JURNAL LOCUS: Penelitian & Pengabdian
Volume 4 No. 11 November 2025
E-ISSN 2829-7334| P-ISSN 2829-5439
Hompage: https://locus.rivierapublishing.id/index.php/jl

Analisis Kesiapan PT. XYZ Sebagai Penyedia Layanan TI Dalam Mengadopsi Standar Nist CSF dan ISO 27001

Rona Aulia Wangsa Sea, Nenden Siti Fatonah, Gerry Firmansyah, Habibullah Akbar
Universitas Esa Unggul, Indonesia
Email: rona.aulia2000@student.esaunggul.ac.id, nenden.siti@esaunggul.ac.id, gerry@esaunggul.ac.id, habibullah.akbar@esaunggul.ac.id

Abstrak:
Penelitian ini bertujuan untuk menganalisis tingkat kesiapan PT. XYZ sebagai penyedia layanan teknologi informasi dalam mengadopsi framework keamanan sistem teknologi, khususnya NIST CSF dan ISO 27001. Pendekatan kualitatif digunakan melalui wawancara dengan lima informan jajaran pimpinan dan tim teknis. Analisis data dilakukan menggunakan metode analisis tematik. Temuan menunjukkan bahwa perusahaan masih berada pada tingkat kesiapan awal dan belum memiliki pendekatan sistematis terhadap pengelolaan keamanan informasi. Faktor penghambat utama adalah kurangnya kebijakan formal, keterbatasan sumber daya, dan rendahnya pemahaman terhadap standar internasional. Namun, adanya kesadaran manajemen dan keinginan memperkuat kepercayaan klien menjadi pendorong penting. Strategi peningkatan yang direkomendasikan meliputi pelatihan, penyusunan kebijakan, pembentukan tim keamanan, dan integrasi keamanan dalam proses bisnis. Penelitian ini memberikan gambaran awal bagi perusahaan dalam merancang strategi keamanan berstandar, serta menjadi referensi bagi studi sejenis di sektor layanan TI. Penelitian ini berkontribusi dalam memperluas pemahaman kesiapan organisasi sektor TI terhadap penerapan framework keamanan informasi berbasis NIST CSF dan ISO 27001 dalam konteks perusahaan Indonesia.
Kata kunci: Keamanan Informasi, NIST CSF, ISO 27001, Analisis Tematik, Kesiapan Perusahaan.

Abstract:
This study aims to analyze the readiness level of PT. XYZ, an information technology service provider, in adopting technology security frameworks, specifically NIST Cybersecurity Framework (CSF) and ISO 27001. A qualitative approach was applied through interviews with five informants from the executive level and technical teams. The data were analyzed using thematic analysis. Findings indicate that the company is still at an early stage of readiness and lacks a systematic approach to managing information security. The main inhibiting factors include the absence of formal policies, limited resources, and a low level of understanding of international standards. However, the management's awareness and desire to enhance client trust serve as important driving factors. Recommended improvement strategies include conducting training, establishing formal security policies, forming dedicated security teams, and integrating security into business processes. This study provides a preliminary overview for the company in designing a standardized security strategy and serves as a reference for similar studies in the IT services sector. This research contributes to expanding the understanding of IT sector organizations' readiness in implementing information security frameworks based on NIST CSF and ISO 27001 in the Indonesian corporate context.
Keywords: Information Security, NIST CSF, ISO 27001, Thematic Analysis, Organizational Readiness.

Corresponding: Rona Aulia Wangsa Sea
E-mail: rona.aulia2000@student.esaunggul.ac.id

PENDAHULUAN

Salah satu tujuan utama berbisnis adalah mendapatkan keunggulan kompetitif dengan memberikan solusi terbaik pada pelanggan melalui produk atau layanan yang diberikan (Khadafie, 2025; Ramadhani, 2025). Keinginan pelanggan yang semakin berubah memicu perputaran pasar yang dinamis. Sehingga, Perusahaan harus memiliki rencana strategis agar dapat mewujudkannya dengan tetap sesuai dengan preferensi pelanggan (Hariandja, 2025; Ombuh et al., 2025). Sebagai perusahaan penyedia layanan Teknologi Informasi (TI), pastinya memiliki lingkup pelanggan yang luas (Hasibuan, Bangun, & Sihombing, 2025; Rosida &

Rusdianto, 2025). Mulai dari perusahaan dengan skala kecil, menengah, hingga besar. Ini artinya, perusahaan penyedia layanan TI harus dapat mengikuti kebutuhan yang begitu banyak.

Perkembangan teknologi yang dinamis, memaksa pelanggan untuk mengikuti perkembangan secara cepat. Mereka semakin sadar akan bahaya yang mengancam ketika mereka mengadopsi teknologi di dalam kegiatan bisnisnya (Ambardi, Widhyharto, Madya, & Wibawanto, 2025; Sugiyanto, Sukmayuda, & Andiyana, 2024). Dapat dikatakan bahwa mereka sudah paham betul mengenai masalah keamanan sistem teknologi atau dapat dikatakan sebagai ancaman serangan siber (Maryani, 2025; Undang-Undang, n.d.). Ini membuat mereka untuk semakin peka terhadap keamanan sistem teknologi yang sedang mereka gunakan saat ini ataupun yang akan digunakan di masa mendatang. Sebagai perusahaan penyedia layanan TI, mereka harus dapat menangkap fenomena ini. Kesadaran akan keamanan sistem teknologi haruslah menjadi poin utama dalam solusi yang mereka berikan pada pelanggan (Fitriani & Wardani, 2025; Shadani, Fahrozi, Fahriza, & Alpiansyah, 2025). Selain menjadi nilai lebih, pelanggan akan dapat melihat sebarapa besar tanggung jawab perusahaan tersebut dalam menjaga kualitas layanannya (Chaindra et al., 2024; Sepriano & Judijanto, 2025). Tidak peduli jika pelanggan meraka adalah perusahaan dengan skala kecil, sedang, ataupun besar.

Isu keamanan sistem teknologi haruslah menjadi prioritas utama. Hal ini mendorong perusahaan penyedia layanan TI yang belum siap ataupun matang mengenai keamanan sistem teknologi untuk mulai menata tim internal mereka mengenai solusi yang akan diberikan di waktu (Dewanti & Permana, 2025; Merryana Lestari, Puspita, & Wijaya, 2025). Di dalam persaingan bisnis, tidak menutup kemungkinan jika nantinya kebanyakan calon pelanggan akan menjadikan sistem keamanan teknologi di dalam syarat dari solusi yang ditawarkan (Maulidina et al., 2025; Sinaga et al., 2025). Walaupun saat ini belum menjadi perhatian yang tertuang secara khusus, sebagai perusanaagn penyedia layanan TI sudah harus dapat memahami hal ini. Mereka dapat menggunakan beberapa framework yang berisikan panduan-panduan mengenai keamanan sistem teknologi (Nanda Oktavia Dwi Lestari, 2025). Bagi perusahaan yang akan memulai untuk mengadopsi framework-framework tersebut pastinya harus melakukan analisis kesiapan pada tim internal mereka.

Framework seperti NIST CSF dan ISO 27001 dapat digunakan sebagai panduan keamanan sistem teknologi, khususnya pada kemanan data dari serangan siber. Framework ini dapat diadopsi untuk seluruh jenis perusahaan, mulai dari perusahaan dengan skala kecil, menengah, hingga besar sekalipun. Sehingga, tidak ada alasan untuk tidak peka terhadap keamanan sistem teknologi, apalagi sebagai perusahaan penyedia layanan TI diharuskan untuk selalu memiliki langkah yang lebih maju ketimbang para pelanggannya.

Beberapa penelitian terdahulu telah mengkaji penerapan framework keamanan informasi dalam berbagai konteks organisasi (Firmansyah, 2025; Nugraha & Hendrik, 2025). Penelitian Fadya & Utama (2025) mengintegrasikan NIST CSF dengan COBIT 2019 untuk evaluasi keamanan sistem informasi pada konteks umum, sementara Razikin & Soewito (2022) mengembangkan model pendukung keputusan berbasis analisis risiko dan framework cybersecurity. Namun, penelitian-penelitian tersebut belum secara spesifik menilai kesiapan adopsi NIST CSF dan ISO 27001 pada perusahaan penyedia layanan TI di Indonesia (Alam, Hidayah, Gunawan, Wijaya, & Abdullah, 2025). Oleh karena itu, penelitian ini memberikan

pembaruan konteks melalui pendekatan tematik pada sektor privat Indonesia, dengan fokus pada identifikasi hambatan dan strategi peningkatan kesiapan internal organisasi.

Penelitian ini nantinya akan melakukan analisis kesiapan dari sebuah perusahaan penyedia layanan IT untuk mengadopsi framework keamanan sistem teknologi seperti NIST CSF dan ISO 27001. Dengan dilakukannya analisis kesiapan ini, perusahaan penyedia layanan TI dapat mengerti seberapa jauh mereka sudah memahami isu keamanan sistem teknologi. Dengan memahami kondisi tim internal mereka saat ini, diharapkan mereka dapat meningkatkan kualitas tim internal mereka dalam memberikan solusi terbaik kepada pelanggan. Dilanjutkan dengan menciptakan strategi yang baru, diharapkan mereka dapat memberikan solusi layanan TI yang berorientasi pada keamanan sistem teknologi kepada pelanggan.

Penelitian ini bertujuan untuk mengetahui tingkat kesiapan PT. XYZ dalam mengadopsi framework keamanan sistem teknologi informasi, khususnya NIST CSF dan ISO 27001, serta mengidentifikasi faktor-faktor pendorong dan penghambat yang dihadapi perusahaan dalam proses adopsinya. Selain itu, penelitian ini juga bertujuan merumuskan strategi untuk meningkatkan kapabilitas tim internal dalam menyediakan solusi layanan TI yang berorientasi pada keamanan. Adapun manfaat penelitian ini bagi PT. XYZ adalah memberikan pemahaman mendalam terkait kesiapan internal, mengidentifikasi kesenjangan antara kondisi aktual dan standar ideal berdasarkan framework yang diacu, serta mendorong peningkatan kualitas layanan guna memperkuat daya saing perusahaan. Bagi pelanggan, hasil penelitian ini diharapkan dapat memberikan jaminan sistem yang lebih aman, mengurangi risiko gangguan operasional, serta memberikan ketenangan karena sistem yang digunakan telah memenuhi standar keamanan yang diakui secara global.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif untuk mengkaji kesiapan PT. XYZ dalam menerapkan standar keamanan informasi seperti NIST CSF dan ISO 27001, dengan fokus pada pemahaman, pengalaman, serta hambatan dan peluang yang dirasakan oleh tim internal. Alur penelitian mencakup identifikasi masalah, studi literatur, penyusunan panduan wawancara semi-terstruktur, pengumpulan data melalui wawancara dengan informan kunci, serta analisis data menggunakan metode analisis tematik. Instrumen penelitian dirancang berdasarkan elemen-elemen utama dari kedua standar keamanan tersebut, dan informan dipilih melalui purposive sampling dengan kriteria tertentu. Hasil dari proses ini diharapkan dapat memberikan gambaran menyeluruh mengenai tingkat kesiapan perusahaan dalam mengadopsi standar keamanan informasi, serta merumuskan strategi peningkatan yang relevan. Keabsahan data dijamin melalui triangulasi sumber dan member checking untuk memastikan konsistensi hasil wawancara. Seluruh informan memberikan persetujuan partisipasi secara sukarela dan data disajikan tanpa identitas personal guna menjaga kerahasiaan dan etika penelitian.

HASIL DAN PEMBAHASAN

Analisis Data

Analisis dilakukan secara tematik untuk mengidentifikasi tema-tema kunci yang mencerminkan tingkat kesiapan perusahaan dalam mengadopsi framework keamanan informasi.

Familirisasi Data dan Pengkodean Awal

Pada bagian ini berisikan hasil wawancara yang sudah dirubah menjadi menjadi bahasa formal.

1) Pertanyaan 1

   Seberapa penting keamanan informasi dalam kegiatan operasional harian perusahaan?

   A1 : "Keamanan informasi memang penting, tapi terus terang belum menjadi prioritas harian di level strategis. Fokus utama kami selama ini adalah pengembangan produk dan penetrasi pasar. Namun, kami mulai sadar bahwa isu keamanan ini bisa berdampak besar terhadap kepercayaan klien, apalagi kalau menyangkut data mereka."

   [Kode] : Keamanan tidak jadi prioritas strategis; Keamanan berdampak reputasi.

   A2 : "Saya melihat keamanan informasi itu krusial, apalagi dalam operasional layanan yang bersentuhan langsung dengan sistem klien. Tapi karena belum ada sistem keamanan yang formal atau framework yang kami ikuti, kami masih banyak melakukan pengamanan berdasarkan pengalaman saja, belum berbasis kebijakan."

   [Kode] : Tidak ada sistem formal; Praktik berbasis pengalaman.

   A3 : "Kalau dari sisi teknis, kami paham bahwa keamanan sangat penting. Tapi jujur saja, prosedur keamanan belum menjadi bagian dari SOP rutin. Biasanya kami bertindak saat ada insiden, bukan antisipasi. Padahal idealnya kita harus proaktif."

   [Kode] : Tidak terintegrasi dalam SOP; Penanganan reaktif.

   A4 : "Saya pribadi menilai keamanan informasi sangat penting, terutama karena proyek-proyek kami sering berisi informasi sensitif dari klien. Tapi ya, belum ada kebijakan baku soal ini. Kadang kami hanya mengandalkan pengamanan manual dan kontrol akses sederhana."

   [Kode] : Data sensitif tidak dilindungi oleh kebijakan; Pengamanan manual.

   A5 : "Untuk pengembangan software, keamanan seharusnya ditanamkan sejak awal. Tapi saat ini, fokus kami lebih ke fungsionalitas dan deadline. Belum ada standar atau checklist keamanan yang kami ikuti secara resmi. Jadi, bisa dibilang kesadaran itu ada, tapi belum diterjemahkan ke praktik."

   [Kode] : Prioritas ke fungsi bukan keamanan; Tidak ada panduan pengembangan aman.

2) Pertanyaan 2

   Pernahkah perusahaan mengalami gangguan atau insiden keamanan data/sistem?

   A1 : "Secara umum, kami belum pernah mengalami kebocoran besar yang sampai berdampak luas. Tapi beberapa tahun lalu pernah ada kejadian di mana server kami disusupi malware. Untungnya cepat tertangani oleh tim teknis. Tapi ya, setelah itu tidak ada evaluasi menyeluruh, dan tidak dilanjutkan ke kebijakan khusus."

   [Kode] : Tidak ada tindak lanjut formal.

   A2 : "Pernah. Salah satu proyek yang sedang berjalan mengalami gangguan karena ada akses tidak sah ke server. Kami sempat menghentikan operasional proyek selama dua hari. Kami hanya melakukan tindakan teknis untuk mengembalikan sistem, belum sampai ke level audit atau analisis risiko."

   [Kode] : Gangguan serius tanpa evaluasi risiko.

   A3 : "Beberapa kali kami menghadapi serangan brute-force pada akun admin. Biasanya kami tangani langsung secara teknis, seperti blokir IP atau ganti kredensial. Tapi saya akui,

belum ada pelaporan formal atau sistem pencatatan insiden. Jadi ya, penanganannya masih sangat teknis dan insidensial."

[Kode] : Penanganan teknis saja.

A4 : "Dari sisi proyek, pernah ada kasus di mana file proyek hilang akibat virus di salah satu laptop. Saat itu, kami hanya restore dari backup, tapi kejadian itu tidak ditindaklanjuti ke level kebijakan atau pelatihan. Tidak ada pelaporan resmi, hanya dianggap masalah teknis biasa."

[Kode] : Insiden dianggap masalah biasa.

A5 : "Pernah ada laporan bug dari pengguna yang ternyata menunjukkan celah keamanan di aplikasi kami. Tapi tidak ada protokol tanggap darurat, hanya langsung diperbaiki dan ditutup. Saya kira ini seharusnya jadi pelajaran penting, tapi tidak terdokumentasi secara formal."

[Kode] : Insiden keamanan dianggap masalah biasa.

3) Pertanyaan 3

Apakah pimpinan menunjukkan kepedulian terhadap keamanan TI?

A1 : "Sejujurnya, perhatian saya lebih banyak ke arah pengembangan bisnis dan efisiensi operasional. Untuk keamanan TI, saya menyadari pentingnya itu, tapi kami belum secara eksplisit menjadikannya bagian dari agenda strategis. Mungkin perlu ada dorongan dari bawah agar kami juga bisa menyesuaikan arah kebijakan."

[Kode] : Tidak jadi agenda strategis.

A2 : "Kepedulian itu ada, tapi lebih bersifat pasif. Selama tidak ada masalah berarti, isu keamanan TI belum menjadi topik utama dalam rapat manajemen. Kami lebih sering bicara soal target layanan dan SLA. Jadi, bisa dibilang perhatian ada, tapi belum dalam bentuk kebijakan yang jelas."

[Kode] : Kepedulian pasif, tidak diangkat di manajemen.

A3 : "Kalau dari pimpinan teknis langsung, saya rasa perhatian ada, tapi belum sistematis. Misalnya, belum pernah ada arahan untuk membuat kebijakan keamanan, atau membentuk tim keamanan. Biasanya kami bergerak sendiri kalau ada isu."

[Kode] : Minim dukungan sistematis dari pimpinan.

A4 : "Dari yang saya lihat, pimpinan lebih fokus ke kualitas layanan dan penyelesaian proyek. Saya belum pernah mendengar pembahasan khusus tentang keamanan TI dalam forum manajemen. Saya rasa, masih dianggap sebagai urusan teknis saja, bukan urusan strategis."

[Kode] : Keamanan dianggap urusan teknis.

A5 : "Di level pengembangan, saya tidak pernah mendapatkan arahan eksplisit dari pimpinan soal keamanan. Kami diberi target rilis dan deadline, tapi tidak ada pembahasan soal aspek keamanan. Jadi, sepertinya kepedulian belum diartikulasikan secara konkret."

[Kode] : Keamanan tidak masuk dalam arahan manajemen.

4) Pertanyaan 4

Apakah ada prosedur tertulis untuk menjaga keamanan data?

A1 : "Saat ini, belum ada prosedur tertulis yang spesifik untuk keamanan data. Beberapa panduan teknis mungkin ada di tingkat teknis, tapi secara formal dan menyeluruh belum

pernah kami tetapkan. Ini memang menjadi salah satu hal yang ingin kami benahi ke depannya."

[Kode] : Tidak ada kebijakan formal.

A2 : "Kalau prosedur tertulis secara organisasi, tidak ada. Paling-paling ada arahan umum seperti hati-hati saat mengirim dokumen perusahaan internal ataupun eksternal hingga backup data secara berkala, tapi itu tidak terdokumentasi secara resmi. Jadi, ya belum ada konsistensi juga dalam penerapannya."

[Kode] : Arahan tidak terdokumentasi.

A3 : "Untuk bagian teknis, ada beberapa standar kerja internal seperti pengaturan akses dan backup rutin, tapi itu sifatnya tidak formal dan tidak terdokumentasi sebagai SOP. Semua berjalan berdasarkan kebiasaan. Kalau ada tim baru, biasanya hanya dijelaskan secara lisan."

[Kode] : SOP tidak terdokumentasi, tidak konsisten.

A4 : "Di proyek, tidak ada dokumen SOP yang secara eksplisit membahas keamanan data. Kami biasanya hanya menyimpan data proyek di NAS (Network Attached Storage) yang ada di kantor, dengan pengaturan izin akses, tapi tidak ada dokumentasi yang mengatur itu. Jadi, praktiknya bisa berbeda-beda."

[Kode] : SOP keamanan tidak ada di manajemen proyek.

A5 : "Tidak ada prosedur tertulis soal keamanan aplikasi atau penyimpanan data pengguna. Yang ada hanya kebiasaan internal seperti tidak menyimpan password di program (code). Tapi itu semua tidak tertulis dan tidak ada mekanisme audit. Hanya faktor kebiasaan."

[Kode] : Prosedur keamanan tidak terdokumentasi.

5) Pertanyaan 5

Apakah tim memiliki kemampuan cukup untuk mengelola keamanan TI?

A1 : "Secara umum, tim kami cukup kompeten dalam aspek teknis dasar. Tapi untuk isu keamanan TI secara menyeluruh terutama yang melibatkan standar atau framework tertentu saya rasa kami masih perlu banyak peningkatan. Misalnya, belum ada pelatihan khusus atau sertifikasi di bidang keamanan informasi."

[Kode] : Kekurangan pemahaman standar keamanan.

A2 : "Tim kami kuat dalam aspek operasional, tapi untuk hal-hal seperti manajemen risiko TI, audit keamanan, atau compliance dengan standar keamanan, saya rasa mereka belum punya pengalaman yang cukup. Harus ada peningkatan kompetensi lewat pelatihan atau workshop."

[Kode] : Kurang pengalaman audit & standar keamanan.

A3 : "Saya akui tim teknis punya keterampilan teknis yang baik, tapi belum cukup memahami bagaimana mengelola keamanan secara menyeluruh. Pengetahuan soal framework keamaan informasi juga masih sangat minim. Kita butuh pelatihan dan panduan formal."

[Kode] : Minim wawasan keamanan terstruktur.

A4 : "Dari pengalaman saya, tim proyek juga belum terbiasa memperhatikan aspek keamanan. Kami lebih fokus pada jadwal dan deliverables. Jadi, kemampuan keamanan TI secara proyek masih rendah. Harus ada penguatan di sisi pemahaman risiko dan pengamanan informasi proyek."

[Kode] : Rendahnya kesadaran keamanan dalam proyek.

A5 : "Untuk pengembangan aplikasi, tim punya keahlian teknis, tapi minim pemahaman tentang pengujian keamanan, atau integrasi standar keamanan alias sedikit-sedikit. Jadi kemampuan ada, tapi tidak menyentuh aspek keamanan. Kami butuh pelatihan teknis yang lebih fokus ke cybersecurity."

[Kode] : Kurangnya kompetensi teknis khusus keamanan.

6) Pertanyaan 6

Apa hambatan utama membangun sistem keamanan TI?

A1 : "Hambatan utamanya menurut saya ada pada prioritas. Keamanan TI belum menjadi agenda utama dalam strategi bisnis kami. Fokus kami masih pada ekspansi layanan dan peningkatan pendapatan. Selain itu, belum ada pemahaman yang mendalam di level manajemen tentang urgensi sistem keamanan yang terstruktur."

[Kode] : Prioritas bisnis bukan keamanan.

A2 : "Kami terbatas pada sumber daya baik dari sisi anggaran maupun SDM. Belum ada pengalokasian anggaran khusus untuk membangun sistem keamanan. Ditambah lagi, kami tidak punya staf khusus yang mengurus hal ini secara penuh, jadi seringkali hanya ditangani sambil lalu."

[Kode] : Keterbatasan sumber daya.

A3 "Dari sisi teknis, salah satu kendala utama adalah kurangnya dokumentasi, alat monitoring, dan sistem kontrol akses yang solid. Tapi hambatan terbesarnya menurut saya adalah minimnya dukungan dari manajemen. Tanpa arahan strategis dari atas, kami hanya bisa reaktif, bukan proaktif."

[Kode] : Hambatan teknis dan strategis.

A4 : "Menurut saya, budaya kerja yang ada belum mendukung keamanan sebagai bagian dari proses kerja. Misalnya, keamanan belum masuk dalam checklist proyek atau jadwal pekerjaan. Jadi, kesadaran kolektif untuk menjaga data masih rendah. Orang fokus pada delivery, bukan proteksi."

[Kode] : Budaya kerja abai keamanan.

A5 : "Kita biasa membangun aplikasi dengan fokus ke fungsi, mungkin hanya keamanan dasar. Tidak ada guideline atau framework pengembangan aman yang dijadikan acuan. Sehingga, kesadaran akan keamanan tertinggal."

[Kode] : Minim panduan pengembangan aman.

7) Pertanyaan 7

Langkah apa yang bisa diambil untuk meningkatkan keamanan TI?

A1 : "Saya pikir langkah awal adalah menyusun kebijakan keamanan yang resmi dan menjadikan isu keamanan TI sebagai bagian dari strategi perusahaan. Setelah itu, bisa dilanjutkan dengan pembentukan tim kecil yang fokus ke isu ini, lalu bertahap membangun sistem dan prosedur."

[Kode] : Kebijakan formal dan struktur organisasi.

A2 : "Yang utama adalah alokasi anggaran dan perencanaan program peningkatan kapasitas. Kalau tidak ada investasi khusus untuk keamanan, susah untuk bergerak. Perlu juga membuat roadmap untuk mengaadopsi standar keamanan, supaya kami tahu target dan tahapannya."

[Kode] : Investasi dan perencanaan strategi.

A3 : "Perlu dimulai dari pelatihan keamanan TI untuk semua staf, bukan hanya tim teknis. Lalu disusun SOP seperti manajemen akses, enkripsi data, dan audit log. Kalau bisa, perusahaan menunjuk satu orang untuk fokus di bidang keamanan ini."

[Kode] : Peningkatan kapasitas.

A4 : "Menurut saya, integrasi keamanan dalam setiap fase proyek itu penting. Misalnya dengan menambahkan review keamanan dalam proses manajemen proyek, dan adanya checklist keamanan sejak awal. Tapi harus didukung juga dengan kebijakan dari manajemen."

[Kode] : Keamanan masuk dalam manajemen proyek.

A5 : "Saya menyarankan agar rutin melakukan code review dari sisi keamanan. Selain itu, bisa mulai menerapkan CI/CD pipeline dengan integrasi pengujian keamanan otomatis. Tapi butuh pelatihan dulu untuk tim."

[Kode] : Praktik teknis pengembangan aman.

8) Pertanyaan 8

Apa harapan Anda jika perusahaan menerapkan standar seperti NIST CSF atau ISO 27001?

A1 : "Harapan saya tentu agar perusahaan menjadi lebih profesional dan memiliki sistem yang lebih kuat, terutama dalam hal kepercayaan pelanggan. Kalau kita punya standar yang jelas, maka kita bisa lebih percaya diri saat menawarkan layanan. Ini juga bisa jadi pembeda di pasar."

[Kode] : Citra perusahaan dan kepercayaan pelanggan.

A2 : "Saya berharap penerapan standar ini bisa membawa struktur kerja yang lebih baik, khususnya dalam pengelolaan risiko TI. Dengan adanya panduan dan kontrol yang jelas, operasional kami bisa lebih aman, efisien, dan tentunya siap diaudit jika dibutuhkan."

[Kode] : Struktur dan efisiensi.

A3 : "Dengan standar seperti itu, harapan saya tim teknis punya acuan kerja yang jelas dan tidak asal improvisasi. Ini penting untuk menjaga kualitas layanan dan keamanan. Kami juga bisa lebih mudah mengatur sistem akses, backup, dan insiden kalau ada framework yang diikuti."

[Kode] : Pedoman kerja dan kontrol.

A4 : "Saya ingin melihat keamanan menjadi bagian dari budaya kerja sehari-hari, bukan hanya jadi tanggung jawab tim teknis. Kalau ada standar seperti ISO atau NIST, semua bagian perusahaan jadi punya peran dan paham bagaimana menjaga keamanan data masing-masing."

[Kode] : Peran lintas divisi dalam keamanan.

A5 : "Kalau standar itu diterapkan, saya harap bisa ada guideline jelas saat membangun sistem atau aplikasi. Jadi kami tidak hanya fokus ke fitur, tapi juga ke keamanan sejak awal pengembangan. Ini akan sangat membantu dari sisi teknis dan mengurangi risiko bug keamanan."

[Kode] : Integrasi keamanan dalam proses pengembangan.

Mencari Tema Awal

Pada tahap ini dilakukan untuk mencari tema awal yang diperoleh dari pengelompokkan kode awal.

1) Tema 1 : Kesadaran keamanan belum menjadi prioritas strategis
2) Tema 2 : Ketiadaan sistem dan kebijakan keamanan formal
3) Tema 3 : Penanganan keamanan yang reaktif
4) Tema 4 : Kurangnya Kompetensi & Pelatihan Keamanan
5) Tema 5 : Hambatan organisasi: anggaran, SDM, budaya
6) Tema 6 : Harapan & rekomendasi adopsi standar keamanan

Peninjauan Tema

Berikut merupakan peninjauan tema awal yang sudah dibuat dan dapat dilihat pada Tabel 1.

Tabel 1. Peninjauan Tema.

NO	Tema	Dukungan	Keterangan
1	Kesadaran keamanan belum menjadi prioritas strategis	Semua informan, terutama A1, A2, A3	Sangat kuat, muncul di banyak pertanyaan (1, 3, 6)
2	Ketiadaan sistem dan kebijakan keamanan formal	Semua informan, sangat konsisten di Pertanyaan 2 dan 4	Sangat kuat dan spesifik
3	Penanganan keamanan yang reaktif	A3, A4, A5 secara eksplisit menyebut ini	Valid dan tidak tumpang tindih dengan Tema 2
4	Kurangnya Kompetensi & Pelatihan Keamanan	A1 hinggaA5 secara merata di Pertanyaan 5 dan 6	Tema ini berdiri sendiri dan sangat khas
5	Hambatan organisasi: anggaran, SDM, budaya	A1 hingga A5 di Pertanyaan 6	Sangat menyatu sebagai konteks penyebab lemahnya keamanan
6	Harapan & rekomendasi adopsi standar keamanan	A1 hingga A5 di Pertanyaan 7 dan 8	Tema kuat, sangat relevan dengan kerangka NIST & ISO

Penamaan dan Pendefinisian Tema

Berikut merupakan penamaan dan pendifinisan Tema Final.

1) Tema 1: Kesadaran keamanan belum menjadi prioritas strategis.
   Definisi: Meskipun para pemangku kepentingan di perusahaan menyadari pentingnya keamanan informasi, topik ini belum dimasukkan sebagai bagian dari agenda strategis. Fokus manajemen masih dominan pada aspek pengembangan bisnis, layanan, dan produk, sehingga keamanan belum dianggap krusial secara operasional.
2) Tema 2: Tidak Tersedianya Sistem dan Kebijakan Keamanan Formal.
   Definisi: Perusahaan belum memiliki dokumentasi formal, SOP, framework, maupun kebijakan tertulis mengenai keamanan informasi. Praktik keamanan masih dijalankan berdasarkan pengalaman atau kebiasaan masing-masing unit, yang menyebabkan ketidakkonsistenan dalam implementasi.
3) Tema 3: Penanganan Keamanan yang Reaktif dan Tidak Terstruktur.
   Definisi: Sebagian besar respon terhadap insiden keamanan dilakukan secara ad-hoc dan teknis, tanpa prosedur evaluasi, pelaporan, atau audit pasca kejadian. Penanganan insiden tidak terintegrasi dalam sistem manajemen risiko atau pembelajaran organisasi.
4) Tema 4: Keterbatasan Kompetensi dan Pelatihan Keamanan TI
   Definisi: Tim operasional dan teknis memiliki keterampilan dasar, namun minim pemahaman mengenai standar internasional seperti NIST atau ISO 27001. Tidak tersedia

pelatihan, panduan, atau mekanisme pengembangan kapasitas yang berfokus pada keamanan informasi.

5) Tema 5: Hambatan Organisasi terkait Anggaran, SDM, dan Budaya
   Definisi: Berbagai hambatan struktural seperti keterbatasan anggaran, kurangnya staf khusus, serta budaya kerja yang belum mengintegrasikan keamanan ke dalam proses bisnis menjadi penghalang utama dalam penguatan sistem keamanan informasi di perusahaan.
6) Tema 6: Harapan dan Rekomendasi Adopsi Standar Keamanan
   Definisi: Seluruh informan menekankan pentingnya menerapkan standar keamanan seperti NIST atau ISO untuk meningkatkan kepercayaan klien, efisiensi operasional, serta memberikan arah dan struktur kerja yang jelas dalam pengelolaan keamanan TI.

Narasi Hasil Temuan

Dari delapan pertanyaan yang telah diberikan ke seluruh informan, terdapat enam tema utama yang berhasil diidentifikasi yang menjelaskan kesiapan PT. XYZ dalam mengadopsi standar keamanan seperti NIST CSF dan ISO 27001. Tema-tema ini mengungkap dinamika persepsi, praktik, tantangan, serta harapan yang dirasakan oleh para informan di perusahaan tersebut.

Meskipun seluruh informan mengatakan bahwa keamanan informasi adalah penting, hal tersebut belum diintegrasikan ke dalam kebijakan strategis perusahaan secara nyata. Manajemen masih berfokus pada sisi bisnis sementara isu kemanan masih dianggap aspek teknis. Hal ini menggambarkan bahwa perusahaan tersebut memiliki kekurangan dalam menempatkan isu keamanan sebagai elemen fundamental dalam rencana jangka panjang.

Dari analisis yang dilakukan, dapat diketahui bahwa perusahaan belum memiliki sistem formal (SOP), kebijakan tertulis, ataupun framework mengenai keamanan system informasi yang diterapkan pada perusahaan. Saat ini, mereka hanya mengandalkan kebiasan dan pengalaman individu dari unit kerja masing-masing. Hal ini menyebabkan terjadinya ketidakkonsistenan dalam penerapan praktik keamanan di perusahaan tersebut.

Analisis juga menunjukkan, jika terjadi isu keamanan, mereka (perusahaan) akan melakukan pendekatan reaktif. Artinya, mereka hanya melakukan tindakan yang bersifat teknis dan ad-hoc. Walaupun saat ini belum pernah terjadi isu yang sangat fatal, ketiadaan sistem manajemen insiden seperti ini akan berpotensi terjadi hal-hal serupa atau bahkan yang lebih parah lagi di waktu mendatang.

Selain itu, analisis yang dilakukan berhasil mengidentifikasi bahwa tim teknis yang dimiliki oleh perusahaan tersebut belum memiliki keahlian atau kompetensi di bidang kemanan informasi. Bahkan sebatas memahami beberapa standar keamanan informasi seperti NIST CSF dan ISO 27001. Mereka mungkin mengetahui apa itu ISO, akan tetapi hanya sebatas itu saja. Ini disebabkan karena belum pernah dilakukannya pelatihan internal yang khusus membahas hal seperti ini.

Hambatan struktural juga menjadi faktor yang menyebabkan kondisi perusahaan kurang siap untuk mengadopsi standar keamanan seperti NIST CSF dan ISO 27001. Informan menyebutkan bahwa perusahaan belum pernah secara khusus menyiapkan sumber daya baik secara budget ataupun sumber daya manusia (SDM) yang memang dialokasikan khusus untuk mengurusi hal seperti ini.

Walaupun begitu, di tengah keterbatasan yang dimiliki oleh perusahaan, muncul harapan dari seluruh informan untuk mulai memahami lebih jauh mengenai isu keamanan hingga mengadopsi standar keamanan informasi itu sendiri. Mereka melihat bahwa standar keamanan nantinya bisa menjadi pedoman yang sistematis dalam membantu manajemen untuk membangun kebijakan dan struktur kerja yang jauh lebih jelas dan profesional. Hal ini pada akhirnya ditujukan untuk menjaga citra perusahaan guna meningkatkan kepercayaan pelanggan.

KESIMPULAN

PT. XYZ saat ini berada pada tahap awal dalam kesiapan keamanan sistem informasi, ditandai oleh kesadaran internal terhadap isu keamanan meskipun belum memiliki kebijakan formal, serta pendekatan penanganan yang masih reaktif dan belum terintegrasi dalam sistem manajemen risiko. Faktor penghambat utama mencakup ketiadaan dokumen kebijakan, keterbatasan sumber daya manusia dan anggaran, rendahnya kompetensi teknis, serta budaya organisasi yang belum menjadikan keamanan sebagai prioritas. Namun, terdapat pula faktor pendorong seperti kesadaran pimpinan, dorongan untuk meningkatkan profesionalisme, serta aspirasi kolektif untuk mengadopsi standar seperti NIST dan ISO 27001. Strategi yang direkomendasikan mencakup pelatihan dan sertifikasi, penyusunan kebijakan keamanan, pembentukan unit khusus keamanan, integrasi keamanan dalam desain solusi, serta penanaman budaya keamanan di seluruh organisasi. Mengingat keterbatasan penelitian ini, disarankan agar studi lanjutan melakukan pemetaan langsung terhadap kontrol standar serta mengevaluasi efektivitas strategi setelah diimplementasikan.

DAFTAR PUSTAKA

Alam, R. G. Guntur, Hidayah, Agung Kharisma, Gunawan, Gunawan, Wijaya, Ardi, & Abdullah, Dedy. (2025). *Manajemen Risiko Keamanan Informasi*. Pt. Sonpedia Publishing Indonesia.

Ambardi, Kuskridho, Widhyharto, Derajad S., Madya, Sidiq Hari, & Wibawanto, Gregorius Ragil. (2025). *Masyarakat Digital: Teknologi Kekuasaan Dan Kekuasaan Teknologi*. Ugm Press.

Chaindra, Willy, Damanik, Matthew Bona Daud, Zulfikar, Muhammad, Justin, Justin, Otto, Nathanael, Pratama, Darell Josua, Jamin, Muhammad Agung Putra, & Ningsih, Rahmi Yulia. (2024). Pengaruh Kualitas Layanan Dan Nilai Pelanggan Terhadap Loyalitas Pelanggan. *Jurnal Manajemen Dan Pemasaran Digital*, *2*(3), 212–217.

Dewanti, Paula, & Permana, Putu Adi Guna. (2025). *Keamanan Teknologi Informasi: Strategi Pemulihan, Audit, Dan Manajemen Risiko*. Deepublish.

Fadya, M., & Utama, D. N. (2025). Towards Secure Information Systems: Developing And Implementing An Information Security Evaluation Model Using Nist Csf And Cobit 2019. Tem Journal, 14(1), 182–191. Https://Doi.Org/10.18421/Tem141-17

Firmansyah, Rico Agung. (2025). *Framework Integrasi Digital Forensic Readiness Dan Information Security Management System Di Lingkungan Pemerintahan*. Universitas Islam Indonesia.

Fitriani, Sri, & Wardani, Kadek Devi Kalfika Anggria. (2025). Transaksi Aman, Bebas Khawatir: Meningkatkan Kesadaran Keamanan Kartu Kredit Melalui Poster Digital. *Abdi Moestopo: Jurnal Pengabdian Pada Masyarakat*, *8*(1), 56–64.

Hariandja, Evo Sampetua. (2025). *Pemasaran Strategik: Analisis Pelanggan, Pesaing, Pasar, Dan Lingkungan*. Penerbit Nem.

Hasibuan, Dilla Puspita, Bangun, Budianto, & Sihombing, Volvo. (2025). Pengaruh Implementasi Teknologi Informasi Terhadap Kepuasan Pelanggan Di Industri Jasa. *Jurnal Sistem Informasi, Teknik Informatika Dan Teknologi Pendidikan*, *4*(2), 60–63.

Khadafie, Muammar. (2025). Analisis Literatur: Pengaruh Keunggulan Kompetitif Terhadap Hasil Bisnis Pemasaran: Analysis Of Literature: The Influence Of Competitive Advantage On Business Marketing Outcomes. *Jurnal Tambora*, *9*(1), 38–44.

Lestari, Merryana, Puspita, Maria Entina, & Wijaya, Agustinus Fritz. (2025). Model Tata Kelola Ti Terintegrasi Untuk Keamanan Informasi Di Sektor Fintech. *Jurnal Teknologi Dan Manajemen Industri Terapan*, *4*(3), 766–776.

Lestari, Nanda Oktavia Dwi. (2025). *Rancang Bangun Sistem Informasi Pengelolaan Arsip Berbasis Web Pada Balai Besar Inseminasi Buatan Singosari*. Universitas Islam Negeri Maulana Malik Ibrahim.

Maryani, Ika. (2025). *Artificial Intelligence Dalam Pendidikan: Sebuah Bunga Rampai*. K-Media.

Maulidina, Firda, Siswanto, Heri, Padlah, Siti Nurul, Yuhanah, Nanah, Latifa, Iva, & Ramdhani, Fathul Hari. (2025). *Pemasaran Strategik Dalam Teori Dan Praktik*. Indigo Media.

Nugraha, Fajri, & Hendrik, Billy. (2025). Perbandingan Framework Cobit2019 Dan Togaf Dalam Manajemen Keamanan Informasi. *Journal Of Education Research*, *6*(2), 462–467.

Ombuh, Irvandi Waraney, Piarna, Rian, Rianty, Erfina, Ramadlan, Yogi, Juansa, Andra, & Agusdi, Yayan. (2025). *Manajemen Pemasaran: Strategi Dan Inovasi Produk Dan Jasa Untuk Pertumbuhan Bisnis Berkelanjutan*. Star Digital Publishing.

Ramadhani, Novita. (2025). Analisis Strategi Pemasaran Produk Simpanan Kspps Bmt Buana Mas Purwokerto Dalam Meningkatkan Keunggulan Kompetitif Menggunakan Metode Efas Ifas Dan Matriks Swot. *Universitas Islam Negeri Prof Kh Saifuddin Zuhri Purwokerto*.

Razikin, K., & Soewito, B. (2022). Cybersecurity Decision Support Model To Designing Information Technology Security System Based On Risk Analysis And Cybersecurity Framework. Egyptian Informatics Journal, 23(3), 383–404. Https://Doi.Org/10.1016/J.Eij.2022.03.001

Rosida, Fira, & Rusdianto, R. Yuniardi. (2025). Implementasi Crm Dalam Meningkatkan Kualitas Layanan Pada Pt Pln Icon Plus Sbu Jawa Bagian Timur Dengan Memanfaatkan Sistem Teknologi Informasi. *As-Syirkah: Islamic Economic & Financial Journal*, *4*(1), 127–133.

Sepriano, Sepriano, & Judijanto, Loso. (2025). *Mastering Service Quality, Managing Failures, Dan Delivery Service Recovery*. Pt. Sonpedia Publishing Indonesia.

Shadani, Dery, Fahrozi, Ahmad Irzi, Fahriza, Hafizh, & Alpiansyah, Rizky. (2025). Peran Teknologi Informasi Dalam Melindungi Privasi Pelanggan Terhadap Keamanan Data Dalam E-Commerce. *Jurnal Ilmu Komputer Dan Informatika| E-Issn: 3063-9026*, *1*(3), 51–54.

Sinaga, Ananda Sabrida Tora Br, Rininda, Bella Puspita, Mutmainnah, Riyadhatul, Laoli,

Victorinus, Suwarno, Try Edi, Setianda, Rizky Aldi, & Pebriana, Rina. (2025). *Technopreneureship: Strategi Perencanaan, E-Bussines, & Analisis Kelayakan Di Era Digital*. Cv. Cahaya Arsh Publisher & Printing.

Sugiyanto, Agus, Sukmayuda, Bagus Caesar, & Andiyana, Egi. (2024). *Perilaku Konsumen 5.0*. Pradina Pustaka.

Undang-Undang, Hak Cipta Dilindungi. (N.D.). *Sistem Navigasi Elektronik*.

Zander, S., & Koutsakis, P. (2024). Cybersecurity Preparedness Of Small-To-Medium Businesses: A Western Australia Study With Broader Implications. Computers & Security, 145, 104026. Https://Doi.Org/10.1016/J.Cose.2024.104026