		Tidak
A.16	Manajemen Insiden Keamanan Informasi	Prosedur untuk mendeteksi, merespons, dan mengatasi insiden yang mengancam keamanan informasi.		Tidak
A.17	Aspek Keamanan dalam Manajemen Kontinuitas Bisnis	Menjamin keberlanjutan operasi dengan menjaga keamanan informasi selama situasi darurat atau gangguan.		Tidak
A.18	Kepatuhan	Memastikan organisasi mematuhi semua hukum, peraturan, dan persyaratan terkait keamanan informasi.	Ya	

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

Setelah kendali terpilih, selanjutnya membandingkan kendali yang terpilih dengan kendali keamanan yang sudah ada sebelumnya apakah sudah tepat atau belum. Jika sudah tepat maka tidak perlu direkomendasikan. Namun, jika tidak sesuai maka dapat diusulkan rekomendasi dalam rangka meningkatkan keamanan. Kendali keamanan ISO/IEC 27002:2013 terpilih dan ada kaitannya terhadap LMS tampak di dalam Tabel 3.

Tabel 3 Kendali Keamanan ISO/IEC 27002:2013 Terpilih yang Ada Kaitannya dengan LMS

No.	Kendali	Keterangan
A.9	Kontrol Akses	Pengaturan hak akses sistem dan data berdasarkan peran dan kebutuhan, termasuk autentikasi dan otorisasi.
A.10	Enkripsi	Penggunaan enkripsi untuk melindungi kerahasiaan dan integritas data saat disimpan atau dikirimkan.
A.12	Keamanan Operasi	Pemantauan dan pengelolaan sistem untuk menjaga operasional yang aman, serta penanganan insiden keamanan.
A.13	Keamanan Komunikasi	Mengamankan komunikasi informasi, baik internal maupun eksternal, agar tetap terlindungi dari ancaman.
A.14	Pengembangan dan Pemeliharaan Sistem	Memastikan keamanan diterapkan dalam tahap pengembangan perangkat lunak dan pemeliharaan sistem.
A.18	Kepatuhan	Memastikan organisasi mematuhi semua hukum, peraturan, dan persyaratan terkait keamanan informasi.

Kendali keamanan yang dipilih dijabarkan lagi menjadi sub-sub kendali keamanan secara terinci sesuai dengan ISO/IEC 27002:2022 seperti pada tabel berikut mulai dari A.9, A.10, A.12, A.13, A.14 dan A.18 dapat di lihat pada tabel-tabel berikutnya. Sub-sub kendali keamanan ISO/IEC 27002:2022 untuk A.9 kendali akses dibandingkan dengan kendali keamanan yang sudah ada tampak pada Tabel 4.

Tabel 4. Sub-Sub Kendali Keamanan ISO/IEC 27002:2022 untuk A.9 Kendali Akses versus Kendali yang Ada Sebelumnya

Kendali	Gambaran umum	Penjelasan	Keamanan yang diterapkan sebelumnya
A.9.1 - Kebijakan Pengendalian Akses	Menetapkan kebijakan untuk mengelola dan mengontrol akses ke informasi dan sistem berdasarkan kebijakan keamanan.	Menjamin hanya individu yang berwenang yang dapat mengakses data dan sistem.	Sudah dilakukan salah satunya dosen dan mahasiswa login atau akses ke sistem sesuai dengan kapasitasnya, dosen bisa menilai dan bisa mengubah profile sendiri, begitu juga mahasiswa
A.9.2 - Pengelolaan Akses Pengguna	Mengelola akun pengguna, termasuk pembuatan, perubahan, dan penghapusan akun pengguna untuk memastikan akses yang tepat.	Mengontrol siapa yang dapat mengakses sistem serta hak akses yang diberikan kepada pengguna.	Sudah dilakukan hak akses dosen dan mahasiswa di buat sesuai dengan kapasitasnya dan dilakukan oleh admin dan tentunya dikonfirmasi untuk mahasiswa ke bagian akademik dan dosen ke bagian kepegawaian
A.9.3 - Pengelolaan Akses Sistem	Menentukan kontrol akses yang diperlukan dalam sistem untuk membatasi penggunaan	Menjaga data sensitif dan menghindari akses yang tidak sah.	Sudah dilakukan dengan adanya kesadaran bahwa password tidak dibocorkan bahkan tidak bagikan ke orang lain

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

Kendali	Gambaran umum	Penjelasan	Keamanan yang diterapkan sebelumnya
	data sensitif.		
A.9.4 - Pengendalian Akses Jarak Jauh	Menerapkan kebijakan dan prosedur untuk mengelola akses jarak jauh, termasuk penggunaan VPN dan protokol yang aman.	Melindungi akses jarak jauh terhadap potensi risiko dari jaringan yang tidak aman.	Sudah dilakukan jika admin remote selalu menggunakan VPN dan juga menggunakan SSH jika diperlukan
A.9.5 - Pengelolaan Akses yang Terkait dengan Pengguna Kontrak	Menyusun prosedur untuk kontrol akses pengguna yang bekerja berdasarkan kontrak, termasuk kontraktor dan vendor.	Mengelola akses oleh pihak ketiga dan memastikan mereka hanya memiliki hak akses yang diperlukan.	Sudah dilakukan pembuat aplikasi, sudah ada MOU bahwa control akses sudah diberikan ke pihak pengguna sebagai admin akses penuh
A.9.6 - Peninjauan Akses	Melakukan peninjauan berkala terhadap hak akses pengguna untuk memastikan bahwa hak akses tetap sesuai dengan kebutuhan.	Memastikan hak akses yang diberikan tetap relevan dan sesuai dengan perubahan peran atau kondisi.	Sudah dilakukan jika dosen sudah keluar otomatis user dan password yang melekat pada dirinya akan di hapus dan begitu juga mahasiswa yang sudah keluar atau sudah di wisuda

Sub-sub kendali keamanan ISO/IEC 27002:2022 untuk A.10 enkripsi dibandingkan terhadap kendali keamanan yang sudah ada sebelumnya tampak pada Tabel 5.

Tabel 5. Sub-Sub Kendali Keamanan ISO/IEC 27002:2022 untuk A.10 Enkripsi vs Keamanan Sebelumnya

Kendali	Gambaran umum	Penjelasan	Keamanan yang diterapkan sebelumnya
A.10.1 - Penerapan Perlindungan Malware	Organisasi harus memastikan perangkat keras dan perangkat lunak mereka dilindungi dari ancaman malware dengan menggunakan perangkat lunak antivirus, anti-spyware, serta solusi deteksi ancaman lainnya. Perlindungan ini harus selalu diperbarui untuk menangani ancaman baru.	Mencegah malware yang dapat merusak sistem dan menyebar ke seluruh infrastruktur IT organisasi.	Belum di lakukan karena pengguna baik siswa dan dosen menggunakan perangkat laptop atau smartphone milik sendiri, sehingga kurang terkontrol **rekomendasi:** buat himbauan agar selalu mengupdate operating system yang di gunakan dan juga antivirus /anti malware
A.10.2 - Pemantauan dan Pengendalian Malware	Organisasi harus memantau dan mendeteksi ancaman malware secara terus-menerus, serta memastikan respons yang cepat jika ada infeksi terdeteksi. Pemantauan ini termasuk penggunaan perangkat lunak	Mengurangi potensi kerusakan dan mengidentifikasi ancaman malware secepat mungkin untuk mencegah penyebaran lebih lanjut.	Tidak dilakukan pemantauan karena mendapat kesulitan mahasiswa yang akses banyak **rekomendasi:** dibuatkan pelatihan tentang

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

Kendali	Gambaran umum	Penjelasan	Keamanan yang diterapkan sebelumnya
	keamanan dan analisis perilaku untuk mendeteksi infeksi atau serangan.		antivirus, antimalware
A.10.3 - Penghapusan Malware	Ketika malware terdeteksi, organisasi harus memiliki prosedur yang jelas untuk menghapus perangkat lunak berbahaya dan memulihkan sistem dari ancaman tersebut tanpa merusak data yang sah.	Memulihkan integritas sistem setelah infeksi malware dan mengembalikan sistem ke keadaan aman	Belum ada prosedur dari organisasi atau pucuk pimpinan dalam menangani langkah-langkah prosedur atau SOP tentang Malware **rekomendasi**: membuat SOP untuk cara penghapusan malware.

Sub-sub kendali keamanan ISO/IEC 27002:2022 untuk A.12 keamanan operasi dibandingkan dengan keamanan operasi yang telah diterapkan sebelumnya tampak pada Tabel 6.

Tabel 6. Sub-Sub Kendali Keamanan ISO/IEC 27002:2022 untuk A.12 Keamanan Operasi

Kendali	Gambaran umum	penjelasan	Keamanan yang diterapkan sebelumnya
A.12.1 - Pengelolaan Perubahan	Organisasi harus memiliki kebijakan dan prosedur untuk mengelola perubahan sistem dan aplikasi, memastikan bahwa perubahan dievaluasi dan diterapkan tanpa membawa risiko atau kerentanannya.	Menjamin bahwa perubahan yang dilakukan pada sistem atau aplikasi tidak menimbulkan kerentanan baru.	Belum dilakukan karena belum ada perubahan yang signifikan **rekomendasi:** untuk ke depan jika terjadi perubahan pastikan dilakukan saat trafik tidak tinggi dan juga selalu dievaluasi sebelum dijalankan
A.12.2 - Perlindungan dari Perangkat Lunak Berbahaya	Menggunakan perangkat lunak antivirus, pembaruan rutin, dan pemantauan sistem untuk mendeteksi dan melawan perangkat lunak berbahaya yang bisa mengganggu operasional.	Mencegah malware yang bisa menginfeksi sistem dan merusak integritas data atau mengganggu operasi.	Karena aplikasi di hosting di tempat aman/cloud, maka seharusnya sudah dilakukan oleh pihak pengelola hosting, sehingga menjadi ranah pengelola hosting
A.12.3 - Pengelolaan Kapasitas	Memantau kapasitas sistem dan memastikan bahwa sumber daya cukup untuk menangani kebutuhan operasional saat ini dan masa depan, serta menghindari penurunan kinerja.	Menjaga kinerja sistem dan mencegah gangguan operasional akibat kekurangan kapasitas.	Admin selalu memonitoring kapasitas setiap periode tertentu, jika kapasitas sudah mau penuh segera dilakukan penambahan
A.12.4 - Pemisahan Tugas	Menetapkan pembagian tugas yang tepat di antara staf untuk menghindari penyalahgunaan akses dan memastikan bahwa tidak ada individu yang memiliki kontrol penuh atas sistem atau data.	Mencegah risiko kesalahan atau manipulasi data yang tidak terdeteksi dengan memisahkan tanggung jawab operasional.	Sudah dilakukan pembagian tugas untuk masing-masing sehingga dipastikan kalau ada yang salah bisa dicek di log systemnya **rekomendasi:** belum ada MOU atau perjanjian staff

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

Kendali	Gambaran umum	penjelasan	Keamanan yang diterapkan sebelumnya
			tidak boleh menyalahgunakan wewenang di atas materai.

Sub-sub kendali keamanan ISO/IEC 27002:2022 untuk A.13 keamanan komunikasi dibandingkan terhadap keamanan komunikasi yang sudah ada sebelumnya tampak pada Tabel 7.

Tabel 7. Sub-Sub Kendali Keamanan ISO/IEC 27002:2022 untuk A.13 Keamanan Komunikasi

Kendali	Gambaran Umum	Penjelasan	Keamanan yang diterapkan sebelumnya
A.13.1 - Pengelolaan Keamanan Jaringan	Menetapkan kebijakan dan prosedur untuk melindungi informasi yang dikirimkan melalui jaringan, serta memastikan jaringan organisasi aman dari ancaman eksternal dan internal.	Melindungi data yang dikirimkan melalui jaringan agar tetap aman, menghindari pencurian dan penyalahgunaan data.	Belum ada SOP atau peraturan atau prosedur tentang bagaimana mengamankan data saat menggunakan jaringan **rekomendasi:** buatkan SOP tentang saat mengakses ke aplikasi pastikan menggunakan jaringan yang aman seperti tidak menggunakan akses wifi sembarangan atau rental atau di kafe
A.13.2 - Keamanan Komunikasi	Memastikan bahwa sistem komunikasi, baik itu komunikasi internal maupun eksternal, dilindungi untuk mencegah akses yang tidak sah dan kebocoran data. Ini termasuk pengenalan dan penerapan teknik enkripsi serta kontrol akses.	Melindungi informasi yang dikirim atau diterima untuk menjaga kerahasiaan dan integritas data yang beredar.	Sudah melakukan HTTPS
A.13.3 - Perlindungan Data dalam Transit	Menyediakan mekanisme untuk melindungi data saat dalam perjalanan (data in transit) menggunakan enkripsi atau teknologi keamanan lainnya.	Mencegah akses yang tidak sah terhadap data yang sedang dipindahkan antara sistem atau perangkat.	Admin sudah melakukan VPN untuk transfer data sehingga terlindungi

Sub-sub kendali keamanan ISO/IEC 27002:2022 untuk A.14 keamanan pengembangan dan pemeliharaan sistem dibandingkan dengan keamanan pemngembangan dan pemeliharaan sistem sebelumnya, tampak pada Tabel 8.

Tabel 8. Sub-Sub Kendali Keamanan ISO/IEC 27002:2022 untuk A.14 Keamanan Pengembangan dan Pemeliharaan Sistem

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

Kendali	Gambaran Umum	Penjelasan	Keamanan yang diterapkan sebelumnya
A.14.1 - Keamanan dalam Persyaratan Sistem	Menetapkan persyaratan keamanan yang jelas pada tahap awal pengembangan sistem, mulai dari tahap perencanaan hingga implementasi.	Menjamin bahwa keamanan dipertimbangkan dan diterapkan sejak awal dalam siklus hidup sistem.	Pada tahap awal pembuatan sudah diuji keamanannya secara teknis
A.14.2 - Keamanan dalam Desain dan Pengembangan	Memastikan bahwa desain dan pengembangan sistem mencakup kontrol keamanan yang memadai untuk mencegah potensi risiko. Ini meliputi kontrol akses, pengenkripsi data, dan penerapan teknik pengujian keamanan.	Mencegah potensi kerentanannya dengan mengintegrasikan keamanan ke dalam tahap desain dan pengembangan.	Pada saat pengembangan sudah diuji keamanan secara teknis
A.14.3 - Pengujian Keamanan	Menyediakan pengujian yang memadai untuk mengidentifikasi potensi kerentanannya dalam sistem yang sedang dikembangkan atau diperbarui. Pengujian harus dilakukan sepanjang siklus hidup sistem.	Memastikan bahwa sistem yang dikembangkan aman dari potensi kerentanan yang dapat dieksploitasi.	Pengujian keamanan baik dari segi aplikasi dan source code sudah aman
A.14.4 - Keamanan dalam Pemeliharaan Sistem	Memastikan bahwa pemeliharaan sistem yang ada mempertahankan standar keamanan yang telah ditetapkan dan mengurangi potensi kerentanannya yang dapat muncul setelah perubahan atau pemeliharaan dilakukan.	Menjaga keamanan sistem tetap terjaga seiring berjalannya waktu, termasuk setelah pemeliharaan atau perubahan sistem.	Keamanan saat operasional sudah dilakukan

Sub-sub kendali keamanan ISO/IEC 27002:2022 untuk A.18 tentang kepatuhan dibandingkan dengan keamanan yang diterapkan sebelumnya tampak pada Tabel 9.

Tabel 9. Sub-Sub Kendali Keamanan ISO/IEC 27002:2022 untuk A.18 Kepatuhan

Kendali	Gambaran Umum	Penjelasan	Keamanan yang diterapkan sebelumnya
A.18.1 - Kepatuhan Terhadap Peraturan dan Persyaratan	Organisasi harus memastikan bahwa sistem dan operasi informasi mematuhi persyaratan hukum dan peraturan yang berlaku, baik lokal maupun internasional, termasuk perlindungan data dan hak privasi.	Menjamin bahwa organisasi memenuhi kewajiban hukum dan peraturan yang berkaitan dengan pengelolaan data dan informasi.	belum ada peraturan dari manajemn atau puncak pimpinan atau pelatihan **rekomendasi:** buatkan SOP untuk bagaimana keamanan data dan juga password harus dikelola dengan baik
A.18.2 -	Melakukan audit dan pengawasan	Mengidentifikasi dan	Belum dilakukan audit

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

Pengawasan dan Audit	terhadap sistem dan kebijakan untuk memastikan kepatuhan terhadap kebijakan dan standar keamanan yang telah diterapkan, serta mendeteksi ketidaksesuaian atau pelanggaran.	memperbaiki ketidaksesuaian serta memitigasi potensi pelanggaran keamanan informasi.	system dan juga kebijakan tentang kesadaran keamanan **rekomendasi:** dilakukan audit secara periodik minimal 1 tahun sekali untuk peningkatan keamanan
A.18.3 - Pemantauan dan Penilaian Kepatuhan	Memastikan bahwa mekanisme pemantauan dan penilaian diterapkan secara berkelanjutan untuk menilai kepatuhan terhadap kebijakan dan prosedur keamanan informasi yang ada.	Menilai efektivitas kebijakan dan kontrol keamanan serta memastikan keberlanjutan kepatuhan terhadap standar yang berlaku.	Belum adanya komitmen dari pucuk pimpinan supaya patuh terhadap keamanan system informasi **rekomendasi :** membuat peraturan dan komitmen untuk menjaga keamanan system dari serangan orang yang tidak bertanggung jawab

Keamanan teknis dan non-teknis memainkan peranan yang sangat penting dalam memelihara integritas dan kerahasiaan informasi di dalam organisasi, seperti yang ditekankan oleh ISO 27002. Keamanan teknis meliputi kendali berbasis teknologi yang didesain untuk melindungi data dan sistem dari ancaman pihak luar dan ancaman pihak dalam. Hal ini termasuk enkripsi, *firewall*, kendali akses, dan sistem deteksi intrusi, yang bertujuan mencegah akses yang tidak sah, melindungi data saat ditransmisikan atau disimpan, serta mendeteksi potensi ancaman sebelum menimbulkan kerusakan. Keamanan teknis adalah lapisan pertahanan pertama dalam menjaga keamanan informasi yang sensitif dan menjaga sistem dari serangan *cyber* atau pencurian data yang dapat merusak nama baik organisasi dan menimbulkan kerugian keuangan.

Sementara itu, keamanan non-teknis lebih fokus pada kebijakan, prosedur, dan praktik yang diatur untuk mendukung serta memperkuat keamanan teknis. Hal ini meliputi kebijakan keamanan informasi, pelatihan kesadaran keamanan untuk karyawan, manajemen risiko, serta langkah prosedur untuk menangani insiden atau kebocoran data. ISO 27002 menekankan bahwa meskipun kendali teknis sangat penting, manusia dan proses juga memainkan peran kunci dalam pengelolaan risiko keamanan. Pengguna yang tidak terlatih atau kebijakan yang tidak efektif dapat menjadi celah terbuka yang bisa dipergunakan untuk tujuan yang tidak baik oleh pihak-pihak yang bermaksud tidak baik, meskipun teknologi yang digunakan sudah amat canggih. Oleh karena itu, integrasi antara kendali teknis dan non-teknis sangat penting untuk menciptakan pendekatan keamanan yang holistik dan menyeluruh agar mampu mengatasi ancaman yang berkembang di dunia yang semakin bergantung pada teknologi informasi.

Berdasarkan hasil evaluasi penerapan standard internasional ISO mulai dari Tabel 1 sampai terakhir Tabel 9, maka dapat diusulkan rekomendasi untuk *Learning Management System* pada perguruan tinggi XYZ adalah sebagai berikut:

a. Membuat himbauan/membuat peraturan/SOP yang sudah di sepakati oleh pucuk pimpinan agar selalu memperbaharui atau *update* secara berkala untuk *operating system* yang digunakan dan memasang *antivirus*/*anti malware*.
b. Tanggung jawab serta komitmen bersama dari berbagai pihak yang berkepentingan baik pihak manajemen dan pimpinan untuk melaksanakan pelatihan/*training* serta edukasi cara mendeteksi virus/*malware* dan memberikan solusi bagaimana cara menanganinya.

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

c. Pihak pimpinan berkomitmen membuat SOP untuk mendeteksi dan menangani virus/*malware.*
d. Membuat SOP untuk proses jika terjadi perubahan terhadap sistem *Learning Management System* ini dilakukan saat trafik tidak tinggi dan juga selalu dievaluasi sebelum di jalankan/operasional
e. Dibuatkan surat pejanjian/MOU untuk staff admin yang mempunyai hak akses istimewa yang isinya ”tidak boleh menyalahgunakan wewenang” terkait hak akses di atas materai
f. Membuat SOP tentang mengakses ke aplikasi dengan cara menggunakan jaringan yang aman, seperti tidak menggunakan akses wifi sembarangan atau di rental atau di kafe, atau menggunakan perangkat orang lain.
g. Membuat SOP tentang cara bagaimana keamanan data dan juga *password* harus dikelola dengan baik
h. Melakukan audit secara periodik minimal satu tahun sekali untuk peningkatan keamanan
i. Membuat peraturan untuk menjaga keamanan sistem dari serangan orang yang tidak bertanggung jawab.

Pemasangan antivirus dan *antimalware* memiliki banyak faedah untuk LMS, terutama dalam menjaga keamanan perangkat dan data LMS. Pemasangan antivirus dan *antimalware* pada LMS (*Learning Management System*) sangat berfaedah untuk menjaga keamanan data dan kelancaran sistem. Berikut beberapa manfaatnya:

1. Melindungi Data Pengguna

Mencegah pencurian data pengguna, termasuk informasi pribadi, nilai, dan materi pembelajaran. Peneliti Piquero telah mengkaji kejahatan finansial yang difasilitasi melalui aktivitas kriminal berbasis identitas dengan meneliti pandangan tentang pendekatan teknologi untuk pencegahan pencurian identitas di antara 50 profesional yang bekerja di layanan korban kejahatan berbasis identitas, termasuk mereka yang berasal dari sektor publik dan industri swasta (Piquero et al., 2021). Cara efektif untuk mengurangi ancaman ini adalah dengan meningkatkan pengetahuan karyawan tentang keamanan dunia maya dan menggunakan perangkat lunak serta perangkat keras yang tepat.

2. Menghindari Malware & Ransomware

Mencegah infeksi dari file berbahaya yang diunggah oleh pengguna atau disisipkan melalui celah keamanan. Hal ini dapat diatasi dengan langkah-langkah penerapan deteksi malware. Pada tahun 2023, peneliti Abhiram telah mengembangkan kerangka kerja pembelajaran mendalam untuk mendeteksi malware berbasis algoritma pembuatan domain (Abhiram et al., 2023).

3. Mencegah Phishing & Serangan Siber

Memblokir tautan dan file berbahaya yang dapat mencuri kredensial login pengguna. Pembelajaran mesin telah dideskripsikan sebagai langkah efektif dalam menghindari sebagian besar serangan siber. Oleh karena itu, pengembangan AI telah mendorong peningkatan keamanan untuk sebagian besar serangan komputer. Serangan phishing berisiko dan dapat dicegah melalui solusi berbasis AI. Faktor ini menunjukkan perlunya peningkatan kesadaran akan keamanan siber melalui AI. Mengembangkan kesadaran bagi sebagian besar orang akan mencegah jenis serangan ini. Makalah penelitian Ansari menjelaskan bagaimana kesadaran akan keamanan siber berbasis AI dapat memastikan pengurangan serangan phishing (Ansari et al., 2022). Makalah tersebut menunjukkan efektivitas pelatihan kesadaran keamanan siber berbasis AI yang dapat mempengaruhi kadar serangan siber.

4. Menjaga Performa LMS

Mencegah gangguan akibat malware yang bisa memperlambat atau merusak sistem. Peneliti Ogungbemi menyelidiki strategi keamanan titik akhir untuk tenaga kerja jarak jauh yang memanfaatkan jaringan VPN, dengan fokus pada mitigasi serangan ransomware dan botnet. Pendekatan metode campuran digunakan, menganalisis efektivitas solusi titik akhir yang ada dan mensimulasikan strategi segmentasi jaringan. Penelitian tersebut menyoroti peningkatan efektivitas solusi keamanan titik akhir tradisional ketika dilengkapi dengan teknologi canggih dengan aplikasi khusus termasuk penyaringan email untuk memblokir upaya phishing, MFA untuk memverifikasi identitas pengguna, sistem EDR untuk mendeteksi dan memblokir

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

alat akses tidak sah, dan enkripsi untuk mengamankan data selama layanan cloud. Pengenalan segmentasi jaringan dan arsitektur zero-trust semakin mengamankan pusat data dengan membatasi pergerakan lateral dan memerlukan autentikasi ulang berkelanjutan. Hasil penelitiannya menunjukkan bahwa meskipun solusi keamanan titik akhir tradisional tetap penting, efektivitasnya dapat ditingkatkan melalui pendekatan berlapis yang menggabungkan teknologi canggih dengan penelitian tersebut yang menunjukkan waktu respons yang cepat, efisiensi pengendalian yang tinggi, dan kecepatan pemulihan yang cepat di semua segmen. Hasil ini menggarisbawahi kemampuan rencana dalam mendeteksi, mengendalikan, dan memulihkan dari serangan dengan cepat. Edukasi pengguna secara signifikan meningkatkan kesadaran keamanan siber dan mengurangi kerentanan terhadap serangan. Penelitian tersebut memberikan rekomendasi praktis bagi organisasi untuk memperkuat postur keamanan titik akhir mereka dan melindungi tenaga kerja jarak jauh mereka melalui kombinasi teknologi canggih, tindakan proaktif, dan edukasi pengguna yang berkelanjutan (Ogungbemi et al., 2024).

5. Mengamankan File yang Diunggah

Memeriksa file yang diunggah oleh pengguna agar tidak membawa virus atau skrip berbahaya. Di dunia saat ini, sekadar memiliki kapasitas untuk memindahkan file dari satu area ke area lain belumlah memadai. Bisnis saat ini menghadapi berbagai ancaman keamanan dan lingkungan yang sangat kompetitif. Jadi, mereka memerlukan sistem transfer file yang aman untuk melindungi dan mentransfer data sensitif dan penting bagi bisnis mereka dengan andal. Transfer file yang aman adalah metode berbagi data melalui metode pengiriman yang aman dan andal. Kriptografi adalah teknik yang digunakan untuk mengamankan informasi dan komunikasi di hadapan pihak ketiga. Para peneliti menggunakan teknik ini untuk memastikan bahwa hanya pihak tertentu saja yang menjadi sasaran informasi tersebut yang dapat membacanya. Dengan menggunakan kriptografi, dapat mencegah pengguna yang tidak berwenang mengakses informasi yang dibagikan secara pribadi. Dalam makalah terdahulu, rencana yang diusulkan adalah untuk mengatasi masalah terkait data yang disimpan oleh pengguna di cloud yang harus dienkripsi daripada menyimpannya dalam bentuk biasa sehingga data akan terlindungi dari penyerang yang mencoba membaca, menghapus, atau memanipulasi data. Aplikasi difokuskan pada autentikasi pengguna secara aman, sebelum menyimpan dan membagikan file. Peneliti Madhumala membuat aplikasi yang memungkinkan pengguna mengenkripsi dan mendekripsi semua jenis file tanpa perubahan ukuran selama enkripsi & dekripsi, menyimpan setiap data pengguna dalam bentuk terenkripsi di cloud, untuk menyediakan media komunikasi antara pengguna melalui aplikasi obrolan, untuk memberikan akses langsung ke file untuk operasi CRUD hanya kepada pemiliknya (Madhumala et al., 2021).

6. Mencegah Penyebaran Ancaman ke Jaringan Lain

Jika LMS terhubung dengan sistem lain, antivirus membantu mencegah penyebaran malware ke perangkat atau server lain (Nurhayati, 2019). Penggunaan internet telah tumbuh secara eksponensial, seiring dengan bertambahnya individu dan perusahaan yang melakukan banyak transaksi harian di dunia maya daripada di dunia nyata (Nurhayati, 2021). Pandemi virus corona (COVID-19) telah mempercepat proses ini (Nurhayati, 2022). Sebagai akibat dari meluasnya penggunaan lingkungan digital, kejahatan tradisional juga telah bergeser ke ruang digital. Teknologi yang muncul seperti komputasi cloud, Internet of Things (IoT), media sosial, komunikasi nirkabel, dan mata uang kripto meningkatkan masalah keamanan di dunia maya (Nurhayati et al., 2022). Baru-baru ini, penjahat dunia maya mulai menggunakan serangan dunia maya sebagai layanan untuk mengotomatiskan serangan dan memanfaatkan dampaknya. Penyerang mengeksploitasi kerentanan yang ada di lapisan perangkat keras, perangkat lunak, dan komunikasi. Berbagai jenis serangan dunia maya termasuk *distributed denial of service* (DDoS), *password, phishing, remote, man-in-the-middle, privilege escalation*, dan *malware*. Serangan generasi baru pada teknik penghindaran sistem perlindungan tradisional seperti firewall, sistem deteksi intrusi, perangkat lunak antivirus, daftar kontrol akses, dan lain-lain, tidak lagi efektif dalam mendeteksi serangan canggih ini. Oleh sebab itu, ada keperluan yang mendesak agar bisa menemukan solusi yang inovatif dan lebih layak untuk mencegah serangan siber. Makalah Aslan

DOI : https://doi.org/10.31004/edukatif.v7i2.7775

pertama-tama menjelaskan secara ekstensif alasan utama serangan siber. Kemudian, mengulas serangan, pola serangan, dan teknik deteksi terkini. Ketiga, artikel Aslan membahas solusi teknis dan nonteknis kontemporer untuk mengenali serangan terlebih dahulu. Menggunakan teknologi yang sedang tren seperti pembelajaran mesin, pembelajaran mendalam, *platform cloud*, data besar, dan blockchain dapat menjadi solusi yang menjanjikan untuk serangan siber saat ini dan masa mendatang. Solusi teknologi ini dapat membantu dalam mendeteksi *malware*, deteksi intrusi, identifikasi *spam*, klasifikasi serangan DNS, deteksi penipuan, mengenali saluran tersembunyi, dan membedakan ancaman persisten tingkat lanjut. Namun, beberapa solusi yang menjanjikan, terutama pembelajaran mesin dan pembelajaran mendalam, tidak tahan terhadap teknik penghindaran terhadap serangan siber yang lebih cerdas (Aslan et al., 2023).

Oleh karena itu, selain memasang *antivirus* dan *antimalware*, penting juga untuk selalu memperbarui LMS, menerapkan autentikasi dua faktor (2FA), serta mengedukasi pengguna tentang keamanan siber. Dalam rangka menguatkan keamanan sistem LMS (*Learning Management System*), terdapat tiga tahapan penting yang bisa diterapkan:

1. Memperbaharui LMS (*Learning Management System*)

Tujuan dari memperbaharui LMS adalah untuk menutup kemungkinan celah keamanan yang terbuka agar dapat memperketat stabilitas dengan tahapan sebagai berikut:

a. Memeriksa versi terbaru dari *platform* LMS yang dipakai (seperti *Google Classroom, Moodle, Canvas*, dan lain-lain).
b. Melakukan *backup* data sebelum melakukan pembaruan atau *update* (*file* + *database*).
c. Melakukan *update* sistem melalui:
    1) Panel admin (untuk *platform* seperti Moodle)
    2) *Command line* (jika LMS di-*hosting* sendiri)
d. Melakukan uji fungsionalitas setelah proses *update*: pastikan *plugin*, tema, dan modul tetap berjalan normal.
e. Memeriksa dan memperbaharui *plugin* dengan cara memakai *plugin* resmi dari sumber yang tepercaya, dan melakukan proses *update* secara berkala.

2. Menerapkan autentikasi dua faktor (2FA)

Tujuan dari autentikasi dua faktor ini adalah untuk mempertebal lapisan keamanan tambahan untuk *login* pengguna dengan cara menerapkan:

a. Mengaktifkan 2FA dari pengaturan admin (apabila LMS mendukung native 2FA, seperti Moodle).
b. Menggunakan *plugin* pihak ketiga apabila fitur 2FA tidak tersedia bawaan (contoh: "*Two-Factor Authentication*" *plugin* untuk Moodle).
c. Memilih metode 2FA:
    1) *Authenticator App* (*Google Authenticator, Microsoft Authenticator*)
    2) SMS (kurang aman, tapi tetap lebih baik daripada tidak ada)
d. Diterapkan untuk admin dan dosen terlebih dahulu, kemudian diwajibkan kepada semua pengguna.

3. Mengedukasi pengguna tentang keamanan siber

Tujuan dari edukasi ini adalah untuk menurunkan risiko kesalahan manusia seperti *phishing* serta penggunaan *password* yang lemah yang sebenarnya masih bisa diatasi dengan cara strategi edukasi sebagai berikut:

a. Membuat modul pelatihan *online* tentang:
    1) Cara membuat *password* yang kuat
    2) Bahaya *phishing* dan cara menghindarinya
    3) Pentingnya *logout* setelah akses
b. Kirim *email*/*broadcast* berkala dengan tips keamanan singkat.

c. *Quiz* atau simulasi *phishing*: memberikan contoh email palsu dan menguji reaksi pengguna.
d. Pasang *banner* peringatan saat *login* dengan tips keamanan.

Peran penelitian ini bagi perkembangan keilmuan adalah memberikan usulan rekomendasi bagaimana cara meningkatkan sistem keamanan untuk *Learning Management System* pada perguruan tinggi. Keterbatasan dari penelitian ini, yakni penelitian ini hanya dilakukan pada sebuah perguruan tinggi tertentu saja, belum mencakup seluruh perguruan tinggi di kota Bandung. Perkembangan penelitian selanjutnya adalah akan dikembangkan perbandingan penelitian antar perguruan tinggi lainnya yang ada di wilayah kota Bandung.

SIMPULAN

Berdasarkan hasil pengecekan dengan kontrol/kendali yang telah terpilih sesuai dengan standard ISO/IEC 27002:2022, telah diperoleh hasil bahwa sistem informasi terkait *Learning Management System* yang ada di perguruan tinggi swasta ini masih perlu ditambahkan keamanan non teknisnya. Keamanan secara teknis sudah dilakukan terbukti saat pembuatan, pengoperasian dan juga saat perubahan keamanan teknis selalu diperhatikan, akan tetapi keamanan non teknis masih perlu dilakukan, mengingat dalam standard ISO 27002:2022 menyatakan bahwa keamanan secara teknis sudah dilakukan akan tetap kurang aman jika tidak dilakukan keamanan non teknis.

Keamanan non teknis menjadi kunci karena sekuat-kuatnya keamanan teknis pasti akan jebol juga, jika tidak dilakukan pengamanan secara non teknis, Sebagian besar dari keamanan non teknis inilah yang menjadi faktor kelemahan yang sering terjadi karena manusia atau pengguna yang ceroboh dan juga tidak adanya pengetahuan tentang kesadaran keamanan informasi. Oleh karena itu perlu dilakukan pelatihan dan pengetahuan bagaimana cara menggunakan user dan password yang kuat, serta tidak memberikan user dan password kepada orang lain.

UCAPAN TERIMA KASIH

Penulis mengucapkan banyak terima kasih kepada semua pihak yang telah ikut berkontribusi dalam penelitian ini baik dana maupun sumbang saran untuk kebaikan dari penulisan karya ilmiah ini.

DAFTAR PUSTAKA

Abdymanapov, S. A., Muratbekov, M., Altynbek, S., & Barlybayev, A. (2021). Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems. *IEEE Access*, *9*, 156556–156565. https://doi.org/10.1109/ACCESS.2021.3129488

Abhiram, P., Anver, S. R., & Rahiman, M. A. (2023). A Deep learning framework for domain generation algorithm based malware detection. *Research Square*, *24*(July), 1–31. https://doi.org/https://doi.org/10.21203/rs.3.rs-3154412/v1

Akacha, S. A.-L., & Awad, A. I. (2023). Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability*, *15*(19), 1–27. https://doi.org/10.3390/su151914132

Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2025). Cloud Security Challenges and Solutions : A Review of Current Best Practices. *International Journal of Multidisciplinary Research and Growth Evaluation*, *6*(1), 26–35. https://doi.org/https://doi.org/10.54660/.IJMRGE.2025.6.1.26-35

Alfalah, A. A. (2023). The role of Internet security awareness as a moderating variable on cyber security

perception: Learning management system as a case study. *International Journal of Advanced and Applied Sciences*, *10*(4), 136–144. https://doi.org/10.21833/ijaas.2023.04.017

Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. *International Journal of Smart Sensor and Adhoc Network.*, *3*(3), 61–72. https://doi.org/10.47893/ijssan.2022.1221

Aslan, O., Aktug, S. S., Ozkan-okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(1333), 1–42. https://doi.org/https:// doi.org/10.3390/electronics12061333

Avcı, Ü., & Ergün, E. (2022). Online students' LMS activities and their effect on engagement, information literacy and academic performance. *Interactive Learning Environments*, *30*(1), 71–84. https://doi.org/10.1080/10494820.2019.1636088

Bradley, V. M. (2020). Learning Management System (LMS) Use with Online Instruction. *International Journal of Technology in Education*, *4*(1), 68. https://doi.org/10.46328/ijte.36

Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2023). Enhancing Data Security of Cloud Based LMS. *Wireless Personal Communications*, *130*(2), 1123–1139. https://doi.org/10.1007/s11277-023-10323-5

Egorov, E. E., Prokhorova, M. P., Lebedeva, T. E., Mineeva, O. A., & Tsvetkova, S. Y. (2021). Moodle LMS: Positive and Negative Aspects of Using Distance Education in Higher Education Institutions. *Propósitos y Representaciones*, *9*(SPE2), 1–12. https://doi.org/10.20511/pyr2021.v9nspe2.1104

Falana, O. J., Ebo, I. O., Akinwunmi, O., & Odom, I. O. (2021). Se-LMS: Secured learning management systems for smart school. *International Journal of Software Engineering and Computer Systems*, *7*(1), 36–46. https://doi.org/10.15282/ijsecs.7.1.2021.4.0080

Madhumala, Chhetri, S., KC, A., & Jain, H. (2021). Secure File Storage & Sharing on Cloud Using Cryptography. *International Journal of Computer Science and Mobile Computing*, *10*(5), 49–59. https://doi.org/10.47760/ijcsmc.2021.v10i05.005

Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine Learning for Cloud Security: A Systematic Review. *IEEE Access*, *9*(February), 20717–20735. https://doi.org/10.1109/ACCESS.2021.3054129

Nurhayati, A. (2019). Mapping Perception of Consumer Antivirus Software with Multidimensional Scaling Method. *APTIKOM Journal on Computer Science and Information Technologies*, *4*(3), 91–95. https://doi.org/10.11591/APTIKOM.J.CSIT.13

Nurhayati, A. (2021). The effect of the internet during COVID-19 on work using the manova algorithm The effect of the internet during COVID-19 on work using the manova algorithm. *Journal of Physics: Conference Series*, *1844*, 12030. https://doi.org/10.1088/1742-6596/1844/1/012030

Nurhayati, A. (2022). Pengembangan Jasa Salon Di Masa Pandemi Covid-19 Dengan Factor Analysis Method. *Sistemik*, *10*(1), 33–40. https://doi.org/https://doi.org/10.53580/sistemik.v10i1.68

Nurhayati, A., Gusdevi, H., & Sugiatna, A. (2022). Effect of Social Media Function on Student Graduation Rate. *Social Science Studies*, *2*(6), 461–471. https://doi.org/10.47153/sss26.4092022

Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., & Oladoyinbo, O. B. (2024). Overcoming Remote Workforce Cyber Threats: A Comprehensive Ransomware and Bot Net Defense Strategy Utilizing VPN Networks. *Journal of Engineering Research and Reports*, *26*(8), 161–184. https://doi.org/10.9734/jerr/2024/v26i81237

Piquero, N. L., Piquero, A. R., Gies, S., Green, B., Bobnis, A., & Velasquez, E. (2021). Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders. *Victims and Offenders*, *16*(3), 444–463. https://doi.org/10.1080/15564886.2020.1826023

Prathiba, S. B., Govindarajan, Y., Ganesan, V. P. A., Ramachandran, A., Selvaraj, A. K., Bashir, A. K., &

Gadekallu, T. R. (2024). Fortifying Federated Learning in IIoT: Leveraging Blockchain and Digital Twin Innovations for Enhanced Security and Resilience. *IEEE Access*, *12*(April), 68968–68980. https://doi.org/10.1109/ACCESS.2024.3401039

Suorsa, M., & Helo, P. (2024). Information security failures identified and measured–ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis. *Information Security Journal: A Global Perspective*, *33*(3), 285–306. https://doi.org/10.1080/19393555.2023.2270984

Villalón-Fonseca, R. (2022). The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity. *Computers and Security*, *120*(102805), 1–22. https://doi.org/10.1016/j.cose.2022.102805

Zafir, E. I., Akter, A., Islam, M. N., Hasib, S. A., Islam, T., Sarker, S. K., & Muyeen, S. M. (2024). Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques. *Internet of Things*, *28*(April), 101357. https://doi.org/10.1016/j.iot.2024.101357