JIMT | Jurnal Informatika Multimedia dan Teknik
e-ISSN: 3089-6010
OPEN ACCESS
URL Jurnal : https://yptb.org/index.php/jimt | e-mail : jurnalq17@gmail.com | https://doi.org/10.71456/jimt/v2i1.1362

ANALISIS RISIKO KEAMANAN PADA SISTEM *E-LEARNING* BERDASARKAN ISO 27005

Risk Security Analysis in E-Learning Systems Based on ISO 27005

Rifki Maulana[1*]

Fathoni Mahardika[2]

*[1-2]Universitas Sebelas April Sumedang, Sumedang, Jawa Barat, Indonesia

*email: rifkkimaulana@gmail.com

Abstrak

Penelitian ini menyelami bagaimana sistem e-learning dapat ditingkatkan keamanannya. Dengan menggunakan panduan ISO/IEC 27005 dan melakukan studi literatur yang sistematis, ditemukan berbagai aset penting, baik yang bersifat teknis (seperti server, perangkat lunak, dan data) maupun non-teknis (seperti sumber daya manusia dan kebijakan). Penelitian ini juga mengidentifikasi ancaman umum seperti serangan phishing dan malware, serta titik-titik lemah yang sering muncul, baik dari sisi manusia maupun teknologi. Dengan menerapkan ISO/IEC 27005, risiko dipetakan, dianalisis, dan dinilai menggunakan matriks khusus. Selanjutnya, disusun strategi untuk mengatasi risiko-risiko tersebut, dengan menggabungkan langkah-langkah administratif (seperti pelatihan kesadaran keamanan, kebijakan yang jelas, dan manajemen akses) dan teknis (seperti Multi-Factor Authentication, patching, penguatan jaringan, enkripsi, dan backup data). Penelitian ini diharapkan dapat menjadi panduan praktis untuk mengenali risiko e-learning, menerapkan standar keamanan, dan memberikan rekomendasi yang dapat langsung diimplementasikan. Tujuannya adalah agar pendidikan digital menjadi lebih aman dan sistem e-learning dapat diandalkan sepenuhnya.

Kata Kunci:
Analisis Risiko
Keamanan Informasi
Sistem E-Learning
ISO 27005

Abstract

This research delves into how the security of e-learning systems can be enhanced. By using the ISO/IEC 27005 guidelines and conducting a systematic literature study, various important assets were identified, both technical (such as servers, software, and data) and non-technical (such as human resources and policies). This research also identifies common threats such as phishing attacks and malware, as well as frequently occurring vulnerabilities, both from human and technology sides. By applying ISO/IEC 27005, risks are mapped, analyzed, and assessed using a specialized matrix. Subsequently, strategies are developed to address these risks, combining administrative measures (such as security awareness training, clear policies, and access management) and technical measures (such as Multi-Factor Authentication, patching, network hardening, encryption, and data backups). This research is expected to serve as a practical guide for identifying e-learning risks, implementing security standards, and providing recommendations that can be directly implemented. The goal is to make digital education safer and the e-learning systems fully reliable.

Keywords:
Risk Analysis
Information Security
E-Learning Systems
ISO 27005

Submit Tgl.: 03-Juli-2025 Diterima Tgl.: 05-Juli-2025 Diterbitkan Tgl.: 06-Juli-2025

Cara mengutip Maulana, R., & Mahardika, F. (2025). Analisis Risiko Keamanan pada Sistem E-Learning Berdasarkan ISO 27005. *Jurnal Informatika, Multimedia dan Teknik*, *2*(1), 11–20. Diambil dari https://yptb.org/index.php/jimt/article/view/1362

PENDAHULUAN

Perkembangan teknologi yang begitu pesat telah mendorong adopsi sistem e-learning secara besar-besaran, dimana hal tersebut menjadikannya bagian krusial dalam dunia pendidikan, terutama untuk memfasilitasi pembelajaran jarak jauh yang fleksibel. Namun, di balik kemudahan beradaptasi dengan era digital ini, memunculkan tantangan besar terkait keamanan informasi yang tidak bisa diabaikan. Akses yang mudah dan sentralisasi data pada platform e-learning justru menciptakan celah kerentanan terhadap berbagai risiko, mulai dari pencurian data, serangan

siber, hingga akses tidak sah. Hal-hal ini tentu saja dapat mengganggu proses pembelajaran dan bahkan merusak reputasi institusi. Sejalan dengan apa yang ditemukan oleh (Utami, Supramaji, & Isnaini, 2023) Peningkatan ancaman keamanan pada sistem digital ini menuntut sebuah pendekatan yang sistematis untuk mengidentifikasi dan mengelola risiko-risiko tersebut. Dalam menghadapi tantangan ini, maka perlu penerapan kerangka kerja manajemen risiko yang terstruktur. Standar internasional ISO/IEC 27005:2018 hadir sebagai solusi yang relevan, menyediakan panduan komprehensif untuk manajemen risiko keamanan informasi. Kerangka kerja ini mencakup proses yang sistematis, dimulai dari identifikasi, analisis, evaluasi, hingga penanganan risiko (Hikam, Dewi, & Praditya, 2024). Dengan panduan ini, institusi pendidikan dapat membangun pertahanan keamanan yang lebih kuat untuk melindungi aset informasi pada sistem e-learning mereka. Oleh karena itu, penelitian ini berfokus pada analisis risiko dan keamanan informasi pada sistem e-learning dengan mengadopsi kerangka kerja ISO 27005 dalam bidang ini, khusus nya dalam bidang pendidikan di Indonesia, karena mengingat masih terbatasnya penelitian yang mengaplikasikan ISO 27005 dalam bidang ini. Diharapkan, hasil penelitian ini dapat menghasilkan model rekomendasi mitigasi yang praktis dan relevan, yang pada gilirannya dapat mewujudkan atau mendukung sistem e-learning yang lebih aman dan berkelanjutan. Secara lebih spesifik, penelitian ini bertujuan untuk menjawab beberapa rumusan pertanyaan, yaitu: (1) Bagaimana berbagai jenis risiko keamanan pada sistem e-learning dapat diidentifikasi dan dipahami?, (2) Bagaimana kerangka kerja ISO/IEC 27005 dapat diterapkan secara praktis untuk mengelola risiko keamanan informasi pada sistem e-learning?, (3) Apa saja solusi atau rekomendasi mitigasi yang konkret dan efektif yang bisa dirumuskan untuk mengatasi risiko yang teridentifikasi?, (4) Bagaimana penelitian ini dapat memberikan kontribusi nyata dalam memperkuat keamanan informasi di lingkungan pendidikan digital?.

METODE PENELITIAN

Alat dan Bahan

Dalam penelitian ini, digunakan satu buah laptop (Intel Core i5, RAM 8 GB) sebagai perangkat utama. Untuk perangkat lunak, dimanfaatkan ***Publish or Perish*** untuk mencari artikel, ***Microsoft Word*** untuk menulis laporan, dan ***Mendeley*** untuk mengelola daftar pustaka. Bahan utama penelitian ini adalah artikel-artikel ilmiah dan jurnal terpercaya yang relevan dengan topik. Artikel-artikel yang digunakan diterbitkan antara tahun 2020 hingga 2025 dan ditemukan melalui ***Google Scholar*** serta ***Crossref*** dengan kata *kunci* "*risk analysis e-learning*", "*ISO 27005*", dan "*cybersecurity in education*".

Metode Pelaksanaan

Penelitian ini mengadopsi metode studi literatur, yaitu mengkaji penelitian-penelitian yang sudah ada secara sistematis menggunakan panduan ***PRISMA***. Proses pelaksanaannya adalah sebagai berikut: *Pertama*, dilakukan tahap pencarian sumber. Pada tahap ini, dicari artikel-artikel awal dari **Google Scholar** dan **Crossref** menggunakan kata kunci yang telah ditentukan. Jumlah artikel yang berhasil ditemukan kemudian dicatat. *Kedua*, dilanjutkan ke tahap penyaringan. Di sini, artikel-artikel yang sama (duplikat) dihapus. Setelah itu, artikel-artikel yang tersisa disaring lagi berdasarkan judul dan abstraknya untuk menyisihkan yang tidak relevan dengan fokus penelitian. *Ketiga*, dilaksanakan tahap penilaian kelayakan dan kualitas. Artikel-artikel yang lolos saringan awal akan dibaca seluruh isinya untuk dinilai apakah sudah memenuhi syarat-syarat yang ditentukan (kriteria inklusi dan eksklusi). Bersamaan dengan itu, kualitas dari setiap artikel juga dinilai menggunakan sistem skor yang telah ditetapkan. Artikel yang tidak memenuhi syarat atau kualitasnya kurang baik akan dikeluarkan dari daftar.

Tabel I. Kriteria Inklusi dan Eksklusi

No	Kriteria	Jenis
1	Artikel ilmiah terbitan tahun 2020-2025	Inklusi

2	Fokus pada analisis atau manajemen risiko keamanan informasi	Inklusi
3	Membahas atau menggunakan standar ISO/IEC 27005	Inklusi
4	Relevan dengan sistem e-learning atau akademik	Inklusi
5	Tidak membahas ISO/IEC 27005	Eksklusi
6	Tidak relevan dengan keamanan e-learning	Eksklusi
7	Hanya berupa tinjauan umum tanpa analisis yang spesifik	Eksklusi
8	Tidak bisa diakses secara penuh	Eksklusi

Tabel II. Kriteria Penilaian Kualitas

Kode	Penjelasan
QA1	Apakah tujuan penelitian dijelaskan dengan jelas?
QA2	Apakah cara penelitian sudah sesuai dalam menjawab tujuan?
QA3	Apakah cara menganalisis datanya sudah benar?
QA4	Apakah Kesimpulan yang diambil sudah sesuai dengan hasil yang didapat?

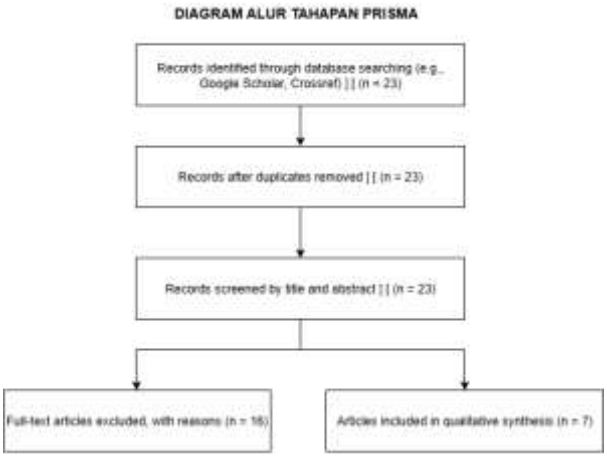
Setelah seluruh proses seleksi selesai, artikel-artikel yang terpilih akan dianalisis lebih lanjut. Data-data penting dari setiap artikel akan diambil *(ekstraksi data)* untuk menemukan apa saja aset, ancaman, dan kelemahan yang sering terjadi pada sistem e-learning. Data tersebut kemudian dianalisis untuk menentukan seberapa besar kemungkinan terjadinya sebuah risiko *(likelihood)* dan seberapa besar dampaknya *(impact)*. Berdasarkan hasil analisis tersebut, dilakukan evaluasi dan penyusunan rekomendasi. Tingkat risiko akan dinilai untuk menentukan mana yang harus ditangani lebih dulu. Setelah itu, barulah disusun saran langkah-langkah pengamanan yang sesuai. *Terakhir*, seluruh temuan dari proses ini disusun secara sistematis ke dalam format artikel ilmiah.

HASIL DAN PEMBAHASAN

Pada bagian ini, disajikan temuan-temuan kunci dari studi literatur yang telah dilakukan. Pembahasan diawali dengan hasil proses seleksi artikel menggunakan kerangka **PRISMA**, kemudian dilanjutkan dengan analisis mendalam untuk menjawab setiap pertanyaan penelitian.

Tinjauan Literatur

Tahap awal analisis adalah mengumpulkan dan menganalisis berbagai artikel ilmiah yang relevan. Proses seleksi artikel ini mengikuti alur **PRISMA** seperti yang digambarkan pada Gambar 1.



Gambar 1. *Diagram Alir PRISMA Proses Seleksi Literatur*

Penjelasan Proses Seleksi:

Proses seleksi diawali dengan tahap identifikasi, di mana pencarian awal menggunakan kata kunci yang relevan menghasilkan total 23 artikel dari berbagai portal akademik. Selanjutnya, dilakukan tahap penyaringan, di mana tidak ada duplikasi yang ditemukan, dan ke-23 artikel tersebut disaring berdasarkan judul serta abstrak. Pada tahap kelayakan, 23 artikel teks lengkap dievaluasi berdasarkan kriteria inklusi, eksklusi, dan kualitas metodologi, yang menghasilkan 16 artikel dikecualikan karena berbagai alasan. Akhirnya, pada tahap inklusi, sebanyak 7 artikel yang memenuhi semua kriteria dimasukkan ke dalam sintesis kualitatif untuk analisis lebih lanjut.

Hasil analisis awal dari seluruh 23 artikel disajikan pada Tabel III. Daftar dan Analisis Seluruh Artikel Ilmiah

Tabel III. Daftar dan Analisis Seluruh Artikel Ilmiah

No	Penulis (Tahun)	Fokus Utama	Relevansi
1	Liderman (2022)	Menjelaskan metodologi 4 tahap (ARL-27005) untuk analisis risiko kualitatif sesuai ISO 27005.	Relevan untuk memahami proses inti ISO 27005.

2	Junior & Arima (2023)	Tinjauan literatur sistematis yang mengidentifikasi motivasi adopsi ISO 27005.	Memberikan justifikasi akademis pentingnya ISO 27005.
3	Utami et al. (2023)	Studi kasus kombinasi ISO 27005 dan DREAD untuk penilaian risiko website.	Contoh praktis kombinasi metode untuk identifikasi ancaman.
4	Riadi (2025)	Studi kasus pada sistem layanan pelabuhan menggunakan ISO 27005 dan FMEA.	Memberikan contoh terstruktur identifikasi aset dan ancaman.
5	Isnaini, Sari, & Kuncoro (2023)	Studi kasus pada aplikasi pelayanan desa, risiko tertinggi adalah server down.	Contoh jelas pembuatan matriks penilaian risiko.
6	Rasyid & Aji (2025)	Studi kasus pada SaaS untuk sistem manajemen sekolah.	Sangat relevan karena sistem manajemen sekolah adalah bentuk e-learning.
7	Sinulingga, Raharjo, & Trisnawaty (2024)	Mengintegrasikan ISO 31000 dan ISO 27005 pada proyek Agile.	Wawasan tentang manajemen risiko dalam siklus hidup pengembangan.
8	Syahindra, Primasari, & Iriantor (2022)	Menggunakan hasil evaluasi Indeks KAMI (ISO 27001) sebagai input untuk manajemen risiko ISO 27005.	Contoh pendekatan gap analysis yang baik.
9	Leasa & Prassida (2024)	Studi kasus pada SIAKAD, mengidentifikasi risiko pada aset data, software, hardware, dan people.	Sangat relevan, contoh konkret risiko pada sistem e-learning.
10	Hikam et al. (2024)	Analisis risiko dipicu oleh ketidakpatuhan terhadap kontrol ISO 27002.	Menunjukkan keterkaitan antar standar dalam seri ISO 27000.
11	Meitarice, Febyana, Fitriansyah, Kurniawan, & Nugroho (2024)	Studi kasus komprehensif pada portal akademik universitas negeri di Indonesia.	Sangat relevan, menyediakan daftar ancaman dan kerentanan yang lengkap.
12	Amirinnisa & Bisma (2023)	Menggunakan ISO 27005 sebagai persiapan sertifikasi ISO 27001.	Menunjukkan peran ISO 27005 sebagai langkah awal implementasi SMKI.
13	Arias & Soriano (2022)	Mengevaluasi risiko adopsi cloud pada UKM, menemukan risiko terbesar adalah kurangnya keahlian internal.	Memberikan perspektif risiko non-teknis (SDM).
14	Achuthan, Ramanathan, Srinivas, & Raman (2024)	Tinjauan literatur sistematis tentang peran AI dalam keamanan siber.	Referensi tingkat tinggi untuk diskusi tren masa depan.
15	Aslan, Aktuğ, Ozkan-Okay, Yilmaz, & Akin (2023)	Tinjauan komprehensif yang mengklasifikasikan berbagai ancaman dan kerentanan.	Sumber fundamental untuk definisi dan kategori.
16	AL-Dosari & Fetais (2023)	Meta-analisis yang mengkritik kerangka kerja risiko yang terlalu abstrak untuk UKM.	Berguna untuk argumen bahwa manajemen risiko perlu disesuaikan.
17	Hamit et al. (2020)	Studi kasus pembuatan risk treatment plan pada sistem klinis.	Contoh praktis yang baik untuk tahap penanganan risiko.
18	Alheadary (2023)	Mengembangkan model penilaian risiko berbasis ISO 27005 untuk konteks lokal.	Menunjukkan pentingnya adaptasi kerangka kerja standar.
19	Putra & Soewito (2023)	Studi kasus integrasi ISO 27005 dan NIST SP 800-30.	Contoh pendekatan hibrida untuk analisis komprehensif.
20	Putri & Hakim (2021)	Studi kasus kombinasi ISO 27005 dan NIST SP 800-30 pada layanan jaringan pemerintah.	Referensi kuat untuk pendekatan hibrida dan kriteria risiko.
21	Septanto, Sabrina, & Irmawati (2022)	Membahas pentingnya kerangka kerja keamanan untuk e-learning di perguruan tinggi.	Sangat relevan, membahas aset non-teknis seperti kebijakan.
22	Jonny, Ambarwati, & Darujati (2021)	Studi kasus pada SIM puskesmas, termasuk matriks penanganan risiko.	Contoh penerapan di sektor publik dengan referensi penanganan risiko.
23	Hidayatullah, Kunthi, & Harwahyu (2024)	Studi kasus pada sistem manajemen audit dengan metode perhitungan risiko yang disesuaikan.	Contoh kustomisasi metode penilaian dalam kerangka ISO 27005.

Hasil Penilaian Kualitas Artikel

Setelah proses seleksi, penilaian kualitas dilakukan terhadap 7 artikel yang diinklusikan. Penilaian ini bertujuan untuk mengevaluasi kekuatan metodologi dari setiap studi. Hasil penilaian kualitas disajikan pada Tabel IV.

Tabel IV. Hasil Penilaian Kualitas

Penulis (Tahun)	QA1	QA2	QA3	QA4	TOTAL
Septanto et al. (2022)	1	1	0,5	1	**3,5**
Leasa & Prassida (2024)	1	1	1	1	**4**
Meitarice et al. (2024)	1	1	1	1	**4**
Rasyid & Aji (2025)	1	1	1	1	**4**
Aslan et al. (2023)	1	1	1	1	**4**
Utami et al. (2023)	1	0,5	0,5	1	**3**
Isnaini et al. (2023)	1	1	1	0,5	**3,5**

Hasil Interpretasi Penilaian Kualitas:

Secara umum, artikel-artikel yang diinklusikan menunjukkan kualitas metodologi yang baik hingga sangat baik (skor total 3.0 - 4.0), yang mendukung keandalan temuan penelitian ini. Artikel dengan skor total tinggi (mendekati 4.0) menunjukkan metodologi yang transparan, analisis yang kuat, dan relevansi yang tinggi dengan topik penelitian. Penilaian kualitas ini memastikan bahwa sintesis yang dilakukan didasarkan pada bukti yang kuat dan relevan.

Analisis Artikel yang Paling Relevan

Dari 23 artikel awal, 7 artikel berikut dinilai paling relevan dan berdampak langsung pada konteks penelitian ini setelah melalui proses penilaian kualitas. Artikel-artikel ini menjadi pilar utama dalam analisis risiko selanjutnya.

Tabel V. Daftar dan Analisis Artikel Ilmiah Relevan

No	Penulis (Tahun)	Fokus Utama	Relevansi
1	Septanto et al. (2022)	Menganalisis kerangka kerja keamanan e-learning di perguruan tinggi, mengidentifikasi kelemahan pada aset kebijakan, kelembagaan, aplikasi, dan infrastruktur.	Sangat Tinggi. Langsung membahas konteks e-learning di perguruan tinggi dan memberikan contoh kategori aset non-teknis yang penting.
2	Leasa & Prassida (2024)	Studi kasus pada Sistem Informasi Akademik (SIAKAD). Mengidentifikasi 18 risiko spesifik pada kategori aset: data, software, hardware, dan people.	Sangat Tinggi. Merupakan studi kasus yang paling mendekati topik Anda, memberikan contoh konkret identifikasi risiko pada SIAKAD.
3	Meitarice et al. (2024)	Studi kasus komprehensif pada portal akademik universitas negeri. Mengidentifikasi 8 kategori aset, 30 ancaman, dan 43 kerentanan.	Sangat Tinggi. Memberikan daftar ancaman dan kerentanan yang sangat lengkap dan spesifik untuk konteks sistem akademik di Indonesia.
4	Rasyid & Aji (2025)	Studi kasus pada penyedia Software as a Service (SaaS) untuk sistem manajemen sekolah. Mengidentifikasi 28 skenario risiko.	Tinggi. Sangat relevan karena sistem manajemen sekolah adalah bentuk dari sistem e-learning. Memberikan daftar risiko yang komprehensif.
5	Aslan et al. (2023)	Tinjauan komprehensif yang mengklasifikasikan berbagai jenis ancaman, kerentanan, dan serangan siber secara umum.	Tinggi. Merupakan sumber fundamental yang sangat baik untuk mendefinisikan istilah-istilah kunci dan mengkategorikan ancaman/kerentanan secara umum.
6	Utami et al. (2023)	Studi kasus yang mengkombinasikan ISO 27005 untuk identifikasi ancaman dengan metode DREAD untuk penilaian risiko pada website.	Medium. Contoh praktis yang baik untuk menunjukkan bagaimana ISO 27005 dapat dikombinasikan dengan metode lain untuk penilaian risiko.
7	Isnaini et al. (2023)	Studi kasus penerapan ISO 27005 yang sangat jelas dari awal hingga akhir, termasuk pembuatan matriks penilaian risiko dan rekomendasi kontrol.	Medium. Meskipun bukan di lingkungan Pendidikan.

RQ1: Bagaimana berbagai jenis risiko keamanan pada sistem e-learning dapat diidentifikasi dan dipahami?

Berdasarkan sintesis dari literatur yang relevan, risiko keamanan pada sistem e-learning dapat diidentifikasi melalui kategorisasi aset, ancaman, dan kerentanan. Adapun penjelasan untuk kategori aset, ancaman, dan kerentanan adalah sebagai berikut:

Berdasarkan Aset

Aset dalam sistem e-learning dan akademik dapat dibagi menjadi dua kategori utama, yaitu aset teknis dan aset non-teknis. Menurut penelitian oleh (Leasa & Prassida, 2024; Meitarice et al., 2024), aset teknis mencakup infrastruktur dan perangkat keras (seperti server, PC, jaringan), perangkat lunak (seperti aplikasi e-learning/SIAKAD, database), serta data dan informasi (seperti data pribadi, data akademik). Di sisi lain, temuan dari (Leasa & Prassida, 2024; Septanto et al., 2022) menyoroti pentingnya aset non-teknis, seperti manusia (seperti staf, dosen, mahasiswa) dan aset organisasional, termasuk kebijakan keamanan dan reputasi institusi.

Berdasarkan Ancaman

Ancaman yang paling sering diidentifikasi dapat dikelompokkan berdasarkan dampaknya terhadap aspek keamanan. Berdasarkan temuan (Aslan et al., 2023; Isnaini et al., 2023), ancaman terhadap ketersediaan (availability) meliputi kegagalan sistem seperti server down dan serangan DDoS. Ancaman terhadap kerahasiaan (confidentiality) mencakup akses tidak sah dan phishing, sementara ancaman terhadap integritas (integrity) terdiri dari malware, ransomware, dan serangan SQL injection, seperti yang dipaparkan oleh (Aslan et al., 2023; Meitarice et al., 2024).

Berdasarkan Kerentanan

Kerentanan dalam sistem e-learning dapat berasal dari faktor manusia dan teknis. Beberapa penelitian menunjukkan bahwa kerentanan terkait manusia dan proses menjadi yang paling dominan, seperti kurangnya kesadaran keamanan pengguna, manajemen akses yang lemah, serta ketiadaan kebijakan dan prosedur yang jelas (Leasa & Prassida, 2024; Meitarice et al., 2024; Septanto et al., 2022). Di sisi lain, kerentanan teknis juga sering ditemukan, misalnya perangkat lunak yang usang, kesalahan konfigurasi, kurangnya mekanisme keamanan fundamental, serta desain kode yang tidak aman yang memungkinkan serangan seperti SQL Injection (Aslan et al., 2023; Meitarice et al., 2024; Rasyid & Aji, 2025).

RQ2: Bagaimana kerangka kerja ISO/IEC 27005 dapat diterapkan secara praktis untuk mengelola risiko keamanan informasi pada sistem e-learning

Penerapan kerangka kerja ISO/IEC 27005 dalam manajemen risiko keamanan informasi pada sistem e-learning melibatkan serangkaian langkah sistematis. Berdasarkan studi kasus yang dianalisis, implementasi praktisnya dimulai dengan pembentukan ruang lingkup dan kriteria risiko yang jelas. Langkah ini dilanjutkan dengan identifikasi risiko, di mana aset, ancaman, dan kerentanan diidentifikasi. Setelah itu, dilakukan analisis risiko untuk menentukan tingkat kemungkinan dan dampak, yang kemudian dievaluasi dalam tahap evaluasi risiko untuk menentukan prioritas. Risiko yang tidak dapat diterima kemudian ditangani melalui tahap perlakuan risiko. Seluruh proses ini didukung oleh komunikasi dan konsultasi serta pemantauan dan tinjauan secara berkala. Beberapa studi kasus menunjukkan bahwa dengan menerapkan tahapan-tahapan ini, institusi pendidikan dapat secara praktis mengelola keamanan sistem e-learning mereka (Isnaini et al., 2023; Leasa & Prassida, 2024; Meitarice et al., 2024).

RQ3: Apa saja solusi atau rekomendasi mitigasi yang konkret dan efektif yang bisa dirumuskan untuk mengatasi risiko yang teridentifikasi

Berdasarkan identifikasi risiko dan penerapan kerangka ISO/IEC 27005, solusi mitigasi yang efektif

dapat dirumuskan dalam dua pilar utama, yaitu: kontrol administratif dan kontrol teknis. Setelah mengidentifikasi aset, ancaman, dan kerentanannya, setiap skenario risiko dianalisis untuk menentukan tingkat kemungkinan *(likelihood)* dan dampaknya *(impact)*. Hasil analisis ini kemudian dipetakan pada matriks risiko untuk menentukan level risiko keseluruhan. Risiko dengan level "*Tinggi*" atau "*Ekstrem*" akan menjadi prioritas utama untuk penanganan.

Tabel VI. Matriks Evaluasi Risiko

Kemungkinan (Likelihood) ↓ / Dampak (Impact) →	Sangat Rendah (1)	Rendah (2)	Sedang (3)	Tinggi (4)	Sangat Tinggi (5)
Sangat Tinggi (5)	4	4	5	5	5
Tinggi (4)	3	4	4	5	5
Sedang (3)	2	3	4	4	5
Rendah (2)	2	2	3	3	4
Sangat Rendah (1)	1	2	2	3	3

Penjelasan Matriks Risiko:

Matriks risiko ini menggabungkan dua variabel penting dalam penilaian risiko, yaitu *Likelihood (Kemungkinan)* dan *Impact (Dampak)*. *Likelihood* mengacu pada seberapa sering atau besar kemungkinan suatu ancaman terjadi, dengan skala penilaian mulai dari 1 (Sangat Rendah) hingga 5 (Sangat Tinggi). Sementara itu, Impact mengacu pada seberapa besar kerugian atau konsekuensi negatif yang ditimbulkan jika ancaman tersebut berhasil dieksploitasi, dengan skala penilaian juga berkisar dari 1 (Sangat Rendah) hingga 5 (Sangat Tinggi).

Berdasarkan kombinasi antara *Likelihood* dan *Impact*, level risiko dapat ditentukan. Risiko dengan level Sangat Rendah dapat diabaikan atau diterima tanpa tindakan khusus, sedangkan Risiko Rendah dapat diterima tetapi mungkin memerlukan pemantauan. Risiko Sedang memerlukan perhatian lebih dan mitigasi jika sumber daya memungkinkan. Risiko Tinggi memerlukan mitigasi segera dan menjadi prioritas utama, sementara Risiko Ekstrem adalah risiko yang tidak dapat diterima dan harus segera ditangani dengan tindakan mitigasi yang agresif.

Untuk penanganan risiko yang lebih efektif, fokusnya terbagi dalam dua kategori utama, yaitu: kontrol administratif dan kontrol teknis. Kontrol administratif berfokus pada aspek manajerial dan kebijakan, seperti pelatihan kesadaran keamanan bagi pengguna sistem, pengembangan kebijakan dan prosedur yang jelas, serta penerapan manajemen hak akses yang ketat. Selain itu, kontrol administratif juga mencakup perencanaan *Business Continuity Plan (BCP)*, yang memastikan bahwa sistem tetap dapat beroperasi meskipun terjadi gangguan besar atau insiden keamanan (Leasa & Prassida, 2024; Meitarice et al., 2024; Rasyid & Aji, 2025).

Di sisi teknis, kontrol yang efektif meliputi beberapa langkah penting. Salah satunya adalah penguatan autentikasi menggunakan *Multi-Factor Authentication (MFA)* untuk memperkuat keamanan akses. Selain itu, manajemen kerentanan yang berkelanjutan dan patching perangkat lunak harus dilakukan secara rutin untuk mencegah celah keamanan. Penting juga untuk memperkuat keamanan jaringan menggunakan *firewall*, *VPN*, dan teknik enkripsi data. Selain itu, penerapan enkripsi data sangat penting untuk menjaga kerahasiaan informasi yang ada dalam sistem. Terakhir, adanya proses backup dan pemulihan data yang teruji akan memastikan data tetap aman dan dapat dipulihkan setelah insiden yang tidak diinginkan. Temuan dari (Isnaini et al., 2023; Meitarice et al., 2024) menunjukkan bahwa penerapan kontrol teknis ini dapat secara signifikan mengurangi potensi eksploitasi kerentanan dalam sistem e-learning, sehingga meningkatkan tingkat keamanan secara keseluruhan.

RQ4: Bagaimana penelitian ini dapat memberikan kontribusi nyata dalam memperkuat keamanan informasi di lingkungan pendidikan digital

Penelitian ini memberikan kontribusi praktis yang signifikan dalam beberapa aspek. Pertama, dengan

mengidentifikasi aset, ancaman, dan kerentanan yang relevan, penelitian ini menyediakan peta risiko spesifik untuk e-learning yang dapat menjadi titik awal bagi institusi pendidikan, seperti yang ditunjukkan oleh (Leasa & Prassida, 2024; Meitarice et al., 2024; Septanto et al., 2022). Kedua, penelitian ini menawarkan panduan penerapan ISO/IEC 27005 yang terkontekstualisasi untuk e-learning, memberikan panduan langkah demi langkah yang praktis berdasarkan temuan dari (Isnaini et al., 2023; Leasa & Prassida, 2024). Ketiga, penelitian ini merumuskan rekomendasi mitigasi yang aplikatif, mencakup kontrol teknis dan non-teknis yang dapat langsung diterapkan, sejalan dengan hasil studi oleh (Meitarice et al., 2024; Rasyid & Aji, 2025). Selanjutnya, dengan menyoroti pentingnya pelatihan, penelitian ini mendorong peningkatan kesadaran dan budaya keamanan. Temuan dari penelitian ini, khususnya dari (Septanto et al., 2022), juga dapat menjadi dasar untuk pengembangan kebijakan dan prosedur keamanan di institusi. Pada akhirnya, implementasi rekomendasi ini dapat meningkatkan kepercayaan pengguna dan memberikan kontribusi pada literasi keamanan siber di sektor pendidikan.

KESIMPULAN

Analisis komprehensif terhadap risiko keamanan pada sistem e-learning, yang didukung oleh tinjauan literatur sistematis dan penerapan kerangka kerja ISO/IEC 27005, mengidentifikasi aset teknis dan non-teknis, ancaman umum seperti phishing dan malware, serta kerentanan yang terkait dengan faktor manusia dan teknis. Penerapan ISO/IEC 27005 secara praktis dimulai dengan pembentukan ruang lingkup, dilanjutkan dengan identifikasi, analisis, dan evaluasi risiko menggunakan matriks tingkat risiko. Proses ini kemudian diikuti dengan perlakuan risiko melalui kontrol administratif (seperti pelatihan kesadaran, pengembangan kebijakan, manajemen akses, dan *Business Continuity Plan/BCP)* serta kontrol teknis (termasuk *Multi-Factor Authentication/MFA, patching*, keamanan jaringan, enkripsi, dan backup data). Penelitian ini memberikan kontribusi praktis dengan menyediakan peta risiko yang spesifik untuk e-learning, panduan penerapan ISO/IEC 27005 yang disesuaikan, serta rekomendasi mitigasi yang dapat diterapkan. Selain itu, penelitian ini mendorong peningkatan kesadaran keamanan dan pengembangan kebijakan untuk memperkuat keamanan informasi dan meningkatkan keandalan sistem e-learning di lingkungan pendidikan digital. Untuk penelitian selanjutnya, disarankan agar dilakukan studi kasus implementatif untuk menguji efektivitas kontrol keamanan yang direkomendasikan dalam lingkungan e-learning yang sesungguhnya, serta mengukur dampaknya terhadap postur keamanan secara kuantitatif, sehingga dapat memberikan validasi empiris yang lebih mendalam.

REFERENSI

Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Frontiers in Big Data*, *7*, 1497535. doi:10.3389/FDATA.2024.1497535/XML/NLM

AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics 2023, Vol. 12, Page 3629*, *12*(17), 3629. doi:10.3390/ELECTRONICS12173629

Alheadary, W. G. (2023). Towards Development of a Security Risk Assessment Model for Saudi Arabian Business Environment Based on the ISO/IEC 27005 ISRM Standard. *Journal of Information Security*, *14*(3), 195–211. doi:10.4236/jis.2023.143012

Amirinnisa[1], M., & Bisma[2], R. (2023). *Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun*. *JEISBI* (Vol. 04).

Arias, V. I. G., & Soriano, S. D. (2022). La nube en Pymes mediante las normas ISO 27005. *Revista Ingeniería*, *6*(15), 169–182. doi:10.33996/revistaingenieria.v6i15.98

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks,

and Solutions. *Electronics 2023, Vol. 12, Page 1333*, *12*(6), 1333. doi:10.3390/ELECTRONICS12061333

Hamit, L. C., Sarkan, H. Md., Azmi, N. F. M., Mahrin, M. N., Chuprat, S., & Yahya, Y. (2020). Adopting ISO/IEC 27005:2011-based Risk Treatment Plan to Prevent Patients Data Theft. *International Journal on Advanced Science, Engineering and Information Technology*, *10*(3), 914–919. doi:10.18517/ijaseit.10.3.10172

Hidayatullah, D. E. R., Kunthi, R., & Harwahyu, R. (2024). Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department. *International Journal of Electrical, Computer, and Biomedical Engineering*, *2*(3). doi:10.62146/ijecbe.v2i3.81

Hikam, M. L. B., Dewi, F., & Praditya, D. (2024). ANALISIS MANAJEMEN RISIKO INFORMASI MENGGUNAKAN ISO/IEC 27005:2018 (STUDI KASUS: PT.XYZ). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *9*(2), 728–734. doi:10.29100/jipi.v9i2.4709

Isnaini, K., Sari, G. J. N., & Kuncoro, A. P. (2023). Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa. *Jurnal Eksplora Informatika*, *13*(1), 37–45. doi:10.30864/eksplora.v13i1.696

Jonny, J., Ambarwati, A., & Darujati, C. (2021). Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005. *SISTEMASI*, *10*(1), 1. doi:10.32520/stmsi.v10i1.995

Junior, A. S. C., & Arima, C. H. (2023). CYBER RISK MANAGEMENT AND ISO 27005 APPLIED IN ORGANIZATIONS: A SYSTEMATIC LITERATURE REVIEW. *REVISTA FOCO*, *16*(2). doi:10.54751/revistafoco.v16n2-215

Leasa, Z. V., & Prassida, G. F. (2024). Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ menggunakan ISO 27005:2018. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *6*(4), 649–656. doi:10.47233/jteksis.v6i4.1459

Liderman, K. (2022). Risk analysis for information security in accordance with PN-ISO/IEC 27005 recommendation. *Przegląd Teleinformatyczny*, *10*(1), 19–34. doi:10.5604/01.3001.0054.2961

Meitarice, S., Febyana, L., Fitriansyah, A., Kurniawan, R., & Nugroho, R. A. (2024). Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia: Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 Security Controls. *Journal of Information Technology and Cyber Security*, *2*(2), 58–75. doi:10.30996/jitcs.12099

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, *14*(4). doi:10.14569/ijacsa.2023.0140468

Putri, M. K., & Hakim, A. R. (2021). Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO/IEC 27005:2018 dan NIST SP 800-30 Revisi 1. *Info Kripto*, *15*(3), 134–141. doi:10.56706/ik.v15i3.34

Rasyid, R. M., & Aji, R. F. (2025). Perancangan Manajemen Risiko Keamanan Informasi Menggunakan SNI ISO/IEC 27005: Studi Kasus Integrated School Management System milik PT XYZ. *Jurasik (Jurnal Riset Sistem Informasi Dan Teknik Informatika)*, *10*(1), 226. doi:10.30645/jurasik.v10i1.866

Riadi, B. R. (2025). Risk Management of Information Security in Inaportnet Using ISO/IEC 27005:2018. *INOVTEK Polbeng - Seri Informatika*, *10*(1), 225–236. doi:10.35314/pq4jhh89

Septanto, H., Sabrina, F. N., & Irmawati, N. F. (2022). KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI UNTUK MENUNJANG IMPLEMENTASI ELEARNING PADA PERGURUAN TINGGI. *Jurnal Tera*, *2*(2), 73–83. Retrieved from https://jurnal.undira.ac.id/jurnaltera/article/view/128

Sinulingga, R. M. A., Raharjo, T., & Trisnawaty, N. W. (2024). Risk Management Design and Analysis on Agile Development Project using ISO 31000 Integrated with ISO 27005: A Case Study of SiREV Application. *Jurnal Informatika Ekonomi Bisnis*, 815–821. doi:10.37034/infeb.v6i4.1053

Syahindra, I. P. S., Primasari, C. H., & Iriantor, A. B. P. (2022). EVALUASI RISIKO KEAMANAN INFORMASI DISKOMINFO PROVINSI XYZ MENGGUNAKAN INDEKS KAMI DAN ISO 27005 : 2011. *Jurnal Teknoinfo*, *16*(2), 165. doi:10.33365/jti.v16i2.1246

Utami, G. C., Supramaji, A. B., & Isnaini, K. N. (2023). Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005:2018. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, *8*(1), 47–56. doi:10.32528/JUSTINDO.V811.219