ASSESSMENT TINGKAT RISIKO KEAMANAN INFORMASI MENGGUNAKAN FRAMEWORK ISO/IEC 27005:2022 DAN NIST SP 800-30 REVISI 1 PADA INSTANSI PENDIDIKAN X

Obed El Fatih Syams[1], Candiwan Candiwan[2]
[1] Manajemen Bisnis Telekomunikasi dan Informatika, Universitas Telkom, Indonesia, fatihsyams@student.telkomuniversity.ac.id
[2] Manajemen Bisnis Telekomunikasi dan Informatika, Universitas Telkom, Indonesia, candiwan@telkomuniversity.ac.id

Abstrak

Perkembangan teknologi memberikan kontribusi besar dalam mempermudah akses terhadap informasi, terutama melalui internet. Informasi menjadi elemen penting dalam mendukung proses pengambilan keputusan di suatu organisasi atau perusahaan. Oleh karena itu, dibutuhkan pengelolaan sistem informasi yang efektif agar informasi dapat dimanfaatkan secara optimal dan tetap terlindungi. Informasi yang bersifat rahasia memerlukan kontrol pengamanan yang memadai untuk meminimalkan risiko yang berpotensi menimbulkan kerugian. Penelitian ini bertujuan untuk melakukan penilaian risiko terhadap keamanan informasi pada sistem informasi ZZZ yang digunakan di instansi pendidikan X. Penelitian ini menggunakan pendekatan kualitatif dengan tujuan deskriptif. Teknik pengolahan data dilakukan melalui kombinasi metode perhitungan risiko berbasis dokumen ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1, serta diperkuat dengan teknik triangulasi guna meningkatkan keabsahan hasil penelitian.

Berdasarkan hasil penelitian, ditemukan bahwa terdapat 11 risiko yang perlu dilakukan tindakan mitigasi, sementara 15 risiko lainnya dinilai masih dapat diterima oleh instansi pendidikan X. Risiko yang tergolong dalam kategori sangat rendah (*very low*) berjumlah 12, kategori rendah (*low*) sebanyak 9, kategori sedang (*moderate*) ada 3, dan kategori tinggi (*high*) juga sebanyak 3. Penelitian ini juga mengidentifikasi 15 jenis ancaman yang berkaitan dengan masing-masing aset dalam sistem informasi ZZZ. Selain itu, ditemukan bahwa terdapat 14 kontrol yang diterapkan pada aset-aset tersebut.

Berdasarkan temuan tersebut, dapat disimpulkan bahwa instansi pemerintah X perlu menerapkan manajemen risiko keamanan informasi, setidaknya di lingkungan internal, guna menjaga aspek kerahasiaan, ketersediaan, dan integritas (CIA) informasi. Hasil dari penelitian ini juga dapat dijadikan sebagai dasar untuk penelitian lanjutan, khususnya dalam mengkaji langkah penanganan risiko pada tiap aset dengan mengacu pada standar lain seperti ISO 27002 dan dokumen pendukung lainnya..

Kata kunci : assessment risiko, keamanan informasi, ISO/IEC 27005:2011, NIST SP 800-30 Revisi 1

I. PENDAHULUAN

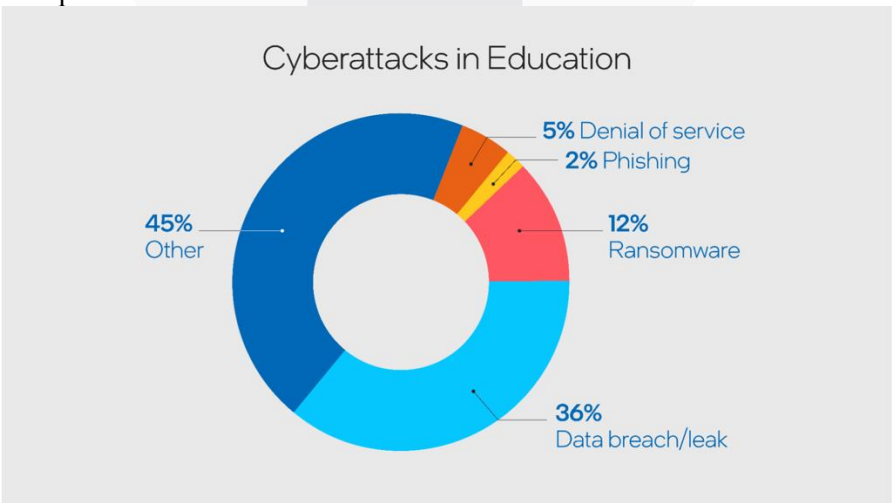
Perkembangan teknologi, khususnya internet, telah mempermudah akses informasi. Menurut GoodStats (2024). Indonesia mengalami lonjakan transformasi digital, ditandai dengan peningkatan signifikan pengguna aktif smartphone—dari 54 juta pada 2015 menjadi 209,3 juta pada 2023. Teknologi ini telah memengaruhi berbagai aspek kehidupan masyarakat. Data tren pengguna smartphone antara 2016 hingga 2019 menunjukkan pertumbuhan yang konsisten.

Gambar 1.1 Pengguna Smartphone di Indonesia
Sumber: GoodStats (2024)

Seiring perkembangan zaman, kebutuhan akan informasi terus meluas dan menjadi semakin kompleks. Informasi menjadi elemen penting bagi sebagai landasan dalam proses pengambilan keputusan. Oleh karena itu, pengelolaan informasi yang baik sangat diperlukan, dan hal ini harus didukung oleh pengelolaan sistem informasi yang efektif dan terstruktur.

Pencatatan data yang sudah menggunakan sistem informasi menunjukkan kemajuan teknologi saat ini. Data tersebut mencakup informasi umum yang berguna untuk mengenali identitas pribadi seseorang. Oleh sebab itu, perlindungan terhadap data menjadi hal yang sangat penting. Menurut (Fikri & Alhakim, 2022) pada tahun 2021 Indonesia pernah dihebohkan oleh kasus dugaan kebocoran data yang diduga dijual di forum daring, yang kabarnya merupakan data dari 2ingkat pemerintah, yaitu BPJS. Kepala Lembaga riset Siber Communication and Information System Security Research Center menyatakan bahwa data yang bocor, sebesar 240MB, berisi informasi sensitif seperti Nomor Induk Kependudukan (NIK), nomor telepon, alamat, alamat e-mail, NPWP, tempat tinggal, jumlah tanggungan, dan data pribadi lainnya. Bahkan disebutkan terdapat sekitar 20 juta data yang menyertakan foto dan detail kartu BPJS Kesehatan, dengan total data yang bocor mencapai sekitar 272,8 juta data penduduk.

Upaya mencegah serangan siber yang mungkin terjadi kepada perusahaan, diperlukan manajemen risiko. Menurut (Semman Ansyari, 2024) manajemen risiko adalah proses pengambilan keputusan strategis yang melibatkan identifikasi, evaluasi, dan mitigasi risiko untuk mengelola ketidakpastian dan meraih peluang, yang pada akhirnya mendukung pencapaian tujuan organisasi dan mendorong pertumbuhan berkelanjutan dalam lingkungan bisnis yang kompetitif.



Gambar 1. 2 CyberAttacks in Education
Sumber: intel (2023)

Dari gambar di atas, menurut data intel (2023) dalam websitenya mengatakan bahwa keamanan siber sangat penting dalam lingkungan bisnis apa pun, terutama dalam bidang pendidikan. Serangan siber tidak hanya

membahayakan keselamatan dan keamanan guru serta administrasi sekolah, tetapi juga privasi siswa—terutama anak di bawah umur di lembaga K–12. Saat ini, jutaan siswa belajar melalui teknologi dalam lingkungan daring, jarak jauh, atau di kelas, oleh karena itu menjaga keamanan perangkat mereka sangat penting untuk pengalaman belajar siswa dan pekerjaan guru. (intel 2023) juga memberikan data serangan siber didalam websitenya. Statistik ini menggambarkan betapa pentingnya keamanan siber dalam dunia pendidikan. Satu dari tiga perangkat di sektor pendidikan menyimpan data sensitif, yang menunjukkan tingginya risiko terhadap kebocoran informasi. Dalam sebuah studi yang melibatkan 5.400 pengambil keputusan TI di 30 negara, sektor pendidikan menempati posisi tertinggi dalam pengakuan terhadap kelemahan keamanannya. Sebanyak 44% manajer TI di sektor ini telah mengalami serangan ransomware, tingkat serangan yang lebih tinggi dibandingkan industri lain seperti perawatan kesehatan, teknologi informasi, dan pemerintah daerah. Bahkan, 87 persen lembaga pendidikan melaporkan pernah menjadi korban serangan siber setidaknya satu kali. Di antara berbagai industri, sektor pendidikan termasuk salah satu yang paling rentan, dan sekolah menjadi target kedua paling menguntungkan bagi pelaku *ransomware*.

Menurut Candiwan & Rianda (2024) Kegagalan pengguna untuk menerapkan praktik keamanan informasi yang komprehensif tidak hanya memudahkan akses ilegal ke data pribadi dan keuangan mereka, tetapi juga meningkatkan kemungkinan terjadinya insiden kejahatan dunia maya. Informasi sangat berharga dan harus dilindungi. Perilaku keamanan dan kesadaran akan keamanan informasi sangat penting untuk menentukan risiko akibat perilaku dan kurangnya kesadaran akan keamanan informasi (Candiwan et al., 2022).

Pemanfaatan teknologi oleh perusahaan mampu menambah tingkatan efektivitas operasional maupun efisiensi, yang akhirnya mempunyai dampaknya dengan positif pada peningkatan kinerja dan daya saing usaha (Hendayani & Fernando, 2023).

1.1 Tujuan Penelitan

1. Melakukan identifikasi risiko terkait sistem informasi ZZZ di Instansi pendidikan X dengan menggunakan kerangka kerja ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1.
2. Melakukan analisis risiko yang berhubungan dengan sistem informasi ZZZ di Instansi pendidikan X berdasarkan kerangka kerja ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1.
3. Melakukan evaluasi terhadap risiko yang telah diidentifikasi dan dianalisis, yang berkaitan dengan sistem informasi ZZZ di Instansi pendidikan X.

II. TINJAUAN LITERATUR

2.1 Sistem Informasi Manajemen

Menurut (Alfatul Hisabi et al., 2022) mengatakan bahwa Sistem Informasi Manajemen (SIM) merupakan jaringan terstruktur yang berfungsi untuk mengelola dan mengolah informasi. Tujuannya adalah menyediakan data yang mendukung proses pengambilan keputusan guna mencapai sasaran organisasi, termasuk dalam hal penghitungan biaya, evaluasi, serta perbaikan berkelanjutan pada layanan dan produk.

2.2 Kemanan Informasi

Menurut (Gorbunov, 2024) menjelaskan bahwa Keamanan informasi adalah proses melindungi data dari akses, pengungkapan, penghancuran, atau modifikasi yang tidak sah. Proses ini memastikan kerahasiaan, integritas, dan ketersediaan informasi dengan menggunakan teknologi serta strategi yang tepat untuk melindungi dari berbagai ancaman dan risiko.

2.3 Risiko Manajemen

Menurut (Yudhaningsih & Syah, 2023) manajemen risiko melibatkan pengenalan, penilaian, dan pengembangan strategi untuk mengurangi berbagai bahaya, termasuk risiko lingkungan, teknologi, organisasi, dan politik. Tujuannya adalah untuk mengurangi risiko ini ke tingkat yang dapat diterima, memastikan keselamatan dan stabilitas dalam operasi.

Candiwan et al. (2022) mengatakan bahwa perilaku pengguna yang tidak aman, seperti penggunaan kata sandi yang sama di berbagai platform, serta rendahnya kesadaran terhadap keamanan informasi, meningkatkan risiko kejahatan siber.

2.4 Manajemen Aset Informasi

Menurut (Yudhaningsih & Syah, 2023) manajemen asset informasi melibatkan proses sistematis untuk menerapkan, mengoperasikan, memelihara, meningkatkan, dan membuang aset lingkungan binaan. Hal ini membutuhkan keterlibatan organisasi dalam perencanaan, pengendalian, dan pemantauan kinerja aset, mengintegrasikan manajemen, keuangan,

ekonomi, dan kegiatan lainnya untuk hasil yang efektif.

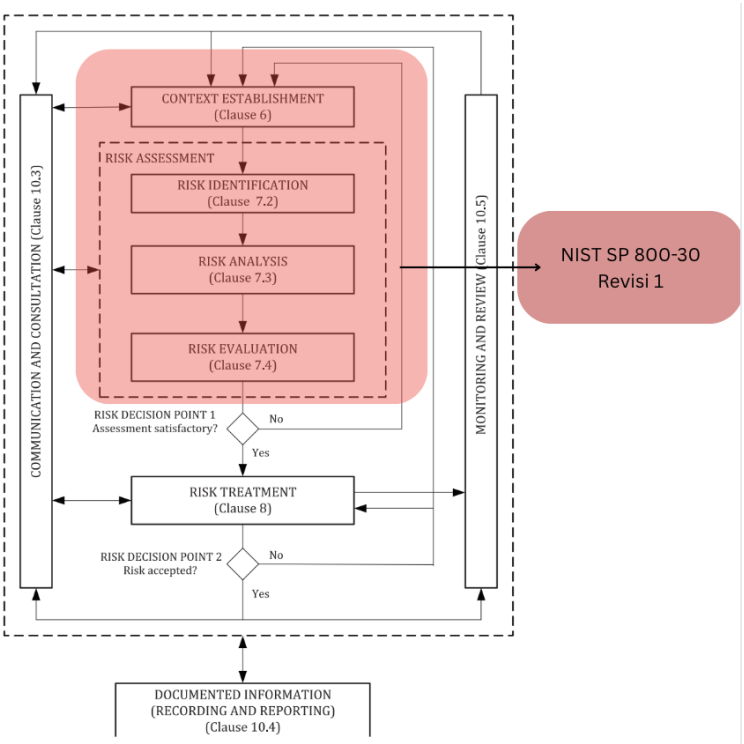
2.5 ISO 27005:2022

Menurut Cerqueira Junior & Arima (2023) mengatakan bahwa ISO 27005:2022 merupakan standar internasional yang memberikan panduan dalam proses Manajemen Risiko Keamanan Informasi. Standar ini membantu organisasi dalam mengenali, menganalisis, mengevaluasi, serta menangani ancaman dan risiko keamanan siber, sehingga mendukung peningkatan pengelolaan keamanan informasi secara lebih baik.

2.6 NIST SP 800-30 Revisi 1

NIST menerbitkan berbagai panduan dalam bentuk publikasi khusus untuk membantu melakukan penilaian risiko terhadap sistem dan organisasi informasi federal. Publikasi khusus NIST SP 800-30 dirancang untuk mendukung pedoman yang terdapat dalam NIST SP 800-39, dengan pendekatan penilaian risiko yang diterapkan pada tiga tingkatan hierarki manajemen risiko. Dokumen ini memberikan panduan rinci untuk melaksanakan setiap langkah dalam proses penilaian risiko, mulai dari mempersiapkan, melaksanakan, hingga mengkomunikasikan hasilnya serta menjaga keberlanjutan penilaian. Selain itu, NIST SP 800-30 juga membantu organisasi dalam mengidentifikasi faktor-faktor risiko fisik yang perlu dipantau secara terus-menerus, sehingga memungkinkan organisasi untuk mengevaluasi apakah tingkat risiko telah meningkat atau tidak (NIST SP 800-30 Revisi 1, 2012).

2.6 Kerangka Penelitian



Gambar 2.1 Kerangka Pemikiran

(Dokumen ISO 27005:2

III. METODOLOGI PENELITIAN

3.1 Jenis Penelitian

Menurut Deb et al. (2019) penelitian merupakan suatu metode sistematis untuk mencari ilmu pengetahuan atau merumuskan teori, yang didorong oleh rasa ingin tahu terhadap hal yang tidak diketahui. Metode penelitian kualitatif merupakan penelitian yang digunakan untuk meneliti pada kondisi obyek yang alamiah Pandey (2024) penelitian ini menggunakan analisis isi dan percakapan dimana menurut Han (2024) analisis isi dan percakapan adalah salah satu jenis penelitian kualitatif yang memusatkan perhatian percakapan dalam sebuah interaksi.

Penelitian ini jika ditinjau berdasarkan waktu pelaksanaan jenisnya menggunakan *cross section* karena penelitian ini tidak dilakukan secara berulang dan hanya satu kali saja. Lalu jika ditinjau berdasarkan unit analisis penelitian ini mengacu pada unit analisis organisasi yaitu instansi pendidikan X. Selanjutnya berdasarkan keterlibatan peneliti, penelitian ini tidak mengintervensi data artinya peneliti tidak memanipulasi data yang ada dan berdasarkan tujuan penelitian ini termasuk ke dalam penelitian deskriptif yang artinya dalam penelitian ini berisi tentang deskripsi hasil analisa. Awal mula penelitian ini dimulai dengan penilaian risiko keamanan informasi yang berupa aset, ancaman (threat) dan segala kemungkinan ancaman yang dapat terjadi kemudian dilakukan perhitungan berdasarkan ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 pada sistem informasi ZZZ instansi pendidikan X. Karakteristik penelitian kali ini dapat dilihat pada tabel 3.1

Tabel 3.1 Karakteristik Penelitian

No	Karakteristik Penelitian	Jenis
1	Berdasarkan Metode	Kualitatif
2	Berdasarkan Tujuan	Deskriptif
3	Berdasarkan Keterlibatan Peneliti	Tidak Mengintervensi Data
4	Berdasarkan Perhitungan Risiko	*Semi Quantitative Value*
5	Berdasarkan Unit Analisis	Organisasi
6	Berdasarkan Waktu Pelaksanaan	*Cross Section*

Sumber:(Sekaran & Bougie, 2016)

3.2 Operasional Variabel

Penentuan variabel dilakukan dengan cara melihat pengaruh terbesar dari aset pada sistem informasi ZZZ instansi pendidikan X yaitu aset dan ancaman. Aset merupakan seluruh alat yang dapat menjalankan dan mendukung layanan operasional sistem informasi ZZZ dalam penggunaan sistem informasi ZZZ. Ancaman merupakan hal-hal yang dapat merusak dan merugikan pengguna sistem informasi ZZZ yang dapat dipengaruhi dari *likelihood*, *vulnerability*, kontrol yang ada, dan risiko yang akan didapatkan. Adapun variabel dan sub variabel pada penelitian ini dapat dilihat pada tabel 3.2.

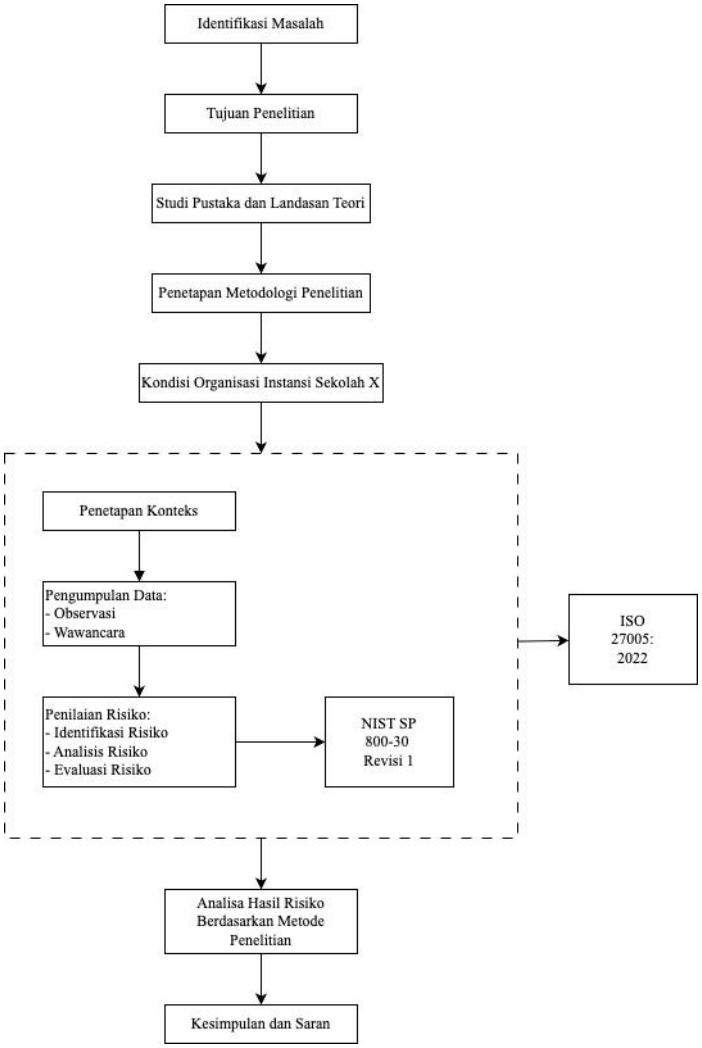
Tabel 3.2 Variabel dan Sub Variabel

Variable	Sub Variabel
Asset - Asset	Asset Utama
	Asset Pendukung
Ancaman	Risiko
	Likelihood

	Vulnerability
	Impact
	Existing Control

Sumber: Data yang diolah penulis, 2024.

3.3 Tahapan Penelitian



Gambar 3. 1 Tahapan Penelitian

Sumber: Fikri et al., (2019), data yang diolah penulis.

3.4 Populasi dan Sampel

Populasi pada penelitian ini berdasar dari tiga elemen:

a. Activity

Penggunaan aset untuk sistem informasi ZZZ berikut dengan ancaman, kerentanan, kemungkinan terjadinya ancaman, dampak, dan nilai risiko terhadap masing-masing aset.

b. Actors

Perwakilan dari instansi pendidikan X yang mengetahui aset dan memahami ancaman, kerentanan, kemungkinan terjadinya ancaman dan dampak terhadap masing-masing aset, dalam hal ini perwakilan yang ditunjuk yaitu Staff IT dan Technical Support data center yang menguasai manajemen keamanan informasi pada sistem informasi ZZZ.

c. Place

Lokasi penelitian di instansi pendidikan X

3.5 Teknik Analisa Data

Dalam penelitian ini teknik analisis data yang digunakan mengacu pada ISO 27005:2022 dan NIST SP 800-30 Revisi 1, sesuai dengan kerangka pemikiran yang dijelaskan pada bab dua. Proses ini dimulai dengan

menetapkan konteks (*context establishment*) dan dilanjutkan dengan penilaian risiko (*risk assessment*) yang mencakup beberapa aspek, seperti identifikasi risiko (*risk identification*), analisis risiko (*risk analysis*), dan evaluasi risiko (*risk evaluation*). Tahap identifikasi risiko didasarkan pada pedoman ISO 27005:2022 dan NIST SP 800-30 Revisi 1, meliputi identifikasi aset, ancaman, kontrol yang sudah ada, serta kerentanan.

Tabel 3.3 Skala Perhitungan

Skala	Deskripsi		Nilai
	Skala *Adversarial*	Skala Non-Adversarial	
Very High	Penyerang hampir pasti untuk melakukan ancaman	Kesalahan, kecelakaan, atau tindakan alam hampir pasti terjadi atau terjadi lebih dari 100 tahun sekali	10
High	Penyerang sangat mungkin untuk melakukan ancaman	Kesalahan, kecelakaan, atau tindakan alam sangat mungkin terjadi atau terjadi lebih dari 10 kali dalam 1 tahun	8
Moderate	Penyerang dapat memulai suatu ancaman	Kesalahan, kecelakaan, atau tindakan alam terjadi antara 1-10 kali dalam setahun	5
Low	Penyerang tidak mungkin untuk melakukan ancaman	Kesalahan, kecelakaan, atau tindakan alam terjadi 1 kali dalam 10 tahun	2
Very Low	Penyerang sangat tidak mungkin untuk melakukan ancaman	Kesalahan, kecelakaan, atau tindakan alamt sangat tidak mungkin terjadi atau kurang dari 1 kali dalam 10 tahun	0

Sumber: Dokumen NIST SP 800-30 Revisi 1, 2012.

Tabel 3.4 Skala Perhitungan – *Likelihood of Threat Event, Resulting in Adverse Impacts*

Skala	Deskripsi	Nilai
Very High	Ancaman berdampak buruk pada organisasi	10
High	Ancaman sangat mungkin berdampak buruk pada organisasi	8
Moderate	Ancaman agak mungkin berdampak buruk pada organisasi	5
Low	Ancaman tidak mungkin berdampak buruk pada organisasi	2
Very Low	Ancaman sangat tidak mungkin berdampak buruk pada organisasi	0

Sumber: Dokumen NIST SP 800-30 Revisi 1, 2012.

Gambar: 3.2 Skala Perhitungan – *Overall Likelihood*

Likelihood Threat Event Initation or Occurrence	*Likelihood Threat Event Result in Adverse Impacts*				
	Very Low	*Low*	*Moderate*	*High*	*Very High*
Very High	*Very Low*	*Moderate*	*High*	*Very High*	*Very High*
High	*Very Low*	*Moderate*	*Moderate*	*High*	*Very High*
Moderate	*Very Low*	*Low*	*Moderate*	*Moderate*	*High*
Low	*Very Low*	*Low*	*Low*	*Moderate*	*Moderate*
Very Low	*Very Low*	*Very Low*	*Very Low*	*Low*	*Low*

Sumber: Dokumen NIST SP 800-30 Revisi 1, 2012.

Tabel 3.5 Skala Perhitungan – *Impact of Threat Events/Level of Impact*

Skala	Deskripsi	Nilai
Very High	Ancaman dapat memiliki dampak yang parah dan mempunyai efek buruk pada organisasi (operasional, aset, individu) maupun organisasi lainnya termasuk negara	10
High	Ancaman dapat diduga akan terjadi bencana yang sangat besar yang dapat berdampak pada organisasi (operasional, aset, individu) maupun organisasi lainnya termasuk negara. Ancaman dapat berupa organisasi tidak dapat menjalankan fungsinya mengakibatkan kerugian finansial, dan mengancam korban jiwa.	8
Moderate	Ancaman dapat diduga akan memiliki efek yang serius yang dapat berdampak pada organisasi (operasional, aset, individu) maupun organisasi lainnya.	5
Low	Bahkan saat ancaman datang, hanya sedikit efek samping pada operasional organisasi, aset organisasi, individu maupun organisasi lainnya.	2
Very Low	Ancaman dapat diduga akan mengakibatkan kerugian yang dapat diabaikan pada operasional organisasi, aset organisasi, individu, maupun organisasi lainnya.	0

Sumber: Dokumen NIST SP 800-30 Revisi 1, 2012

Tabel 3.6 Risk Appetite Matrix

Overall Likelihood	*Level of Impact*				
	Very Low	*Low*	*Moderate*	*High*	*Very High*
Very High	*Accept*	*Mitigate*	*Mitigate*	*Mitigate*	*Mitigate*
High	*Accept*	*Mitigate*	*Mitigate*	*Mitigate*	*Mitigate*
Moderate	*Accept*	*Mitigate*	*Mitigate*	*Mitigate*	*Mitigate*
Low	*Accept*	*Accept*	*Mitigate*	*Mitigate*	*Mitigate*
Very Low	*Accept*	*Accept*	*Accept*	*Mitigate*	*Mitigate*

Sumber: Data yang diolah penulis, 2025.

IV. HASIL DAN PEMBAHASAN

4.1 Idenfitikasi Aset

Berdasarkan hasil wawancara didapatkan jumlah aset sebanyak 15 yang terdiri dari 7 aset teknologi, empat aset proses bisnis, 4 aset informasi 4 aset SDM.

4.2 Identifikasi Ancaman dan Sumber Ancaman

Hasil wawancara dengan narasumber didapatkan 11 sumber ancaman adversarial dan 10 ancaman non adversarial yang mempunyai tingkat relevansi yang berbeda pada masing-masing aset. Jenis ancaman yang diidentifikasi berjumlah 15.

4.3 Identifikasi Kontrol yang ada

Berdasarkan data yang didapatkan ditemukannya kontrol yang sudah dilakukan oleh instansi pendidikan X dengan jumlah 22. Contoh dari kontrol yang sudah ada antara lain melakukan testing terhadap sistem (C1), menerapkan firewall (C2), membuat priveleges user (C3), memberikan pemahaman mengenai awareness security (C4) dan lain sebagainya.

4.4 Identifikasi Kerentanan

Identifikasi kerentanan pada masing-masing aset bertujuan untuk mengetahui kelemahan pada aset yang digunakan sebagai pertimbangan penilaian risiko. Berdasarkan data yang didapatkan, telah diidentifikasi 15 jenis kerentanan. Contoh dari kerentanan antara lain rusak pada perangkat lunak (V1), tidak adanya proses logout otomatis saat meninggalkan workstation (V2), password yang tidak dibatasi (V3), pemeliharaan perangkat yang tidak berkala (V4) dan lain sebagainya.

4.5 Analisis Risiko

Hasil analisis risiko merupakan tahapan kedua untuk melakukan penilaian risiko. Tujuan dari analisis risiko adalah untuk menentukan *overall likelihood* dan *impact* atas ancaman yang mungkin terjadi pada masing-masing aset. Berdasarkan hasil wawancara dari analisis risiko, didapatkan hasil bahwa 25 skenario risiko yang mungkin terjadi dengan rincian *impact of threat events*, *likelihood of threat event initiation* dan *likelihood of threat event resulting in adverse impacts*. Hasil dari *likelihood of threat event initiation/occurrence* yaitu 9 *high*, 4 *moderate*, 2 *low* dan 10 *very low*. Hasil dari *likelihood of threat event resulting in adverse impacts* yaitu dengan rincian 30 moderate, dan 23 low. Berdasarkan hasil dari kombinasi *likelihood of threat event initiation/occurrence* didapatkan hasil *overall likelihood*. dominan terjadi pada pemilik aset bagian technical support sedangkan untuk ancaman yang bernilai moderate dan high pada level of impact terjadi pada pemilik aset yang ada pada instansi pendidikan X. Ancaman tersebut mayoritas terjadi pada aset jenis teknologi yaitu *hardware* dan *software* dan jenis aset sumber daya manusia (personnel).

4.6 Evaluasi Risiko

Setelah didapatkan analisis risiko maka selanjutnya dilakukan evaluasi risiko dengan melihat risk appetite matrix untuk mengetahui tindakan setiap risiko pada masing-masing aset. Untuk kategori moderate akan menjadi prioritas utama yang harus dilakukan tindakan mitigasi, kategori low akan menjadi prioritas kedua yang harus ditindak lanjuti dan kategori *very low* akan menjadi prioritas terakhir atau tidak akan menjadi prioritas.

Tabel 4.1 Evaluasi Risiko

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15
A1															
A2															
A3															
A4															
A5															
A6															
A7															
A8															
A9															
A10															
A11															
A12															
A13															
A14															
A15															

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan identifikasi, analisis, dan evaluasi risiko menggunakan ISO/IEC 27005:2022 dan NIST SP 800-30 Rev. 1 pada sistem informasi ZZZ di Instansi Pendidikan X, diperoleh hasil sebagai berikut:

1. **Identifikasi Risiko:** Terdapat 15 aset (4 utama, 11 pendukung) dan 25 insiden ancaman dari 20 sumber (11 adversarial, 9 non-adversarial). Ancaman utama berasal dari hacker (tinggi) dan kriminal komputer (moderat), dengan 15 kerentanan dan 14 kontrol diterapkan. Kerentanan bernilai moderate hingga high perlu perhatian khusus.

2. **Analisis Risiko:** Ditemukan 25 skenario risiko dengan tingkat likelihood dan impact bervariasi. Likelihood tertinggi berasal dari bagian technical support, sedangkan impact paling signifikan pada hardware, software, dan SDM di instansi pendidikan.

3. **Evaluasi Risiko:** Sebanyak 11 risiko perlu dimitigasi dan 15 risiko diterima. Risiko prioritas terdapat pada aset proses bisnis (low) dan perangkat lunak (moderate). Prioritas mitigasi: moderate (utama), low (kedua), very low (terakhir).

5.2 Saran

1. Penguatan Manajemen Risiko: Instansi Pendidikan X disarankan membentuk kerangka kerja manajemen risiko keamanan informasi serta menerapkan standar keamanan minimal secara internal. Kontrol perlu diperkuat pada aset dengan risiko moderate dan low (mitigate), sementara pengawasan tetap dilakukan untuk risiko very low dan low (accept).l

2. Mitigasi Ancaman Utama: Mengingat ancaman dari hacker dan kriminal komputer bernilai high dan moderate, peningkatan keamanan diperlukan pada aset penting seperti sistem informasi ZZZ, OS Windows, database server, dan jaringan internal. Penambahan kontrol juga direkomendasikan untuk aset terkait layanan perizinan, front office, serta tim teknis dan administrator.

3. Peningkatan Kesadaran dan Infrastruktur: Ancaman signifikan pada personil, proses bisnis, dan sistem informasi perlu ditanggapi dengan pelatihan keamanan bagi seluruh personil serta penguatan infrastruktur TI, termasuk update perangkat lunak dan kontrol akses. Proses bisnis juga harus diperketat melalui prosedur dan pengawasan yang lebih baik. Audit keamanan dan evaluasi risiko perlu dilakukan secara berkala untuk memastikan efektivitas kontrol.

REFERENSI

Alfatul Hisabi, Amelia Azura, Dhita Lutfiah, & Nurbaiti. (2022). PERKEMBANGAN SISTEM INFORMASI MANAJEMEN (SIM) DI INDONESIA. *Juremi: Jurnal Riset Ekonomi*, *1*(4), 364–371. https://doi.org/10.53625/juremi.v1i4.775

Cerqueira Junior, A. S., & Arima, C. H. (2023). CYBER RISK MANAGEMENT AND ISO 27005 APPLIED IN ORGANIZATIONS: A SYSTEMATIC LITERATURE REVIEW. *REVISTA FOCO*, *16*(02), e1188. https://doi.org/10.54751/revistafoco.v16n2-215

Deb, D., Dey, R., & Balas, V. E. (2019). *Introduction: What Is Research?* (pp. 1–7). https://doi.org/10.1007/978-981-13-2947-0_1

Fikri, M., & Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. *Jurnal Hukum & Hukum Islam*, *9*.

GoodStats. (2024, June 12). *Pengguna Aktif Smartphone di Indonesia*. GoodStats. https://data.goodstats.id/statistic/2093-juta-orang-di-indonesia-menggunakan-smartphone-pada-tahun-2023-cbha0

Gorbunov, I. A. (2024). Information security: international legal aspects of its provision. *Международное Право*, *1*, 29–38. https://doi.org/10.25136/2644-5514.2024.1.70440

Han, X. (2024). From Conversation to Interaction: A Pedagogical Exploration of Applying Conversation Analysis in EFL Classrooms. *Teaching English as a Second or Foreign Language--TESL-EJ*, *28*(3). https://doi.org/10.55593/ej.28111a7

Hendayani, R., & Fernando, Y. (2023). Adoption of blockchain technology to improve Halal supply chain performance and competitiveness. Journal of Islamic Marketing, 14(9), 2343–2360. https://doi.org/10.1108/JIMA-02-2022-0050

intel. (2023, October 26). *Cybersecurity in Education*. Intel.Com. https://www.intel.co.id/content/www/id/id/education/it-in-education/cyber-security.html

Pandey, S. R. (2024). Rummaging on a Research Method. *Journal of NELTA Koshi (JoNK)*, *2*(1), 100–110. https://doi.org/10.3126/jonk.v2i1.69661

Sekaran, U., & Bougie, R. (2016). *An easy way to help students learn, collaborate, and grow*. www.wileypluslearningspace.com

Semman Ansyari. (2024). Implementation of Risk Management in Strategic Decision Making. *Journal of Scientific Interdisciplinary*, *1*(1), 35–44. https://doi.org/10.62504/t7c2r379

Yudhaningsih, A., & Syah, T. Y. R. (2023). Risk Management Analysis of Coffee Dregs Brisket Innovation; Alternative Fuels in Indonesia. *MANAJEMEN DEWANTARA*, *8*(1), 45–59. https://doi.org/10.30738/md.v8i1.16488

Candiwan, C., Azmi, M., & Alamsyah, A. (2022b). Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era. *International Journal of Safety and Security Engineering*, *12*(2), 229–237. https://doi.org/10.18280/ijsse.120212

Candiwan, C., Prabowo, A. F. S., & Hidayatulloh, S. D. (2024). Sosialisasi Awareness Keamanan Informasi Untuk Guru Yayasan Fitrah Insani. *Jurnal Pengabdian Masyarakat Akademisi*, *3*, 75–81.

Candiwan, C., & Rianda, L. M. (2024). Transactions at Your Fingertips: Influential Factors in Information Security Behavior for Mobile Banking Users. *International Journal of Safety and Security Engineering*, *14*(3), 795–806. https://doi.org/10.18280/ijsse.140312