KEAMANAN INFORMASI

AUDIT & KEPATUHAN; STUDI KASUS DAN PRESENTASI PROYEK AKHIR (ISMS SEDERHANA / ANALISIS RISIKO / SECURE CODING REPORT).

Disusun oleh:

JORDI HILMI FEBRIAN 2344390005

S1 SISTEM INFORMASI

FAKULTAS TEKNIK

UNIVERSITAS PERSADA INDONESIA YAI

JAKARTA PUSAT

2025

DAFTAR ISI

BAB XIV

AUDIT & KEPATUHAN; STUDI KASUS DAN PRESENTASI PROYEK AKHIR (ISMS SEDERHANA / ANALISIS RISIKO / SECURE CODING REPORT).

A. Pendahuluan

Keamanan informasi bukan lagi sekadar pelengkap dalam dunia teknologi modern. Ia telah menjadi fondasi utama bagi organisasi, perusahaan, maupun lembaga publik yang bergantung pada sistem digital untuk menjalankan operasi sehari-hari. Seiring meningkatnya ketergantungan terhadap teknologi informasi, risiko seperti pencurian data, serangan siber, dan kebocoran informasi pribadi juga semakin tinggi. Fenomena ini membuat kebutuhan terhadap sistem keamanan informasi yang terstruktur dan terstandar menjadi hal yang tidak dapat ditawar lagi.

Dalam konteks tersebut, peran audit dan kepatuhan (compliance) terhadap standar keamanan menjadi semakin penting. Audit bukan hanya alat pemeriksaan, melainkan mekanisme evaluasi menyeluruh yang memastikan seluruh komponen keamanan informasi berjalan sesuai kebijakan dan standar internasional. Salah satu standar yang paling banyak digunakan di dunia adalah ISO/IEC 27001:2022, yang menekankan pentingnya penerapan Information Security Management System (ISMS). ISMS berfungsi sebagai kerangka kerja untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi organisasi melalui pendekatan berbasis risiko.

Selain itu, ada pula kerangka kerja dari NIST (National Institute of Standards and Technology) seperti SP 800-53 Rev.5 dan Cybersecurity Framework (CSF) 2.0, yang memberikan panduan praktis dalam membangun sistem keamanan dan privasi yang terintegrasi. Sementara di ranah pengembangan aplikasi, organisasi seperti OWASP (Open Web Application Security Project) telah merumuskan daftar risiko keamanan paling kritis melalui OWASP Top 10, yang menjadi referensi utama bagi pengembang dan auditor perangkat lunak.

Makalah ini membahas secara mendalam penerapan audit dan kepatuhan dalam konteks keamanan informasi melalui studi kasus fiktif pada PT SecureNet, sebuah perusahaan penyedia layanan digital yang mengimplementasikan ISMS sederhana. Kajian ini juga melibatkan analisis risiko, penerapan secure coding, serta evaluasi terhadap kesesuaian praktik perusahaan dengan standar internasional.

B. Landasan teori dan konsep dasar

1. Konsep Dasar Keamanan Informasi

Keamanan informasi mencakup serangkaian kebijakan, prosedur, dan teknologi yang dirancang untuk melindungi informasi dari ancaman, baik internal maupun eksternal. Menurut William Stallings (2022), keamanan informasi bertujuan menjaga tiga aspek utama yang dikenal sebagai CIA Triad, yaitu Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan).

1. Kerahasiaan (Confidentiality) berarti hanya pihak yang berwenang yang dapat mengakses informasi tertentu.
2. Integritas (Integrity) memastikan bahwa data tidak diubah secara tidak sah atau rusak selama penyimpanan dan transmisi.
3. Ketersediaan (Availability) menjamin informasi selalu dapat diakses oleh pihak yang berhak kapan pun diperlukan.

Konsep CIA Triad menjadi fondasi bagi semua kebijakan keamanan informasi modern. Tanpa keseimbangan antara ketiganya, organisasi tidak dapat menjamin perlindungan data secara menyeluruh.

2. Information Security Management System (Isms)

ISMS merupakan pendekatan sistematis dalam mengelola keamanan informasi yang melibatkan kebijakan, prosedur, sumber daya manusia, dan teknologi. ISO/IEC 27001:2022 menjadi standar acuan global dalam penerapan ISMS. Standar ini menggunakan pendekatan Plan–Do–Check–Act (PDCA), yang mencerminkan siklus peningkatan berkelanjutan:

a. Plan: menetapkan kebijakan keamanan, sasaran, dan proses yang relevan.
b. Do: melaksanakan dan mengoperasikan kontrol keamanan.
c. Check: meninjau dan menilai kinerja sistem keamanan.
d. Act: memperbaiki dan meningkatkan efektivitas sistem secara berkelanjutan.

Dalam konteks organisasi digital, ISMS membantu memastikan bahwa pengelolaan keamanan bukan hanya tanggung jawab tim IT, tetapi juga menjadi bagian integral dari tata kelola perusahaan.

3. Audit Dan Kepatuhan Dalam Keamanan Informasi

Audit keamanan informasi merupakan proses sistematis untuk mengevaluasi apakah kontrol keamanan telah diterapkan sesuai dengan kebijakan dan standar yang berlaku. Audit bisa bersifat internal (dilakukan oleh tim perusahaan sendiri) maupun eksternal (oleh lembaga

independen). Sementara itu, kepatuhan (compliance) berarti pemenuhan terhadap regulasi dan standar tertentu yang telah ditetapkan oleh otoritas atau industri.

Audit dan kepatuhan memiliki hubungan simbiotik. Audit membantu organisasi memastikan kepatuhan terhadap standar, sementara kepatuhan menciptakan kerangka kerja untuk melaksanakan audit secara terarah.

4. Secure Coding

Secure coding merupakan praktik pengembangan perangkat lunak yang bertujuan mencegah munculnya celah keamanan sejak tahap perancangan. Berdasarkan OWASP (2021), risiko terbesar dalam aplikasi web sering kali muncul dari kelalaian dalam validasi input, manajemen sesi, dan autentikasi. Oleh karena itu, penerapan prinsip-prinsip secure coding sangat penting dalam siklus pengembangan perangkat lunak modern atau dikenal dengan istilah Secure Software Development Life Cycle (SSDLC).

5. Kerangka Risiko (Risk Framework)

Manajemen risiko dalam keamanan informasi berfokus pada identifikasi, analisis, evaluasi, dan mitigasi risiko yang dapat mengganggu aset informasi organisasi. Menurut NIST (2020), pendekatan ini melibatkan beberapa tahap utama:

a. Identifikasi aset dan ancaman.
b. Analisis kerentanan dan dampak.
c. Penilaian tingkat risiko.
d. Implementasi kontrol mitigasi.
e. Pemantauan dan evaluasi berkelanjutan.

Dengan pendekatan berbasis risiko, organisasi dapat memprioritaskan tindakan keamanan berdasarkan tingkat ancaman dan nilai aset yang dilindungi.

C. Standar dan framework internasional dalam keamanan informasi

1. Konsep Dasar Penerapan Standar

Standar keamanan informasi hadir untuk memberikan arah dan keseragaman dalam membangun sistem keamanan yang komprehensif. Tanpa adanya standar, organisasi sering kali membangun sistem keamanan secara terpisah-pisah, hanya berdasarkan intuisi atau kebutuhan sesaat. Padahal, keamanan informasi membutuhkan pendekatan yang sistematis, terukur, dan dapat diaudit.

Dalam konteks global, tiga kerangka kerja utama yang sering digunakan untuk mengelola keamanan informasi adalah ISO/IEC 27001:2022, NIST SP 800-53 Rev.5, dan NIST Cybersecurity Framework (CSF) 2.0, serta panduan teknis dari OWASP (Open Web Application Security Project) untuk keamanan aplikasi. Keempatnya bukan sekadar panduan, melainkan sistem berpikir yang membentuk pola tata kelola keamanan yang menyeluruh, mulai dari kebijakan, kontrol teknis, hingga perilaku manusia di dalam organisasi.

2. Iso/Iec 27001:2022 Sistem Manajemen Keamanan Informasi (Isms)

ISO/IEC 27001:2022 merupakan versi terbaru dari standar internasional yang menjadi pedoman utama dalam membangun dan mengelola Information Security Management System (ISMS). Edisi 2022 membawa beberapa perubahan penting dari versi sebelumnya, antara lain penyesuaian struktur dengan High-Level Structure (HLS) ISO yang terbaru, serta penambahan kontrol keamanan yang relevan dengan era digital modern seperti keamanan cloud, privasi data, dan manajemen ancaman siber.

Standar ini mengatur bagaimana organisasi harus merencanakan, melaksanakan, memantau, dan memperbaiki sistem manajemen keamanan informasi mereka. Pendekatannya berbasis siklus PDCA (Plan–Do–Check–Act), di mana setiap tahap memiliki tujuan yang jelas:

a. Plan mencakup penentuan konteks organisasi, risiko, serta kebutuhan keamanan.
b. Do mencakup penerapan kebijakan dan kontrol keamanan.
c. Check berisi kegiatan audit internal dan tinjauan manajemen.
d. Act berisi kegiatan perbaikan berkelanjutan berdasarkan hasil audit dan temuan.

Dalam ISO 27001, keamanan informasi tidak hanya dipandang sebagai tanggung jawab teknis tim IT, melainkan bagian integral dari strategi bisnis perusahaan. Penerapan standar ini memungkinkan organisasi seperti PT SecureNet untuk menunjukkan komitmen mereka terhadap keamanan data pelanggan, yang sekaligus meningkatkan kepercayaan publik dan daya saing di pasar digital.

Salah satu elemen penting dari ISO 27001 adalah Annex A, yang mencakup 93 kontrol keamanan yang dikelompokkan ke dalam empat domain besar:

a. Organizational Controls: berkaitan dengan kebijakan, tata kelola, dan peran tanggung jawab dalam organisasi.
b. People Controls: fokus pada kesadaran, pelatihan, dan perilaku karyawan.
c. Physical Controls: meliputi keamanan gedung, perangkat keras, dan fasilitas penyimpanan.
d. Technological Controls: berhubungan dengan kontrol akses, enkripsi, keamanan jaringan, dan pemantauan sistem.

Dalam studi kasus PT SecureNet, penerapan ISMS sederhana dilakukan dengan memprioritaskan Organizational Controls dan Technological Controls. Hal ini karena risiko terbesar perusahaan berada pada pengelolaan data pelanggan di sistem cloud dan aplikasi berbasis web yang mereka gunakan.

3. Nist Sp 800-53 Revision 5 Kontrol Keamanan Dan Privasi

Dokumen NIST SP 800-53 Rev.5 diterbitkan oleh National Institute of Standards and Technology (NIST) untuk membantu organisasi dalam membangun sistem keamanan dan privasi yang kuat. Edisi ini berfokus pada pendekatan berbasis hasil (outcome-based), artinya organisasi diberi fleksibilitas dalam menentukan bagaimana cara mencapai tujuan keamanan, asalkan hasilnya sesuai dengan prinsip perlindungan yang ditetapkan.

Dalam praktiknya, NIST SP 800-53 menyediakan ratusan kontrol keamanan yang terbagi dalam beberapa keluarga besar seperti:

a. Access Control (AC): pengaturan siapa yang dapat mengakses data dan sistem tertentu.
b. Audit and Accountability (AU): pencatatan dan pemantauan aktivitas sistem.
c. Incident Response (IR): prosedur tanggap insiden dan pemulihan pasca serangan.
d. Risk Assessment (RA): proses identifikasi dan penilaian risiko.
e. System and Communications Protection (SC): meliputi enkripsi, segmentasi jaringan, dan proteksi komunikasi.

Salah satu keunggulan NIST SP 800-53 adalah kemampuannya diadaptasi untuk berbagai konteks organisasi, baik pemerintahan maupun swasta. Dalam studi kasus PT SecureNet, kerangka ini digunakan untuk membangun kontrol teknis dan prosedural seperti enkripsi data pelanggan, kebijakan autentikasi ganda, serta audit log untuk setiap transaksi sistem.

Dengan mengacu pada NIST, auditor keamanan dapat melakukan verifikasi mendalam terhadap setiap aspek sistem, mulai dari pengelolaan identitas hingga pencegahan kebocoran data (Data Loss Prevention/DLP). Hal ini memastikan bahwa keamanan bukan hanya tertulis di dokumen, tetapi juga terimplementasi secara nyata di sistem operasional perusahaan.

4. Nist Cybersecurity Framework (Csf) 2.0 Kerangka Manajemen Risiko Siber

NIST Cybersecurity Framework (CSF) versi 2.0, yang dirilis tahun 2024, menjadi evolusi dari kerangka kerja sebelumnya yang berfokus pada manajemen risiko siber secara holistik. Framework ini terdiri atas lima fungsi utama yang bersifat siklus, yaitu Identify, Protect, Detect, Respond, dan Recover.

a. Identify bertujuan mengenali aset penting, konteks operasional, serta risiko yang mungkin timbul.
b. Protect memastikan perlindungan sistem dengan kebijakan dan kontrol yang memadai.
c. Detect membantu organisasi mendeteksi insiden dengan lebih cepat melalui sistem pemantauan real-time.
d. Respond menekankan pentingnya rencana respons insiden agar serangan dapat dikendalikan dengan cepat.
e. Recover mengatur langkah pemulihan dan peningkatan sistem setelah terjadi gangguan.

Dalam studi kasus PT SecureNet, fungsi Identify dilakukan dengan membuat inventaris aset digital dan mengklasifikasikan data pelanggan berdasarkan tingkat sensitivitasnya. Fungsi Protect diterapkan melalui enkripsi data dan pembatasan hak akses. Sedangkan fungsi Detect dan Respond diimplementasikan lewat sistem Security Information and Event Management (SIEM) yang memonitor aktivitas mencurigakan secara otomatis.

Pendekatan ini menunjukkan bahwa NIST CSF tidak hanya berperan dalam tahap pencegahan, tetapi juga pemulihan, yang menjadi salah satu kelemahan utama dari banyak organisasi kecil dan menengah dalam menghadapi insiden siber.

5. Owasp Top 10 (2021) Dan Prinsip Secure Coding

OWASP berfokus pada pengamanan aplikasi, terutama aplikasi berbasis web, yang kini menjadi tulang punggung bisnis digital. Daftar **OWASP Top 10 (2021)** menggambarkan sepuluh risiko terbesar yang umum ditemukan pada aplikasi modern, di antaranya Broken Access Control, Injection, Security Misconfiguration, dan Insecure Design.

Di PT SecureNet, auditor menemukan adanya celah Cross-Site Scripting (XSS) dan kurangnya sanitasi input pada beberapa modul web. Celah ini masuk ke dalam kategori Injection pada OWASP Top 10 dan dapat menyebabkan kebocoran data pengguna jika tidak ditangani dengan benar. Untuk mengatasinya, tim pengembang menerapkan secure coding guidelines dari OWASP, termasuk validasi input, penggunaan parameterized queries untuk mencegah SQL Injection, dan penerapan Content Security Policy (CSP) untuk mencegah

serangan injeksi skrip. Prinsip-prinsip tersebut tidak hanya mencegah kerentanan, tetapi juga meningkatkan kualitas perangkat lunak secara keseluruhan.

6. Integrasi Standar Iso, Nist, Dan Owasp

Ketiga kerangka ini memiliki peran yang saling melengkapi. ISO memberikan fondasi manajemen dan tata kelola, NIST memberikan panduan teknis dan kontrol yang terperinci, sedangkan OWASP fokus pada keamanan di level aplikasi. Dalam implementasinya di PT SecureNet:

a. ISO digunakan untuk membangun struktur kebijakan dan tanggung jawab keamanan informasi.
b. NIST digunakan untuk mendesain dan mengevaluasi kontrol teknis.
c. OWASP digunakan untuk memastikan keamanan kode dan aplikasi web perusahaan.

Pendekatan integratif seperti ini menciptakan sistem keamanan yang tidak hanya kuat di atas kertas, tetapi juga terbukti efektif di lapangan.

D. Metodologi audit dan manajemen risiko

1. Pendekatan Audit Keamanan Informasi

Audit keamanan di PT SecureNet dirancang untuk menilai sejauh mana kebijakan, prosedur, dan kontrol keamanan telah dijalankan sesuai dengan standar ISO/IEC 27001, NIST, dan OWASP. Audit dilakukan secara internal oleh tim keamanan perusahaan yang dibantu konsultan independen.

Pendekatan audit menggabungkan dua metode utama:

1. Audit Kepatuhan (Compliance Audit): memeriksa kesesuaian dengan kebijakan dan standar yang berlaku.
2. Audit Teknis (Technical Audit): menguji langsung efektivitas kontrol keamanan melalui simulasi serangan (penetration testing) dan analisis konfigurasi sistem.

Kedua pendekatan ini dilakukan secara bersamaan untuk memastikan hasil audit mencakup seluruh aspek, mulai dari kebijakan manajemen hingga tingkat kode aplikasi.

2. Tahapan Audit

Tahapan audit terdiri dari lima langkah utama yang saling berkesinambungan.

Tahap 1: Perencanaan Audit

Pada tahap ini, auditor menentukan ruang lingkup dan tujuan audit. Di PT SecureNet, ruang lingkupnya mencakup aplikasi web utama, server database, dan sistem autentikasi internal. Tujuan utamanya adalah menilai kepatuhan terhadap ISO 27001 serta menemukan potensi kerentanan aplikasi.

Tahap 2: Pengumpulan Data

Auditor mengumpulkan dokumen kebijakan keamanan, log sistem, serta hasil konfigurasi perangkat jaringan. Selain itu, dilakukan wawancara dengan tim IT dan manajemen untuk memahami konteks operasional dan kebijakan keamanan yang berlaku.

Tahap 3: Evaluasi dan Analisis

Hasil pengumpulan data dianalisis dengan membandingkannya terhadap kontrol pada Annex A ISO 27001 dan kontrol teknis dari NIST SP 800-53. Misalnya, kontrol AC-2 (Account Management) dari NIST digunakan untuk menilai kebijakan pengelolaan akun pengguna, sementara kontrol ISO A.9 digunakan untuk menilai efektivitas pengaturan hak akses.

Tahap 4: Pengujian Teknis (Technical Assessment)

Tim melakukan uji penetrasi terbatas terhadap sistem aplikasi PT SecureNet. Hasilnya menunjukkan dua temuan penting: pertama, sistem tidak menerapkan pembatasan percobaan login yang memadai; kedua, terdapat endpoint API yang tidak memiliki autentikasi token yang kuat. Kedua temuan ini berpotensi menyebabkan brute force attack dan unauthorized data access.

Tahap 5: Pelaporan dan Rekomendasi

Auditor menyusun laporan lengkap yang berisi temuan, risiko yang ditimbulkan, dan rekomendasi perbaikan. Misalnya, untuk mencegah brute force attack, auditor merekomendasikan penerapan mekanisme account lockout policy dan multi-factor authentication (MFA).

3. Analisis Risiko

Analisis risiko di PT SecureNet dilakukan menggunakan pendekatan kualitatif, di mana setiap ancaman dievaluasi berdasarkan dua dimensi utama: kemungkinan terjadinya (likelihood) dan dampak (impact). Kombinasi kedua faktor ini menghasilkan tingkat risiko yang dikategorikan sebagai rendah, sedang, atau tinggi.

Contoh hasil analisis:

a. Risiko kebocoran data pelanggan dikategorikan sebagai tinggi, karena berdampak besar terhadap reputasi dan kepercayaan pelanggan.
b. Risiko SQL Injection dikategorikan sedang, dengan dampak signifikan namun dapat dikendalikan melalui secure coding.
c. Risiko kegagalan sistem backup dikategorikan rendah, karena sudah ada sistem redundansi data yang baik.

Hasil analisis risiko ini menjadi dasar dalam menentukan prioritas tindakan mitigasi dan pengalokasian sumber daya keamanan.

4. Teknik Evaluasi Dan Validasi

Evaluasi dilakukan dengan mengacu pada tiga pilar utama:

a. Evaluasi Administratif: menilai kebijakan, prosedur, dan dokumentasi organisasi.
b. Evaluasi Teknis: memeriksa sistem, konfigurasi, dan kode sumber aplikasi.
c. Evaluasi Manajerial: melihat bagaimana manajemen mendukung dan mengawasi pelaksanaan kebijakan keamanan.

Untuk validasi, digunakan pendekatan triangulasi data, yaitu mengonfirmasi setiap temuan melalui lebih dari satu sumber. Misalnya, jika ditemukan kesalahan konfigurasi firewall, auditor

akan memeriksa log jaringan, mewawancarai administrator, dan menguji konektivitas sistem secara langsung.

DAFTAR PUSTAKA

ISO/IEC 27001:2022 Information Security Management Systems Requirements. International Organization for Standardization (ISO), Geneva, 2022.

NIST SP 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology (NIST), 2020.

NIST Cybersecurity Framework (CSF) 2.0, February 2024. Managing Cybersecurity Risk in Organizations. NIST Publications.

OWASP (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks. OWASP Foundation.