Analisis Keamanan Website Halodoc Dengan Implementasi Standar Keamanan Sistem Informasi ISO 27001

Halodoc Website Security Analysis with the Implementation of ISO 27001 Information System Security Standards

Irhas Agung Nur Muhammad Al-Hafidz[1], Dinda Silviani[2], Andre Ariel Hizkia[3], Justin Alfredo Kosasi[4], Diovianto Putra Rakhmadani[5]

[1,2,3,4,5] Program Studi Bisnis Digital, Fakultas Rekayasa Industri dan desain, Institut Teknologi Telkom Purwokerto
e-mail: *2311111069@ittelkom-pwt.ac.id

Abstrak *- Keterbukaan informasi melalui teknologi masa kini menjadi salah satu alasan Gen Z lebih terbuka terhadap kesehatannya. Seiring berjalannya waktu, kesadaran akan pentingnya masalah kesehatan mental semakin meningkat. Halodoc merupakan platform kesehatan digital yang menyediakan layanan kesehatan komprehensif dan nyaman melalui aplikasi berbasis website dan mobile. Akan tetapi, seiring dengan munculnya isu privasi dan penyalahgunaan data, banyak pengguna yang mengkhawatirkan keamanan data dalam bertransaksi data dengan halodoc. Penelitian ini bertujuan untuk menguji tingkat keamanan sistem informasi dengan pengimplementasian security compliance ISO 27001. Dari 92 butir compliance check terhadap website halodoc, terdapat 75 indikator yang sesuai dan 17 indikator yang tidak sesuai dengan standar keamanan. Sehingga sistem informasi di website halodoc mengimplementasikan standar ISO 27001 sebanyak 81,52%. Dengan menerapkan praktik keamanan sistem informasi maka diharapkan pengguna akan lebih aman dan nyaman dalam mengakses sistem informasi milik halodoc.*

Kata kunci – halodoc; ISO 27001; Keamanan Website

Abstract *- The Openness to information through today's technology is one of the reasons Gen Z is more open about their health. As time goes by, awareness of the importance of mental health problems is increasing. Halodoc is a digital health platform that provides comprehensive and convenient health services through website and mobile-based applications. However, along with the emergence of privacy issues and data misuse, many users are concerned about data security when transacting data with halodoc. This research aims to test the level of information system security by implementing security compliance ISO 27001. Of the 92 compliance check items on the halodoc website, there are 75 indicators that are appropriate and 17 indicators that are not in accordance with security standards. So the information system on the halodoc website implements the ISO 27001 standard 81.52% of the time. By implementing information system security practices, it is hoped that users will be safer and more comfortable in accessing Halodoc's information system.*

Keywords – halodoc; ISO 27001; Website Security

I. PENDAHULUAN

Halodoc merupakan pionir ekosistem layanan kesehatan yang canggih dengan misi untuk meningkatkan akses terhadap layanan kesehatan dengan menyelesaikan masalah pengguna dengan layanan yang mudah diakses, andal, dan berkualitas tinggi. Halodoc telah meningkatkan literasi kesehatan di Indonesia melalui komunikasi, edukasi, dan informasi kesehatan (KIE) yang mudah digunakan. Ekosistem yang berkembang menawarkan berbagai layanan kesehatan yang nyaman, seperti laboratorium internal untuk pengujian kesehatan perawatan di rumah, akses tak terbatas ke asuransi tunai My Insurance untuk manfaat rawat jalan, konsultasi jarak jauh dengan dokter dan profesional kesehatan berlisensi, serta akses ke toko kesehatan. untuk membeli obat, suplemen nutrisi, dan berbagai produk kesehatan dari apotek mitra terpercaya[1].

Didalam perkembangannya, salah satu tantangan terbesar Halodoc adalah memastikan layanan mereka aman dan melindungi data sensitif pengguna. Selain itu, perusahaan harus memastikan bahwa layanan mereka dapat diakses oleh semua orang, termasuk mereka yang mungkin memiliki masalah kesehatan atau disabilitas. Untuk mengatasi masalah ini, Halodoc dituntut untuk menerapkan praktik terbaik keamanan dan memberikan pelatihan yang dapat diakses oleh karyawannya[2]. Metode ISO 27001 mengenai standar keamanan sistem informasi digunakan untuk menganalisis keamanan website Halodoc dan mengidentifikasi potensi risiko keamanan informasi [3]. Metode ISO 27001 dalam melakukan analisis keamanan situs web Halodoc diharapkan dapat membantu meningkatkan keamanan situs web dan melindungi informasi sensitif dari potensi ancaman. Metode ini dapat membantu mengidentifikasi dan mengatasi potensi risiko keamanan, menerapkan tindakan perbaikan, dan mengukur efektivitas tindakan tersebut [4].

II. METODE

Dalam melakukan analisis keamanan website Halodoc, pendekatan yang dipilih adalah menggunakan pendekatan berbasis standar ISO 27001 yang merupakan standar internasional untuk sistem manajemen keamanan informasi (ISMS). Pendekatan ini mencakup serangkaian langkah sistematis yang dirancang untuk mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi. Penelitian ini dilakukan dengan cara menentukan ruang lingkup yang mencakup seluruh aset informasi terkait dengan website Halodoc. Aset informasi yang dianalisis meliputi data pengguna, data medis, dan sistem *backend* yang mendukung operasi website dan aplikasi Halodoc. Ruang lingkup ini juga mencakup seluruh komponen aplikasi web dan *mobile* yang digunakan oleh pengguna dan tenaga medis [5].Tahap berikutnya adalah identifikasi aset informasi penting dan risiko yang mungkin terjadi. Setelah mengidentifikasi aset, dilakukan analisis terhadap potensi ancaman yang bisa membahayakan keamanan aset tersebut, seperti ancaman siber, kebocoran data, dan kegagalan sistem.Penilaian risiko dilakukan dengan menilai dampak dan kemungkinan terjadinya ancaman terhadap aset informasi yang telah diidentifikasi. Proses penilaian risiko meliputi setiap ancaman diberi skor berdasarkan dampak dan kemungkinan terjadinya, kemudian dikategorikan dalam tingkat risiko: tinggi, sedang, atau rendah. Berdasarkan penilaian risiko, dibuat kebijakan keamanan yang difokuskan pada mitigasi risiko yang memiliki dampak tinggi [6].

Metode yang dilakukan adalah ceklist terhadap *security complains* sebanyak 92 indikator antara lain 5 sampai 18, metode 18 tersebut berisi tentang information *security policies*,

organization of information security, human resources security, asset management, access control, cryptography, physical and enviromental security, operations security, comunication security, system aquisition develompemt and maintenance, supplier relationship, information security incident management, information security aspects of busines continuity management, compliance.[7]

III. HASIL DAN PEMBAHASAN

Berdasarkan hasil dari uji *security compliance* dengan Standar ISO 27001 yang merupakan standar manajemen risiko informasi internasional yang mengidentifikasi dan mengelola risiko yang terkait dengan sistem informasi organisasi [8] dan mengevaluasi penerapan standar keamanan ISO 27001 pada sistem informasi [9]. Adapun hasil pengujian dijabarkan pada tabel 1 berikut.

Tabel 1. Hasil Uji ISO 27001

No	Kategori	In Compliance	Not in compliance
1.	Information security policies	2	1
2.	Organization of information security	6	1
3.	Human resources security	3	3
4.	Asset management	10	0
5.	Access Control	11	1
6.	Cryptography	2	0
7.	Physical and Environmental Security	11	4
8.	Operations Security	10	5
9.	Communication Security	7	1
10.	System Aquisition, Development and Maintenance	3	0

11.	Supplier Relationship	1	0
12.	Information Security Incident Management	1	0
13.	Information Security Aspects of Business Continuity Management	1	0
14.	Compliance	6	0

Dengan pengujian ISO 27001 dapat diambil beberapa analisa antara lain :

1. Identifikasi dan Analisis Risiko : Halodoc harus melakukan identifikasi dan analisis risiko secara komprehensif untuk mengidentifikasi potensi risiko yang terkait dengan sistem informasi[10]. Hal ini mencakup identifikasi potensi ancaman, penilaian potensi dampak ancaman, dan identifikasi potensi risiko.
2. Menerapkan kontrol keamanan : Berdasarkan analisis risiko, Halodoc harus menerapkan kontrol keamanan yang sesuai untuk memitigasi risiko yang teridentifikasi[10]. Hal ini mencakup penerapan kontrol fisik dan logis seperti enkripsi data, kontrol akses, dan penggunaan kata sandi yang kuat.
3. Penilaian Risiko: Halodoc harus melakukan penilaian risiko secara berkala untuk mengevaluasi efektivitas kontrol keamanan yang diterapkan. Hal ini termasuk menilai risiko yang tersisa dan menentukan apakah pengendalian tambahan perlu diterapkan [10].
4. Pemantauan dan Pelaporan: Halodoc harus memantau dan melaporkan hasil penilaian risiko kepada pemangku kepentingan, termasuk pemangku kepentingan internal dan eksternal. Hal ini termasuk memberikan laporan tahunan mengenai situasi risiko dan mengidentifikasi peluang perbaikan.

Secara keseluruhan, penerapan standar keamanan sistem informasi ISO 27001 membantu Halodoc mengidentifikasi dan mengelola risiko yang terkait dengan sistem informasi, termasuk risiko terkait keamanan, privasi, dan integritas data [11].
Dengan menerapkan standar ini, Halodoc dapat memastikan keamanan dan konsistensi sistem informasinya serta membangun kepercayaan pasien dan pemangku kepentingan lainnya.

IV. KESIMPULAN

Hasil dari pengujian tingkat keamanan sistem informasi Halodoc dengan standar ISO 27001 menunjukkan bahwa 75 dari 92 *compliance check* sesuai dengan standar keamanan, sehingga keamanan sistem informasi Halodoc mencapai 81,52%. Dalam upaya meningkatkan keamanan sebuah sistem informasi berbasis web, Halodoc membutuhkan 17 *compliance* yang dapat dilengkapi untuk dapat lolos standar keamanan sistem informasi ISO 27001, sehingga dapat meningkatkan tingkat kepercayaan pelanggan dalam bertransaksi data dengan menggunakan aplikasi Halodoc. Selain itu, hasil survei juga menunjukkan bahwa halodoc

telah mencapai tingkat keamanan yang cukup tinggi dalam sistem informasinya dan sesuai dengan beberapa klausul, Halodoc juga telah berkomitmen untuk menjaga dan meningkatkan keamanan data pengguna kedepannya.

DAFTAR PUSTAKA

[1] D. Aji Saputra and R. Kumala Dewi, "Hubungan Kualitas Pelayanan Terhadap Kepuasan Pengguna Platform Telemedicine Halodoc Tahun 2022", [Online]. Available: https://www.halodoc.com/media

[2] A. J. Febianto *et al.*, "ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY) FRAMEWORK."

[3] N. I. Muhammad Bakri, "ANALISIS DAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SIMHP BPKP MENGGUNAKAN STANDAR ISO 27001," *Muhammad Bakri, Nia Irmayana*.

[4] T. Informatika, "Penerapan Framework ITILV3 Dalam Tata Kelola Infrastruktur Teknologi Informasi SMK Di Kabupaten Banyuasin Adiktia [1] , Widya Cholil [2]," *Sistem Informasi dan Komputer)*, vol. 11, no. 1, pp. 19–24, doi: 10.32736/sisfokom.

[5] E. Meylani, G. J. Waleleng, J. S. Kalangi, K. Kunci, P. Aplikasi, and K. I. Kesehatan, "PENGARUH PENGGUNAAN APLIKASI HALODOC TERHADAP PEMENUHAN KEBUTUHAN INFORMASI KESEHATAN di KELURAHAN PANIKI BAWAH KECAMATAN MAPANGET KOTA MANADO."

[6] S. Agata Ramadhani, "KOMPARASI PENGATURAN PERLINDUNGAN DATA PRIBADI DI INDONESIA DAN UNI EROPA COMPARISON OF PERSONAL DATA PROTECTION REGULATION IN INDONESIA AND THE EUROPEAN UNION." [Online]. Available: https://jhlg.rewangrencang.com/

[7] S. Nurul, S. Anggrainy, and S. Aprelyani, "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)," vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.

[8] M. A. Kushendriawan, H. B. Santoso, P. O. H. Putra, and M. Schrepp, "Evaluating User Experience of a Mobile Health Application Halodoc using User Experience Questionnaire and Usability Testing," 2021.

[9] S. Kasus *et al.*, "Coding : Jurnal Komputer dan Aplikasi."

[10] H. Penelitian, J. Pengabdian, E. Retno Indriyarti, and S. Wibowo, "BISNIS KESEHATAN BERBASIS DIGITAL: INTENSI PENGGUNA APLIKASI DIGITAL HALODOC," vol. 4, no. 2, [Online]. Available: https://journal.ubm.ac.id/index.php/pengabdian-

[11] Chalifa Chazar, "STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005." [Online]. Available: www.republika.co.id,