Journal of Indonesian Management Vol: 4, No 4, 2024, Page: 1-9

Implementasi Kerangka Keamanan NIST Dan ISO/IEC 27001 Dalam Menghadapi Ancaman Risiko Siber

Nadyfa Ramadhanty

UPN "Veteran"Jakarta

Abstrak: Artikel ini memberikan gambaran komprehensif mengenai implementasi kerangka kerja keamanan dari NIST dan standar internasional ISO/IEC 27001 untuk memperkuat keamanan siber organisasi di era digital. Dengan ancaman risiko siber yang terus meningkat, kebutuhan akan sistem keamanan yang andal menjadi sangat mendesak bagi organisasi dari berbagai sektor. Penelitian ini berfokus pada identifikasi aset-aset penting organisasi yang rentan terhadap serangan, analisis terhadap berbagai jenis kerentanan yang mungkin timbul, serta penentuan jenis-jenis ancaman yang dihadapi. Selain itu, penelitian ini mengusulkan kebijakan dan prosedur mitigasi yang dirancang untuk meningkatkan kontrol dan respons keamanan informasi. Melalui studi komparatif dan analisis mendalam, artikel ini mengkaji efektivitas standar NIST dan ISO/IEC 27001 dalam memandu proses identifikasi, penilaian, dan pengelolaan risiko keamanan informasi. Penerapan standar internasional ini memberikan manfaat penting, seperti peningkatan kesadaran akan pentingnya keamanan informasi di kalangan staf dan mahasiswa, penguatan tata kelola keamanan informasi, dan pengembangan strategi mitigasi yang lebih komprehensif. Dengan demikian, artikel ini dapat membangun fondasi keamanan siber yang kokoh sehingga dapat membantu organisasi menghadapi kompleksitas ancaman siber di era digital seperti saat ini.

Kata Kunci: Manajemen Risiko, Keamanan Informasi, ISO/IEC 27001, NIST, Siber.

DOI: https://doi.org/10.53697/jim.v4i4.1973
Correspondence: Nadyfa Ramadhanty
Email: 2310111186@mahasiswa.upnvj.ac.id

Received: 11-10-2024
Accepted: 15-11-2024
Published: 03-12-2024

Abstract: *This article provides a comprehensive overview of implementing the NIST cybersecurity framework and the international standard ISO/IEC 27001 to strengthen organizational cybersecurity in the digital era. With the increasing threats of cyber risks, the need for reliable security systems has become critical for organizations across various sectors. This study focuses on identifying key organizational assets vulnerable to attacks, analyzing potential vulnerabilities, and determining the types of threats faced. Furthermore, the study proposes mitigation policies and procedures designed to enhance information security controls and response mechanisms. Through comparative studies and in-depth analysis, this article examines the effectiveness of NIST and ISO/IEC 27001 standards in guiding the processes of identifying, assessing, and managing information security risks. The implementation of these international standards offers significant benefits, such as increased awareness of information security among staff and students, strengthened information security governance, and the development of more comprehensive mitigation strategies. As such, this article aims to build a robust cybersecurity foundation, equipping organizations to tackle the complexities of cyber threats in today's digital era.*

Keywords: *Risk Management, Information Safety, ISO/IEC 2001, NIST, Siber.*

Pendahuluan

Seiring dengan meningkatnya insiden siber, perusahaan di berbagai sektor mulai menyadari bahwa risiko siber tidak hanya berdampak pada aspek teknis, tetapi juga membawa implikasi serius bagi kelangsungan bisnis dan reputasi perusahaan(Kumar, 2017; LeBoff, 2022; Watts, 2018). Di Indonesia, sektor perbankan dan kesehatan menjadi target utama karena tingginya nilai informasi sensitif yang mereka miliki, seperti data keuangan, informasi medis, dan data pribadi pelanggan. Serangan yang berhasil dapat mengakibatkan kebocoran data pribadi, penipuan finansial, hingga gangguan operasional yang mempengaruhi pelayanan kepada masyarakat (Lana, 2021).

Menurut laporan terbaru dari BSSN (Badan Siber dan Sandi Negara), pada tahun 2022 terjadi lebih dari 1,5 juta insiden siber yang tercatat di Indonesia, di mana sebagian besar serangan merupakan bentuk *phishing*, *malware*, dan serangan *ransomware* yang dirancang untuk mendapatkan keuntungan finansial atau akses ilegal ke sistem informasi(Chen, 2017; Kusumoto, 2017; Lucendo, 2017). Risiko ini diperparah dengan meningkatnya adopsi teknologi digital oleh perusahaan di berbagai industri tanpa penguatan infrastruktur keamanan yang memadai. Banyak organisasi belum memiliki strategi yang komprehensif dalam manajemen risiko siber, seperti penerapan standar keamanan internasional (misalnya, ISO/IEC 27001) atau kerangka kerja NIST yang dirancang untuk meningkatkan deteksi, perlindungan, dan respons terhadap insiden siber.

Transformasi digital yang cepat sering kali diikuti oleh kurangnya pelatihan bagi karyawan dalam mengidentifikasi dan menghindari ancaman siber, yang menjadikan faktor manusia sebagai salah satu kelemahan utama dalam rantai keamanan siber. Insiden seperti kesalahan akses, kelalaian dalam menangani data, dan mudahnya karyawan menjadi korban serangan phishing menunjukkan bahwa investasi dalam keamanan siber harus mencakup teknologi sekaligus edukasi yang menyeluruh bagi seluruh lapisan perusahaan(Coates, 2015; Goodwin, 2016; Malhi, 2015; Safford, 2015). Oleh karena itu, penting bagi perusahaan di Indonesia dan global untuk menerapkan pendekatan keamanan siber yang proaktif, berkelanjutan, dan terintegrasi, termasuk pengembangan kebijakan keamanan yang ketat, audit berkala, serta penerapan kontrol teknologi yang mampu mendeteksi dan mencegah ancaman secara dini(Ruemmele, 2014; Ruggiero, 2014; Scheen, 2015).

Penelitian sebelumnya mengenai manajemen risiko siber di berbagai organisasi telah menyoroti pentingnya mitigasi ancaman siber dan pendekatan keamanan informasi. Fenny Anita dan Kennardi Tanujaya (2023) dalam penelitian berjudul *"Pengaruh Kejahatan Siber terhadap Kinerja Organisasi dengan Moderasi Kesadaran Keamanan Informasi di Sektor Perbankan Kota Batam"* mengungkapkan pentingnya kesadaran keamanan informasi di kalangan karyawan sebagai faktor penentu kinerja organisasi di sektor perbankan. Penelitian ini mencatat dampak signifikan kejahatan siber terhadap kinerja perusahaan, namun tidak membahas strategi adaptasi teknologi terkini seperti AI dan *blockchain* untuk penguatan keamanan (Fenny Anita & Tanujaya, 2023).

Yudi Herdiana, Zen Munawar, dan Novianti Indah Putri (2021) melalui studi berjudul *"Mitigasi Ancaman Risiko Keamanan Siber di Masa Pandemi Covid-19"* menyoroti

peningkatan ancaman siber selama pandemi dan kebutuhan mendesak akan strategi mitigasi komprehensif. Walaupun penelitian ini menyediakan berbagai pendekatan praktis untuk mitigasi, masih terdapat *gap* dalam eksplorasi mendalam terkait manajemen risiko pada perusahaan kecil dan menengah yang memiliki keterbatasan anggaran (Herdiana et al., 2021).

Penelitian dari Edy Soesanto et al. (2023) yang berjudul *"Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher"* mengeksplorasi bagaimana pengamanan *file* dan objek vital dapat meningkatkan efektivitas sistem manajemen keamanan pada yayasan penerbitan digital. Namun, penelitian ini belum membahas bagaimana adaptasi kebijakan keamanan pada perusahaan yang memiliki sifat dinamis dan beroperasi dalam sektor yang lebih komersial dibandingkan nirlaba (Soesanto et al., 2023). Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi jenis risiko siber utama yang dihadapi perusahaan, menjelaskan metode manajemen risiko yang tepat, dan memberikan rekomendasi strategis yang dapat diimplementasikan untuk meminimalisir risiko siber.

Metode Penelitian

Penelitian ini menggunakan metode studi pustaka atau *library research* dengan pendekatan kualitatif, mengandalkan sumber utama dari literatur tentang manajemen risiko siber serta standar keamanan informasi, seperti *NIST Cybersecurity Framework dan ISO/IEC* 27001. Selain itu, jurnal-jurnal terkini terkait strategi mitigasi risiko siber dan peran kesadaran keamanan di organisasi juga ditelaah. Metode ini memungkinkan analisis mendalam dan interpretasi yang komprehensif, mengidentifikasi celah penelitian, serta menawarkan rekomendasi bagi perusahaan dalam menghadapi ancaman siber dengan pendekatan kebijakan dan teknologi yang efektif.

Hasil dan Pembahasan

Menurut *National Institute of Standards and Technology* (NIST), kerangka kerja keamanan siber adalah *"suatu panduan yang membantu organisasi dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan ancaman siber"* (Moore, 2024). Kerangka ini dikenal sebagai NIST *Cybersecurity Framework (CSF)* yang banyak digunakan oleh organisasi untuk memperkuat keamanan informasi. NIST CSF dirancang untuk mendukung sistem keamanan yang fleksibel sehingga memungkinkan perusahaan dari berbagai skala untuk mengelola risiko siber secara adaptif.

ISO/IEC 27001 didefinisikan oleh *International Organization for Standardization* sebagai standar global untuk sistem manajemen keamanan informasi atau ISMS (*Information Security Management System*). Menurut Whitman dan Mattord dalam buku *"Principles of Information Security"*, standar ini memberikan panduan sistematis dalam "menjamin kerahasiaan, integritas, dan ketersediaan informasi perusahaan melalui pengelolaan risiko dan kontrol keamanan yang terstruktur" (Whitman & Mattord, 2011). Dengan ISO/IEC 27001, perusahaan dapat memiliki tata kelola yang jelas terkait keamanan informasi,

termasuk dalam penerapan kontrol akses, kebijakan, dan audit berkala untuk mempertahankan kepatuhan dan keamanan.

Kerangka keamanan NIST dan ISO/IEC 27001 melibatkan beberapa dimensi utama yang harus diimplementasikan perusahaan untuk melindungi informasi digital dari berbagai ancaman (Amin, 2014):

1. Identifikasi (*Identify*)

   Menyangkut proses mengenali aset penting, sistem yang rentan, dan faktor risiko yang perlu dikelola. Tujuannya adalah untuk membangun pemahaman menyeluruh tentang eksposur risiko organisasi.
2. Perlindungan (*Protect*)

   Meliputi langkah-langkah untuk melindungi aset informasi dari ancaman yang teridentifikasi. Dimensi ini mencakup pengendalian akses, pelatihan keamanan, serta penerapan teknologi seperti enkripsi untuk menjaga keamanan data.
3. Deteksi (*Detect*)

   Mengacu pada kemampuan untuk mengidentifikasi insiden siber secara cepat dan akurat melalui pemantauan berkelanjutan. Perusahaan menggunakan alat seperti SIEM (Security Information and Event Management) dan pemindai kerentanan untuk mendeteksi aktivitas mencurigakan.
4. Respons (*Respond*)

   Merupakan tindakan yang harus diambil dalam menghadapi insiden siber. Ini termasuk prosedur tanggap darurat dan komunikasi dengan pemangku kepentingan terkait.
5. Pemulihan (*Recover*)

   Setelah insiden tertangani, proses pemulihan bertujuan untuk mengembalikan sistem ke kondisi normal. Tahap ini memastikan bahwa perusahaan dapat melanjutkan operasi dengan dampak minimal.

ISO/IEC 27001 juga menekankan dimensi *konteks organisasi*, di mana perusahaan diharuskan untuk menyesuaikan ISMS dengan karakteristik dan kebutuhan bisnisnya. Hal ini menambah fleksibilitas dalam implementasi, sehingga dapat disesuaikan dengan spesifik industri yang berbeda.

Setiap dimensi dalam kerangka NIST dan ISO/IEC 27001 memiliki hubungan timbal balik yang penting. Beberapa hubungan utama antara variabel dalam kerangka kerja ini meliputi:

1. Identifikasi dan Perlindungan

   Identifikasi aset penting dan kerentanan membantu menentukan langkah perlindungan yang dibutuhkan. Contohnya, setelah mengidentifikasi sistem yang rentan, perusahaan bisa meningkatkan kontrol akses atau memperbarui perangkat lunak untuk melindungi sistem tersebut.
2. Deteksi dan Respons

   Kemampuan deteksi yang akurat memungkinkan perusahaan untuk merespons insiden lebih cepat. Misalnya, jika sistem deteksi menemukan pola aktivitas tidak biasa, respons dapat diambil untuk menutup celah atau memblokir akses yang mencurigakan sebelum serangan berlangsung.

3. Respons dan Pemulihan

Setelah mengambil langkah respons, perusahaan harus melanjutkan ke tahap pemulihan untuk mengembalikan sistem yang terdampak. Hubungan ini memastikan bahwa perusahaan dapat kembali beroperasi dengan normal secepat mungkin setelah insiden.

Penelitian terbaru terkait implementasi kerangka keamanan NIST dan ISO/IEC 27001 dalam menghadapi ancaman siber menunjukkan hasil yang beragam, tetapi secara keseluruhan mendukung efektivitas kedua kerangka ini dalam memperkuat keamanan informasi. Sebuah studi oleh Riyan Farismana dan Dian Pramadhana yang berjudul *"Risk Management in Final Semester Exam Information System Using NIST 800-30 Method (Case Study of SMKN 2 Baleendah)"* menyoroti bagaimana penerapan NIST SP 800-30 membantu dalam mengidentifikasi, menilai, dan memitigasi risiko yang mengancam sistem ujian *online* di sekolah menengah kejuruan tersebut (Farismana & Pramadhana, 2022).

Penelitian ini menemukan bahwa risiko terbesar datang dari gangguan jaringan dan *error* perangkat lunak yang dapat mengganggu proses ujian. Dengan menerapkan langkah-langkah dalam kerangka NIST, termasuk karakterisasi sistem, identifikasi ancaman, dan analisis kontrol, penelitian ini menunjukkan bahwa penerapan NIST dapat meningkatkan deteksi dini dan respons terhadap insiden yang pada akhirnya membantu mengurangi potensi kerusakan pada operasional ujian.

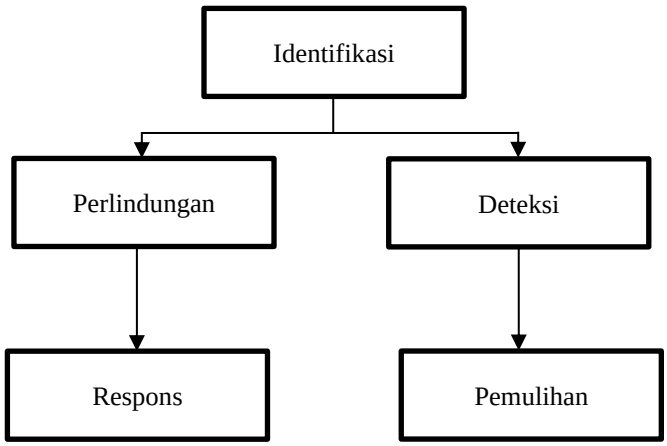
Penelitian lain yang dilakukan oleh Laqma Dica Fitrani di Universitas XYZ, yang berjudul *"Risk Assessment and Development of Access Control Information Security Governance Based on ISO/IEC 27001:2013"*, berfokus pada implementasi ISO 27001 dalam mengelola keamanan informasi untuk mendukung pembelajaran jarak jauh. Hasil penelitian ini menunjukkan bahwa risiko keamanan informasi sering kali kurang mendapat perhatian, meskipun sangat penting untuk menjaga kelancaran layanan digital (Fitrani, 2022). ISO/IEC 27001:2013 digunakan untuk mengidentifikasi aset penting, ancaman, dan kelemahan dalam sistem, yang selanjutnya dianalisis untuk memahami dampaknya pada proses bisnis universitas. Berdasarkan hasil analisis risiko dan pemetaan risiko yang didasarkan pada klausul ISO, penelitian ini merekomendasikan sejumlah dokumen kebijakan, prosedur kerja, dan instruksi untuk meningkatkan kontrol keamanan informasi. Temuan utama dari penelitian ini adalah bahwa standar ISO 27001 tidak hanya membantu mengidentifikasi risiko secara sistematis tetapi juga memberikan panduan bagi universitas untuk mengembangkan tata kelola keamanan informasi yang lebih baik serta meningkatkan kesadaran keamanan di kalangan staf dan mahasiswa.

Penelitian oleh Allisha Apriany dan Antoni Wibowo dari Universitas Bina Nusantara, yang berjudul *"Analysis of the Implementation of ISO 27001:2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms"*, menyoroti pentingnya penerapan ISO 27001:2022 dalam konteks perusahaan konsultasi. Berdasarkan analisis yang dilakukan menggunakan ISO 27001 dan Indeks KAMI, hasil penelitian menunjukkan bahwa banyak perusahaan konsultasi belum menerapkan prosedur keamanan informasi yang memadai, dengan skor kepatuhan terhadap ISO yang hanya mencapai 39%. Hal ini

menunjukkan perlunya perbaikan yang signifikan untuk memenuhi standar ISO (Apriany et al., 2022).

Penelitian ini juga mencatat bahwa aspek seperti pengembangan kebijakan dan prosedur yang terstruktur menjadi langkah awal yang penting untuk memperkuat manajemen keamanan informasi. Rekomendasi dari penelitian ini mencakup peningkatan dalam pelatihan keamanan untuk staf dan penerapan prosedur keamanan yang lebih ketat, yang diharapkan dapat meningkatkan tingkat kematangan manajemen keamanan informasi di perusahaan tersebut. Hasil penelitian ini mendukung pentingnya ISO 27001 sebagai standar yang membantu perusahaan dalam menetapkan dan memelihara sistem manajemen keamanan informasi yang efektif, terutama di tengah meningkatnya ancaman siber yang kompleks dan terus berkembang.

Ketiga penelitian ini menunjukkan bahwa baik NIST maupun ISO/IEC 27001 memiliki peran penting dalam mengelola risiko siber di berbagai sektor. Kerangka NIST terbukti efektif dalam menangani ancaman operasional yang spesifik seperti yang terlihat di SMKN 2 Baleendah, sedangkan ISO 27001 membantu organisasi dalam menetapkan tata kelola dan prosedur keamanan yang lebih komprehensif, seperti yang terlihat di universitas dan perusahaan konsultasi. Implementasi keduanya memberikan panduan yang sistematis dalam mengelola risiko keamanan, meningkatkan kesadaran, serta membangun kontrol yang memadai untuk melindungi aset informasi dari berbagai ancaman siber.



Bagan 1. Konseptual Model

Kesimpulan

Di era digital saat ini, ancaman siber telah berkembang menjadi isu yang tidak hanya teknis tetapi juga strategis bagi keberlangsungan bisnis di berbagai sektor. Insiden siber yang melibatkan pencurian data, peretasan sistem, hingga serangan *ransomware* menunjukkan bahwa keamanan informasi bukan lagi pilihan, tetapi kebutuhan mendesak bagi setiap perusahaan. Penerapan standar keamanan internasional seperti ISO/IEC 27001 dan kerangka NIST terbukti efektif dalam membangun sistem keamanan yang mampu mendeteksi, merespons, dan memulihkan insiden siber secara cepat dan terstruktur.

Penelitian juga menunjukkan bahwa perusahaan yang menerapkan strategi keamanan siber komprehensif memiliki ketahanan yang lebih kuat terhadap berbagai bentuk serangan. Meski teknologi keamanan yang canggih sangat penting, faktor manusia tetap menjadi komponen krusial dalam keamanan siber. Faktor *human error*, seperti kesalahan akses atau ketidaktahuan dalam mengenali *phishing*, dapat menjadi titik lemah yang dimanfaatkan oleh pelaku ancaman. Dengan demikian, keamanan siber yang efektif memerlukan pendekatan holistik yang mencakup teknologi, kebijakan, dan edukasi berkelanjutan bagi seluruh karyawan.

Rekomendasi

1. Implementasi Standar Keamanan
   Perusahaan disarankan untuk menerapkan standar keamanan informasi seperti ISO/IEC 27001 dan kerangka kerja NIST. Standar ini membantu perusahaan dalam mengidentifikasi risiko, membangun prosedur keamanan, serta memantau dan mengevaluasi efektivitas kontrol keamanan.
2. Peningkatan Kesadaran dan Pelatihan Karyawan
   Selain teknologi faktor manusia juga harus diperkuat. Perusahaan perlu rutin mengadakan pelatihan untuk meningkatkan kesadaran karyawan tentang ancaman siber dan praktik keamanan. Simulasi serangan seperti phishing dapat membantu karyawan memahami dan mengenali potensi ancaman.
3. Pemantauan dan Audit Berkala
   Pemantauan dan audit keamanan secara berkala penting untuk memastikan bahwa sistem tetap terlindungi dari ancaman terbaru. Dengan audit rutin, perusahaan dapat mengidentifikasi kelemahan yang muncul dan memperbarui kontrol keamanan sesuai kebutuhan.

Referensi

Amin, M. (2014). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda). Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika, 5(1), 15–24.

Apriany, A., Wibowo, A., Manajemen, S., Informasi, K., & Risiko, M. (2022). Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms 1,2.

Farismana, R., & Pramadhana, D. (2022). Manajemen Risiko pada Sistem Informasi Ujian Akhir Semester Menggunakan Metode NIST 800-30 (Studi Kasus SMKN 2 Baleendah). Jurnal Ilmu Komputer An Nuur, 2, 21–27.

Fenny Anita, & Tanujaya, K. (2023). Pengaruh Kejahatan Siber Terhadap Kinerja Organisasi Dengan Moderasi Kesadaran Keamanan Informasi. Jurnal Ekuilnomi, 5(2), 266–275. https://doi.org/10.36985/ekuilnomi.v5i2.743

Fitrani, L. D. (2022). Risk Risk Assessment and Development of Access Control Information Security Governance Based on ISO/IEC 27001:2013 At XYZ University. JATISI (Jurnal

Teknik Informatika Dan Sistem Informasi), 9(2), 891–907. https://doi.org/10.35957/jatisi.v9i2.1643

Herdiana, Y., Munawar, Z., & Indah Putri, N. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. Jurnal ICT : Information Communication & Technology, 20(1), 42–52. https://doi.org/10.36054/jict-ikmi.v20i1.305

Lana, A. (2021). Dampak Kejahatan Siber Terhadap Teknologi Informasi Dan Pengendalian Internal. Sosial Dan Pendidikan, 1(3), 1–13.

Moore, T. (2024). The NIST Cybersecurity. 32. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Soesanto, E., Saputra, F., Puspitasari, D., & Danaya, B. P. (2023). Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher. Jurnal Ilmu Multidisplin, 2(1), 23–29. https://doi.org/10.38035/jim.v2i1.221

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. Learning, 269, 289.

Chen, Y. (2017). Short-term electrical load forecasting using the Support Vector Regression (SVR) model to calculate the demand response baseline for office buildings. *Applied Energy*, *195*, 659–670. https://doi.org/10.1016/j.apenergy.2017.03.034

Coates, A. S. (2015). Tailoring therapies-improving the management of early breast cancer: St Gallen International Expert Consensus on the Primary Therapy of Early Breast Cancer 2015. *Annals of Oncology*, *26*(8), 1533–1546. https://doi.org/10.1093/annonc/mdv221

Goodwin, G. M. (2016). Evidence-based guidelines for treating bipolar disorder: Revised third edition recommendations from the British Association for Psychopharmacology. *Journal of Psychopharmacology*, *30*(6), 495–553. https://doi.org/10.1177/0269881116636545

Kumar, S. (2017). Review of Childhood Obesity: From Epidemiology, Etiology, and Comorbidities to Clinical Assessment and Treatment. *Mayo Clinic Proceedings*, *92*(2), 251–265. https://doi.org/10.1016/j.mayocp.2016.09.017

Kusumoto, F. M. (2017). 2017 HRS expert consensus statement on cardiovascular implantable electronic device lead management and extraction. *Heart Rhythm*, *14*(12). https://doi.org/10.1016/j.hrthm.2017.09.001

LeBoff, M. S. (2022). The clinician's guide to prevention and treatment of osteoporosis. *Osteoporosis International*, *33*(10), 2049–2102. https://doi.org/10.1007/s00198-021-05900-y

Lucendo, A. J. (2017). Guidelines on eosinophilic esophagitis: evidence-based statements and recommendations for diagnosis and management in children and adults. *United European Gastroenterology Journal*, *5*(3), 335–358. https://doi.org/10.1177/2050640616689525

Malhi, G. S. (2015). Royal Australian and New Zealand College of Psychiatrists clinical practice guidelines for mood disorders. *Australian and New Zealand Journal of Psychiatry*, *49*(12), 1087–1206. https://doi.org/10.1177/0004867415617657

Ruemmele, F. M. (2014). Consensus guidelines of ECCO/ESPGHAN on the medical management of pediatric Crohn's disease. *Journal of Crohn's and Colitis*, *8*(10), 1179–1207. https://doi.org/10.1016/j.crohns.2014.04.005

Ruggiero, S. L. (2014). American association of oral and maxillofacial surgeons position paper on medication-related osteonecrosis of the jaw - 2014 update. *Journal of Oral and Maxillofacial Surgery*, *72*(10), 1938–1956. https://doi.org/10.1016/j.joms.2014.04.031

Safford, B. (2015). Use of an aggregate exposure model to estimate consumer exposure to fragrance ingredients in personal care and cosmetic products. *Regulatory Toxicology and Pharmacology*, *72*(3), 673–682. https://doi.org/10.1016/j.yrtph.2015.05.017

Scheen, A. (2015). Pharmacodynamics, efficacy and safety of sodium-glucose co-transporter type 2 (SGLT2) inhibitors for the treatment of type 2 diabetes mellitus. *Drugs*, *75*(1), 33–59. https://doi.org/10.1007/s40265-014-0337-y

Watts, N. (2018). The 2018 report of the Lancet Countdown on health and climate change: shaping the health of nations for centuries to come. *The Lancet*, *392*(10163), 2479–2514. https://doi.org/10.1016/S0140-6736(18)32594-7