BAB I
PENDAHULUAN

1.1. Gambaran Umum Objek Penelitian

1.1.1. Profil Objek Penelitian

Instansi Pendidikan X adalah sekolah menengah kejuruan berbasis pesantren yang terletak di Jalan Raya Dayeuh Kp. Tegal Putat, RT.01/RW.06, Desa Sukasirna, Kecamatan Jonggol, Kabupaten Bogor, Jawa Barat. Sekolah ini menggabungkan pendidikan vokasi dengan nilai-nilai keagamaan, bertujuan untuk memberikan pendidikan yang holistik, memadukan keterampilan teknis dan pengembangan karakter. Instansi Pendidikan X memiliki tiga jurusan utama. Program Pengembangan Perangkat Lunak dan Gim (PPLG) mengajarkan siswa untuk mengembangkan aplikasi berbasis web, desktop, mobile, serta gim. Program ini mempersiapkan siswa untuk menjadi ahli di bidang teknologi informasi, mengikuti perkembangan teknologi di era digital. Jurusan Usaha Pertanian Terpadu (UPT) memberikan keterampilan dalam pengelolaan pertanian dan peternakan. Siswa akan mempelajari cara mengelola usaha pertanian terpadu yang mencakup peternakan, pengolahan hasil pertanian, dan manajemen usaha, dengan penekanan pada praktik yang mendukung keberlanjutan usaha. Sementara itu, jurusan Teknik Konstruksi dan Perumahan (TKP) berfokus pada keterampilan di bidang konstruksi bangunan. Siswa akan dilatih dalam perencanaan dan pengawasan proyek konstruksi, serta keterampilan teknis seperti pengukuran tanah dan pembuatan gambar teknik, mempersiapkan mereka untuk bekerja di konstruksi dan properti. Selain fokus pada pendidikan akademik dan kejuruan, SMK Skill Village Islamic School juga menitikberatkan pada pengembangan karakter siswa melalui berbagai program seperti tahfidz Al-Qur’an, kegiatan spiritual, dan program pembangunan karakter seperti Skillage Supercamp. Sekolah ini berkomitmen untuk mencetak lulusan yang unggul, baik dari segi keterampilan teknis maupun akhlak, sehingga mereka siap bersaing di dunia kerja dengan landasan moral yang kuat (SMK Skill Village Islamic School, 2024).

1.1.2. VISI dan MISI

1. VISI

   Menjadikan Skill Village Islamic School sebagai kampung pembelajaran terbaik untuk menghasilkan lulusan berakhlakul karimah yang Profesional, Entrepreneur, Leader, Religius memiliki kecerdasan unggul di bidang otak (IQ), qalb (EQ) ruhani (SQ), dan tangguh (AQ) (SMK Skill Village Islamic School, 2024).

2. MISI

   Membangun ekosistem "Kampung Tumbuh Berbasis Masjid" yang mendukung pendidikan pesantren integratif holistik. Berkolaborasi dengan keluarga, masyarakat, dan pemerintah untuk membentuk akhlak mulia serta karakter unggul, memadukan program akademis dengan pemberdayaan masyarakat. Mengembangkan budaya komunikasi dalam Bahasa Arab dan Inggris, literasi unggul seperti Tahfidz Qur'an dan baca kitab kuning, serta kemitraan untuk profesionalisme, kewirausahaan, dan kepemimpinan. Menjalin sinergi dengan program pembangunan pemerintah di berbagai sektor (SMK Skill Village Islamic School, 2024).

1.2. Latar Belakang Penelitian

Perkembangan teknologi memegang peran penting dalam mendapatkan informasi terutama dengan adanya internet, akses untuk mendapatkan informasi akan lebih mudah. Menurut (GoodStats, 2024) mengatakan bahwa Indonesia mengalami transformasi digital yang signifikan dalam beberapa tahun terakhir. Teknologi *smartphone* telah menjadi salah satu pendorong utama perubahan ini, mempengaruhi berbagai aspek kehidupan masyarakat. Jumlah pengguna aktif *smartphone* di Indonesia telah meningkat secara konsisten setiap tahunnya. Pada tahun 2015, terdapat sekitar 54 juta pengguna aktif. Angka ini melonjak drastis menjadi 209,3 juta pada tahun 2023. Berikut disajikan tabel pengguna smartphone di Indonesia dari tahun 2016 – 2019 yang bersumber dari data.goodstats.id.

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. 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).

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 tingkat 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.

Kasus lainnya berdasarkan artikel yang ditulis oleh Fadli et al. (2024) mengatakan bahwa pada tanggal 12 Mei 2021, Indonesia mengalami kasus serius terkait kebocoran informasi atau data pribadi yang melibatkan sekitar 279 juta data warga. Informasi yang tersedia mencakup detail seperti nama lengkap sesuai Kartu Tanda Penduduk (KTP), nomor telepon, alamat email, Nomor Identitas (NIK), lokasi tinggal, serta perkiraan pendapatan. Lebih dari 20 juta data juga dilengkapi dengan foto pribadi penduduk.

Menurut Wulff & Finnestrand (2023) data sangat terkait dengan informasi, dimana data berfungsi sebagai elemen dasar yang membentuk informasi yang bernilai bagi perusahaan. Untuk memastikan informasi yang diperoleh relevan dan akurat, data perlu diolah secara sistematis dengan pendekatan yang terstruktur dan didukung oleh sumber yang terpercaya. Pengolahan data yang cermat menghasilkan informasi yang dapat diandalkan sebagai pedoman dalam pengambilan keputusan strategis perusahaan. Selain itu, penting bagi perusahaan untuk menjaga integritas, kerahasiaan, dan keamanan informasi, karena data yang dimiliki merupakan aset berharga yang tidak hanya mendukung operasional dan strategi bisnis tetapi juga rentan terhadap ancaman kejahatan siber.

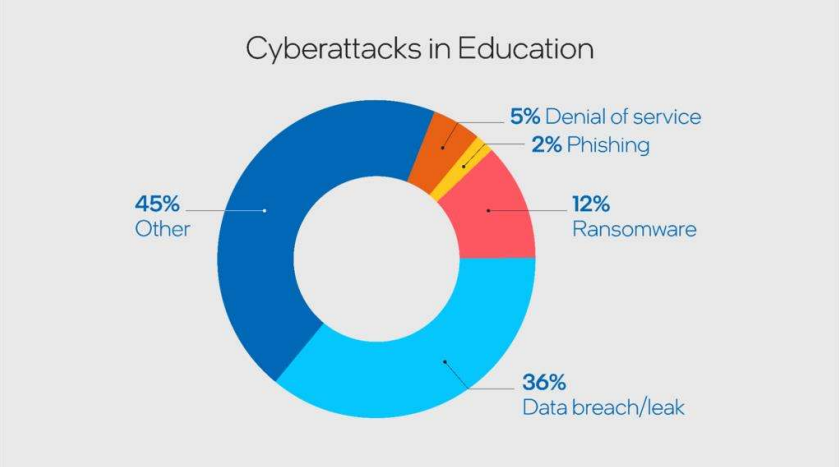
Menurut (Sukamto et al., 2021) tata Kelola Teknologi Informasi (TI) mencakup aspek kepemimpinan, pengaturan struktur, serta proses dalam organisasi yang dirancang untuk memastikan bahwa pemanfaatan TI berjalan secara maksimal. Tata kelola ini memiliki cakupan luas dan berfokus pada peningkatan kinerja serta transformasi TI, sehingga dapat memenuhi berbagai kebutuhan yang ada saat ini maupun di masa mendatang. Selain itu, Tata Kelola TI mempertimbangkan kebutuhan dari perspektif internal organisasi, seperti efisiensi operasional, serta faktor eksternal, termasuk respons terhadap perkembangan teknologi dan persaingan di pasar. Tujuan akhirnya adalah untuk menjadikan TI sebagai aset strategis yang memberikan nilai tambah dan mendorong pencapaian

tujuan organisasi. Menurut Maulana (2024) mengatakan bahwa Tata Kelola Teknologi Informasi (ITG) adalah manajemen organisasi yang memastikan penerapan TI yang efektif dan efisien untuk mencapai tujuan. Tata kelola ini berfokus pada penyelarasan TI dengan tujuan organisasi, pengukuran efektivitas proses bisnis, penggunaan sumber daya, manajemen risiko, dan peningkatan kinerja organisasi secara keseluruhan.

Keamanan informasi telah menjadi isu krusial di era Industri 4.0, khususnya setelah pandemi Covid-19. Perubahan gaya hidup masyarakat Indonesia semakin memperlihatkan ketergantungan pada internet untuk menunjang berbagai aktivitas sehari-hari, baik itu pekerjaan, pendidikan, hiburan, hingga transaksi keuangan. Pertumbuhan penggunaan perangkat seluler seperti smartphone dan laptop pun melonjak, dan kian banyak masyarakat yang memanfaatkan koneksi Wi-Fi publik di ruang-ruang kota. Fenomena ini kini sangat lazim ditemukan, terutama di area publik seperti kafe, perpustakaan, dan pusat perbelanjaan di berbagai kota besar di Indonesia.(Candiwan et al., 2024).

Menurut Ardiansyah et al. (2023) pemahaman tentang keamanan siber sangat penting bagi Perusahaan di semua bidang agar mereka mampu mengenali berbagai bentuk ancaman digital yang semakin kompleks dan canggih di era teknologi ini. Dengan literasi keamanan siber yang baik, mereka dapat mengetahui langkah-langkah yang efektif untuk melindungi data pribadi, menjaga privasi, serta mengamankan informasi penting yang ada di perangkat mereka. Pengetahuan ini juga memungkinkan mereka untuk lebih waspada terhadap upaya peretasan, penyebaran *malware*, dan ancaman lain yang berpotensi merusak sistem atau mencuri informasi berharga.

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 Kyle Chin dalam website UpGuard (2024) menyatakan bahwa Lembaga pendidikan menjadi salah satu target utama serangan siber, bersaing dengan sektor seperti layanan kesehatan, keuangan, dan ritel. Sektor ini mengalami peningkatan serangan siber sebesar 44 persen dibandingkan tahun sebelumnya, dengan rata-rata 2.300 serangan dilaporkan setiap minggunya. Penjahat siber menargetkan sektor pendidikan karena berbagai alasan, terutama karena lembaga ini mengelola data pribadi siswa, informasi pinjaman, data penelitian yang sensitif, serta sering kali memiliki sistem keamanan siber yang kurang memadai. Minimnya kesadaran akan risiko siber di sektor pendidikan, terutama di kalangan staf yang lebih mengutamakan kolaborasi dan solusi praktis dibandingkan pertimbangan keamanan data, membuat institusi pendidikan menjadi target yang rentan terhadap serangan siber. Kondisi ini diperburuk oleh keterbatasan anggaran untuk keamanan siber, yang menyebabkan kurangnya perlindungan terhadap data pribadi dan sistem jaringan, sehingga semakin membuka peluang bagi para pelaku kejahatan digital.

Penelitian serupa dari Daulay & Hidayat (2023) mengatakan bahwa Manajemen risiko di SMP Intan Al-Sali mencakup proses mengenali, menilai, dan mengendalikan berbagai risiko baik dari dalam maupun luar yang dapat memengaruhi pencapaian tujuan pendidikan. Risiko dari dalam sekolah meliputi persoalan operasional dan tantangan dalam pengelolaan sumber daya manusia, sementara risiko dari luar berkaitan dengan citra sekolah dan berbagai ancaman eksternal. Penerapan manajemen risiko yang tepat membantu mengoptimalkan penyediaan sarana dan prasarana pendidikan, memperkuat sistem keamanan, serta mendukung perencanaan strategis. Untuk mengatasi berbagai risiko tersebut dan meningkatkan mutu pendidikan, sekolah melakukan evaluasi secara sistematis melalui peninjauan dan penilaian manajemen.

Penelitian lain dari Miftahuldzanah & Hidayat (2025) mengatakan bahwa Manajemen risiko di SMKN 4 Bandung belum sepenuhnya didukung oleh kesadaran akan pentingnya *risk awareness*. Meskipun tantangan seperti perbedaan

pemahaman siswa dan keterbatasan fasilitas telah dikenali, respons sekolah masih bersifat prosedural tanpa pendekatan risiko yang menyeluruh. Masalah koordinasi guru dan manajemen waktu yang terus berulang menunjukkan lemahnya budaya sadar risiko, sehingga dibutuhkan peningkatan kerja sama dan perencanaan yang lebih berkelanjutan.

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).

Bisnis di era digital harus memberikan perhatian serius dalam melindungi aset mereka dari ancaman serangan siber. Salah satu langkah penting untuk memastikan keamanan sistem adalah dengan mematuhi standar keamanan yang berlaku di industri. Dari 90 persen perusahaan di berbagai sekotor telah mengadopsi satu atau lebih standar keamanan, seperti NIST, ISACA, ISO 27001,ISO 27002, ISO 27005. Standar-standar ini memberikan pedoman tentang praktik keamanan yang perlu diterapkan oleh organisasi untuk melindungi aset bisnis mereka (Budiman et al., 2023).

Menurut Putra & Soewito, (2023) ISO 27005 merupakan standar yang berfokus pada manajemen risiko keamanan informasi. Standar ini memberikan panduan dalam merancang, mengimplementasikan, memelihara, serta meningkatkan proses manajemen risiko secara berkelanjutan. Standar ini juga mendukung penerapan kontrol keamanan yang tercantum dalam ISO 27001 dan ISO 27002, sehingga mampu meningkatkan perlindungan informasi secara menyeluruh. Menggunakan *risk management* ISO 27005 dapat memberikan panduan yang dapat diterapkan dalam berbagai situasi di organisasi. Standar ini juga dapat digunakan oleh semua jenis organisasi, baik di lingkungan pemerintahan, komersial, maupun nonkomersial (Al Fikri et al., 2019)

Menurut Marbun et al. (2024) NIST SP 800-30 adalah kerangka kerja manajemen risiko yang dikembangkan oleh *National Institute of Standards and Technology*. Kerangka kerja ini menyediakan panduan untuk melakukan penilaian risiko guna mengidentifikasi, mengevaluasi, dan mengurangi risiko terhadap sistem informasi, serta memastikan praktik manajemen risiko yang efektif.

Menurut Putra & Soewito, (2023) ISO 27005 dan NIST SP 800-30 revisi 1 berkolaborasi dengan mengintegrasikan kerangka kerja manajemen risiko dan pedoman penilaian risiko, meningkatkan kemampuan organisasi untuk melakukan penilaian risiko yang komprehensif dan menerapkan strategi manajemen risiko keamanan informasi yang efektif.

Dalam penelitian yang dilakukan oleh Al Fikri et al. (2019), dipilih kombinasi antara ISO/IEC 27005 dan NIST SP 800-30 Revision 1 karena keduanya merupakan standar internasional yang saling melengkapi dalam proses manajemen risiko keamanan informasi. ISO 27005 menyediakan kerangka kerja manajerial untuk penilaian risiko, sementara NIST SP 800-30 menawarkan langkah teknis yang lebih rinci untuk mengidentifikasi ancaman, menilai dampak, dan menghitung tingkat risiko. Penulis tidak menggunakan variabel lain seperti ISO 31000 atau metode COSO karena pendekatan tersebut bersifat umum dan tidak secara spesifik membahas aspek teknis keamanan informasi. Oleh karena itu, kombinasi ISO dan NIST dipilih agar menghasilkan metode penilaian risiko yang aplikatif, sistematis, dan relevan dengan kebutuhan organisasi berbasis teknologi informasi.

Sesuai dengan hasil wawancara yang dilakukan oleh penulis dengan informan yang berasal dari Instansi pendidikan X mengatakan bahwa Instansi pendidikan X belum pernah melakukan penilaian risiko terhadap sistem informasi. Informan mengatakan bahwa perlunya untuk melakukan penilaian risiko agar dapat mengetahui risiko mana yang perlu untuk ditindak lanjuti, Informan juga mengatakan bahwa terkadang terjadi permasalahan pada sistem seperti pada saat melakukan proses pelayanan perizinan akses ke database mengalami disconnected. Hal tersebut menjadi salah satu permasalahan karena dapat menghambat pekerjaan sehingga tujuan organisasi sulit untuk dicapai.

Berdasarkan paparan latar belakang sesuai dengan fenomena yang terjadi di atas, peneliti akan membahas tentang tingkat risiko keamanan informasi yang menggunakan standarisasi ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 untuk meningkatkan kualitas informasi dan objek yang akan dibahas oleh penulis adalah proses bisnis pada sistem informasi ZZZ Instansi pendidikan X. Alasan penulis mengambil objek tersebut karena Instansi pendidikan X belum melakukan penilaian risiko pada sistem informasi ZZZ dan menerapkan standar keamanan informasi untuk tetap menjaga kualitas. Oleh karenanya perusahaan perlu mengukur tingkat keamanan data sehingga kepentingan pengguna dapat terlindungi.

Namun, berdasarkan kajian terhadap sejumlah penelitian terdahulu, ditemukan bahwa sebagian besar studi hanya menggunakan salah satu framework, baik ISO/IEC 27005 maupun NIST SP 800-30 secara terpisah. Sangat sedikit penelitian yang menggabungkan kedua framework tersebut dalam konteks instansi pendidikan, khususnya pada sekolah menengah kejuruan berbasis pesantren yang memiliki karakteristik sistem informasi dan struktur organisasi yang unik. Kesenjangan ini menunjukkan perlunya pendekatan baru yang lebih komprehensif dan kontekstual. Oleh karena itu, penelitian ini hadir untuk mengisi celah tersebut dengan melakukan penilaian risiko keamanan informasi menggunakan kombinasi ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 pada Instansi Pendidikan X.

Maka dari itu, peneliti terinspirasi untuk membuat judul penelitian **"ASSESSMENT TINGKAT RISIKO KEAMANAN INFORMASI MENGGUNAKAN FRAMEWORK ISO/IEC 27005:2022 DAN NIST SP 800-30 REVISI 1 PADA INSTANSI PENDIDIKAN X"**

1.3. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, penelitian ini berfokus pada beberapa permasalahan utama terkait sistem informasi ZZZ di Instansi pendidikan X. Adapun rumusan masalah yang akan dibahas dalam penelitian ini adalah sebagai berikut:

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

1.4. Tujuan Penelitian

Berdasarkan pertanyaan penelitian yang telah dijabarkan sebelumnya, penelitian ini bertujuan untuk:

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.

1.5. Manfaat Penelitian

Berdasarkan uraian tujuan penelitian di atas, penulis mengharapkan penelitian ini dapat bermanfaat untuk:

1. Aspek Teoritis

   Penelitian ini diharapkan dapat dijadikan masukan untuk mengkaji bagaimana *assessment* tingkat risiko keamanan informasi pada suatu proses bisnis terhadap sistem informasi yang mengacu pada standarisasi ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1. Penelitian ini juga diharapkan dapat berguna bagi bidang keilmuan manajemen risiko keamanan informasi dan

temuan-temuan yang diperoleh dapat memberikan pandangan terhadap analisa tingkat risiko keamanan informasi bagi penelitian selanjutnya.

2. Aspek Praktis

Penelitian ini digunakan sebagai informasi dan referensi dalam hal penerapan keamanan informasi dalam suatu perusahaan untuk melindungi aset yang ada pada perusahaan tersebut dengan tujuan meyakinkan integritas, keamanan, ketersediaan dan pengelolaan data yang ada. Penelitian ini memberikan gambaran mengenai sejauh mana penerapan keamanan informasi berdasarkan ISO/IEC 27005:2022 dan NIST SP 800-30 Revisi 1 pada sistem informasi ZZZ Instansi pendidikan X dan laporan analisa evaluasi tingkat risiko keamanan informasi tersebut.

Penelitian ini diharapkan dapat memberikan wawasan serta menjadi bahan pertimbangan bagi perusahaan, terutama dalam meningkatkan inovasi dan kualitas produk yang berkontribusi pada keunggulan kompetitif.

1.6. Sistematika Penulisan

Sistematika penulisan penelitian berguna untuk memberikan gambaran yang jelas mengenai penelitian yang dilakukan, sistematika penulisan penelitian ini adalah sebagai berikut:

a. BAB I PENDAHULUAN

Bab ini berisikan cakupan gambaran umum objek penelitian, latar belakang penelitian, perumusan masalah, pertanyaan penelitian, manfaat penelitian, penelitian dan sistematika penulisan tugas akhir.

b. BAB II TINJAUAN PUSTAKA

Bab ini berisikan landasan teori mengenai hal-hal yang berkaitan dengan penelitian dan model penelitian. Bab ini juga memperlihatkan beberapa penelitian terdahulu yang digunakan sebagai perbandingan, kerangka pemikiran.

c. BAB III METODE PENELITIAN

Bab ini berisikan tentang uraian, pendekatan, metode dan teknik yang digunakan untuk mengumpulkan dan menganalisis data yang dapat menjawab rumusan masalah yang ada pada penelitian ini.

d. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisikan hasil pengolahan data yang didapat dan hasilnya akan dianalisis sesuai dengan data yang didapatkan

e. BAB V KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan serta saran-saran dari hasil penelitian yang telah dilakukan.