JURNAL INFORMATIKA RESONAT ALGORITHMUS

https://jurnal.unipi.ac.id/index.php/ALGORITHMUS
ISSN ONLINE : ----------

AUDIT KEAMANAN *INTERNET SERVICE PROVIDER* MENGGUNAKAN STANDAR ISO 27001 : 2022 (Studi Kasus : Mini ISP Namnet SMKN 6 Garut)

Anas Wahyudin[1], Errysa Subkthi[2], Chaerul Abbas[3], Andriansyah[4]

[1] Informatika, Universitas Persatuan Islam
[2] Informatika, Universitas Persatuan Islam
[3] Informatika, Universitas Persatuan Islam
[4] Informatika, Universitas Persatuan Islam
Jl.Peta. No. 154 Jawa Barat, Kota Bandung , Indonesia 40234
answay02@gmail.com, errysa@unipi.ac.id, welayash55@gmail.com, andriansyahh901@unipi.ac.id

Abstract

This study aims to conduct an information security audit of the Mini ISP Namnet at SMKN 6 Garut using the ISO/IEC 27001:2022 standard. The audit evaluates the security level based on the Confidentiality, Integrity, and Availability principles and identifies risks and vulnerabilities that could threaten service continuity. The method follows the PDCA cycle, with data gathered through observations, interviews, and documentation. The audit results reveal several critical assets such as servers, routers, authentication systems, and backbone cables with medium to high risk levels, mainly due to system vulnerabilities, lack of documentation, and weak access control. Additionally, there were mismatches between the applied controls and ISO 27001:2022 clauses. Based on the findings, recommendations include improving security controls, developing standard operating procedures (SOPs), and providing security awareness training. This study is expected to serve as a reference for other educational institutions in implementing an effective ISMS aligned with international standards.

Keyword *: Information Security Audit, ISO 27001:2022, Mini ISP, Security Risk, Information Security Management System (ISMS)*

Abstrak

Penelitian ini bertujuan untuk melakukan audit keamanan informasi pada Mini ISP Namnet SMKN 6 Garut menggunakan standar ISO/IEC 27001:2022. Audit dilakukan untuk menilai tingkat keamanan terhadap aspek *Confidentiality, Integrity,* dan *Availability*, serta mengidentifikasi risiko dan kelemahan yang dapat mengancam kelangsungan layanan. Metode yang digunakan mengikuti pendekatan siklus PDCA, dengan pengumpulan data melalui observasi, wawancara, dan dokumentasi aset. Hasil audit menunjukkan bahwa terdapat beberapa aset penting seperti *server, router*, sistem autentikasi, dan kabel *backbone* yang memiliki tingkat risiko sedang hingga tinggi, terutama akibat kerentanan sistem, kurangnya dokumentasi keamanan, serta ketiadaan pengendalian akses yang kuat. Selain itu, ditemukan pula ketidaksesuaian antara kontrol yang diterapkan dengan klausul dalam ISO 27001:2022. Berdasarkan temuan tersebut, diberikan rekomendasi perbaikan berupa peningkatan kontrol keamanan, penambahan SOP, dan pelatihan keamanan informasi. Penelitian ini diharapkan dapat menjadi acuan bagi institusi pendidikan lain dalam menerapkan SMKI secara efektif sesuai standar internasional.

Kata Kunci : Audit Keamanan Informasi, ISO 27001:2022, Mini ISP, Risiko Keamanan, Sistem Manajemen Keamanan Informasi

1. PENDAHULUAN

Di era digital, Internet Service Provider memiliki peran vital dalam penyediaan layanan internet, namun juga menghadapi ancaman siber yang semakin kompleks seperti peretasan, malware, serangan DDoS, dan pencurian data [1]. ISO 27001:2022 hadir sebagai standar internasional yang menyediakan kerangka kerja Sistem Manajemen Keamanan Informasi berbasis risiko untuk melindungi data, meningkatkan kepercayaan, serta memastikan kepatuhan terhadap regulasi [2]. Tantangan utama yang dihadapi ISP tidak hanya berasal dari kompleksitas infrastruktur jaringan

Diterima (tanggal), Direvisi (tanggal), Diterima untuk publikasi (tanggal)

dan teknologi seperti cloud dan IoT, tetapi juga dari faktor manusia yang masih lemah dalam kesadaran keamanan [3].

Mini ISP Namnet SMKN 6 Garut menghadapi berbagai permasalahan, mulai dari gangguan layanan, lemahnya prosedur keamanan yang terdokumentasi, hingga rendahnya kontrol akses. Selain itu, ancaman eksternal seperti serangan siber semakin memperbesar risiko operasional. Untuk itu, penelitian ini dilakukan dengan pendekatan kualitatif melalui wawancara, observasi, dan analisis dokumen, serta dilengkapi pendekatan kuantitatif menggunakan parameter Confidentiality, Integrity, dan Availability serta kalkulasi risiko berbasis ISO 27001:2022.

Dengan audit ini, penelitian diharapkan dapat memberikan gambaran menyeluruh mengenai kondisi keamanan informasi Mini ISP Namnet serta menawarkan rekomendasi praktis sesuai standar internasional. Implementasi yang baik akan membantu ISP mengurangi kerentanan, meningkatkan kesiapan menghadapi insiden, dan menjaga kepercayaan pelanggan [4].

2. TINJAUAN PUSTAKA

2.1 Definisi Audit

Audit merupakan proses sistematis dan objektif yang dilakukan oleh pihak independen dan kompeten untuk mengumpulkan serta mengevaluasi bukti terkait informasi atau pernyataan tertentu. Tujuannya adalah menilai kesesuaian informasi dengan standar atau kriteria yang telah ditetapkan serta menyampaikan hasilnya kepada pihak yang berkepentingan [5]. Dengan perencanaan yang matang, audit dapat mengidentifikasi kekurangan, menilai kepatuhan terhadap standar, serta memberikan dasar perbaikan proses organisasi.

Proses audit menurut Davis et al meliputi enam tahap utama:

1. Perencanaan (*Planning*): Menetapkan sasaran, ruang lingkup, dan metode audit.
2. Pekerjaan Lapangan & Dokumentasi *(Fieldwork & Documentation*): Melaksanakan audit dan mendokumentasikan bukti.
3. Identifikasi & Validasi Isu (*Issues Discovery & Validation*): Menemukan, mengklarifikasi, dan menilai permasalahan signifikan.
4. Pengembangan Solusi (*Solution Development*): Menyusun rencana perbaikan atas temuan audit.
5. Penyusunan & Penyampaian Laporan (*Report Drafting & Issuance*): Menyusun laporan resmi hasil audit.
6. Pelacakan Isu (*Issue Tracking*): Memantau tindak lanjut penyelesaian temuan audit[6].

2.1.1 Tujuan Audit

Audit bertujuan memberikan opini independen mengenai kewajaran penyajian laporan serta meningkatkan kepercayaan pihak terkait terhadap informasi yang dipublikasikan.

2.1.2 Jenis Audit

Menurut Mulyadi, audit dibagi menjadi tiga jenis:

1. Audit Laporan Keuangan: Menilai kewajaran laporan keuangan berdasarkan standar akuntansi.
2. Audit Kepatuhan: Mengevaluasi kepatuhan terhadap aturan, kebijakan, atau peraturan tertentu.
3. Audit Operasional: Menilai efisiensi, efektivitas, serta memberikan rekomendasi perbaikan proses kerja [7].

2.2 *Internet Service Provider* (ISP)

ISP adalah perusahaan atau entitas yang menyediakan layanan akses internet kepada individu maupun organisasi, termasuk pengelolaan IP, email, web hosting, dan keamanan jaringan. ISP menghubungkan pengguna akhir ke infrastruktur internet global dan berperan sebagai jembatan ke server dan layanan di seluruh dunia. ISP terbagi menjadi Tier-1 (*backbone global*), Tier-2 (membeli bandwidth dari Tier-1), dan Tier-3 (akses pengguna akhir) [8].

2.3 Sistem Informasi

Sistem informasi adalah gabungan teknologi, manusia, dan proses untuk mengelola, menyimpan, dan mendistribusikan informasi [9]. Komponen utamanya: *hardware, software, database*, jaringan, manusia, dan proses. Teknologi modern termasuk *cloud computing* mendukung akses data *real-time* dan fleksibilitas operasional.

2.4 Manajemen Keamanan Informasi

Manajemen keamanan informasi melindungi kerahasiaan, integritas, dan ketersediaan informasi melalui kebijakan, prosedur, dan pengelolaan risiko [10]. Prinsip utama dikenal sebagai CIA Triad:

A. *Confidentiality*: akses terbatas pada pihak berwenang.
B. *Integrity*: memastikan informasi akurat dan utuh.
C. *Availability*: informasi dapat diakses saat dibutuhkan.

2.5 Jaringan Komputer

Jaringan komputer adalah kumpulan perangkat yang saling terhubung untuk pertukaran data dan sumber daya [11]. Fungsi utama: komunikasi, berbagi sumber daya, dan akses informasi *real-time*. Klasifikasi: LAN, MAN, WAN.

2.6 *Two-Factor Authentication* (2FA)

2FA adalah metode keamanan yang memerlukan dua bentuk verifikasi sebelum akses diberikan, termasuk:

A. Sesuatu yang diketahui pengguna (password, PIN).
B. Sesuatu yang dimiliki (token, ponsel).
C. Sesuatu yang melekat secara biometrik (sidik jari, wajah).
D. Manfaat: lapisan keamanan ekstra, mencegah akses tidak sah.
E. Tantangan: perangkat kedua hilang, SIM-swapping, kesulitan akses.

2.7 Sistem Manajemen Keamanan Informasi

SMKI atau ISMS sesuai ISO 27001:2022 bertujuan melindungi kerahasiaan, integritas, dan ketersediaan informasi. Fokusnya pada pengurangan risiko dan kelangsungan bisnis [12].

2.8 ISO 27001:2022

Standar internasional untuk SMKI, berbasis manajemen risiko, meliputi 10 klausul dan 93 kontrol keamanan. Revisi 2022 menekankan:

A. Annex A selaras ISO 27002:2022.
B. Pendekatan fleksibel dalam manajemen risiko.
C. Integrasi keamanan siber.

Klausul utama: konteks organisasi, kepemimpinan, perencanaan, dukungan, operasi, evaluasi kinerja, perbaikan.

2.9 Metode PDCA (*Plan-Do-Check-Act*)

PDCA digunakan untuk penerapan SMKI secara berkelanjutan:

A. *Plan*: perencanaan kontrol, kebijakan, prosedur.
B. *Do*: implementasi kontrol dan kebijakan.
C. *Check*: audit internal dan evaluasi efektivitas SMKI.
D. *Act*: perbaikan dan tindakan pencegahan berdasarkan temuan.

2.10 Penilaian Risiko

Penilaian risiko (risk assessment) mengidentifikasi ancaman dan kelemahan aset untuk menentukan prioritas penanganan.

Langkah utama:

A. Identifikasi aset: nilai aset ditentukan berdasarkan CIA Triad.
B. Identifikasi ancaman dan kelemahan: ancaman fisik, manusia, alam; kelemahan sistem, perangkat keras/software, pengguna.
C. Evaluasi risiko: menghitung Nilai Risiko = NA × BIA × NT, lalu memutuskan strategi mitigasi.[13]

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan gabungan kualitatif dan kuantitatif. Data diperoleh melalui observasi lapangan terhadap infrastruktur Mini ISP, wawancara dengan kepala dan staf operasional ISP, serta dokumentasi aset dan prosedur yang ada. Analisis dilakukan dengan mengacu pada siklus PDCA, yaitu :

1. *Plan* : Identifikasi aset utama, pendukung, dan kritis; analisis ancaman dan kelemahan; serta penilaian risiko berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA).
2. *Do* : Pelaksanaan audit teknis, termasuk pengukuran tingkat risiko dan kesesuaian dengan klausul ISO/IEC 27001:2022.
3. *Check* : Evaluasi kesenjangan (*gap analysis*) antara kondisi aktual dengan standar ISO.
4. *Act* : Penyusunan rekomendasi perbaikan, pembuatan SOP, dan strategi mitigasi risiko.

TAHAP AWAL	HASIL
Studi Literartur	Landasan Teori
Identifikasi dan Analisa Masalah 1. Observasi 2. Wawancara 3. Kuesioner	Visi, Misi, tupoksi dan Dokumen permasalahan yang teridentifikasi

TAHAP PENGEMBANGAN		HASIL
Plan	Menentukan Ruang Lingkup SMKI	Ruang Lingkup yang di Setujui
	Melakukan Identifikasi Aset	Dokumen Daftar Aset
Do	Analisis Penilaian Aset	Dokumen Penilaian Aset
	Analisis Dampak dan Risiko Aset	Penilaian Prioritas Dampak dan Risiko
Check	Memilih Objek Kontrol Keamanan Sistem Informasi	Daftar Kontrol Keamanan yang di pilih
Act	Penelusuran Bukti	Laporan Bukti Penerapan Kontrol
	Pemberian Rekomendasi	Laporan Rekomendasi Perbaikan
	Penyusunan SOP	SOP yang telah disesuaikan dengan rekomendasi perbaikan

TAHAP AKHIR	HASIL
Hasil Analisa	Informasi hasil dari penelitian
Kesimpulan dan Saran	Ringkasan dari hasil temuan dan pemberian rekomendasi untuk pengembangan kebijakan prosedur yang ada

Gambar 3.1 Kerangka Penelitian

4. HASIL DAN PEMBAHASAN

4.1 Identifikasi Aset

Berdasarkan hasil audit, teridentifikasi tiga kategori aset, yaitu:

1. Aset Utama
   A. Server digunakan sebagai pusat layanan penyimpanan data dan autentikasi pengguna. Server merupakan jantung operasional ISP, sehingga kerusakan perangkat atau serangan terhadap server dapat menyebabkan layanan berhenti total.
   B. Router berfungsi menghubungkan jaringan internal dengan internet. Router menjadi target utama serangan berupa DDoS maupun eksploitasi firmware.
   C. Sistem Autentikasi mencakup username/password siswa dan staf. Sistem ini menentukan validitas akses pengguna, sehingga apabila terjadi kebocoran kredensial maka layanan berpotensi disalahgunakan.
2. Aset Pendukung
   A. PC Unit digunakan staf untuk administrasi jaringan. Kerentanannya terletak pada kemungkinan infeksi malware yang dapat mengakses konfigurasi jaringan.
   B. Switch menghubungkan perangkat dalam jaringan lokal. Kegagalan switch dapat menimbulkan

bottleneck atau bahkan memutus akses ke layanan internet.

C. Access Point menyediakan akses nirkabel bagi pengguna. Lemahnya konfigurasi keamanan (misalnya penggunaan WPA lama) dapat membuka peluang serangan sniffing.

3. Aset Kritis

A. Kabel Backbone sebagai jalur utama distribusi jaringan. Kerusakan fisik kabel dapat menghentikan layanan secara menyeluruh.

B. Firewall menjadi pertahanan pertama terhadap serangan eksternal. Konfigurasi yang tidak diperbarui secara rutin meningkatkan risiko bypass keamanan.

C. Data Konfigurasi berisi pengaturan server, router, dan switch. Jika data ini hilang atau rusak, pemulihan layanan akan memakan waktu lama.

4.2 Analisis Risiko Berdasarkan CIA

Jika dilihat berdasarkan prinsip *Confidentiality*, *Integrity*, dan *Availability*, maka terdapat sejumlah temuan yang signifikan. Dari sisi kerahasiaan (*confidentiality*), sistem autentikasi yang masih berbasis username dan password dinilai belum memadai karena rentan terhadap serangan brute force. Selain itu, data kredensial belum sepenuhnya dienkripsi, sehingga membuka peluang adanya penyalahgunaan akses. Kelemahan terbesar adalah belum adanya penerapan multi-factor authentication (MFA) yang dapat memperkuat lapisan keamanan. Dari sisi integritas (*integrity*), risiko utama terletak pada kemungkinan perubahan atau hilangnya data konfigurasi oleh pihak yang tidak berwenang. Tidak adanya mekanisme verifikasi integritas, seperti checksum, memperbesar peluang terjadinya inkonsistensi. *Update* perangkat lunak yang tidak terkelola dengan baik juga menjadi celah yang dapat menimbulkan masalah pada konsistensi sistem. Sementara itu, dari sisi ketersediaan (*availability*), sistem masih sangat rentan terhadap kegagalan layanan. Gangguan pada server atau *backbone* dapat menghentikan akses internet secara total karena tidak terdapat server cadangan maupun jalur alternatif. Sistem monitoring lalu lintas jaringan juga belum berjalan optimal, sehingga sulit mendeteksi dini jika terjadi serangan DDoS atau *overload bandwidth*.

No	Nama Aset	Nilai Aset	Nilai BIA	Nilai Ancaman	Nilai Risiko	Level Risiko
1	Koneksi Internet	6	100	0.4	240	*High*
2	Sistem Autentikasi (*Hotspot, Radius*, *User Manager*)	7	80	0.17	95.2	*High*
3	*Bandwidth*	8	70	0.3	168	*High*
4	Akun admin utama	5	100	0.22	110	*High*
5	*Portal login captive*	4	80	0.13	41.6	*Medium*
6	*Router*	8	80	0.23	147.2	*High*
7	*Switch*	8	80	0.18	115.2	*High*
8	*Server* (untuk *DHCP, DNS, Proxy*, atau Autentikasi)	10	85	0.36	306	*High*
9	*PC Unit*	7	70	0.28	137.2	*High*
10	*Access Point*	6	60	0.24	86.4	*High*
11	Sistem monitoring jaringan	6	60	0.1	36	*Medium*
12	*Modem* Utama	8	100	0.2	160	*High*
13	*Power suply*	9	100	0.22	198	*High*
14	Kabel *backbone*	9	95	0.25	213.75	*High*
15	*Firewall*	8	85	0.22	149.6	*High*
16	Data konfigurasi	10	100	0.2	200	*High*

Tabel 4.1 Hasil Nilai Analisis Risiko

4.3 *Gap Analysis* terhadap ISO 27001:2022

Apabila dibandingkan dengan standar ISO/IEC 27001:2022, hasil audit ini menunjukkan adanya kesenjangan pada beberapa klausul penting. Pada klausul manajemen insiden, belum terdapat prosedur resmi untuk mendeteksi, melaporkan, maupun merespons insiden keamanan. Hal ini menyebabkan staf tidak memiliki panduan baku ketika menghadapi serangan siber. Pada klausul keberlanjutan layanan, tidak tersedia dokumen *Disaster Recovery Plan* (DRP) sehingga proses pemulihan layanan masih bergantung pada upaya manual teknisi. Klausul kontrol akses juga belum terpenuhi sepenuhnya karena masih menggunakan mekanisme login standar tanpa MFA dan tanpa kebijakan pergantian kata sandi secara berkala. Selain itu, klausul monitoring dan logging juga belum diimplementasikan secara optimal. Tidak ada pencatatan aktivitas jaringan yang komprehensif, sehingga percobaan akses ilegal sulit ditelusuri secara detail.

4.4 Rekomendasi Perbaikan

Berdasarkan temuan tersebut, terdapat sejumlah rekomendasi perbaikan yang perlu diprioritaskan. Pertama, peningkatan kontrol akses melalui penerapan multi-factor authentication, kebijakan pergantian password secara berkala, serta enkripsi database kredensial. Kedua, penguatan infrastruktur teknis dengan menyediakan server cadangan, jalur backbone alternatif, serta penambahan sistem *intrusion detection system* (IDS) dan *firewall* yang

selalu diperbarui. Ketiga, pengembangan sistem monitoring dan logging yang mampu merekam aktivitas jaringan secara real-time, dengan catatan aktivitas minimal disimpan selama 90 hari untuk kebutuhan audit. Keempat, penyusunan prosedur standar operasional terkait penanganan insiden, manajemen risiko, dan pemeliharaan jaringan. Hal ini penting agar staf memiliki pedoman yang jelas dalam menghadapi potensi serangan. Terakhir, peningkatan kapasitas sumber daya manusia melalui pelatihan keamanan informasi secara berkala serta simulasi penanganan insiden yang dilakukan minimal satu kali setiap tahun.

Dengan penerapan rekomendasi tersebut, diharapkan Mini ISP Namnet dapat memperkuat aspek kerahasiaan, integritas, dan ketersediaan sistem, sekaligus memperkecil kesenjangan dengan standar internasional ISO 27001:2022. Secara keseluruhan, hasil audit menegaskan bahwa penerapan keamanan informasi di Mini ISP masih berada pada tahap awal pengembangan, namun memiliki peluang besar untuk ditingkatkan melalui implementasi kontrol yang lebih formal, terstruktur, dan berkelanjutan.

5. KESIMPULAN

5.1 Kesimpulan

Berdasarkan audit berbasis PDCA ISO 27001:2022, tingkat kematangan SMKI Mini ISP Namnet SMKN 6 Garut masih berada pada fase awal. Perencanaan (*Plan*) dan sebagian operasional (*Do*) sudah diterapkan, namun evaluasi (*Check*) dan perbaikan berkelanjutan (*Act*) belum optimal.

Aset kritis seperti modem, router, server, kabel backbone, dan data konfigurasi memiliki risiko tinggi jika terjadi insiden. Aspek teknis cukup berjalan, tetapi prosedur dan pengendalian administratif masih lemah, misalnya: belum ada autentikasi ganda, dokumentasi konfigurasi belum rapi, sistem pelaporan insiden minim, dan backup data manual.

Kontrol keamanan Annex A sebagian besar belum terlaksana, sehingga perlu SOP, kebijakan formal, manajemen risiko, dan pelatihan SDM. Secara keseluruhan, Mini ISP Namnet memiliki potensi, namun perlu penguatan sistem keamanan untuk mencapai layanan yang lebih andal, aman, dan sesuai standar internasional.

5.2 Saran

A. Dokumentasi dan perencanaan SMKI: Susun SOP, kebijakan, dan panduan teknis untuk standar kerja harian.
B. Penerapan kontrol dasar: Gunakan autentikasi ganda, backup otomatis, dan sistem pelaporan insiden.
C. Budaya sadar keamanan: Berikan pelatihan dan edukasi risiko bagi seluruh SDM internal.
D. Manajemen risiko: Prioritaskan risiko dan susun rencana penanganannya agar siap menghadapi insiden.
E. Evaluasi rutin: Lakukan audit internal berkala untuk memastikan kontrol berjalan efektif dan memperbaiki kekurangan secara berkelanjutan.

Jika ingin berkembang lebih luas, standarisasi keamanan sesuai ISO 27001 akan menjadi modal utama untuk membangun kepercayaan pengguna.

DAFTAR PUSTAKA

[1] Kaspersky, I. C. S. (2021). *Threat landscape for industrial automation systems. Statistics for H*, *1*, 2021.

[2] ISO/IEC, *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection*. International Organization for Standardization, 2022.

[3] Brown, R., & Lee, R. M. (2021). 2021 sans cyber threat intelligence (cti) survey. In *Tech. Rep*. SANS Institute.

[4] Verizon, Data Breach Investigations Report 2022. Verizon Enterprise, 2022.

[5] Arens, A. A., Elder, R. J., & Beasley, M. S. (2017). Auditing and assurance services: An integrated approach (16th ed.). Pearson Education.

[6] Davis, C., Schiller, M., & Wheeler, K. (2011). *IT Auditing: Using Controls to Protect Information Assets*. McGraw-Hill.

[7] Mulyadi, R. (2017). Pengaruh karakteristik komite audit dan kualitas audit terhadap profitabilitas Perusahaan. *Jurnal Akuntansi*, *4*(2).

[8] Forouzan, B. A. (2012). *Data Communications and Networking Global Edition 5e*. McGraw Hill.

[9] Loudon, M. (2016). A platform studies approach to the role of technology in the ICTD ecosystem: The SMS in m4d interventions. *Information Technology for Development*, *22*(sup1), 7-25.

[10] ISO/IEC. (2013). Informasi Berbasis SNI ISO */ Iec.* 1–40.

[11] Yudianto, M. J. N., & Noor, J. (2014). Jaringan komputer dan Pengertiannya. *Ilmukomputer. Com*, *1*, 1-10.

[12] Basyarahil, F. A., Astuti, H. M., & Hidayanto, C. (2017). *Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya*. *6*(1).

[13] Apriene Shalsabila. (2024). Audit Keamanan Sistem Informasi Pada Dinas Komunikasi Dan Informatika Kota Mojokerto Berdasarkan Standar Iso 27001:2013. Surabaya: Universitas Dinamika.