P-ISSN : 2549-7480
E-ISSN : 2549-6301

JURNAL ILMIAH INFORMATIKA
E-ISSN : 2549-6301
ISSN : 2549-7480
Faculty of Sains and Technology, Ibrahimy University
S4-Accredited : 85/M/KPT/2020
Journal page is available to : https://journal.ibrahimy.ac.id/index.php/JIMI

ANALYSIS OF INFORMATION SECURITY USING ISO 27001 AND TRIANGULAR FUZZY NUMBER WEIGHTING

Siti Alvi Sholikhatin[1)], Khairunnisak Nur Isnaini[2)]

[1,2] *Program Studi Informatika, Universitas Amikom Purwokerto*

email: [1] sitialvi@amikompurwokerto.ac.id, [2] nisak@amikompurwokerto.ac.id

ARTICLE INFO

Article History:
Recieved : 22 April 2021
Revised : 27 June 2021
Accepted : 28 June 2021
Published : 30 June 2021

Keywords:
ISO 27001
Information Security
Fuzzy
Fuzzy Number

IEEE style in citing this article:
S. A. Sholikhatin and K. N. Isnaini, "Analysis of Information Security Using ISO 27001 and Triangular Fuzzy Number Weighting", Jurnal.ilmiah.informatika, vol. 6, no. 1, pp. 43-49, Jun. 2021.

ABSTRACT

The business process of an organization can't be done properly without appropriate information management, in which information is an important asset that needs to be protected with the utmost care and concern. Information security is a way to protect information from large scale threats, thus to ensure the sustainability of the organization's operational, to reduce business risks and to increase business opportunity and return of investment. This research is conducted to measure the accountability of ISO 27001 in assisting the organization to document the information security policy. ISO/IEC 27001:2005 is a standard of information security that is widely used, openly accepted and implemented, and suitable for providing rules related to implementation and evaluation of the information security system. The assessment from ISO controls and objectives will be converted into a triangular fuzzy number to help in the analysis purpose. The fuzzy number is used to simplify the measurement. The result shows that the organization is not yet complying with the standard procedures of the Information Security Management System so it is needed to document the security policy based on the ISO 27001 framework standard.

© 2021 Jurnal Ilmiah Informatika (Scientific Informatics Journal) with CC BY NC licence

1. PENDAHULUAN

Informasi adalah aset penting bagi sebuah organisasi, sama seperti aset bisnis lainnya, informasi perlu mendapatkan perlindungan yang baik dan konsekuen. Proses bisnis organisasi tidak bisa lepas dari pengelolaan informasi, oleh karena itu organisasi harus mampu melindungi informasi-informasi penting dan sensitif untuk menjaga stabilitas dan integritas organisasi. Pentingnya menjaga keamanan teknologi informasi dalam suatu organisasi terkait dengan berbagai alasan, antara lain mencegah pelanggaran terhadap keamanan informasi yang menyebabkan beberapa kerugian, bahkan kerugian secara finansial dan reputasi perusahaan [1]. Keamanan informasi menjadi isu penting bagi organisasi terutama karena informasi berdampak

DOI : https://doi.org/10.35316/jimi.v6i1.1224
© 2021 Jurnal Ilmiah Informatika with CC BY NC licence

P-ISSN : 2549-7480
S. A. Sholikhatin dkk/ JIMI 6 (1) pp. 43-49 E-ISSN : 2549-6301

langsung pada regulasi dan penanganan risiko terhadap potensi kerusakan dan kehilangan data [2]. Keamanan sistem informasi yang dimaksud yaitu menyangkut *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan).

Confidentiality (kerahasiaan) adalah aspek yang memastikan informasi dapat diakses oleh pihak yang memiliki otoritas [3]. *Integrity* (integritas) yaitu aspek yang menyediakan data dan memastikan data tersebut tidak diubah atau dimodifikasi tanpa ijin dari pihak yang memiliki otoritas, aspek ini juga berfungsi untuk menjaga akurasi data. *Availability* (ketersediaan) yaitu aspek yang memastikan data selalu tersedia ketika dibutuhkan. Ketiga aspek ini yaitu CIA (*confidentiality, integrity, availability)* harus diimplementasikan di data senter sehingga keamanan informasi dapat diraih.

Penilaian dalam mengukur seberapa aman informasi yang tersedia dan dikelola dalam suatu organisasi, dapat dilakukan dengan menggunakan serangkaian proses, alat dan teknik standar yang disebut *Information Security Management System* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI). Pelanggaran akses aset informasi bisa berasal dari permasalahan internal organisasi, yang sebetulnya bisa dicegah dengan mengeliminasi penyebab masalah sedini mungkin. Oleh sebab itu, ISMS diperlukan oleh organisasi sebagai kontrol untuk mencegah kemungkinan pelanggaran terhadap aset informasi dari lingkungan internal. Aspek lain yang perlu diperhatikan adalah serangan dan pelanggaran siber begitu kompleks, akan tetapi keamanan sistem yang mayoritas berjalan berdasarkan observasi masih dilakukan dengan cara-cara yang konvensional [4].

Menggunakan framework ISO 27001 sebagai standar yang membantu organisasi dalam menyusun kebijakan keamanan informasi bukan tanpa alasan. ISO 27001 secara lengkap dan menyeluruh mencakup semua aspek keamanan informasi dan manajemen risiko yang berpotensi mengancam keamanan informasi tersebut. Seperti diungkapkan pada artikel [5] bahwa ISO/IEC 27001:2005 adalah sebuah standar keamanan informasi yang saat ini menjadi yang paling banyak diterima dan digunakan, serta sesuai untuk menyediakan aturan-aturan dalam implementasi dan evaluasi pengukuran sistem keamanan informasi. Dalam melindungi informasi dari ancaman, perlu memperhatikan dua lingkungan yaitu internal dan eksternal organisasi. Karena, potensi ancaman tidak hanya berasal dari eksternal organisasi, namun seringkali berasal dari dalam organisasi itu sendiri.

Seringkali keamanan sistem informasi kurang mendapat perhatian oleh *stakeholder* sebuah organisasi [6]. Pengamanan dilakukan pada saat sudah terjadi ancaman terhadap keamanan sistem informasi. Ancaman keamanan informasi bisa berupa ancaman fisik (api, banjir, kehilangan fisik) dan ancaman nonfisik (*hack* atau *crack*). Oleh karena itu, kesadaran sebuah organisasi untuk mengamankan sistem informasinya menjadi penting untuk ditindaklanjuti dan dilakukan, lebih baik lagi jika sudah diterapkan pada saat instalasi sistem pertama kali. Pentingnya menjaga keamanan sistem informasi di sebuah organisasi adalah upaya untuk menjaga integritas, kerahasiaan dan ketersediaan informasi yang akurat dan berkualitas dalam mendukung kegiatan dan proses bisnis sehingga tujuan organisasi bisa dicapai.

2. KAJIAN LITERATUR

Framework dan standardisasi *Information System Security* (ISS) telah

DOI : https://doi.org/10.35316/jimi.v6i1.1224
© 2021 Jurnal Ilmiah Informatika with CC BY NC licence

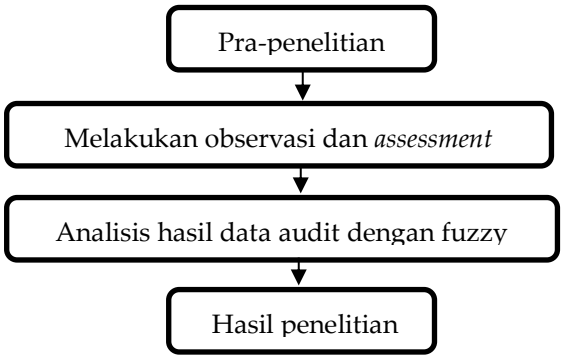
berkembang dari tahun ke tahun dan ISO 27001 adalah salah satu yang cukup lengkap dan terbarukan serta menjadi tiga besar framework yang paling banyak digunakan dalam assessment, selain ISO 9001dan ISO 14001 [7]. Beberapa keunggulan penggunaan *framework* ISO 27001 sehingga menjadi cukup terkenal untuk menyediakan sistem manajemen keamanan informasi antara lain: meningkatkan efisiensi bisnis, mengurangi risiko operasional, memastikan keamanan informasi benar-benar diaplikasikan dengan baik, sebagai asuransi untuk organisasi dan klien melalui sertifikasi yang digunakan sebagai marketing inisiatif, dan meningkatkan kesadaran tentang keamanan informasi oleh karyawan dan manajer [8].

Beberapa penelitian yang telah dilakukan oleh *researchers* dengan menggunakan framework ISO 27001 yaitu penelitian oleh [9] yang melakukan assessment keamanan informasi dengan menggunakan *maturity model*. Kemudian penelitian yang dilakukan oleh [10] yang mengadopsikan framework ISO 27001 dengan data mining, didasarkan pada data temuan yang menyatakan bahwa organisasi di Eropa tidak hanya membutuhkan sertifikasi. Penelitian terkait selanjutnya yaitu dari [11] yang meneliti *gap* antara ISO 27001, 27002, 27003, dan 27005, penelitian tersebut mengajukan security management guidelines yang mampu mengakomodasi kepatuhan karyawan dalam menjaga keamanan informasi.

Penelitian yang cukup mendalam dilakukan oleh [12] yang mengembangkan sistem manajemen keamanan informasi dengan ISO 27001 dan Zachman *framework*. Audit dengan menggunakan berbagai *framework* dan *workflow* pada [4] dalam rangka menjaga privasi dan keamanan di era digital . Kemudian *assessment* pada Data Center dan Data Recovery Kementrian Dalam Negeri dengan menggunakan ISO 27001 dilakukan untuk menilai apakah framework tersebut efektif dalam menyediakan kebijakan (*policy*) dan sertifikasi dalam menjaga keamanan informasi [13]. Rujukan penelitian selanjutnya yaitu Perencanaan Sistem Manjemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013, yang mana scope ISO ini lebih matang dari versi 2005 sehingga diharapkan mampu melahirkan kebijakan keamanan informasi yang lebih baik [14].

3. METODE PENELITIAN

Langkah-langkah penelitian dapat dilihat pada bagan berikut:



Gambar 1. Alur penelitian

Penelitian ini menggunakan 133 kontrol dalam framework ISO 27001 dan menggabungkannya dengan *fuzzy number* untuk memudahkan analisis hasil.

DOI : https://doi.org/10.35316/jimi.v6i1.1224
© 2021 Jurnal Ilmiah Informatika with CC BY NC licence

P-ISSN : 2549-7480
E-ISSN : 2549-6301

Pra-penelitian

Pra-penelitian pada penelitian ini yaitu dengan menganalisis penelitian-penelitian sebelumnya yang menggunakan metode serupa, kemudian membobotkan hasilnya dengan *fuzzy number*.

Melakukan observasi dan assessment

Observasi dan *assessment* yaitu dengan mengkaji kekurangan-kekurangan pada penelitian sebelumnya yang menjadi rujukan. Fokus utama yaitu pada penggunaan *fuzzy* number untuk memudahkan analisis hasil.

Pendekatan *self-assessment* dan perbaikan secara berkelanjutan dalam menjaga keamanan sistem informasi menjadi salah satu metode SMKI (Sistem Manajemen Keamanan Informasi) yang banyak diadaptasi dan diimplementasikan oleh organisasi. *Self-assessment* dilakukan terutama untuk mengidentifikasi risiko dan potensi ancaman terhadap sistem dan informasi yang mungkin bisa terjadi pada organisasi. Identifikasi risiko adalah langkah awal sebagai bentuk tindakan preventif terhadap *information breaches* dan ancaman, yang kemudian akan menjadi faktor penting dalam mengembangkan dan mempertahankan sistem manajemen keamanan informasi sesuai standar.

Analisis hasil data audit dengan fuzzy

Penelitian ini dilakukan dengan mengadaptasi dari penelitian yang dilakukan oleh [3] dimana penelitian tersebut menggunakan alur siklus PDCA serta menganalisis *vulnerability* SMKI. Lebih lanjut, penelitian ini menggunakan *triangular fuzzy number* sebagai nilai bobot yang mewakili hasil *assessment* yang dilakukan. Pembobotan menggunakan *fuzzy theory* juga pernah dilakukan oleh Silva dengan menggunakan *Trapezoidal Fuzzy Number* sebagai dimensi bobot untuk evaluasi keamanan informasi manajemen risiko berdasarkan *Failure Mode and Effects Analysis* (FMEA). Hasil *assessment* berdasarkan klausul kemudian dipetakan ke dalam level yang diadaptasi dari *maturity index* yaitu level 1 adalah *initial* (proses dilaksanakan tapi tidak terdokumentasikan), level 2 adalah *defined* (proses dilaksanakan dan ada dokumentasi), level 3 adalah *optimizing* (proses terus berkembang dan berinovasi). Ketiga level hasil *assessment* tersebut kemudian diterjemahkan secara matematis ke dalam bentuk *triangular fuzzy number* untuk mempermudah analisis.

Hasil penelitian

Hasil penelitian adalah membaca dan menyimpulkan dari proses analisis dan assessment yang dilakukan pada tahap sebelumnya. Kemudian dari kesimpulan tersebut, disusun saran yang bermanfaat untuk organisasi dalam menentukan dokumen kebijakan yang tepat dalam melindungi informasi.

4. HASIL DAN PEMBAHASAN

Metode pengumpulan data yang dilakukan pada penelitian ini yaitu menggunakan observasi langsung. Dari hasil observasi akan dilakukan *self-assessment* menggunakan klausul standar ISO 27001 untuk kemudian ditentukan dimana posisi keamanan informasi yang telah berjalan serta mencegah resiko terjadinya potensi ketidakamanan informasi.

Standar ISO 27001 menggunakan *project check list* untuk mengukur tingkat keamanan informasi sebuah organisasi dengan klausul-klausul yang berbeda, yang terdiri dari 11 klausul kontrol keamanan, 39 kontrol objektif dan 133 kontrol keamanan. Dimana semua kontrol dan objektif tersebut bersifat krusial untuk diterapkan dan digunakan sebagai standar dalam menyusun kebijakan keamanan informasi disebuah organisasi.

Kemudian, setiap klausul dipetakan ke dalam level yang telah diadaptasi dari

DOI : https://doi.org/10.35316/jimi.v6i1.1224
© 2021 Jurnal Ilmiah Informatika with CC BY NC licence

P-ISSN: 2549-7480
S. A. Solikhatin dkk/ JIMI 6 (1) pp. 43-49 E-ISSN: 2549-6301

maturity *index* yaitu Level 1 adalah *initial* (proses dilaksanakan tapi tidak terdokumentasikan), Level 2 adalah *defined* (proses dilaksanakan dan ada dokumentasi), Level 3 adalah *optimizing* (proses terus berkembang dan berinovasi). Implementasi ke dalam TFN yaitu: *initial* (0, 3,0), *defined* (0, 5, 0) dan *optimizing* (0, 7, 0), seperti dijabarkan pada Tabel 1.

Tabel 1. *Triangular Fuzzy Number* terhadap hasil

Bobot hasil	***Triangular Fuzzy number***
Level 1: *Initial*	(0, 3, 0)
Level 2: *Defined*	(0, 5, 0)
Level 3: *Optimizing*	(0, 7, 0)

Selanjutnya, dilakukan proses *self-assessment* menggunakan 39 kontrol objektif dan 133 kontrol keamanan dari *framework* ISO 27001, dengan diberikan nilai bobot angka *fuzzy* yang telah didefinisikan pada Tabel 1.

Dari 133 kontrol keamanan yang menjadi poin penting *self-audit* dan *assessment* dapat disimpulkan bahwa kepatuhan dalam melindungi aset informasi sudah cukup baik dikelola oleh sistem informasi dan integrasinya, namun untuk dokumentasi dan kebijakan keamanan informasi dan aset penting perlu mendapat perhatian khusus karena selama ini belum ada prosedur khusus yang menjadi tonggak dalam pencegahan pelanggaran informasi.

Pendekatan teori *Fuzzy* yang dikombinasikan dengan ISO 27001 dalam menganalisis sistem manajemen keamanan informasi secara sederhana meringkas hasil observasi yang telah dijabarkan pada klausul ISO 27001 di atas menjadi 3 analisis dimensi keamanan informasi [15] yaitu: kontrol akses, infrastruktur dan manajemen teknik keamanan informasi. Lebih lanjut dapat dilihat pada Tabel 2.

Tabel 2. Dimensi keamanan informasi

Elemen dimensi	**Keterangan**	**Klausul ISO 27001 terkait**
Kontrol Akses	Bagaimana aktifitas dalam memonitor akses terhadap informasi.	A11
Infrastruktur	Keamanan jaringan dan *hardware* penting terhadap pengamanan informasi.	A.7, A.8, A.9, A.10
Manajemen teknis keamanan informasi	Pengelolaan dan pengembangan kebijakan keamanan informasi agar terinisialisasi dan terus mengevaluasi diri agar keamanan informasi tetap berjalan secara optimal.	A.5, A.6, A.12, A.13, A.14, A.15

DOI : https://doi.org/10.35316/jimi.v6i1.1224
© 2021 Jurnal Ilmiah Informatika with CC BY NC licence

P-ISSN : 2549-7480
E-ISSN : 2549-6301

Kemudian dilakukan penilaian *fuzzy* terhadap dimensi keamanan informasi, perhitungan didasarkan pada hasil *assessment* sebelumnya, seperti dijelaskan pada Tabel 3. berikut ini:

Tabel 3. Nilai *triangular fuzzy* terhadap dimensi keamanan informasi

Elemen dimensi	***Triangular Fuzzy number***
Kontrol Akses	(0, 3, 0)
Infrastruktur	(0, 5, 0)
Manajemen teknis keamanan informasi	(0, 3, 0)

Berdasarkan hasil *assessment* menggunakan ISO 27001 dengan melakukan pembobotan hasil menggunakan *triangular fuzzy number*, dapat disimpulkan bahwa sistem manajemen keamanan informasi berada pada tingkat *Initial*, yaitu semua proses telah dilaksanakan dengan cukup baik namun dokumentasi kebijakan belum tersusun sesuai dengan standar keamanan informasi. Dengan infrastruktur yang dikelola cukup baik, diharapkan keamanan informasi segera didokumentasikan sesuai dengan standar.

5. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah mendukung penelitian ini sehingga dapat diselesaikan dengan baik.

6. KESIMPULAN

Penelitian ini bertujuan utama untuk mengetahui bagaimana ISO 27001 dapat membantu organisasi untuk menyusun dokumen kebijakan keamanan informasi berdasarkan klausul kontrol dan objektif, setelah melakukan observasi dan *self-audit* didapatkan hasil bahwa organisasi X belum sepenuhnya menerapkan standar keamanan informasi sesuai dengan standar ISO 27001, sehingga saran-saran yang dapat dianjurkan melalui penelitian ini antara lain: 1) Menyusun dokumen kebijakan keamanan sistem dan informasi berdasarkan hasil identifikasi risiko serta mengacu pada standar ISO 27001; 2) Mengidentifikasi potensi ancaman yang mungkin bisa mengganggu keamanan sistem dan informasi, mendokumentasikan peran dan tanggung jawab serta penanganan kejadian (*incident handlings*) secara lugas; dan 3) Melakukan *re-assessment* dan *re-audit* secara berkala sesuai dengan jangka waktu yang telah ditetapkan terhadap sistem manajemen keamanan informasi, agar efektifitas proses pengamanan tetap berjalan sesuai dengan standar.

7. REFERENSI

[1] C. Hsu, T. Wang, and A. Lu, "The impact of ISO 27001 certification on firm performance," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2016-March, pp. 4842–4848, 2016.

[2] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Comput. Secur.*, vol. 70, pp. 663–674, 2017.

[3] D. Achmadi, Y. Suryanto, and K. Ramli, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center," *2018 Int. Work. Big Data Inf. Secur. IWBIS 2018*, pp. 149–157, 2018.

DOI : https://doi.org/10.35316/jimi.v6i1.1224
© 2021 Jurnal Ilmiah Informatika with CC BY NC licence

[4] S. Gritzalis, E. R. Weippl, S. K. K. G. Anderst-kotsis, I. Conference, and G. Goos, *Trust , Privacy and Security*. 2019.

[5] R. Almeida, R. Lourinho, M. M. Da Silva, and R. Pereira, "A model for assessing COBIT 5 and ISO 27001 simultaneously," *Proceeding - 2018 20th IEEE Int. Conf. Bus. Informatics, CBI 2018*, vol. 1, pp. 60–69, 2018.

[6] T. Kristanto, M. Sholik, D. Rahmawati, and M. Nasrullah, "Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ," *JISA(Jurnal Inform. dan Sains)*, vol. 2, no. 2, pp. 30–33, 2019.

[7] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *TQM J.*, vol. 33, no. 7, pp. 76–105, 2021.

[8] S. Al-Dhahri, M. Al-Sarti, and A. Abdul, "Information Security Management System," *Int. J. Comput. Appl.*, vol. 158, no. 7, pp. 29–33, 2017.

[9] D. Proença and J. Borbinha, *Information security management systems - A maturity model based on ISO/IEC 27001*, vol. 320. Springer International Publishing, 2018.

[10] M. Mirtsch, J. Kinne, and K. Blind, "Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis," *IEEE Trans. Eng. Manag.*, vol. 68, no. 1, pp. 87–100, 2021.

[11] I. Topa and M. Karyda, "From theory to practice: guidelines for enhancing information security management," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 326–342, 2019.

[12] A. Aginsa, I. Y. Matheus Edward, and W. Shalannanda, "Enhanced information security management system framework design using ISO 27001 and zachman framework - A study case of XYZ company," *Proc. - ICWT 2016 2nd Int. Conf. Wirel. Telemat. 2016*, pp. 62–66, 2017.

[13] A. Kurnianto, R. Isnanto, and A. P. Widodo, "Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs," *E3S Web Conf.*, vol. 31, pp. 0–5, 2018.

[14] T. Hartati, "Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001: 2013," *KOPERTIP J. Ilm. Manaj. Inform. dan Komput.*, vol. 1, no. 2, pp. 63–70, 2017.

[15] A. P. H. De Gusmão, L. C. E Silva, M. M. Silva, T. Poleto, and A. P. C. S. Costa, "Information security risk analysis model using fuzzy decision theory," *Int. J. Inf. Manage.*, vol. 36, no. 1, pp. 25–34, 2016.

DOI : https://doi.org/10.35316/jimi.v6i1.1224
© 2021 Jurnal Ilmiah Informatika with CC BY NC licence