RABIT : Jurnal Teknologi dan Sistem Informasi Univrab ISSN CETAK : 2477-2062
Volume 6 No. 2 | Juli 2021 : Hal : 116-121 ISSN ONLINE : 2502-891X

STUDI KOMPARASI *FRAMEWORK* NIST DAN ISO 27001 SEBAGAI STANDAR AUDIT DENGAN METODE DESKRIPTIF STUDI PUSTAKA

[1] Hendi Sama, [2] Licen, [3] Jodi Saputra Dermawan Saragi, [4] Meiliverani Erline, [5] Kelvin, [6] Yudi Hartanto, [7] Jenry Winata, [8] Melvy Devalia

[1,2,3,4,5,6,7,8] Sistem Informasi, Fakultas Teknik, Universitas Internasional Batam
[1,2,3,4,5,6,7,8] Jl. Gajah Mada Batam – Kepulauan Riau - Indonesia
E-mail : [1]*hendi@uib.ac.id*, [2]*1831076.li@uib.edu,* [3]*1831119.jodi@uib.edu,* [4]*1831126.meiliverani@uib.edu,* [5]*1831148.kelvin@uib.edu,* [6]*1831151.yudi@uib.edu,* [7]*1831153.jenry@uib.edu,* [8]*1831158.melvy@uib.edu*

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat telah memberikan berbagai dampak positif bagi perusahaan yang menerapkannya dalam rangka mencapai visi, misi serta tujuan mereka. Namun, manfaat dari perkembangan teknologi informasi juga membawa berbagai ancaman dan risiko penggunaannya. Salah satu risiko yang dimaksud adalah serangan *cyber*. Terdapat berbagai standar framework yang dapat digunakan untuk meng-audit/mengukur tingkat keamanan cybersecurity, diantaranya NIST dan ISO 27001. Tujuan dari penelitian ini adalah melakukan perbandingan dari standar *framework cybersecurity* NIST dan ISO 27001 dengan metode deskriptif studi pustaka. Hasil dari penelitian tersebut memperoleh kelebihan dan kekurangan dari masing-masing standar *framework*.

Kata Kunci: NIST CSF, ISO 27001, Keamanan Informasi, keamanan cyber

ABSTRACT

The rapid development of information technology has had various positive impacts on companies that implement it in order to achieve their vision, mission, and goals. However, the benefits of the development of information technology also carry various threats and risks of its use. One of the risks referred to is cyber attacks. There are various standard frameworks that can be used to audit/measure the level of cybersecurity security, including NIST and ISO 27001. The purpose of this study is to make a comparison of the cybersecurity framework standards NIST and ISO 27001 with descriptive literature study methods. The results of this study obtain the advantages and disadvantages of each standard framework.

Keyword: *NIST CSF, ISO 27001, Information Security, cyber security*

PENDAHULUAN

Teknologi informasi merupakan sebuah fasilitas dari aplikasi *hardware*/*software* yang dapat digunakan untuk mencari, mengolah hingga menyebarkan sebuah informasi. Perkembangan teknologi informasi yang semakin pesat kini telah membawa berbagai kemudahan bagi kita untuk memperoleh informasi di mana saja dan kapan saja. Berbagai perusahaan telah mulai menerapkan teknologi informasi untuk mendukung strategi bisnisnya dalam rangka mencapai visi, misi serta tujuan mereka. Namun, manfaat dari perkembangan teknologi informasi juga membawa berbagai ancaman dan risiko penggunaannya. Salah satu risiko yang dimaksud penulis adalah serangan *cyber* [1].

Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN) tercatat bahwa jumlah kasus serangan *cyber* di Indonesia sejak awal tahun 2020 sampai dengan tanggal 12 April 2020 adalah sebanyak 88 juta. Dari angka tersebut, teridentifikasi kasus serangan *trojan activity* sebesar 56%, kasus upaya i*nformation gathering* sebesar 43% dan kasus *web application attack* sebesar 1% [2]. Sedangkan hasil monitoring total kasus

serangan *cyber* di Indonesia pada akhir tahun 2020 mencapai 495 juta dengan serangan terbanyak berupa *trojan activity* dan pencurian data [3]. Hal tersebut menunjukan bahwa terjadi peningkatan serangan *cyber* di Indonesia sebesar 205 juta jika dibandingkan dengan jumlah kasus serangan *cyber* pada tahun 2019 yang sebanyak 290 juta kasus [4].

Penerapan keamanan informasi merupakan hal yang penting untuk dilakukan oleh suatu organisasi. Keamanan informasi didefinisikan sebagai perlindungan informasi dari pembuatan hingga pembuangan data, melalui langkah-langkah logis, teknis, fisik dan organisasi yang menangkal hilangnya kerahasiaan, integritas dan ketersediaan informasi [5]. Keamanan informasi ini perlu diterapkan untuk memastikan keamanan yang spesifik agar tujuan dari suatu perusahaan atau organisasi dapat dipenuhi [1]. Menurut survei yang dilakukan pada *United Kingdom* (UK), diketahui bahwa sebesar 74% sektor industri teknologi dari hasil penelitiannya mengungkapkan bahwa keamanan teknologi yang tinggi menjadi salah satu hal yang paling krusial dalam manajemen senior organisasi mereka [6].

Cybersecurity merupakan bagian dari keamanan informasi yang melindungi aset informasi dari ancaman terhadap informasi yang diproses, disimpan, dikirimkan oleh sistem informasi yang saling berhubungan [7]. Untuk meningkatkan keamanan informasi di dalam organisasi, perlu dilakukan pengontrolan khusus untuk mengukur tingkat keamanan *cybersecurity* yang telah diimplementasikan. Terdapat berbagai standar *framework* yang dapat digunakan untuk meng-audit/mengukur tingkat keamanan *cybersecurity*, diantaranya NIST dan ISO 27001 [8]. Namun, meski terdapat beragam standar, kebutuhan dari masing-masing organisasi yang unik membatasi penggunaan jenis *framework* yang tersedia [1].

Pada umumnya, keamanan informasi yang dimaksud terdiri dari 3 aspek penting yang disebut dengan CIA (*Confidentiality, Integrity dan Availability*) [9]. *Confidentiality* merupakan aspek yang berfokus pada kerahasiaan, yaitu menjaga akses pada data/informasi kepada pihak yang berwenang, sedangkan *Integrity* merupakan aspek yang berfokus pada perlindungan perubahan data tanpa ijin dari pihak yang berwenang (*auhorized*), dan terakhir *Availability* berfokus pada ketersediaan data yang akan digunakan ketika dibutuhkan oleh *user* [10].

Dari uraian tersebut, maka penelitian ini akan membahas tentang perbandingan standar-standar *framework* NIST dan ISO 27001 dalam melakukan audit *cybersecurity*. Tujuan dari penelitian ini adalah mendapatkan hasil perbandingan dari standar *framework* NIST dan ISO 27001. Penulis berharap penelitian ini dapat dijadikan sebagai referensi untuk organisasi maupun perusahaan untuk menentukan penggunaan *framework* yang paling tepat dalam melakukan audit keamanan informasi sesuai kebutuhannya masing-masing.

METODE

Metodologi yang diterapkan untuk penelitian ini adalah penelitian studi pustaka dengan metode deskriptif, di mana objek penelitiannya adalah berupa karya-karya kepustakaan. Karya kepustakaan yang dimaksud adalah berupa jurnal ilmiah, buku, artikel dalam media massa, maupun data-data statistika [11]. Pada penelitian ini, penulis akan melakukan perbandingan *framework cybersecurity* berdasarkan studi pustaka yang telah ada.

HASIL

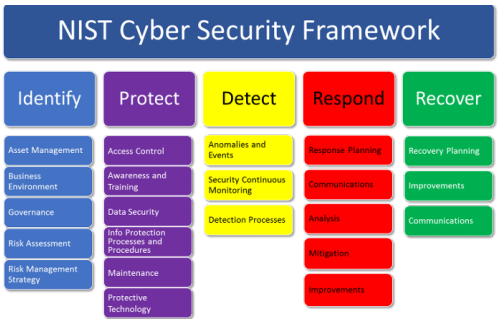
Perbandingan framework NIST dan ISO 27001

1. NIST CSF

NIST (*National Institute Standards Technology*) merupakan *framework* keamanan informasi yang dikembangkan oleh organisasi pemerintah Amerika Serikat, yang bertujuan untuk meningkatkan kemampuan suatu organisasi dalam mencegah, mendeteksi, hingga merespon serangan *cyber* [8]. Keunggulan dari framework NIST adalah memiliki format yang terstruktur dan terencana yang memudahkan organisasi untuk menerapkan di tingkat perusahaan [12]. Pada dasarnya *framework* NIST diatur dalam 5 fungsi inti yang dikenal sebagai *core,* yang berfungsi sebagai gambaran umum tingkat tinggi tentang situasi keamanan siber organisasi [8]:

1. *Indentification* (Identifikasi), yang merupakan pengembangan pemahaman organisasi tentang lingkungan *cyber*, khususnya terhadap sistem, aset, data, dan kapabilitas.
2. *Protect* (Perlindungan), yang merupakan penyebaran dan pengembangan yang tepat untuk membatasi potensi peristiwa kecelakaan keamanan siber.
3. *Detection* (Deteksi), yang merupakan pengembangan dan penerapan yang sesuai untuk mengidentifikasi kegiatan peristiwa keamanan siber dengan cepat.
4. *Respond* (Menanggapi), yaitu pengembangan dan pelaksanaan kegiatan yang sesuai untuk menghindari dampak yang tidak diinginkan dari peristiwa keamanan siber.
5. *Recover* (Pemulihan), yang merupakan kegiatan pengembangan dan pemulian yang sesuai untuk untuk ketahanan dan untuk memulihkan kemampuan dan memulihkan kemampuan yang mungkin terganggu oleh insiden keamanan siber.

Kelima fungsi ini memberikan cara sistematis untuk mengkategorikan risiko keamanan yang membuatnya lebih mudah untuk menerapkan kontrol. 5 fungsi ini dibagi menjadi 23 kategori dan 108 subkategori, ditunjukin pada gambar 1 [8].



Gambar 1. Kategori dan Sub Kategori *framework* NIST

Keuntungan yang dimiliki oleh *framework* NIST adalah sebagian besar kategori dan subkategori menggunakan referensi dari kerangka kerja *framework* lain seperti ISO 27001 dan COBIT. Referensi kerangka kerja tersebut merupakan referensi teknis terperinci yang dimaksudkan untuk memberi organisasi titik awal untuk menerapkan praktik guna mencapai hasil yang diinginkan dari kerangka yang dijelaskan dalam bagian terkait [12].

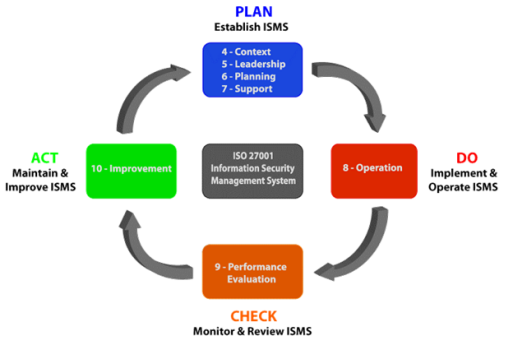
Framework NIST juga menerapkan konsep *profile* untuk evaluasi keamanan secara keseluruhan. *Profile* kerangka kerja merepresentasikan penyesuaian dan

prioritas kegiatan dan hasil untuk berbagai industri dan organisasi sesuai dengan kebutuhan mereka [8]. Dengan cara ini, sangat mudah untuk melacak celah keamanan suatu perusahaan, dan kemudian rencana tindakan dapat dikembangkan untuk menutup celah-celah tersebut [12].

2. ISO 27001

ISO 27001 adalah standar *framework information security* yang diterbitkan pada tahun 2013 dan merupakan revisi dari ISO 27001:2009 [13]. *Framework* tersebut menerapkan prinsip-prinsip dasar *Information Security Management Systems* PCDA (*Plan-Do-Check-Act*) dan ISO 27001 merupakan salah satu standar *framework* yang paling terkenal karena tidak hanya diterapkan di organisasi Amerika Serikat, tetapi di seluruh dunia [14]. Pada dasarnya *framework* ISO 27001 terdiri atas 7 persyaratan yang harus dipenuhi [15]:

1. *Context of the organization,*
2. *Leadership,*
3. *Planning,*
4. *Support,*
5. *Operation,*
6. *Performance evaluation, dan*
7. *Improvement.*



Gambar 2. Model PCDA ISO 27001

Urutan-urutan persyaratan pada standar tersebut tidak mengartikan bahwa persyaratan tersebut wajib dilaksanakan, melainkan ketujuh urutan tersebut hanya untuk tujuan referensi [15]. Di samping itu, ISO 27001:2013 juga menetapkan 14 klausa yang di dalamnya terdapat 133 kontrol untuk keamanan informasi, yaitu:

1. Information security policies,
2. How information security is organized,
3. Human resources security,
4. Asset management,
5. Access controls and managing user access,
6. Cryptographic technology,
7. Physical security of the organisation's sites and equipment,
8. Operational security,
9. Secure communications and data transfer,
10. Secure acquisition, development and support of information systems,
11. Security for suppliers and third parties,
12. Incident management,
13. Business continuity/disaster recovery,
14. Compliance.

Keunggulan dari *framework* ISO 27001 adalah perusahaan bisa mendapat sebuah sertifikat. Sertifikat ini mengindikasikan bahwa perusahaan yang menerapkan standar ini dapat secara efektif meyakinkan klien, mitra dan pemangku kepentingan lainnya bahwa perusahaan tersebut mampu menyediakan kerangka kerja manajemen risiko yang aman dan efektif [12].

Tabel 1. Perbandingan *Framework*

Area	NIST CSF	ISO 27001
Function	Information Security Framework	Information Security Framework
Basis	Risk Management	Risk Management
Certifiable	No	Yes
Scope	Optional guidelines, best-practices and standards for implementing and improving cybersecurity programs	Information security standard that describes how to implement an ISMS (Information Security Management System)
Structure	Core divided into 5 function, 23 categories and 108 subcategories	Consist 7 section of PDCA, 14 clase and 133 control

Di tabel atas di jelaskan bahwa NIST CSF dan ISO 27001 memiliki fungsi yang sama yaitu fokus terhadap keamanan informasi dan berbasis manajemen risiko. Perbedaan dari kedua *framework* tersebut adalah bahwa penerapan NIST CSF tidak memiliki sertifikasi untuk perusahaan yang menerapkannya, sedangkan ISO 27001 memiliki sertifikasi yang dapat menyatakan bahwa perusahaan tersebut telah menerapkan standarnya secara efektif.

Cakupan dari NIST CSF berupa sebuah panduan opsional, praktik terbaik untuk standar penerapan dan peningkatan program keamanan siber, sedangkan cakupan ISO 27001 berupa Standar keamanan informasi yang menjelaskan bagaimana mengimplementasikan ISMS (Information Security Management System). NIST CSF terdiri atas 5 fungsi inti, 23 kategori dan 108 sub kategori yang diperlukan untuk pelaksanaan dalam audit sistem informasi sedangkan ISO 27001 mencakup total 7 proses opsional dalam PDCA (*Plan-Do-Check-Act*),14 klausa dan 133 kontrol.

KESIMPULAN

Dengan adanya manajemen keamanan informasi yang baik, diharapkan perusahaan ataupun organisasi yang menerapkannya dapat menghadapi risiko-risiko yang muncul akibat penyalahgunaan data ataupun serangan *cybersecurity* lainnya. Standar ISO 27001 merupakan standar yang sangat ideal untuk diterapkan dalam manajemen keamanan informasi di sebuah organisasi/perusahaan, karena standar tersebut menyediakan sertifikasi yang dapat menyatakan bahwa organisasi/perusahaan tersebut telah menerapkan standar keamanan informasi yang efektif. Sedangkan, standar NIST CSF lebih baik dalam hal penataan area keamanan yang akan diimplementasikan melalui konsep *profile* keamanan yang ingin dicapai.

Dari kedua standar keamanan informasi tersebut, dapat disimpulkan bahwa masing-masing standar memiliki kelebihan dan kekurangan dalam melakukan audit keamanan informasi. Karena penerapan standar tersebut sangat tergantung terhadap kondisi organisasi atau perusahaan yang akan diaudit.

DAFTAR PUSTAKA

[1] E. Handoyo, "Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST Sp 800 – 55," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 1, no. 2, pp. 76–83, 2020.

[2] "Rekap Serangan Siber (Januari – April 2020) | bssn.go.id." .

[3] "BSSN: Malware Trojan Dominasi Serangan Siber di 2020 - Tempo.co." .

[4] "Laporan Tahunan 2019 PUSOPSKAMSINAS BSSN | bssn.go.id." .

[5] A. Ključnikov, L. Mura, and D. Sklenár, "Information security management in smes: Factors of success," *Entrep. Sustain. Issues*, vol. 6, no. 4, pp. 2081–2094, 2019.

[6] Department for Digital Culture Media and Sport, "Reino Unido Cyber Security 2018," *Cyber Secur. Breaches Surv.*, no. 1, pp. 1–58, 2018.

[7] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation," *Risk Anal.*, 2021.

[8] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss," *Int. J. Informatics Vis.*, vol. 4, no. 4, pp. 225–230, 2020.

[9] A. Ramadhani, "Keamanan Informasi," *Nusant. - J. Inf. Libr. Stud.*, vol. 1, no. 1, p. 39, 2018.

[10] R. Hadianto and T. W. Purboyo, "A Survey Paper on Botnet Attacks and Defenses in Software Defined Networking," *Int. J. Appl. Eng. Res.*, vol. 13, no. 1, pp. 483–489, 2018.

[11] D. R. F. Dits Prasanti, "Penelitian Kepustakaan (Library Research) dalam Penelitian Pendidikan IPA," *Pembentukan Anak Usia Dini keluarga, Sekolah, Dan Komunitas*, vol. 2, no. 1, p. 15, 2018.

[12] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," *2020 Natl. Conf. Emerg. Trends Sustain. Technol. Eng. Appl. NCETSTEA 2020*, vol. 53, pp. 27001–27003, 2020.

[13] D. Rutanaji, S. S. Kusumawardani, W. W. Winarno, U. Gadjah, and J. Grafika, "ISO 27001 Sebagai Metode Alternatif Bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan Untuk Diterapkan di Arsip Nasional RI)," pp. 168–173, 2017.

[14] P. Paradise, K. Kusrini, and A. Nasiri, "Audit Keamanan Aplikasi E-Cash Menggunakan ISO 27001," *Creat. Inf. Technol. J.*, vol. 5, no. 4, p. 243, 2020.

[15] M. B. Firmansyah, "Manajemen Keamanan Informasi di Perpustakaan Menggunakan Framework SNI ISO/IEC 27001," *Media Pustak.*, vol. 25, no. 1, pp. 46–53, 2018.