Contents list avaliable at Directory of Open Access Journals (DOAJ)

JUTIN : Jurnal Teknik Industri Terintegrasi

Volume 7 Issue 3 2024, Page 1971-1979

ISSN: 2620-8962 (Online)

Journal Homepage: https://journal.universitaspahlawan.ac.id/index.php/jutin/index

Analisis Bibliometrik Tren Publikasi pada Kajian Risiko Sistem Manajemen Keamanan Informasi

Nuraini Rahmad[1]✉, Riri Nasirly[2], Fadli Arsi[3], Fachri Ibrahim Nasution[3]

Program Studi Teknik Industri, Institut Teknologi Perkebunan Pelalawan Indonesia(1,2,3)

Program Studi Teknologi Pascapanen, Institut Teknologi Perkebunan Pelalawan Indonesia(3)

DOI: 10.31004/jutin.v7i3.33423

✉ Corresponding author:
[nuraini.rahmad@itp2i-yap.ac.id]

Article Info

Kata kunci:
Keamanan Informasi;
Manajemen Risiko;
Bibliometrik;
Vosviewer

Abstrak

Risiko keamanan mencakup segala aspek, diantaranya pengguna biasanya merasa kehilangan atau adanya kebocoran data diri, sehingga seringkali terjadi komplain oleh pengguna yang merasa tidak puas kepada suatu perusahaan. Manajemen risiko terhadap keamanan informasi merupakan suatu metodologi untuk mengidentifikasi dan menilai risiko keamanan dengan menerapkan, mengontrol dan menangani risiko untuk melindungi suatu kepentingan organisasi. Penelitian ini mengkaji karakteristik bibliometrik dan tren artikel tentang "Risiko Sistem Manajemen Keamanan Informasi". Data dari database Scopus dikumpulkan, diterbitkan antara tahun 1987 hingga 2023. Melalui pencarian database scopus ditemukannya 1.351 artikel. Bibliometrik analisis dilakukan menggunakan alat bantu vosviewer untuk memvisualisasikan tren penelitian studi ini. Artikel "Risk Management" dan "Information Security Management Systems" terdapat di 165 institusi dan 87 negara. Analisis bibliometrik mengungkapkan bahwa Universitas Norges Teknisk-Naturvitenskapelige memiliki publikasi penelitian "Risk Management" dan "Information Security Management Systems" terbanyak, dengan total 28 dokumen.

Keywords:
Information Security;
Risk Management;
Bibliometrics;
Vosviewer

Abstract

Security risks cover all aspects, including users usually feel lost or there is a leak of personal data, so there are often complaints by users who feel dissatisfied with a company. Risk management of information security is a methodology to identify and assess security risks by implementing, controlling and handling risks to protect an organization's interests. This research examines the bibliometric characteristics and trends of articles on "Risk of Information Security Management System". Data from the Scopus database was collected, published between 1987 and 2023. Through searching the Scopus database, 1,351 articles were found. Bibliometric analysis was conducted using the vosviewer tool to visualize the research trends of this study. "Risk Management" and 'Information Security

Received 30 June 2024; Received in revised form 6 July 2024 year; Accepted 8 July 2024
Available online 10 July 2024 /

Management Systems' articles were found in 165 institutions and 87 countries. The bibliometric analysis revealed that Norges Teknisk-Naturvitenskapelige University had the most "Risk Management" and "Information Security Management Systems" research publications, with a total of 28 documents.

1. INTRODUCTION

Semakin berkembangnya teknologi khususnya dalam bidang sistem informasi memiliki peran yang sangat penting sejalan dengan arus globalisasi. Sistem informasi yang sudah menginjak era digital memberikan pengaruh besar kepada masyarakat yang mengubah cara mereka dalam melakukan komunikasi, salah satunya dalam penggunaan internet. Adanya internet memungkinkan bagi seseorang untuk melakukan komunikasi jarak dekat maupun jarak jauh dengan pihak lain tanpa dibatasi oleh waktu dan jarak. Pengguna internet dapat didefinisikan sebagai individu yang memiliki akses ke internet melalui komputer maupun perangkat seluler (Kohran, 2018). Pengguna internet di dunia terus mengalami peningkatan, dikarenakan dengan adanya internet kita bisa mendapatkan banyak informasi terbaru tentang berbagai hal tanpa batas ruang. Terlebih dengan perkembangan yang terjadi, internet tidak hanya digunakan sebagai media komunikasi melainkan dapat digunakan untuk penelusuran informasi, transaksi perbankan, hingga berbelanja online adalah manfaat yang bisa didapat. Internet juga banyak digunakan oleh perusahaan maupun suatu organisasi untuk mempermudah bisnis mereka, sehingga ketergantungan terhadap dunia internet saat ini semakin signifikan bagi perkembangan kebutuhan hidup.

Saat ini, perusahaan maupun organisasi hanya mengandalkan layanan internet dan sistem informasi untuk meningkatkan operasi bisnis mereka, serta memfasilitasi pengambilan keputusan manajemen dan menyebarkan strategi bisnisnya. Dalam hal ini, informasi dianggap sebagai aset utama sebuah perusahaan maupun organisasi, sehingga hal tersebut dapat menimbulkan risiko yang konstan. Sebagian besar risiko yang muncul merupakan hasil dari evolusi internet yang telah mengarahkan pada perusahaan maupun organisasi untuk berbagi informasi. Bagi penyelenggaraan tata kelola sistem informasi, faktor keamanan informasi merupakan aspek yang sangat penting untuk diperhatikan, mengingat kinerja tata kelola sistem informasi akan terganggu jika informasi sebagai salah satu objek utama mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), ketersediaan (*availability*) dan keutuhan (*integrity*) (Alosaimi dan Alnuem, 2016). Keamanan informasi ini menjadi satu hal yang penting, karena keamanan informasi memiliki tujuan untuk menjaga suatu kerahasiaan, integritas, dan ketersediaan yang ada dalam perorangan, perusahaan ataupun organisasi lain. Apabila suatu keamanan informasi yang tidak dirawat dengan baik dan benar maka akan menimbulkan suatu permasalahan dan ancaman yang tidak terduga untuk perusahaan atau organisasi tersebut.

Risiko keamanan mencakup segala aspek, diantaranya pengguna biasanya merasa kehilangan atau adanya kebocoran data diri, sehingga seringkali terjadi komplain oleh pengguna yang merasa tidak puas kepada suatu perusahaan (Ernst & Young, 2012). Manajemen risiko terhadap keamanan informasi merupakan suatu metodologi untuk mengidentifikasi dan menilai risiko keamanan dengan menerapkan, memantau, mengontrol dan menangani risiko tersebut untuk melindungi suatu kepentingan organisasi (Spears dan Barki, 2010). Ketika serangkaian risiko menyerang sistem informasi, hal tersebut tentu akan menjadi lebih berbahaya karena ketergantungan akan sistem informasi mengarahkan kepada peningkatan penyalahgunaan keamanan sistem informasi. Penyalahgunaan keamanan pada sistem informasi biasa disebabkan karena kegagalan teknis, kerentanan terhadap sistem, penipuan, kegagalan manusia dalam membuat sistem dan kejadian eksternal lainnya (Lundgren, 2020). Oleh karena itu, keamanan informasi menjadi sangat penting bagi kelangsungan hidup suatu perusahaan maupun organisasi untuk meminimalkan suatu risiko yang akan membahayakan operasi bisnis dan untuk menjaga kerahasiaan data.

Penelitian ini akan menyajikan kontribusi yang signifikan terhadap kajian literatur mengenai manajemen resiko dalam sistem manajemen keamanan informasi. Pentingnya penelitian ini untuk memberikan gambaran yang jelas mengenai bidang manajemen risiko dari segi keamanan informasi dan organisasi yang bersangkutan karena perannya yang signifikan dalam mengidentifikasi risiko dan menetapkan kontrol yang tepat untuk mengelola atau menghilangkan risiko, serta fleksibilitas dalam menetapkan kontrol dan mendapatkan kepercayaan dari pemangku kepentingan maupun pelanggan bahwa data mereka dilindungi. Penelitian ini akan melihat bagaimana karakteristik bibliometrik dan tren publikasi penelitian terkait manajemen risiko dan keamanan sistem informasi yang telah terindeks di Scopus oleh penulis dari seluruh dunia melalui analisis komprehensif terhadap data database *scopus* dan penerapan metode bibliometrik. Bagaimana tren penelitian mengenai

manajemen risiko dan keamanan sistem informasi saat ini? Bagaimana penyebaran penelitian berdasarkan studi tersebut? dan Bagaimana kajian literaturnya mengenai manajemen risiko dan keamanan sistem informasi?

2. METHODS

Metodologi berisi mengenai tahapan yang dilakukan dalam studi literatur penelitian ini. Literatur ini mencakup berbagai topik yang berhubungan dengan manajemen resiko dalam sistem manajemen keamanan informasi. Penelitian ini menggunakan analisis bibliometrik untuk menampilkan ringkasan serta melihat tren penelitian yang muncul dalam artikel ataupun jurnal, pola kolaborasi antar autor maupun negara, dan mengeksplorasi dampak publikasi di dunia (Donthu et. al, 2021). Data dikumpulkan dari sumber database elektronik seperti Scopus. Berbagai kombinasi kata kunci yang digunakan dalam mesin pencari elektronik yaitu, keamanan informasi (*information security*), manajemen resiko (*risk management*) dan sistem manajemen keamanan informasi (*information security management system*) yang menghasilkan ratusan artikel. Setiap artikel diperiksa untuk memastikan bahwa isinya relevan dari perspektif topik atau tujuan penelitian. Pemeriksaan dan pemilihan artikel didasarkan pada kriteria bahwa hanya artikel yang kontribusi utamanya berkisar pada manajemen risiko pada keamanan sistem informasi yang akan dipilih. Alat bantu yang digunakan dalam analisis bibliometrik adalah dengan bantuan *Vosviewer*. Alat bantu *vosviewer* banyak digunakan oleh peneliti untuk melakukan analisis visualisasi jaringan (Jadwani et. al, 2024). Alat ini menggunakan metode pengumpulan dan desain sistem untuk membayangkan beberapa jaringan yang ada dalam kumpulan data literatur apa pun. *Vosviewer* berguna untuk mengevaluasi hubungan di antara beberapa parameter, misalnya hubungan atau jaringan antar-negara berdasarkan *co-authorship*. Dengan adanya *vosviewer*, mampu menggambarkan peta visualisasi yang dapat membantu dalam mengidentifikasi tren penelitian dan kolaborasi pada bidang studi manajemen risiko dan keamanan sistem informasi.

3. RESULT AND DISCUSSION

3.1. Analisis Artikel berdasarkan Tren Publikasi

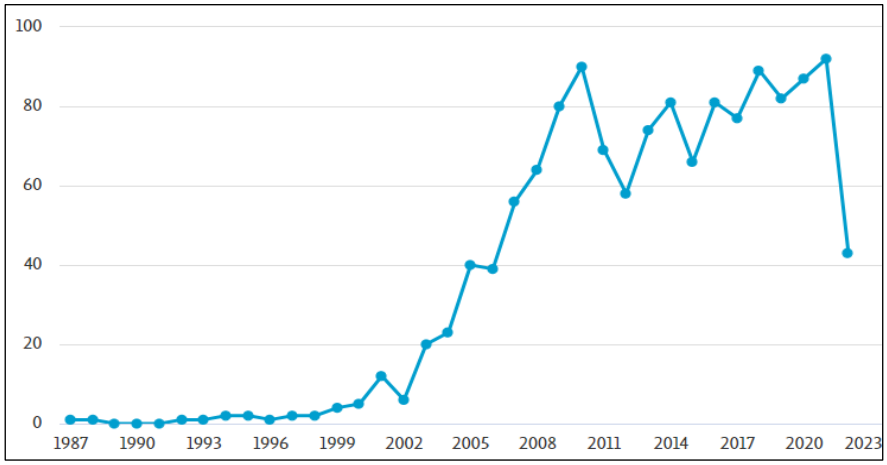
Pencarian artikel dalam database Scopus menggunakan kata kunci "*Risk Management" and "Information Security" and "Information Security Management Systems*" didapatkan 1.351 dokumen yang telah memenuhi kriteria seleksi. Jenis dokumen yang paling sering muncul adalah conference paper (697) dengan proporsi 51,6%. Posisi kedua adalah bertipe artikel (455) dengan proporsi 33,7%. Jenis dokumen lainnya yaitu, bertipe *book chapter* (68) dengan proporsi 5%, bertipe *conference review* (59) dengan proporsi 0,9%, bertipe *review* (34) dengan proporsi 2,5%, bertipe *book* (27) dengan proporsi 2%, bertipe *note* (7) dengan proporsi 0,7%, bertipe *short survey* (3) dengan proporsi 0,2%, dan 1 dokumen bertipe *retracted* dengan proporsi 0,1%. Berikut merupakan tabel 1 yang mencantumkan jenis tipe dokumen, jumlah dan proporsi.

Tabel 1. Jenis Dokumen yang dipilih

Jenis Dokumen	Frekuensi	Persentase
Conference paper	697	51,6%
Article	455	33,7%
Book chapter	68	5%
Conference review	59	4,4%
Review	34	2,5%
Book	27	2%
Note	7	0,5%
Short survey	3	0,2%
Retracted	1	0,1
Total	1.351	100%

Gambar 1. mengilustrasikan tren tahunan publikasi terkait "*Risk Management dan Information Security Management Systems*". Seperti yang ditunjukkan dalam gambar 1, ada peningkatan publikasi terkait "*Information Systems Risk Analysis and Management*" di negara-negara maju maupun berkembang dalam 36 tahun terakhir yang menunjukkan adanya ketertarikan minat di bidang tersebut. Sejak artikel pertama diterbitkan pada tahun 1987 berjumlah, penelitian terkait *Risk Management dan Information Security Management Systems* mengalami peningkatan yang sangat lambat dalam 15 tahun berikutnya. Kemudian, peningkatan publikasi penelitian paling pesat terjadi antara tahun 2002 hingga 2010 dan mengalami peningkatan lagi mulai dari tahun 2012 hingga 2023.

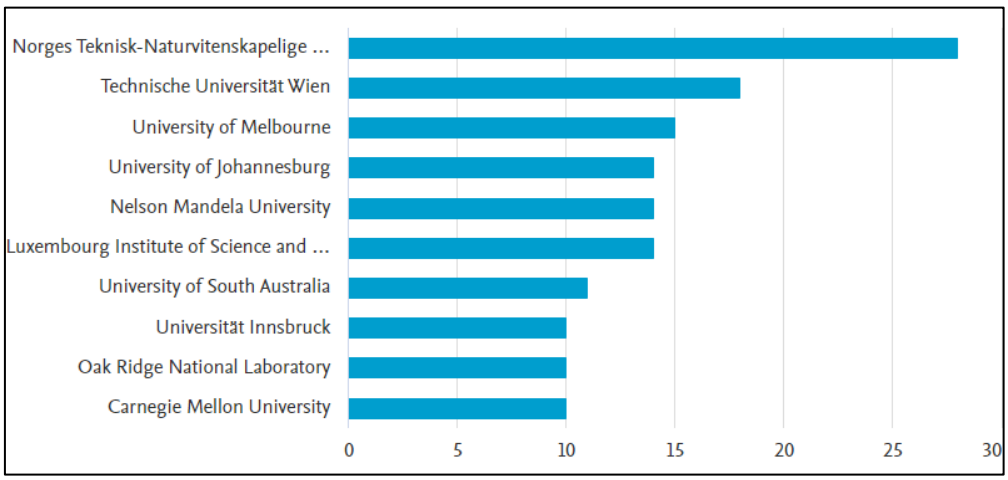
Dengan demikian, semakin banyak akademisi yang mulai meneliti bidang tersebut. Hal ini menyebabkan terjadinya lonjakan jumlah publikasi.



Gambar 1. Tren Publikasi Berdasarkan Tahun

3.2. Analisis Artikel berdasarkan Penyebaran Lembaga Studi

Pencarian artikel dalam database scopus juga didapatkan penyebaran artikel di beberapa lembaga studi atau institusi yang terlibat dalam kajian mengenai manajemen resiko dalam keamanan sistem informasi, 165 institusi yang terlibat dalam study Risk Management dan Information Security Management Systems.



Gambar 2. Penyebaran berdasarkan Lembaga Studi

Universitas Norges Teknisk-Naturvitenskapelige memiliki jumlah publikasi terbanyak dengan total 28 artikel. Artikel yang paling populer dikutip dari Norges Teknisk-Naturvitenskapelige ditulis oleh Wangen, et. al, (2018) sebanyak 55 kutipan. Wangen et. al, (2018) menyelidiki tentang metode penilaian risiko keamanan informasi yang akan menghasilkan perkiraan risiko, dimana risiko merupakan produk dari kemungkinan terjadinya suatu peristiwa dan konsekuensi terhadap suatu organisasi tertentu. Penelitian Wangen dkk (2018) menyebutkan bahwa pendekatan fungsional prosedur penilaian risiko, yang merupakan metode penilaian risiko keamanan informasi akan berfokus pada penilaian aset, ancaman, kerentanan, dan perlindungan. Studi tersebut menggunakan pendekatan ISO/IEC 27005 dalam penilaian risiko keamanan system informasi. Selanjutnya, posisi kedua adalah Technische Universitat Wien dengan penerbitan 18 artikel. Artikel yang paling populer dikutip dari Technische Universitat Wien sebanyak 188 kutipan, kemudian diikuti oleh Universitas of Melbourne sebanyak 18 artikel, University of Johannesburg sebanyak 14 artikel, Nelson Mandela University sebanyak 14 artikel, Luxembourg Intitute of Science and Technology sebanyak 14 artikel, University of South Australia sebanyak 11 artikel, dan Universitat Innsbruck, Oak Ridge National Lanpratory, Carnegie Mellon University masing-masing menemukan sebanyak 10 artikel.

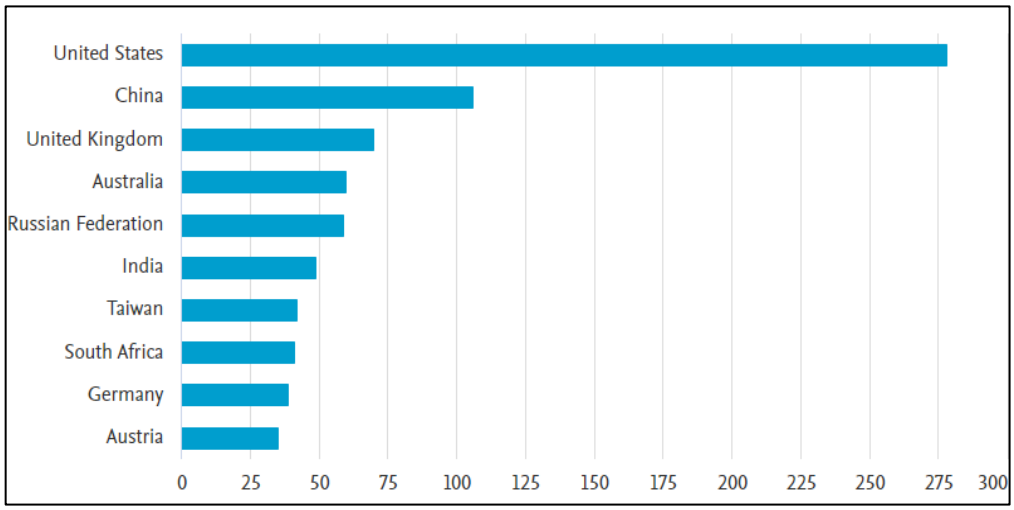
3.3. Analisis Artikel berdasarkan Penyebaran Author dan Negara Penerbit

Penelitian ini menemukan 1.351 artikel yang diterbitkan di 87 negara berbeda. Dalam hal ini, sangat penting bagi peneliti untuk mengetahui berbagai penulis terkemuka supaya peneliti dapat menganalisis dan mempelajari dari penelitian mereka.

Tabel 2. Penyebaran Author yang paling relevan dan Jumlah Kutipan

Author	Dokumen	Kutipan
Fenz, S.	18	515
Ahmad, A.	15	273
Von, S.	12	599
Naubauer, T.	10	218
Mayer, N.	10	42
Abercrombie, R.	9	119
Sheldon, F.	9	119
Zhang, J.	7	7
Snekkeness, E.	6	33
Wangen, G.	6	83

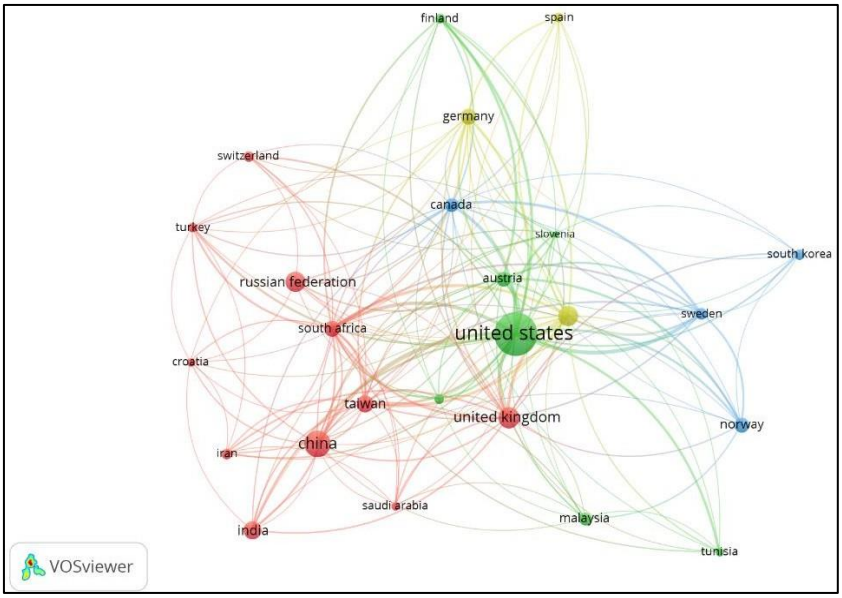
Berdasarkan data yang diambil dari database Scopus, seluruh 1.351 dokumen diterbitkan oleh 159 penulis. Tabel 2 memberikan informasi tentang 10 penulis teratas dengan jumlah kutipan yang paling dominan. Jumlah kutipan pada artikel menunjukkan kualitas publikasi. Penulis dengan jumlah dokumen terbanyak adalah Fenz S. (18 dokumen) dengan jumlah kutipan 515, diikuti oleh Ahmad A. (15 dokumen) dengan jumlah kutipan 273, Von S. (12 dokumen) dengan jumlah kutipan 599 Naubuer, T. (10 dokumen) dengan jumlah kutipan 218, Mayer, N. (10 dokumen) dengan jumlah kutipan 42, Abercrombie, R. Dan Sheldon, F. masing-masing 9 dokumen dengan jumlah kutipan 119, Zhang, J. (7 dokumen) dengan jumlah kutipan 7, Snekkeness, E. (6 dokumen) dengan jumlah kutipan 33, dan Wangen, G. (6 dokumen) dengan jumlah kutipan 83. Kutipan Von, S. memiliki jumlah kutipan yang lebih tinggi dibandingkan dengan artikel Fenz, S. Gambar 3 menunjukkan visualisasi data dari artikel kajian studi *Risk Management* dan *Information Security Management Systems* dalam hal jumlah publikasi yang ditetapkan per negara penulis.



Gambar 3. Penyebaran Artikel 10 Negara Teratas

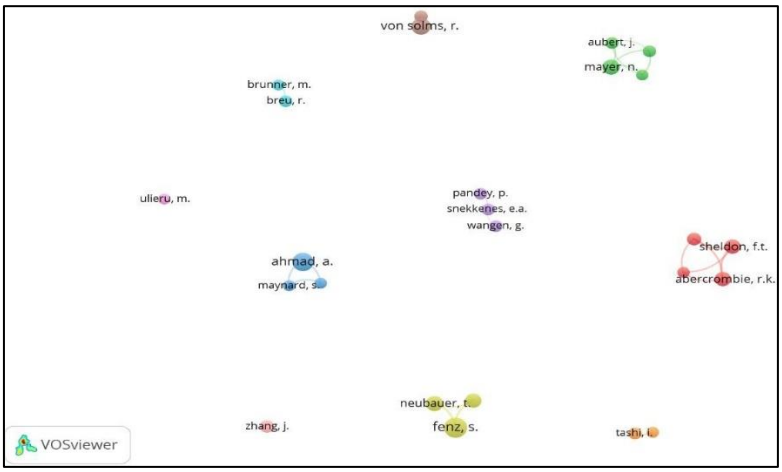
3.4. Analisis Hubungan *Co-authorship*

Penelitian berdasarkan *co-authorship* merupakan poin penting dari analisis bibliometrik dan menunjukkan tingkat kolaborasi penelitian untuk menilai status penelitian terkini dalam bidang tertentu. Analisis jaringan *co-authorship* dilakukan dengan menggunakan software Vosviewer. Hal ini dapat memberikan informasi lebih luas melalui tingkat komunikasi antar negara serta negara-negara berpengaruh di bidang penelitian ini. Jaringan berdasarkan hubungan *co-authorship* antar negara ditunjukkan pada gambar 4.



Gambar 4. Jaringan *co-authorship* berdasarkan antar-negara

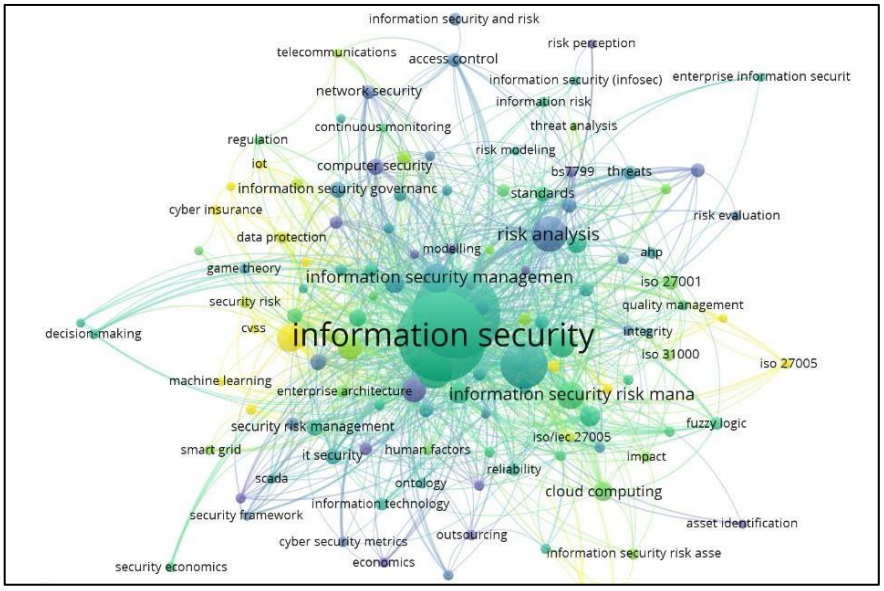
Gambar 4 menunjukkan hubungan *co-authorship* berdasarkan antar negara publikasi dengan menggunakan 200 dokumen yang sudah di seleksi sesui dengan kata kunci yang akan digunakan. Analisis data menunjukkan bahwa penulis dari negara Amerika Serikat lebih mendominasi bidang dengan menempati peringkat pertama yaitu sebanyak 278 publikasi dokumen dari jumlah total, dan pusat penelitian benua Asia berada di China sebanyak 106 publikasi dokumen, United Kingdom sebanyak 70 publikasi dokumen, Australia sebanyak 60 publikasi dokumen, Rusia sebanyak 59 dokumen, India sebanyak 48 dokumen, Taiwan sebanyak 42 dokumen, Afrika Selatan sebanyak 40 dokumen, Jerman sebanyak 38 dokumen, dan Austria sebanyak 34 dokumen seperti yang ditunjukkan pada gambar 3. Pusat jaringan adalah terletak pada negara Amerika Serikat, China, dan United Kingdom.



Gambar 5. Jaringan *co-authorship* berdasarkan penulis

3.5. Analisis Peta Visualisasi Jaringan berdasarkan *Keyword*

Peta jaringan bedasarkan *co-word* digunakan untuk mengidentifikasi tema penelitian utama. Untuk mengetahui peta jaringan utama pada penelitian ini, maka digunakan *co-occurance analysis* pada VOS-*viewer* guna menampilkan data keterkaitan antar kata kunci dan tema yang akan digunakan (Donthu et. al, 2021). Berdasarkan hasil yang digunakan menggunakan kata kunci *"Risk Management" and "Information Security" and "Information Security Management Systems"*pada 200 dokumen menampilkan hasil seperti pada gambar 6.



Gambar 6. Peta visualisasi jaringan *co-word* (keyword *co-occurrence*) dengan *Vosviewer*

Gambar 6 menunjukkan peta visualisasi pada *keyword "Risk Management" and "Information Security" and "Information Security Management Systems*". Peta visualisasi ini menunjukkan bahwa "keamanan informasi" menjadi kata kunci yang utama. Peta ini juga menunjukkan bahwa *co-word* ini sangat terkait dengan analisis risiko, risiko keamanan, pemodelan risiko, manajemen risiko keamanan, risiko informasi, manajemen kualitas, persepsi risiko, pendekatan ISO/IEC 27005, pendekatan *game theory*, AHP, metrik keamanan siber, jaminan siber, analisis keputusan, penilaian risiko keamanan informasi, evaluasi risiko, dan lain sebagainya seperti yang tampak pada gambar 6. Hal ini mendukung fakta bahwa berbagai kategori risiko, seperti risiko keamanan dan risiko informasi saling terkait. Penilaian risiko yang menyeluruh dan manajemen risiko yang terpadu merupakan cara untuk mengelola risiko keamanan tersebut (Jadwani et. al, 2024). Adanya kebocoran data, penipuan, *hacker* dapat menjadi beberapa penyebab risiko keamanan.

3.6. Kajian Literatur Risiko Sistem Manajemen Keamanan Informasi

Berikut ini merupakan ringkasan beberapa kajian literatur berdasarkan peneliti sebelumnya mengenai manajemen risiko dalam sistem keamanan informasi.

Identifikasi Risiko	Background	Metode	Hasil	Referensi
Terjadinya pencurian, penyalahgunaan sistem pada mesin ATM, dan kebocoran data.	*Cyber Security* dan ATM ***Studi case :*** Eropa	*Security Risk Assessment Methodology* SESAR (SecRAM), ISO/IEC 27005	Rekomendasi berupa dukungan alat, mendorong bekerja dalam tim, memperjelas penggunaan katalog, memperjelas klasifikasi mengenai informasi, menyelenggarakan pelatihan keamanan, meluncurkan SecRAM.	Bernsmed et. al, (2022)
Kerentanan terhadap keamanan sistem informasi perguruan tinggi karena bersifat terbuka.	Perguruan Tinggi **Studi case :** Uni Eropa, Norway, USA	*Fuzzy Logic,* ISO/IEC 27001	Mampu mengevaluasi sistem dan proses pengambilan keputusan dan memberikan gambaran yang tepat evaluasi risiko untuk mengelola keamanan Informasi Universitas	Sikman et. al, (2022)
Pelanggaran privasi, kegagalan integritas, gangguan aksesibilitas informasi, tim keamanan informasi tidak bisa menanggapi kebutuhan klien	Perusahaan Jasa Konsultan IT ***Studi case :*** Eropa	ISO 27000	Penerapan ISO 27000 akan berdampak dalam jangka menengah pada operasi bisnis sehari-hari, menghasilkan pengurangan beban kerja dan duplikasi upaya, dan optimalisasi tugas.	Kitsios et. al, (2022)
Adanya ancaman terhadap keamanan teknologi informasi.	Keamanan Arsitektur ***Studi case :*** Indonesia	ISO/IEC 27001	Peningkatan nilai rata-rata evaluasi kepatuhan ISO/IEC 27001 dari 36,27 menjadi 82,37 artinya terdapat pengaruh yang signifikan antara ancaman terhadap teknologi informasi sistem keamanan	Razikin dan Soewito (2022)

Terjadinya kebocoran data dan terjadi kerugian yang timbul dari peluang dan konsekuensi dalam proses bisnis keamanan informasi.	Keamanan informasi Perusahan Telekomunikasi ***Studi case :*** Indonesia	ISO 27005	Menghasilkan 26 skenario dampak untuk kategori peringkat tertinggi dan 12 skenario dampak sebagai prioritas utama. Hasil evaluasi risiko, perlu adanya pertimbangan untuk mendukung keamanan informasi, sehungga dapat digunakan untuk pengambilan keputusan perencanaan dan program kerja pengendalian risiko.	Putra, et al. (2020)
Ada insiden keamanan yang menurunkan tingkat layanan, kurangnya tinjauan audit / kontrol, penggunaan langkah-langkah perlindungan fisik dan teknologi terbatas, kurangnya pelatihan/pengembangan professional.	Keamanan pada sektor administrasi publik ***Studi case :*** Eropa	ISMS	Menghasilkan solusi Uni Eropa, yaitu Peraturan GDPR dan NIS Directive, telah mempengaruhi peningkatan tingkat keamanan informasi dalam administrasi publik dan secara signifikan membatasi terjadinya penyimpangan yang teridentifikasi. Hasil penelitian memungkinkan untuk mengasumsikan bahwa penyampaian keamanan informasi dalam administrasi publik memerlukan pendekatan sistemik yang timbul dari kebutuhan untuk perbaikan permanen.	Szczepaniuk et. al, (2020)
Layanan TI perguruan tinggi belum memenuhi persyaratan standar ISO 27001:2013.	Perguruan Tinggi ***Studi case :*** Indonesia	ISO/IEC 27001, *Indonesia's Information Security Index* (IISI)	Hasil penelitian digunakan untuk meningkatkan tata kelola organisasi terkait keamanan informasi pada suatu perguruan tinggi negeri sebagai lembaga pelayanan publik.	Yustanti et. al, (2018)
Banyak bank yang gagal untuk melindungi sistem informasinya, adanya *cyber-attack* (kecurian)	Bank ***Studi case :*** Eropa, Amerika Serikat	*Soft Systems Methodology* (SSM)	Hasilnya menunjukkan bahwa SSM efektif untuk menganalisis keamanan informasi yang rentan.	Damenu dan Chris (2017)
Banyak data yang diimplementasikan dengan cara yang tidak aman, sehingga mudah untuk ditembus (dicuri, disabotase / dirusak).	Keamanan informasi Perusahan Telekomunikasi ***Studi case :*** Indonesia	ISO 27002	Hasil penelitian menyatakan 87,72% tingkat kesesuaian hasil penilaian risiko dan 5,26% terjadinya kesalahan dampak kecil, 7,02% terjadinya kesalahan non-fatal dan 0% terjadinya kesalahan berbahaya dalam memberikan rekomendasi.	Shiwi et. al, (2017)
Keamanan yang rentan, sehingga sangat sulit untuk mewujudkan dan memastikan kepatuhan terhadap standar ISO 27001.	IT Company ***Studi case :*** Norway	ISMS- CORAS	CORAS diperlukan untuk menetapkan Sistem Manajemen Keamanan Informasi sesuai dengan standar. Penelitian ini mampu memvalidasi metode dengan menerapkannya ke skenario dari domain *smart grid*.	Beckers et. al, (2014)

4. CONCLUSION

Penelitian ini bertujuan untuk menjelaskan fitur bibliografi secara lengkap dari penelitian *Risk Management* dan *Information Security Management Systems* yang diterbitkan dalam jurnal terindeks Scopus oleh semua penulis di seluruh dunia. Studi mengenai *Risk Management* dan *Information Security Management Systems* dari tahun ke tahun mengalami peningkatan yang cukup pesat. Hal ini dapat ditunjukkan bahwa penelitian tersebut telah diakui secara luas oleh peneliti diseluruh dunia berdasarkan lembaga, jurnal dan negara tempat dokumen diterbitkan. Variasi lembaga, jurnal, dan negara juga menunjukkan keragaman topik yang dibahas *Risk Management dan Information Security Management Systems* sekitar 165 institusi, 200 jurnal, dan 87 negara yang terlibat dalam kajian *Risk Management* dan *Information Security Management Systems*. Universitas Norges Teknisk-Naturvitenskapelige merupakan institusi dengan jumlah publikasi yang signifikan, dengan total 28 dokumen. Kemudian, Negara Amerika Serikat mendominasi Negara yang teratas dalam publikasi dengan menempati 278 dokumen. Analisis *co-authorship* dalam hal penulis menunjukkan bahwa penulis dengan jumlah artikel tertinggi adalah Fenz, S. (18 dokumen) dengan jumlah kutipan 515, diikuti oleh Ahmad, A. (15 dokumen) dengan jumlah kutipan 273. Kemudian analisis *co–occurance* dari segi kata kunci menunjukkan 10 kata kunci teratas untuk *Risk Management* dan *Information Security* Management Systems dari tahun 1987 hingga 2023 adalah *information security, security risk management, risk analysis, information security management, risk modelling, information security management*, ISO 27005, *integrity, protection, information security governence, dan information tecchnology*.

5. REFERENCES

Alosaimi, R., & Alnuem, M. (2016). A survey on security risk management frameworks in cloud computing. *Computer Science and Information Technology*. 1-11. doi : 10.5121/csit.2016.60901

Beckers, K., Heisel, K., Solhaug, B., & Stolen, K. (2014). ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System. *Engineering Secure Future Internet Services and Systems. 8431*, 315-344. doi : 10.1007/978-3-319-07452-8_13

Bernsmed, K., Bour, G., Lundgren, M., & Erik Bergstrom. (2022). An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects. *Journal of Air Transport Management. 102* (3), 1-18. doi: 10.1016/j.jairtraman.2022.102223

Damenu, T. K., Chris, B. (2017). Analysing information security in a bank using soft systems methodology. *Information and Computer Security*. *25* (3), 240-258. doi : 10.1108/ICS-07-2016-0053

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research. 133,* 285-296. https://doi.org/10.1016/j.jbusres.2021.04.070

Ernst & Young. (2012). *Global Information Security Survey 2012: Fighting to Close the Gap*, EYGM Limited, EYG No. AU1889

Jadwani, B., Parkhi, S., & Mitra, P. K. (2024). Operational Risk Management in Banks: A Bibliometric Analysis and Opportunities for Future Research. *J. Risk Financial Manag. 17* (3). 95. doi: 10.3390/jrfm17030095

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability. 4* (2), 2-19. doi : 10.3390/su14031269

Korhan, O., & Ersoy, M. (2016). Usability and functionality factors of the social network site application users from the perspective of uses and gratification theory. *Quality and Quantity*. *50* (4), 1799– 1816. doi : 10.1007/s11135-015-0236-7

Lundgren, M. (2020). Rethinking capabilities in information security risk management: a systematic literature review. *International Journal Risk Assessment and Management. 23* (2), 169-190. doi : 10.1504/IJRAM.2020.106978

Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal. 28* (3), 383-404. doi: https://doi.org/10.1016/j.eij.2022.03.001

Shiwi, S., Andriyanto, F., & Anggrainingsih, R. (2016). An expert system for risk assessment of information system security based on ISO 27002. *IEEE International Conference on Knowledge Engineering and Applications.* 57-61. doi : 10.1109/ICKEA.2016.7802992

Putra, S. J., Gunawan, M. N., Sobri A. F., Muslimin, J.M., Amilin & Saepudin, D. (2020). **I**nformation Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company. *IEE (Institute of Electrical and Electronics Engineers),* doi : 10.1109/CITSM50537.2020.9268845

Sikman, L., Latinovic, T., &Sarajlic, N. (2022). Modelling of Fuzzy Expert System for an Assessment of Security Information Management System UIS (University Information System). Tehnicki Vjesnik. 22 (10), 60-65.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management, *MIS Quartely.* 34 (3), 503–522. doi : 10.2307/25750689

Szczepaniuk, K., Szczepaniuk, H., Rokicki, T., & Klepack, B. (2020). Information security assessment in public administration. *Computers and Security. 90* (10), 2-11. https://doi.org/10.1016/j.cose.2019.101709

Wangen. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*. *17*, 681-699. DOI:10.1007/s10207-017-0382-0

Yustanti, W., Qoiriah, A., Bisma, R., & Prihanto, A. (2018). An analysis of Indonesia's information security index: A case study in a public university. *IOP Conference Series: Material Science and Engineering. 296* (1), 1-7. doi : 10.1088/1757-899X/296/1/012038