Audit Keamanan Website Layanan Publik Mengacu pada ISO/IEC 27001: Studi Kasus Dugaan Penyalahgunaan Situs PeduliLindungi

M. Saleh[1], Muhammad Dede Fitriawan[2]
[12]Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Islam Indragiri,
Email: msaleh0205@gmail.com[1], [5]dedeacc1122@gmail.com[2]

ABSTRAK

Meningkatnya ancaman siber terhadap situs layanan publik di Indonesia menimbulkan kekhawatiran terhadap keamanan informasi, khususnya pasca-operasional sistem digital seperti situs *PeduliLindungi* yang dialihkan ke SATUSEHAT. Penelitian ini bertujuan untuk mengevaluasi tingkat kepatuhan keamanan informasi situs tersebut terhadap standar ISO/IEC 27001:2013, serta mengidentifikasi risiko yang timbul akibat kelalaian pengelolaan keamanan pasca-transisi. Metode yang digunakan adalah penelitian kuantitatif deskriptif dengan desain studi kasus, menggunakan 10 kontrol utama ISO/IEC 27001 sebagai sampel audit. Data diperoleh melalui observasi, analisis forensik digital, serta pemindaian menggunakan tools keamanan seperti SSL Labs dan VirusTotal. Teknik analisis dilakukan secara deskriptif kuantitatif melalui skoring kontrol (0–4) dan penilaian dampak risiko. Hasil penelitian menunjukkan bahwa situs *PeduliLindungi* memiliki skor rata-rata 0,74 dari 4, dengan tingkat kepatuhan hanya 17,5%, dan lima dari sepuluh kontrol memperoleh skor nol. Temuan ini mendukung hipotesis bahwa situs tidak memenuhi standar minimum keamanan informasi, terutama pada aspek komunikasi data (A.13) dan perlindungan privasi (A.18). Penelitian ini memberikan kontribusi teoretis dengan memperluas cakupan audit keamanan pada domain digital nonaktif, serta memiliki implikasi praktis bagi pemerintah untuk memperkuat pengawasan dan manajemen risiko terhadap domain layanan publik yang telah dinonaktifkan.

Kata Kunci: Keamanan Informasi, ISO/IEC 27001, Situs Layanan Publik, Audit Keamanan, Pedulilindungi.

ABSTRACT

The increasing cyber threats to public service sites in Indonesia have raised concerns about information security, especially after the operation of digital systems such as the PeduliLindungi site which was transferred to SATUSEHAT. This study aims to evaluate the level of information security compliance of the site with the ISO/IEC 27001:2013 standard, and to identify risks arising from negligence in post-transition security management. The method used is descriptive quantitative research with a case study design, using 10 key ISO/IEC 27001 controls as audit samples. Data were obtained through observation, digital forensic analysis, and scanning using security tools such as SSL Labs and VirusTotal. The analysis technique was carried out descriptively quantitatively through control scoring (0–4) and risk impact assessment. The results showed that the PeduliLindungi site had an average score of 0.74 out of 4, with a compliance rate of only 17.5%, and five out of ten controls scored zero. These findings support the hypothesis that the site does not meet minimum information security standards, especially in the aspects of data communication (A.13) and privacy protection (A.18). This research provides theoretical contributions by expanding the scope of security audits to inactive digital domains, and has practical implications for governments to strengthen supervision and risk management of inactive public service domains.

Keywords: Information Security, ISO/IEC 27001, Public Service Site, Security Audit, Pedulilindungi.

1 PENDAHULUAN

Dalam era transformasi digital yang berkembang pesat, keberadaan website sebagai sarana layanan publik menjadi sangat vital bagi pemerintah dalam menyelenggarakan pelayanan kepada masyarakat. Di Indonesia, digitalisasi layanan publik meningkat secara signifikan, terutama sejak

pandemi COVID-19, di mana aplikasi seperti PeduliLindungi menjadi platform utama dalam pelacakan dan pengelolaan data kesehatan masyarakat. Namun, setelah masa pandemi mereda dan platform tersebut mengalami transformasi menjadi SATUSEHAT, muncul berbagai isu terkait keamanan siber, termasuk dugaan penyalahgunaan domain PeduliLindungi menjadi situs judi daring. Fenomena ini menyoroti pentingnya keberlanjutan pengelolaan keamanan informasi terhadap situs layanan publik yang sudah tidak aktif namun tetap memiliki risiko tinggi bila tidak diawasi secara tepat.

Keamanan informasi menjadi isu strategis global yang semakin relevan seiring meningkatnya jumlah serangan siber. Menurut data dari Badan Siber dan Sandi Negara (BSSN), terjadi lebih dari 361 juta insiden siber di Indonesia pada tahun 2023, meningkat drastis dibandingkan tahun sebelumnya. Mayoritas serangan tersebut menargetkan sektor publik, termasuk lembaga kesehatan dan pemerintahan, yang seringkali belum memiliki sistem keamanan yang memadai. Salah satu penyebab utamanya adalah belum optimalnya penerapan standar keamanan informasi seperti ISO/IEC 27001, yang dirancang sebagai kerangka kerja sistem manajemen keamanan informasi (SMKI) secara internasional. Standar ini memberikan pedoman menyeluruh dalam menetapkan, mengimplementasikan, memelihara, dan meningkatkan keamanan informasi dalam suatu organisasi, termasuk sektor publik. Sejumlah penelitian sebelumnya telah mengidentifikasi lemahnya implementasi keamanan informasi di institusi publik Indonesia. Misalnya, studi oleh Meitarice et al. (2024) menunjukkan bahwa banyak perguruan tinggi negeri di Indonesia belum memenuhi persyaratan minimum ISO/IEC 27001. Penelitian lain oleh Yuliana dan Hasibuan (2022) juga menemukan bahwa kerangka kerja tata kelola keamanan TI di lembaga pemerintahan masih terfragmentasi, dengan tingkat kepatuhan yang rendah terhadap standar internasional. Meskipun beberapa instansi telah mengadopsi kerangka ISO, penerapannya sering tidak menyeluruh, terbatas pada aspek teknis tanpa memperhatikan kebijakan, manajemen risiko, dan kesadaran keamanan dari para pemangku kepentingan. Namun, sangat sedikit studi yang mengkaji secara spesifik tentang keamanan situs layanan publik yang telah beralih fungsi atau non-aktif namun masih memiliki jejak digital aktif seperti PeduliLindungi. Belum ada audit sistematis yang mengevaluasi potensi kerentanan keamanan domain semacam ini dalam konteks pasca-operasional. Padahal, keberadaan domain publik yang tidak dijaga dapat menjadi titik masuk bagi peretas untuk melakukan manipulasi DNS, spoofing, hingga pengalihan situs ke aktivitas ilegal seperti perjudian online. Ketiadaan kajian kuantitatif yang mengukur tingkat kepatuhan domain publik terhadap ISO/IEC 27001 menunjukkan adanya kesenjangan riset yang perlu segera diisi.

Penelitian ini bertujuan untuk melakukan audit keamanan website layanan publik menggunakan kerangka ISO/IEC 27001 dengan fokus pada studi kasus situs PeduliLindungi. Audit ini menggunakan pendekatan kuantitatif untuk mengukur sejauh mana elemen-elemen dalam ISO/IEC 27001 telah atau tidak diterapkan, serta mengidentifikasi potensi risiko yang muncul akibat kelemahan pengelolaan keamanan informasi. Dengan menggunakan kuesioner berbasis kontrol ISO, analisis risiko, dan data teknis situs yang tersedia secara publik, penelitian ini diharapkan dapat memberikan gambaran objektif terhadap kondisi keamanan situs layanan publik yang sudah tidak aktif namun masih rentan terhadap ancaman siber. Kontribusi penelitian ini bersifat teoretis dan praktis. Secara teoretis, studi ini memperkaya khazanah literatur mengenai penerapan ISO/IEC 27001 dalam konteks digitalisasi layanan publik, terutama pada fase pasca-operasional situs. Secara praktis, hasil temuan ini dapat menjadi acuan bagi pembuat kebijakan, instansi pemerintah, dan pengelola sistem digital nasional untuk menyusun strategi perlindungan terhadap domain publik, termasuk pembaruan kebijakan penghapusan domain atau pengalihan aset digital yang lebih aman. Temuan ini juga dapat digunakan oleh BSSN dan Kemenkominfo untuk menilai efektivitas pengawasan terhadap domain publik dan memperkuat tata kelola keamanan siber nasional secara menyeluruh.

2 METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian deskriptif evaluatif yang bertujuan untuk mengaudit dan mengevaluasi tingkat kepatuhan keamanan informasi pada website layanan publik berdasarkan standar ISO/IEC 27001:2013, dengan studi kasus pada situs PeduliLindungi. Desain penelitian yang digunakan adalah studi kasus terfokus pada satu unit analisis, yaitu domain PeduliLindungi, yang ditelusuri melalui metode forensik digital dan audit sistem informasi. Populasi dalam penelitian ini mencakup elemen-elemen kontrol keamanan informasi dalam ISO/IEC 27001, khususnya domain kontrol teknis (A.9, A.12, A.13), dengan sampel berupa 25 indikator audit yang dipilih secara purposive karena paling relevan terhadap sistem keamanan situs web. Teknik pengambilan sampel bersifat purposive sampling, berdasarkan relevansi indikator terhadap aspek keamanan teknis situs publik. Instrumen yang digunakan berupa checklist audit dan lembar evaluasi maturity level dengan skala penilaian 0–4 untuk menilai tingkat penerapan masing-masing kontrol keamanan. Data dikumpulkan melalui observasi dokumentasi teknis, pemindaian DNS/domain menggunakan tools keamanan digital (WHOIS, SSL Labs, Shodan), serta analisis sekunder dari laporan dan kebijakan keamanan pemerintah. Teknik analisis data menggunakan analisis deskriptif kuantitatif, dengan penghitungan skor rata-rata tiap kontrol serta visualisasi dalam bentuk diagram radar untuk menggambarkan profil keamanan situs secara menyeluruh.

3 HASIL DAN PEMBAHASAN

Tabel 1. Tabel Ceklist Audit

No	Kode Kontrol	Deskripsi Kontrol	Hasil Audit	Skor	Bukti Audit	Kategori Kepatuhan	Level Dampak
1	A.9.1.1	Kebijakan kontrol akses	Tidak ada kebijakan akses dipublikasikan	1	Tidak ditemukan halaman kebijakan akses	Sangat Rendah	Tinggi
2	A.9.2.2	Pencabutan hak akses pengguna lama	Tidak ada proses pencabutan akun	0	Tidak ada pengumuman migrasi akun	Tidak Patuh	Tinggi
3	A.9.4.2	Kontrol akses ke fungsi sistem	Fungsi login admin tertutup	3	Endpoint admin tidak terbuka	Sedang	Sedang
4	A.12.1.2	Kontrol perubahan sistem	Tidak terdokumentasi proses transisi domain	1	Tidak ada changelog domain	Sangat Rendah	Sedang
5	A.12.2.1	Proteksi terhadap malware	Ditemukan malware ringan	1	Scan VirusTotal menandai berbahaya	Sangat Rendah	Tinggi
6	A.12.4.1	Monitoring log sistem	Tidak tersedia log sistem	0	Tidak ada informasi log	Tidak Patuh	Tinggi
7	A.12.6.1	Manajemen kerentanan teknis	Tidak ada pemindaian berkala	1	Tidak ada IDS/WAF aktif	Sangat Rendah	Tinggi

8	A.13.1.1	Pengamanan komunikasi (HTTPS)	SSL tidak aktif	0	Scan SSL Labs tidak valid	Tidak Patuh	Kritis
9	A.13.2.3	Pemantauan trafik komunikasi	Tidak ada sistem pemantauan	0	Tidak ada firewall/IDS aktif	Tidak Patuh	Tinggi
10	A.18.1.4	Perlindungan data pribadi	Tidak ada kebijakan privasi	0	Tidak ada kebijakan privasi aktif	Tidak Patuh	Kritis

Selain tingkat kepatuhan yang sangat rendah, audit ini juga menunjukkan bahwa sebagian besar kontrol yang tidak dipenuhi memiliki tingkat dampak tinggi hingga kritis terhadap keberlangsungan keamanan informasi. Dua kontrol dengan dampak kritis, yakni pengamanan komunikasi (HTTPS) dan perlindungan data pribadi, berpotensi menyebabkan kebocoran informasi sensitif, pelanggaran hukum (UU PDP), serta hilangnya kepercayaan publik. Dampak tinggi juga terlihat pada kontrol pencatatan log, manajemen kerentanan, dan deteksi malware, yang jika tidak dijalankan, membuat situs sangat rentan terhadap penyusupan dan manipulasi ilegal.

Audit keamanan informasi terhadap situs layanan publik PeduliLindungi dilakukan dengan menggunakan instrumen evaluasi berbasis kontrol dalam standar ISO/IEC 27001:2013. Sebanyak 10 kontrol utama dipilih dari empat domain kunci, yaitu: A.9 (Kontrol Akses), A.12 (Keamanan Operasional), A.13 (Keamanan Komunikasi), dan A.18 (Kepatuhan terhadap Regulasi Perlindungan Data). Masing-masing kontrol diberi skor antara 0 sampai 4 berdasarkan kondisi aktual di lapangan, yang dievaluasi melalui observasi sistem, dokumentasi terbuka, serta hasil pemindaian menggunakan alat bantu seperti VirusTotal, SSL Labs, dan pengecekan arsip situs (Internet Archive dan WHOIS).

Hasil audit menunjukkan bahwa dari total skor maksimal 40, situs PeduliLindungi hanya memperoleh skor 7, atau rata-rata 0,74 per kontrol, yang termasuk dalam kategori "Belum Memadai" (Initial) menurut tingkat kematangan sistem manajemen keamanan informasi. Sebagian besar kontrol tidak diterapkan secara aktif, dan bahkan 5 dari 10 kontrol mendapat skor 0, menandakan ketidakpatuhan absolut. Hanya satu kontrol, yaitu kontrol akses ke fungsi sistem (A.9.4.2), yang memperoleh skor relatif tinggi (3), karena dashboard admin situs tidak lagi aktif secara public. Tabel checklist menunjukkan bahwa dua domain paling kritis adalah A.13 dan A.18, yang menyangkut keamanan komunikasi data dan perlindungan data pribadi, karena kedua domain ini memperoleh skor 0 secara menyeluruh. Ini mengindikasikan bahwa tidak ada implementasi teknis maupun kebijakan minimum yang melindungi komunikasi dan privasi pengguna setelah situs tidak lagi aktif.

Tabel 2. Tabel Saran Perbaikan

No	Kode Kontrol	Uraian Temuan	Bukti Audit	Dampak	Saran Tindakan Perbaikan
1	A.9.1.1	Tidak ada kebijakan kontrol akses pengguna yang terdokumentasi.	Tidak ditemukan halaman atau dokumen terkait.	Akses tidak terkontrol, potensi penyalahgunaan.	Susun dan publikasikan kebijakan akses pengguna untuk domain dan sistem yang tidak aktif.

2	A.9.2.2	Akun lama tidak dinonaktifkan atau dimigrasikan.	Tidak ada informasi pemindahan atau penghapusan akun.	Akses ilegal dari akun tidak sah (akun zombie).	Lakukan audit dan penutupan akun pengguna, serta umumkan status akun pasca-migrasi.
3	A.9.4.2	Dashboard admin tertutup namun tidak terdokumentasi.	Tidak ditemukan endpoint login, tanpa dokumentasi.	Ketidakpastian status backend.	Dokumentasikan dan umumkan status backend situs yang telah dimigrasikan.
4	A.12.1.2	Migrasi situs tidak disertai dokumentasi perubahan sistem.	Tidak ada changelog atau rilis resmi.	Potensi kehilangan kendali atau jejak sistem.	Rilis changelog publik dan dokumentasi pemindahan domain.
5	A.12.2.1	Malware terdeteksi pada domain.	Scan VirusTotal: 6 engine menandai berbahaya.	Risiko penyalahgunaan domain untuk judi/phishing.	Nonaktifkan atau ambil alih DNS domain. Lakukan pembersihan dan verifikasi ulang.
6	A.12.4.1	Tidak tersedia sistem logging.	Tidak ada indikator log sistem.	Tidak ada jejak audit aktivitas situs.	Terapkan sistem logging minimal untuk mendeteksi dan mencatat aktivitas domain.
7	A.12.6.1	Tidak ada bukti vulnerability scanning atau IDS.	Tidak ditemukan WAF/IDS aktif.	Rentan terhadap serangan yang tak terdeteksi.	Pasang dan aktifkan sistem IDS/WAF untuk pemantauan keamanan berkala.
8	A.13.1.1	Sertifikat SSL tidak aktif.	SSL Labs menunjukkan sertifikat kadaluarsa/tidak ada.	Koneksi rentan terhadap penyadapan.	Perpanjang dan aktifkan sertifikat SSL, alihkan HTTP ke HTTPS.
9	A.13.2.3	Tidak ada sistem pemantauan trafik atau firewall.	Tidak ditemukan sistem IDS, firewall, atau filter trafik.	Lalu lintas tidak terlindungi dari anomali/serangan.	Terapkan pemantauan trafik menggunakan firewall & analisis log.
10	A.18.1.4	Tidak ada kebijakan perlindungan data pribadi.	Tidak ada halaman privasi atau disclaimer data.	Pelanggaran prinsip privasi & UU PDP.	Susun dan tampilkan kebijakan privasi sesuai UU No. 27/2022 tentang Perlindungan Data Pribadi.

Hasil audit yang dituangkan dalam tabel temuan menunjukkan sejumlah kelemahan signifikan dalam pengelolaan keamanan informasi situs PeduliLindungi pasca-operasional.

Dari 10 kontrol yang diperiksa, seluruhnya memunculkan temuan teknis dan administratif yang berpotensi menimbulkan dampak serius terhadap keamanan digital dan kepercayaan publik. Temuan mencakup ketiadaan kebijakan akses, tidak adanya proses pencabutan akun pengguna lama, hingga tidak aktifnya sertifikat SSL, yang berarti komunikasi pengguna tidak lagi aman.

Temuan yang paling kritis terdapat pada kontrol A.13.1.1 dan A.18.1.4, yaitu ketidakaktifan sertifikat SSL dan tidak adanya kebijakan perlindungan data pribadi. Kedua kontrol ini berisiko tinggi menyebabkan kebocoran data, serangan man-in-the-middle, dan pelanggaran terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain itu, kontrol lain seperti A.12.2.1 menunjukkan bahwa domain telah terdeteksi sebagai situs berbahaya oleh enam mesin pemindai malware (VirusTotal), mengindikasikan bahwa domain tersebut kemungkinan telah disusupi atau dimanipulasi oleh pihak ketiga. Setiap temuan dikaitkan dengan tingkat dampaknya, yang diklasifikasikan sebagai tinggi atau kritis pada sebagian besar kontrol, serta diberikan saran perbaikan yang realistis. Di antaranya adalah penonaktifan total domain yang tidak lagi aktif, penyusunan ulang kebijakan privasi, penghapusan akun lama, pengamanan DNS, dan penerapan ulang sertifikat SSL. Saran ini tidak hanya bertujuan untuk mengatasi kelemahan teknis, tetapi juga mendorong penerapan tata kelola keamanan informasi yang lebih berkelanjutan di ranah layanan publik digital.

4 KESIMPULAN

Berdasarkan hasil analisis audit keamanan situs layanan publik PeduliLindungi menggunakan pendekatan kuantitatif berbasis ISO/IEC 27001:2013, ditemukan bahwa tingkat kepatuhan terhadap standar keamanan informasi berada pada kategori sangat rendah, dengan skor rata-rata 0,74 dari 4. Temuan ini menunjukkan bahwa mayoritas kontrol, terutama pada aspek komunikasi aman dan perlindungan data pribadi, tidak diterapkan secara efektif, bahkan separuh kontrol memperoleh skor nol. Dengan demikian, hipotesis bahwa situs PeduliLindungi tidak memenuhi standar minimum keamanan informasi diterima, dan hasil penelitian ini secara langsung menjawab rumusan masalah terkait rendahnya implementasi kontrol ISO/IEC 27001 pada domain layanan publik digital pasca-operasional. Hasil ini menguatkan temuan sebelumnya (Meitarice et al., 2024; Yuliana & Hasibuan, 2022) yang menyatakan bahwa institusi publik di Indonesia belum optimal dalam penerapan standar keamanan informasi, khususnya dalam manajemen risiko digital jangka panjang. Penelitian ini memberikan kontribusi nyata dalam literatur keamanan informasi dengan mengkaji fase pasca-operasional situs publik, yang selama ini masih jarang disentuh dalam riset-riset terdahulu. Implikasinya, secara akademik, studi ini memperluas cakupan audit ISO dari hanya sistem aktif menjadi juga sistem nonaktif atau teralihkan; sedangkan secara praktis, penelitian ini mendorong pembuat kebijakan untuk menyusun protokol keamanan terhadap domain layanan publik yang telah tidak digunakan agar tidak disalahgunakan. Untuk penelitian selanjutnya, disarankan mengevaluasi situs publik lainnya yang telah mengalami transisi sistem atau pengalihan domain, serta menambahkan pengujian penetrasi (penetration testing) guna memperkuat dimensi teknis evaluasi keamanan.

REFERENSI

[1] S. Meitarice, L. Febyana, and A. Fitriansyah, "Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 Security Framework in an Academic Information System at a Public University in Indonesia," International Journal of Information and Cyber Security, 2024. [Online]. Available: https://core.ac.uk/download/pdf/648065024.pdf

[2] R. Yuliana and Z. A. Hasibuan, "Best Practice Framework for Information Technology Security Governance in Indonesian Government," International Journal of Information and Computer

Security, vol. 17, no. 3, 2022. [Online]. Available: https://pdfs.semanticscholar.org/9cd7/ab644c7be5bb2fd9d219c99262f13a24b949.pdf

[3] M. Kamal, M. Muhamad, and Y. Sudianto, "Information Technology Security Audit at the YDSF National Zakat Institution Using the ISO 27001 Framework," Jurnal Sisfokom, vol. 13, no. 1, pp. 3542, 2024. [Online]. Available: https://jurnal.atmaluhur.ac.id/index.php/sisfokom/article/view/1987

[4] P. A. W. Putro, D. I. Sensuse, and W. S. S. Wibowo, "Framework for Critical Information Infrastructure Protection in Smart Government: A Case Study in Indonesia," Information and Computer Security, 2024. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/ics-03-2023-0031/full/html

[5] Y. Nugraha, "The Future of Cyber Security Capacity in Indonesia," Oxford Research Archive, 2016. [Online]. Available: https://ora.ox.ac.uk/objects/uuid:70392ace-4bd6-4066-818e-a3adc1eeedf3/files/mc56736ae4aafcccdeae5411f144ebc9c

[6] R. B. Hadiprakoso, H. Setiawan, and I. K. S. Buana, "Cloud Security Maturity Index to Measure the Cybersecurity Maturity Level of Cloud Service Providers in Indonesia," Journal of OIC-CERT, vol. 5, no. 1, pp. 1–10, 2024. [Online]. Available: https://www.oic-cert.org/en/journal/pdf/5/1/1.pdf

[7] M. Y. D. Candiwan and Y. Priyadi, "Analysis of Information Security Audit Using ISO/IEC 27001:2013 & ISO/IEC 27002:2013 at IT Division X Company in Bandung, Indonesia," Journal of Basic and Applied Scientific Research, vol. 6, no. 4, pp. 23–30, 2016. [Online]. Available: https://www.researchgate.net/publication/301688857

[8] W. A. Prabowo, "Developing Compliant Audit Information System for Information Security Index," JOIV: International Journal on Informatics Visualization, vol. 8, no. 2, pp. 126–134, 2024. [Online]. Available: https://joiv.org/index.php/joiv/article/view/1845