Perancangan Pengelolaan Risiko Keamanan Informasi Pada PT. XYZ Menggunakan ISO 27005:2022

1st Rico Galuh Pamungkas
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
ricopamungkas@student.telkomuniversity.ac.id

2nd Ryan Adhitya Nugraha
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
ranugraha@telkomuniversity.ac.id

3rd Widyatasya Agustika Nurtrisha
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
nurtrisha@telkomuniversity.ac.id

Keamanan informasi adalah aspek krusial bagi kelangsungan bisnis, termasuk bagi PT. XYZ yang bergerak di bidang konstruksi dan properti. Perusahaan ini belum memiliki sistem manajemen risiko keamanan informasi yang terstruktur dan juga belum memiliki prioritas terhadap resiko yang telah dilakukan, sehingga rentan terhadap berbagai ancaman digital. Penelitian ini bertujuan merancang sebuah sistem pengelolaan risiko keamanan informasi dengan mengacu pada standar internasional ISO/IEC 27005:2022. Menggunakan metode kualitatif dengan pendekatan studi kasus pada Divisi TI PT. XYZ, penelitian ini mengacu dan mengikuti pada tahapan sistematis standar tersebut yang meliputi penetapan konteks, penilaian risiko, dan penanganan risiko. Hasil penelitian berhasil mengidentifikasi 87 potensi risiko dari total aset TI yang dimiliki perusahaan. Setelah dievaluasi berdasarkan kriteria penerimaan risiko, ditemukan 18 risiko dengan level sedang hingga sangat tinggi yang memerlukan penanganan lebih lanjut melalui implementasi kontrol keamanan yang spesifik. Penelitian ini menghasilkan sebuah rancangan pengelolaan risiko yang tervalidasi dan siap menjadi fondasi bagi PT. XYZ untuk meningkatkan tata kelola keamanan informasinya secara efektif.

Kata Kunci: *manajemen risiko, keamanan informasi, ISO/IEC 27005:2022, aset TI, studi kasus*

I. PENDAHULUAN

Di era digital, teknologi informasi (TI) telah menjadi elemen fundamental bagi operasional bisnis di berbagai sektor, termasuk konstruksi. Peningkatan pemanfaatan TI ini diiringi dengan meningkatnya ancaman siber, kebocoran data, dan gangguan operasional yang dapat merugikan perusahaan. Oleh karena itu, manajemen risiko TI menjadi aktivitas krusial untuk menjaga efektivitas dan keberlanjutan organisasi.

PT. XYZ adalah sebuah perusahaan yang bergerak di bidang kontraktor, konsultan properti, dan layanan konstruksi di Indonesia. Dalam menjalankan operasional hariannya, PT. XYZ sangat bergantung pada aset TI. Namun, berdasarkan evaluasi internal, teridentifikasi adanya kesenjangan antara praktik yang ada dengan standar manajemen risiko internasional, karena perusahaan belum memiliki sistem manajemen risiko keamanan informasi yang terdokumentasi dan terstruktur. Kondisi ini, ditambah dengan adanya dorongan regulasi dari Badan Siber dan Sandi Negara (BSSN), melatarbelakangi kebutuhan mendesak untuk merancang sebuah kerangka kerja pengelolaan risiko.

Penelitian ini bertujuan untuk menjawab kebutuhan tersebut dengan merancang sistem pengelolaan risiko keamanan informasi untuk PT. XYZ dengan mengacu pada panduan standar ISO/IEC 27005:2022. Fokus utama penelitian ini adalah: (1) Bagaimana merancang proses penilaian risiko (*risk assessment*) untuk mengidentifikasi ancaman dan kerentanan pada aset TI perusahaan?; (2) Bagaimana mengevaluasi dan memprioritaskan risiko yang teridentifikasi?; dan (3) Bagaimana merumuskan rekomendasi penanganan risiko (*risk treatment*) yang efektif untuk mitigasi?

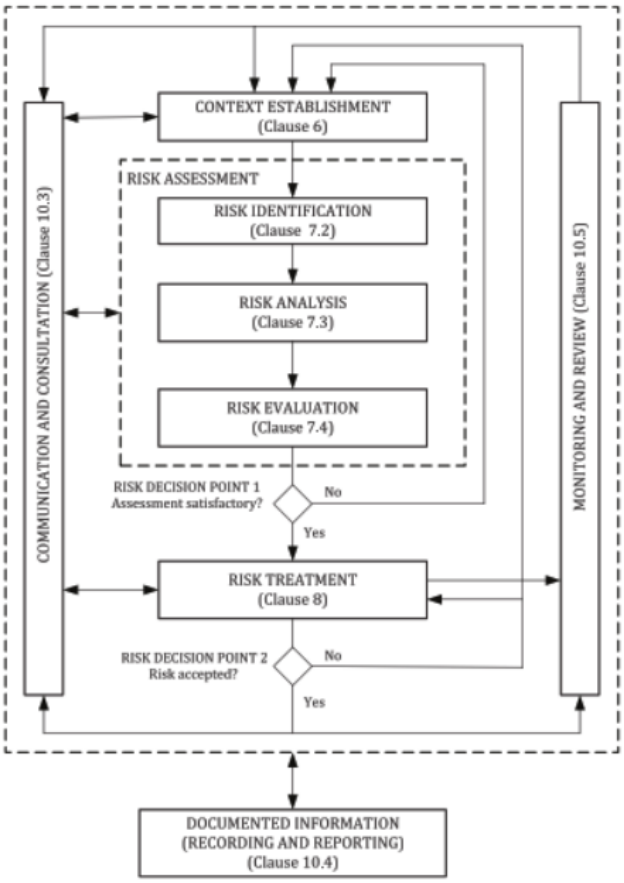
II. KAJIAN TEORI

A. *Manajemen Risiko Keamanan Informasi*

Manajemen risiko keamanan informasi adalah proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang berpotensi memengaruhi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) aset informasi. Tujuannya adalah untuk meminimalkan dampak negatif dari ancaman, sekaligus menjadi alat bantu dalam pengambilan keputusan strategis terkait keamanan.

B. ISO/IEC 27005:2022

ISO/IEC 27005:2022 adalah standar internasional yang menyediakan panduan spesifik untuk manajemen risiko keamanan informasi. Standar ini tidak mensyaratkan satu metode spesifik, namun menawarkan proses berulang yang fleksibel dan dapat diadaptasi oleh organisasi.



Proses utama yang diadopsi dalam penelitian ini terbatas pada tiga tahap inti:

1) ***Penetapan Konteks (*****Context Establishment*****):*** *Menentukan ruang lingkup, kriteria dasar (seperti dampak dan kemungkinan), dan batasan untuk semua aktivitas manajemen risiko.*

2) ***Penilaian Risiko (*****Risk Assessment*****):*** *Proses inti yang mencakup identifikasi risiko (*risk identification*), analisis risiko (*risk analysis*), dan evaluasi risiko (*risk evaluation*).*

3) ***Penanganan Risiko (*****Risk Treatment*****):*** *Proses memilih dan menerapkan kontrol untuk memodifikasi risiko yang tidak dapat diterima oleh organisasi.*

III. METODE

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus yang difokuskan pada Divisi TI PT. XYZ. Pengumpulan data dilakukan melalui **analisis dokumen** internal perusahaan, **wawancara mendalam** dengan personel kunci Divisi TI, serta **studi pustaka** terhadap standar ISO/IEC 27005:2022.

Proses penelitian mengikuti alur sistematis yang diadaptasi dari standar tersebut. Dimulai dengan **penetapan konteks**, di mana kriteria dampak dan kemungkinan risiko disusun menjadi matriks risiko. Tahap selanjutnya adalah **penilaian risiko**, yang mencakup inventarisasi aset, identifikasi ancaman dan kerentanan, serta analisis untuk menentukan level setiap risiko. Hasil dari penilaian ini kemudian divalidasi oleh pihak perusahaan dalam tahap **evaluasi risiko** untuk menentukan risiko mana yang dapat diterima (*retention*) dan mana yang memerlukan penanganan (*treatment*). Untuk risiko yang tidak dapat diterima, dirumuskan rekomendasi kontrol berdasarkan ISO/IEC 27001:2022.

IV. HASIL DAN PEMBAHASAN

A. *Analisis Risiko*

Proses analisis risiko dimulai dengan mengidentifikasi dan menginventarisasi seluruh aset TI yang berada di bawah pengelolaan Divisi TI PT. XYZ. Dari proses ini, teridentifikasi total **30 aset utama** yang diklasifikasikan ke dalam empat kategori: Perangkat Keras (*Hardware*), Perangkat Lunak (*Software*), Informasi/Data, dan Layanan & Infrastruktur. Selanjutnya, dilakukan pemetaan potensi ancaman (*threat*) dan kerentanan (*vulnerability*) yang relevan untuk setiap aset. Dari proses pemetaan ini, berhasil diidentifikasi sebanyak **87 skenario risiko** yang berpotensi mengancam keamanan informasi PT. XYZ.

B. *Penilaian Risiko*

Setiap dari 87 risiko yang teridentifikasi kemudian dinilai menggunakan matriks risiko (skala 1-5 untuk dampak dan kemungkinan) untuk menentukan *Level of Risk*. Hasil perkalian skor dampak dan kemungkinan menghasilkan distribusi level risiko sebagai berikut:

1) ***Sangat Tinggi (Skor 20-25):*** *2 Risiko*
2) ***Tinggi (Skor 16-19):*** *0 Risiko*
3) ***Sedang (Skor 10-15):*** *16 Risiko*
4) ***Rendah (Skor 6-9):*** *7 Risiko*
5) ***Sangat Rendah (Skor 1-5):*** *62 Risiko*

Distribusi ini menunjukkan bahwa meskipun mayoritas risiko berada pada level rendah, terdapat sejumlah risiko signifikan yang memerlukan perhatian segera.

C. *Evaluasi Risiko*

Berdasarkan kriteria penerimaan risiko (*risk acceptance criteria*) yang telah divalidasi oleh PT. XYZ, risiko dengan level **Sedang, Tinggi, dan Sangat Tinggi** dianggap tidak dapat diterima dan memerlukan tindakan mitigasi. Dengan demikian, dari total 87 risiko, sebanyak **18 risiko** diprioritaskan untuk masuk ke tahap penanganan risiko (*risk treatment*). Sisa 69 risiko lainnya diterima (*risk retention*) dengan tetap dilakukan pemantauan secara berkala.

D. *Penanganan Risiko*

Untuk ke-18 risiko prioritas, disusunlah rekomendasi kontrol mitigasi dengan mengacu pada **Annex A ISO/IEC 27001:2022**. Rekomendasi ini dirancang untuk mengurangi kemungkinan terjadinya risiko atau meminimalkan dampaknya.

E. *Klasifikasi Kontrol Risiko*

Setiap rekomendasi kontrol yang diusulkan juga diklasifikasikan berdasarkan fungsinya untuk menciptakan pertahanan berlapis (*defense-in-depth*):

1) ***Preventive (Pencegahan):*** *Kontrol yang dirancang untuk mencegah insiden terjadi. Contohnya adalah penerapan kebijakan hak akses ketat dan enkripsi data.*

2) ***Detective (Deteksi):*** *Kontrol untuk mengidentifikasi insiden yang sedang atau telah terjadi, seperti pemantauan audit log.*

3) ***Corrective (Perbaikan):*** *Kontrol untuk meminimalkan dampak dan memulihkan sistem setelah insiden, contohnya adalah prosedur pemulihan data dari backup.*

Mayoritas kontrol yang direkomendasikan untuk PT. XYZ bersifat **preventif**, yang bertujuan membangun fondasi keamanan yang kuat dari awal untuk mencegah kerugian.

F. *Kesimpulan dan Saran*

1) Kesimpulan: Penelitian ini telah berhasil merancang sebuah sistem pengelolaan risiko keamanan informasi yang sistematis dan komprehensif untuk PT. XYZ dengan mengacu pada standar ISO/IEC 27005:2022. Dari total 30 aset TI, teridentifikasi 87 potensi risiko, di mana 18 di antaranya dievaluasi sebagai risiko prioritas (level sedang hingga sangat tinggi) yang memerlukan tindakan mitigasi lebih lanjut. Rancangan ini, yang mencakup identifikasi risiko, penilaian, hingga rekomendasi penanganan yang tervalidasi, dapat menjadi fondasi yang kokoh bagi perusahaan untuk membangun dan meningkatkan postur keamanan informasinya secara efektif dan terstruktur.

2) Saran: Berdasarkan hasil penelitian, beberapa saran diajukan kepada PT. XYZ:

a) ***Implementasi dan Tinjauan Berkala:*** *Mengimplementasikan rancangan pengelolaan risiko yang telah disusun dan melakukan tinjauan secara berkala agar tetap relevan dengan perkembangan bisnis dan teknologi.*

b) ***Monitoring dan Evaluasi:*** *Menerapkan manajemen risiko secara disiplin dengan melakukan monitoring dan evaluasi rutin terhadap efektivitas kontrol yang ada.*

c) ***Penguatan Budaya Keamanan:*** *Meningkatkan kesadaran dan kompetensi keamanan informasi di kalangan karyawan melalui program pelatihan berkelanjutan.*

d) ***Perbaikan Berkelanjutan:*** *Mengadopsi prinsip* continuous improvement *agar sistem pengelolaan risiko senantiasa adaptif terhadap lanskap ancaman yang terus berubah.*

V. REFERENSI

[1] Ariyani, S., & Sudarma, M. (2016). Implementation Of The ISO/IEC 27005 In Risk Security Analysis Of Management Information System. *Journal of Engineering Research and Application, 6*.

[2] Hoshmand, M. O., & Ratnawati, S. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *AICOMS, 2*(2).

[3] ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. International Organization for Standardization.

[4] Paul Hopkin. (2017). *Fundamentals of Risk Management*.

[5] Sahira, S., Fauzi, R., & Santosa, I. (2020). Analisis Manajemen Risiko pada Aplikasi E-Office yang Dikelola oleh PT Telkom Indonesia Menggunakan Standar ISO/IEC 27005:2018. *e-Proceeding of Engineering, 7*(2).