Indonesian Journal of Digital Business

Journal homepage: https://ejournal.upi.edu/index.php/IJDB

Analisis Data Security Management Data Breach dan COBIT 2019 dengan Publish or Perish dan VOS Viewer

Salwa Syaravina Rachmnaiyah[1], Nisrina Salsabila[2], Risya Yurifia Putri[3], Vericha Aurel Salsabilla[4], Rizki Rahmawati[5]

[1,2,3,4,5] Department of Digital Business, Faculty of Economics, Universitas Negeri Surabaya, Jalan Ketintang, Surabaya 60231, Indonesia

Correspondence: E-mail: jdbmi@unesa.ac.id

ABSTRAK

Manajemen keamanan data terhadap pelanggaran data telah menjadi topik utama dalam bisnis yang dijalankan secara digital. Kerangka kerja COBIT 2019 telah menjadi pendekatan yang digunakan secara luas untuk mengelola keamanan data dalam organisasi, namun keamanan data serta respons terhadap pelanggaran data masih terbatas dalam analisis implementasi COBIT 2019. Studi ini menggunakan Publish or Perish dan VOS Viewer sebagai alat analisis literatur yang relevan tentang manajemen keamanan data, pelanggaran data, dan penggunaan COBIT 2019 yang berguna untuk memberikan pemahaman tentang topik bahasan ini. Sementara itu VOS Viewer digunakan untuk visualisasi dan analisis jaringan penelitian terkait topik ini

INFO ARTIKEL

Riwayat Artikel:
Received 11 Januari 2025
First Revised 13 Januari 2025
Accepted 18 April 2025
Available online 29 April 2025
Publication Date 30 April 2025

Kata Kunci:
manajemen keamanan data; pelanggaran data; COBIT 2019.

1. PENDAHULUAN

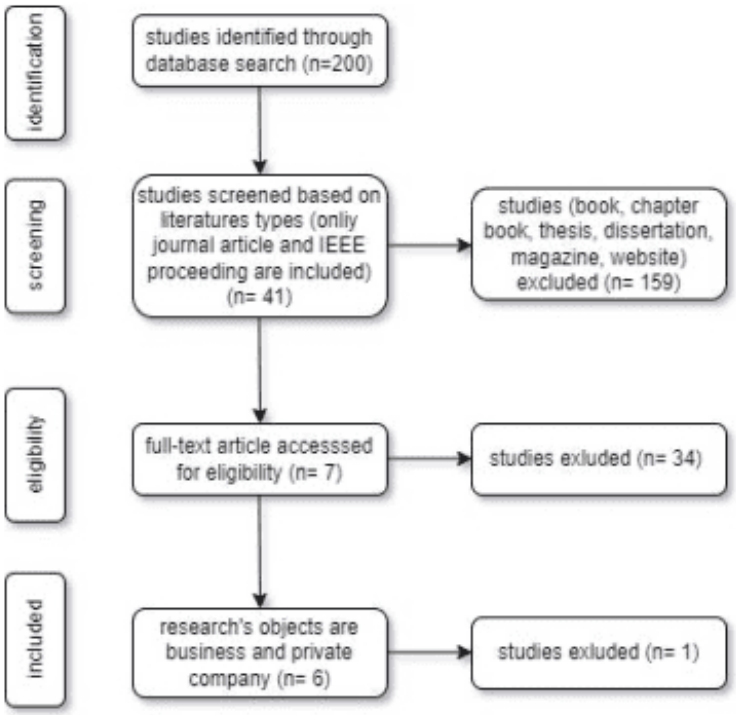
Pada era digital saat ini, teknologi informasi dan komunikasi telah semakin meluas, memungkinkan organisasi untuk mengelola data mereka dengan lebih efisien. Namun, penggunaan teknologi ini juga membawa risiko keamanan dan privasi yang perlu diatasi. Oleh karena itu, penting bagi organisasi untuk memiliki sistem keamanan yang kuat guna melindungi data mereka dari ancaman seperti kebocoran, penggunaan tidak sah, dan manipulasi.

Salah satu pendekatan untuk melindungi data adalah dengan mematuhi standar keamanan yang telah ditetapkan oleh regulasi dan standar industri. Tujuannya adalah agar organisasi memenuhi persyaratan keamanan yang ditetapkan oleh pihak yang berwenang dan menghindari risiko sanksi atas pelanggaran privasi dan keamanan data.

COBIT (Control Objectives for Information and Related Technology) adalah kerangka kerja manajemen TI yang digunakan oleh organisasi untuk memastikan keamanan dan privasi data mereka. COBIT mencakup prinsip-prinsip dan praktik manajemen TI, termasuk keamanan data, serta memberikan panduan tentang bagaimana organisasi dapat mematuhi persyaratan keamanan data dan mengurangi risiko keamanan.

2. METODE

PRISMA adalah panduan yang digunakan untuk melakukan penilaian terhadap sebuah systematic reviews dan atau meta analysis. PRISMA membantu para penulis dan peneliti dalam menyusun sebuah systematic review dan meta analysis yang berkualitas dengan langkah – langkah yang ditunjukkan dengan bagan sebagai berikut:

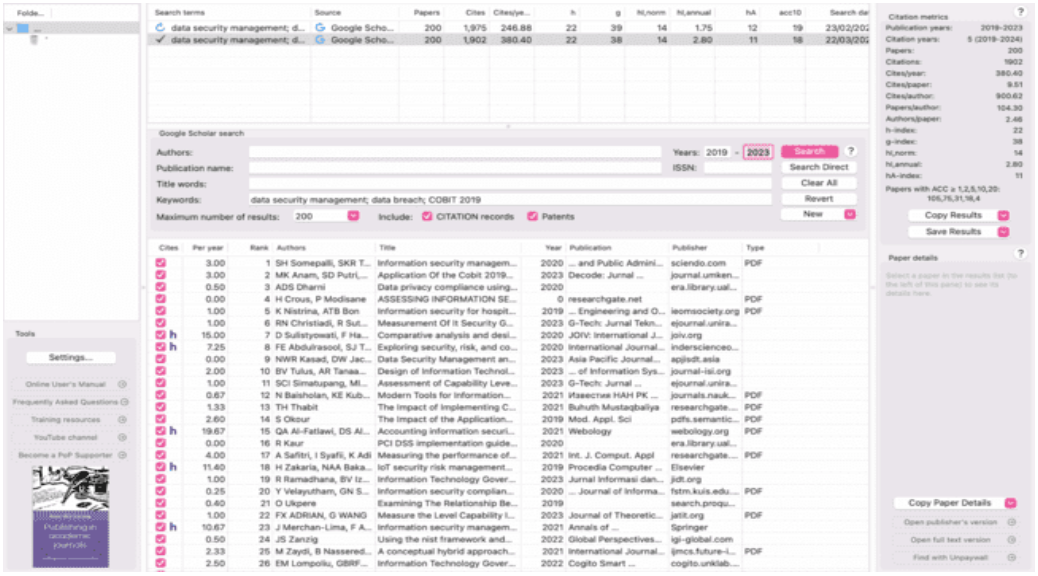


Gambar 1. Metode Penelitian PRISMA

3. HASIL DAN PEMBAHASAN

A. Analisis Data dengan Publish or Perish

Aplikasi Publish or Perish adalah software yang dapat membantu para peneliti menganalisis dan mengevaluasi publikasi ilmiah yang telah diterbitkan. Berikut ini merupakan hasil pencarian menggunakan Publish or Perish dengan keyword “data security management; data breach; COBIT 2019” pada 4 tahun terakhir yakni 2019 hingga 2023 dan terdapat 200 jurnal yang telah memiliki citation records dan patents.



Gambar 2. Analisis Data Publish or Perish

B. Analisis Data dengan VOSviewer

1. Network Visualization

Network Visualization merupakan visualisasi jejaring dari analisis data. Analisis yang kami lakukan menggunakan analisis normalization dengan metode association strength. Dari analisis yang kami lakukan terdapat warna yaitu merah, hijau, dan biru. Setiap warna mewakili masing – masing cluster seperti merah (cluster 1), hijau (cluster 2), dan biru (cluster 3). Hasil analisis dari 200 jurnal pada VOSviewer terdapat 14 item, 3 clusters, 75 links, dan 552 total links strength.

Tabel 1. Network Visualization

Cluster	Item
Cluster 1 (9 item)	1. Cobit 2. Framework 3. Security Management 4. Cobit Framework 5. Control 6. Information 7. Research 8. Information Technology 9. Risk
Cluster 2 (4 Item)	1. Information Security Managemen 2. Iso iec 3. Iso 4. Standard
Cluster 3 (1 Item)	1. Data

Berikut merupakan hasil keterhubungan artikel VOSviewers dari network visualization dimana banyak penelitian yang membahas mengenai cobit dan framework. Dari analisis yang kami lakukan masih sedikit penelitian yang membahas mengenai Security Management, Control, Information, research, information technology, risk, information security management, iso iec, iso, standard, data.

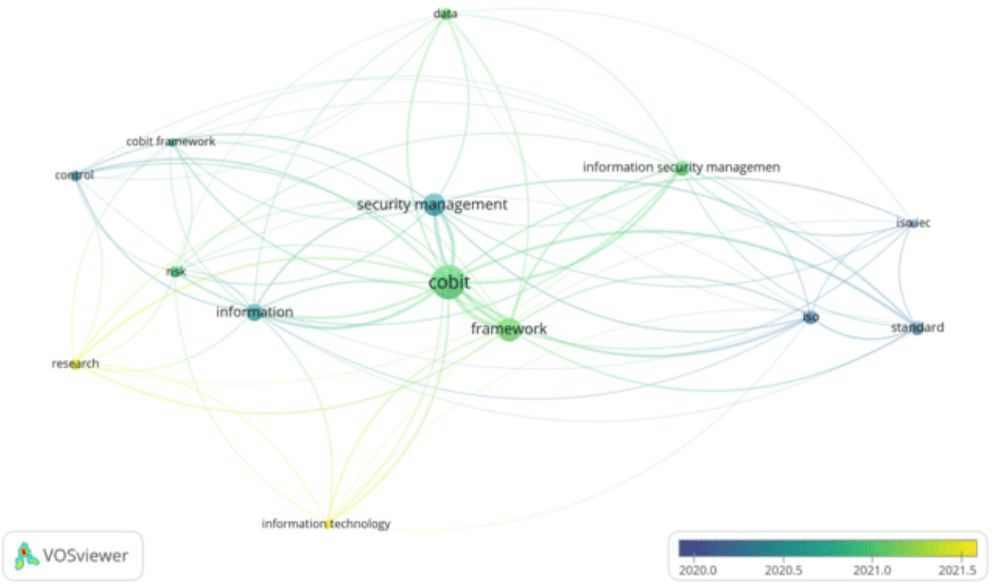
Gambar 3. Hasil keterhubungan artikel VOSviewers dari network visualization

2. Overlay Visualization

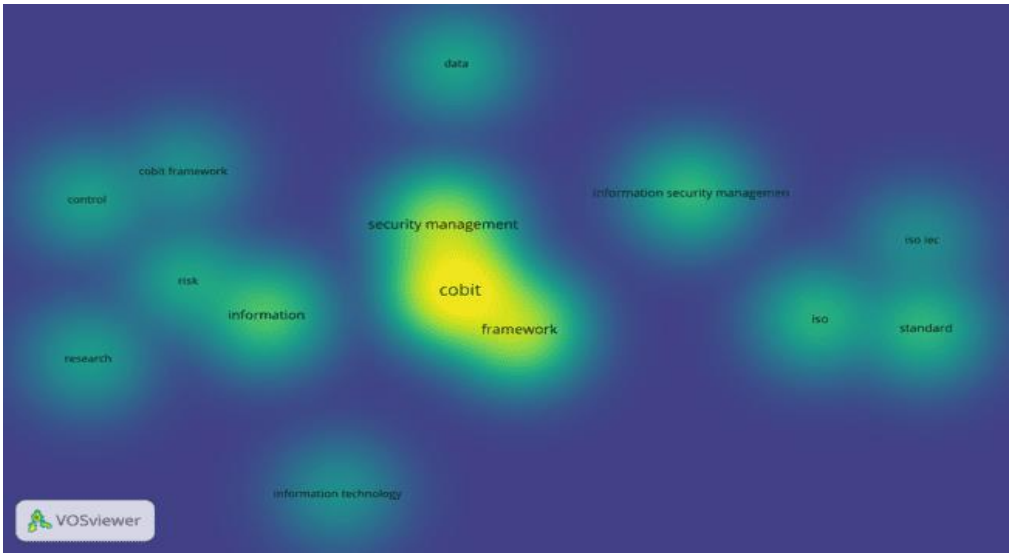
Overlay Visualization merupakan visualisasi dari rentang waktu penelitian yang telah dilakukan. Dari hasil analisis yang kami lakukan apabila warna item semakin ke kiri atau warna semakin gelap (mendekati warna ungu) maka publish dari penelitian tersebut sudah lama dilakukan dan apabila warna item semakin ke kanan atau warna semakin cerah maka publish dari penelitian tersebut masih baru dilakukan.Pada gambar dibawah terlihat bahwa penelitian yang membahas mengenai Research, Information Technology dipublish pada tahun 2021 keatas, lalu penelitian yang membahas mengenai Cobit, Framework, Information Security Management, Risk di publish pada tahun 2021, sementara penelitian yang membahas mengenai Security Management, Information, Cobit Framework, Control, Iso, Iso Iec, Standard di publish pada tahun 2020 kebawah.

3. Density Visualization

Density Visualization merupakan visualisasi mengenai kepadatan yang berkaitan dengan jumlah kemunculan. Kepadatan dapat dipengaruhi oleh item. Semakin warna tersebut terang (warna kuning) maka data tersebut semakin padat atau semakin sering istilah tersebut muncul dalam suatu dokumen. Dari hasil analisis kami dapat dilihat pada gambar dibawah terlihat bahwa istilah Cobit, Framework dan Security Management memiliki kepadatan atau istilah – istilah tersebut sering muncul dalam suatu dokumen.



Gambar 4. Overlay visualization



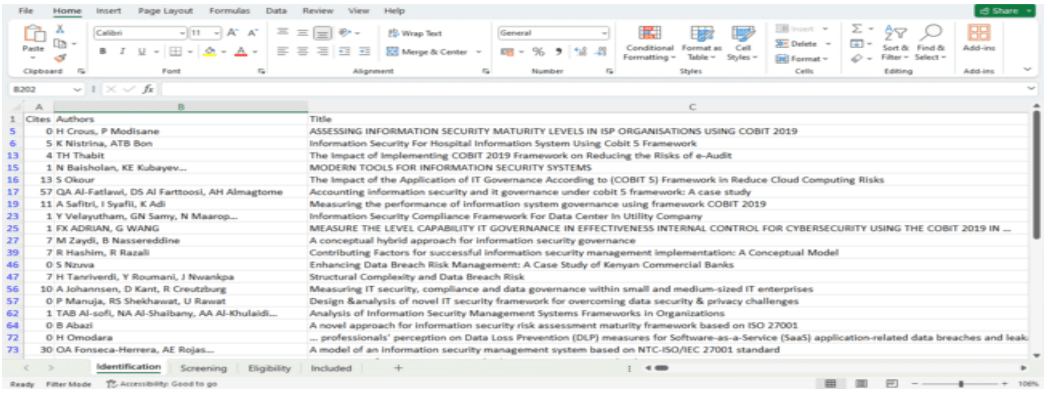
Gambar 5. Density visualization

Kepadatan dapat dipengaruhi oleh cluster. Dari hasil analisis kami yang telah kami lakukan dapat dilihat pada gambar dibawah terlihat bahwa masing – masing item sudah dikelompokkan berdasarkan clusternya. Cluster 1 terdiri atas Cobit, Framework, Security Management, Cobit Framework., Control, Information, Research, Information Technology, Risk. Cluster 2 terdiri atas information security management,Iso Iec, Iso, Standard.

C. Analisis Data Dengan Excel

Dari hasil pencarian menggunakan Publish or Perish dengan keyword “data security management ;data breach; cobit 2019” pada 4 tahun terakhir yakni 2019 hingga 2023 dan

terdapat 198 jurnal yang telah memiliki citation records dan patents. Kemudian dari 199 data jurnal tersebut kami lakukan identification dengan melakukan filter pada type dengan hanya memilih jurnal dengan tipe pdf. Setelah dilakukan identification maka diperoleh 39 data jurnal yang menggunakan tipe pdf.



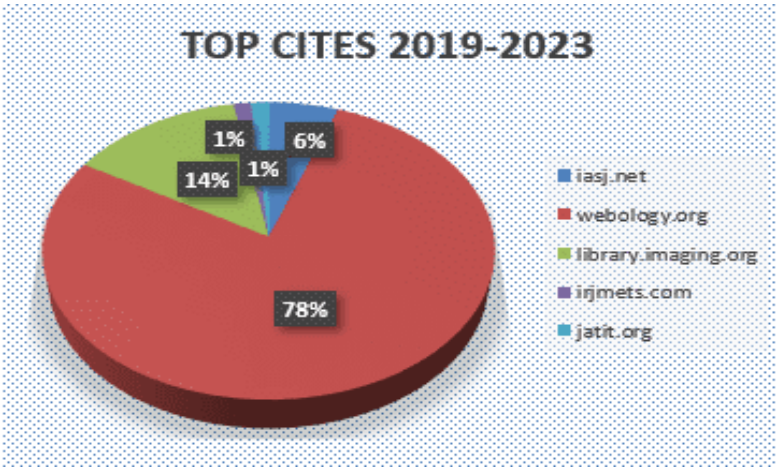
Cites	Authors	Title
0	H Crous, P Modisane	ASSESSING INFORMATION SECURITY MATURITY LEVELS IN ISP ORGANISATIONS USING COBIT 2019
5	K Nistrina, ATB Bon	Information Security For Hospital Information System Using Cobit 5 Framework
4	TH Thabit	The Impact of Implementing COBIT 2019 Framework on Reducing the Risks of e-Audit
1	N Baisholan, KE Kubayev...	MODERN TOOLS FOR INFORMATION SECURITY SYSTEMS
13	S Okour	The Impact of the Application of IT Governance According to (COBIT 5) Framework in Reduce Cloud Computing Risks
57	QA Al-Fatlawi, DS Al Farttoosi, AH Almagtome	Accounting information security and it governance under cobit 5 framework: A case study
11	A Safitri, I Syafii, K Adi	Measuring the performance of information system governance using framework COBIT 2019
1	Y Velayutham, GN Samy, N Maarop...	Information Security Compliance Framework For Data Center In Utility Company
1	FX ADRIAN, G WANG	MEASURE THE LEVEL CAPABILITY IT GOVERNANCE IN EFFECTIVENESS INTERNAL CONTROL FOR CYBERSECURITY USING THE COBIT 2019 IN ...
7	M Zaydi, B Nassereddine	A conceptual hybrid approach for information security governance
7	R Hashim, R Razali	Contributing Factors for successful information security management implementation: A Conceptual Model
0	S Nzuva	Enhancing Data Breach Risk Management: A Case Study of Kenyan Commercial Banks
7	H Tanriverdi, Y Roumani, J Nwankpa	Structural Complexity and Data Breach Risk
10	A Johannsen, D Kant, R Creutzburg	Measuring IT security, compliance and data governance within small and medium-sized IT enterprises
0	P Manuja, RS Shekhawat, U Rawat	Design &analysis of novel IT security framework for overcoming data security & privacy challenges
1	TAB Al-sofi, NA Al-Shalbany, AA Al-Khulaidi...	Analysis of Information Security Management Systems Frameworks in Organizations
0	B Abazi	A novel approach for information security risk assessment maturity framework based on ISO 27001
0	H Omodara	... professionals' perception on Data Loss Prevention (DLP) measures for Software-as-a-Service (SaaS) application-related data breaches and leak...
30	OA Fonseca-Herrera, AE Rojas...	A model of an information security management system based on NTC-ISO/IEC 27001 standard

Gambar 6. Analisis Excel

Tahap yang kedua yakni screening, setelah diperoleh 39 data jurnal yang menggunakan tipe pdf selanjutnya kami melakukan filter pada publisher dengan hanya memilih publisher yang credible sehingga setelah dilakukan proses screening diperoleh 21 data jurnal yang di publish oleh Lembaga yang credible.

Tahap yang ketiga yakni eligibility, setelah diperoleh 40 data jurnal yang di publish oleh Lembaga yang credible selanjutnya kami melakukan filter pada title jurnal yang sesuai dan berkaitan dengan keyword yang akan kami analisis sehingga diperoleh 21 data jurnal yang memiliki kesesuaian dengan topik yang akan kami analisis.

Berikut ini merupakan 5 data jurnal yang included dalam topik yang akan kami analisis, yaitu topik yang masih berkaitan dengan keyword "data security management ;data breach; cobit 2019" pada 4 tahun terakhir yakni 2019 hingga 2023 dimana publisher iasj.net sebanyak 4 cites dengan 14%, webologi.org sebanyak 57 cites dengan 78%, irjmets.com sebanyak 1 cites dengan 1%, jatit.org dengan 1 cites sebanyak 1%.



Gambar 7. Top Cites 2019-2023

HASIL

A. Pengertian COBIT

Control Objectives for Information and Related Technology (COBIT) adalah sebuah kerangka kerja tata kelola yang populer. COBIT adalah kerangka kerja governance TI yang komprehensif yang memberikan panduan kepada manajer TI dalam mengelola dan mengatur TI perusahaan. Makalah ini menyusun dan menganalisis penelitian yang ada tentang COBIT. Berdasarkan hasil analisis kami menunjukkan bahwa para peneliti telah mempelajari COBIT melalui beberapa perspektif dan sebagian besar makalah/jurnal fokus pada pengembangan/komparasi kerangka kerja secara keseluruhan atau area-area tertentu di dalam COBIT seperti keamanan, manajemen risiko, pengembangan sistem, efektivitas, dan pengendalian internal.

Analisis kami juga menunjukkan bahwa banyak makalah/jurnal yang diterbitkan berada pada domain akuntansi. Ruang lingkup COBIT telah meningkat selama beberapa tahun dan saat ini mencakup banyak area terkait IS. Oleh karena itu, saran untuk penelitian masa depan di bidang IS terkait COBIT juga diartikulasikan dalam studi ini. Kerangka kerja COBIT sering digunakan sebagai titik acuan oleh para profesional sistem informasi yang mencari pedoman mengenai pengelolaan TI di dalam sebuah organisasi. Misalnya, model kematangan COBIT dapat digunakan untuk menilai perkembangan proses pengelolaan di dalam sebuah organisasi.

Kerangka kerja COBIT juga dapat digunakan untuk memahami dan mengelola semua jenis risiko TI yang signifikan. Kerangka kerja ini juga menyediakan platform untuk bertukar pengalaman mengenai praktik terbaik pada suatu industri. Meskipun para CIO dapat melihat pandangan holistik yang diberikan oleh COBIT, karyawan garis depan dapat melihat detail terkait disiplin mereka masing – masing. Survei dari penelitian beberapa tahun lalu mengungkapkan arah dan kedalaman penelitian di dalam COBIT. Namun, sebagian besar penelitian dilakukan di area Akuntansi. Dari analisis yang kami lakukan, perlu lebih banyak penelitian IS tentang COBIT, sebuah kerangka kerja penting untuk mengatur dan mengelola TI di dalam organisasi.

B. Kontribusi COBIT 2019 Terhadap Manajemen Keamanan Data dan Pengelolaan Insiden Pelanggaran Data

COBIT 2019 memberikan kontribusi terhadap manajemen keamanan data dengan menyediakan kerangka kerja untuk menilai, mengarahkan, dan memantau TI dalam organisasi. Selain itu, COBIT 2019 juga membantu dalam pengelolaan insiden pelanggaran data dengan memungkinkan manajemen kinerja yang lebih fleksibel menggunakan pengukuran kematangan dan kemampuan.

COBIT 2019 berkontribusi terhadap manajemen keamanan data dan manajemen insiden pelanggaran data dengan memberikan pedoman pengendalian internal dan langkah-langkah keamanan siber yang efektif. Hal ini membantu organisasi memahami dan mengelola risiko TI yang signifikan, menyelaraskan tujuan bisnis dengan TI, dan meningkatkan produktivitas dengan menciptakan keselarasan yang kuat antara bisnis dan TI. COBIT 2019 juga menawarkan rekomendasi untuk manajemen insiden, analisis forensik keamanan siber, dan pengelolaan layanan keamanan untuk meningkatkan keamanan data dan merespons insiden pelanggaran data secara efektif.

C. Dampak Penggunaan COBIT 2019 Dalam Mengelola Kebocoran Data Terhadap Keamanan Informasi Organisasi

Penggunaan COBIT 2019 dalam mengelola kebocoran data dapat memberikan dampak positif pada keamanan informasi organisasi dengan memberikan pedoman pengendalian internal dan langkah-langkah keamanan siber yang efektif. COBIT 2019 membantu organisasi memahami dan mengelola risiko TI yang signifikan, menyelaraskan tujuan bisnis dengan TI, dan meningkatkan produktivitas dengan menciptakan keselarasan yang kuat antara bisnis dan TI

Dengan menerapkan COBIT 2019 dengan baik, organisasi dapat meningkatkan kemampuan mereka dalam mengelola kebocoran data, mengurangi risiko keamanan informasi, dan meningkatkan kepercayaan publik terhadap sistem kontrol internal dan eksternal. Berikut adalah detail mengenai bagaimana COBIT 2019 memberikan kerangka kerja yang komprehensif dalam hal manajemen keamanan data dan pengelolaan insiden pelanggaran data:

Menilai Risiko Keamanan Data: COBIT 2019 memberikan kerangka kerja untuk melakukan penilaian risiko terkait keamanan data. Ini mencakup identifikasi, evaluasi, dan penanganan risiko keamanan yang berpotensi mengancam data sensitif dan informasi penting organisasi. Dengan melakukan penilaian risiko yang komprehensif, organisasi dapat mengidentifikasi area-area yang rentan terhadap kebocoran data dan mengambil langkah-langkah proaktif untuk mengatasi risiko tersebut.

1. Mengarahkan Kebijakan Keamanan Data

COBIT 2019 membantu organisasi dalam mengarahkan kebijakan keamanan data yang sesuai dengan standar industri dan regulasi yang berlaku. Hal ini meliputi pengembangan kebijakan, prosedur, dan praktik terbaik yang bertujuan untuk melindungi data organisasi dari akses yang tidak sah, manipulasi, atau kebocoran. Dengan memiliki kebijakan yang jelas dan diterapkan dengan baik, organisasi dapat meningkatkan kontrol terhadap data dan mengurangi risiko pelanggaran data.

2. Memantau Insiden Pelanggaran Data

Kerangka kerja untuk memantau insiden pelanggaran data secara efektif. Ini meliputi deteksi, respons cepat, investigasi, dan tindakan perbaikan pasca-insiden. Dengan memantau insiden pelanggaran data secara teratur dan merespons dengan cepat, organisasi dapat mengurangi dampak negatif dari pelanggaran data, memulihkan data yang terpengaruh, dan mencegah kejadian serupa di masa depan.

3. Meningkatkan Kepercayaan Publik

Dengan menerapkan COBIT 2019 dengan baik, organisasi dapat meningkatkan kepercayaan publik terhadap sistem kontrol internal dan eksternal mereka terkait keamanan data. COBIT 2019 membantu organisasi dalam membangun transparansi, akuntabilitas, dan integritas dalam pengelolaan keamanan data. Hal ini dapat meningkatkan reputasi organisasi, memperkuat hubungan dengan pemangku kepentingan, dan menghasilkan kepercayaan yang lebih besar dari pengguna dan pelanggan terhadap perlindungan data mereka.

D. Analisis Data Menggunakan Publish or Perish Dalam Memahami Tren Penelitian Terkait Manajemen Keamanan Data dan COBIT 2019?

Analisis data menggunakan Publish or Perish dapat membantu dalam memahami tren penelitian terkait manajemen keamanan data dan COBIT 2019 dengan memberikan informasi tentang jumlah publikasi ilmiah, kutipan, dan kolaborasi peneliti dalam topik tersebut. Dengan menganalisis data ini, kita dapat melihat seberapa banyak penelitian yang telah dilakukan dalam bidang manajemen keamanan data dan implementasi COBIT 2019, serta tren penelitian yang sedang berkembang. Hal ini dapat membantu dalam mengevaluasi perkembangan dan fokus penelitian terkait topik tersebut, serta memberikan wawasan yang lebih dalam dalam hal keamanan data dan pengelolaan risiko TI.

Publish or Perish memberikan informasi tentang jumlah publikasi ilmiah yang berkaitan dengan manajemen keamanan data dan COBIT 2019. Ini termasuk artikel, makalah, dan buku yang telah dipublikasikan dalam jurnal-jurnal terkemuka atau forum ilmiah lainnya. Dengan mengetahui jumlah publikasi ini, kita dapat melihat seberapa aktifnya penelitian dalam bidang tersebut dan seberapa banyak informasi yang tersedia untuk dipelajari.Selain jumlah publikasi, Publish or Perish juga memberikan informasi tentang jumlah kutipan yang diterima oleh publikasi tersebut.

Kutipan menunjukkan seberapa sering publikasi tersebut dijadikan referensi atau acuan oleh peneliti lain dalam bidang yang sama atau terkait. Semakin tinggi jumlah kutipan, semakin relevan dan berpengaruh publikasi tersebut dalam konteks penelitian keamanan data dan implementasi COBIT 2019.Analisis data menggunakan Publish or Perish juga dapat memberikan gambaran tentang kolaborasi antara peneliti dalam topik manajemen keamanan data dan COBIT 2019. Informasi tentang kolaborasi ini meliputi nama-nama peneliti yang sering bekerja sama, institusi atau lembaga yang terlibat, serta jaringan kerja sama yang terbentuk dalam mengembangkan pengetahuan dan praktik terkait keamanan data dan pengelolaan risiko TI.Dengan menganalisis data yang tersedia melalui Publish or Perish, kita dapat melihat tren penelitian yang sedang berkembang dalam topik manajemen keamanan data dan COBIT 2019. Hal ini mencakup perubahan fokus penelitian, perkembangan metode atau teknologi baru, dan isu-isu terkini yang menjadi sorotan dalam komunitas penelitian.

E. Temuan Utama Dari Analisis Data Menggunakan Excel Terkait Manajemen Keamanan Data, Data Breach, dan Penerapan COBIT 2019 Dalam Praktik Organisasi

Temuan utama dari analisis data menggunakan Excel terkait manajemen keamanan data, data breach, dan penerapan COBIT 2019 dalam praktik organisasi adalah:

1. Adanya peningkatan kesadaran publik tentang pentingnya implementasi COBIT 2019 dalam mengelola keamanan data dan mengurangi risiko pelanggaran data. Analisis data menunjukkan adanya peningkatan kesadaran publik mengenai pentingnya implementasi COBIT 2019 dalam mengelola keamanan data dan mengurangi risiko pelanggaran data. Hal ini mencerminkan respons positif dari berbagai pihak terhadap kebutuhan akan kerangka kerja yang komprehensif dalam mengelola TI, terutama terkait dengan keamanan data.
2. Terdapat tingkat minat yang baik dari auditor dan akademisi dalam memantau perkembangan terbaru dalam tata kelola TI yang berkaitan dengan mengontrol kerahasiaan informasi dan penyimpanan data.

3. Implementasi e-audit melalui penerapan efisien COBIT 2019 dapat meningkatkan posisi profesi audit sebagai alat kontrol penting dan meningkatkan kepercayaan publik terhadap sistem kontrol internal dan eksternal.
4. Identifikasi tren insiden pelanggaran data dan dampaknya terhadap keamanan informasi organisasi.
5. Analisis efektivitas COBIT 2019 dalam mengelola keamanan data dan memitigasi risiko pelanggaran data dalam organisasi.
6. Evaluasi keselarasan antara praktik organisasi dan pedoman COBIT 2019 untuk meningkatkan manajemen keamanan data.

Temuan utama juga menyoroti bahwa implementasi e-audit melalui penerapan efisien COBIT 2019 dapat meningkatkan posisi profesi audit sebagai alat kontrol penting. Selain itu, hal ini juga dapat meningkatkan kepercayaan publik terhadap sistem kontrol internal dan eksternal yang digunakan oleh organisasi dalam mengelola keamanan data dan mengurangi risiko pelanggaran data. Dengan demikian, temuan utama tersebut memberikan gambaran bahwa COBIT 2019 memiliki dampak yang signifikan dalam praktik organisasi terkait manajemen keamanan data, data breach, dan proses audit. COBIT 2019 bukan hanya menjadi panduan penting bagi organisasi dalam mengelola risiko keamanan informasi, tetapi juga menjadi alat yang dihargai oleh auditor dan akademisi dalam mengawasi dan memantau kinerja organisasi dalam mengelola keamanan data secara efektif dan efisien.

4. KESIMPULAN

Analisis ini menunjukkan bahwa COBIT 2019 memiliki peran yang penting dalam manajemen keamanan data dan pengelolaan insiden pelanggaran data. Dengan menggunakan COBIT 2019, organisasi dapat meningkatkan kontrol terhadap data, mengurangi risiko pelanggaran data, dan meningkatkan kepercayaan publik terhadap sistem kontrol internal dan eksternal mereka. Temuan utama juga mencakup peningkatan kesadaran publik tentang pentingnya implementasi COBIT 2019, minat auditor dan akademisi dalam mengontrol kerahasiaan informasi, serta efektivitas COBIT 2019 dalam mengelola keamanan data. Profesi audit juga diidentifikasi sebagai elemen penting dalam mengontrol keamanan data dan mengurangi risiko pelanggaran data, dengan COBIT 2019 berperan sebagai panduan penting dalam proses tersebut. Referensi yang digunakan dalam penelitian ini mencakup berbagai studi tentang implementasi COBIT 2019 dan manajemen keamanan informasi.

7. REFERENSI

Adrian, F. X., & Wang, G. (2023). MEASURE THE LEVEL CAPABILITY IT GOVERNANCE IN EFFECTIVENESS INTERNAL CONTROL FOR CYBERSECURITY USING THE COBIT 2019 IN ORGANIZATION: BANKING COMPANY. Journal of Theoretical and Applied Information Technology, 15(5). www.jatit.org

Thabit, T. H. (2021). The Impact of Implementing COBIT 2019 Framework on Reducing the Risks of e-Audit. https://www.iasj.net/iasj/download/48792fe8bdb882af

Tariq A.Baqi Al-sofi, Dr.Nagi Ali Al-Shaibany, Dr.Abdualmajed Ahmed Al-Khulaidi, & Yasmeen Mohammed Almekhlafi. (2021, February 2). ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEMS FRAMEWORKS IN ORGANIZATIONS. IRJMETS - Low cost journal

with DOI |Rs. 599 publication fees |In 4 hr fast paper publication| Engineering, Scientific journal.https://www.irjmets.com/uploadedfiles/paper/volume3/issue_2_february_2021/6271/1628083262.pdf

Qayssar Ali Al-Fatlawi, Dawood Salman Al Farttoosi, & Akeel Hamza Almagtome. (2021, April). *Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study*. Webology. https://www.webology.org/data-cms/articles/20210429122040pmWEB18073.pdf

Andreas Johannsen, Daniel Kant, & Reiner Creutzburg. (2020). *Measuring IT security, compliance and data governance within small and medium-sized IT enterprises*. IS&T | Library. https://library.imaging.org/admin/apis/public/api/ist/website/downloadArticle/ei/32/3/art00005

Khechekhouche, A., Benhaoua, B., Manokar, M., Sathyamurthy, R., and Driss, Z. (2020). Sand dunes effect on the productivity of a single slope solar distiller. *Heat and Mass Transfer*, *56*(4), 1117-1126.

Khechekhouche, A., Benhaoua, B., Driss, Z.., Attia, M. E. H., and Manokar, M. (2020 A). polluted groundwater treatment in southeastern algeria by solar distillation. *Algerian Journal of Environmental and Sciences*, *6*(1).1207-1211.

Khechekhouche, A., Bouchmel, F., Kaddour, Z., Salim, K., and Miloudi, A. (2020 C). Performance of a wastewater treatment plant in south-eastern Algeria. *International journal of Energetica*, *5*(2), 47-51.

Belbahloul, M., Abdeljalil, Z., and Abdellah, A. (2014). Comparison of the efficacy of two bioflocculants in water treatment. *International Journal of Scientific Engineering and Technology*. *3*(6), 734-737.

Behera, B., and Sethi, N. (2020). Analysis of household access to drinking water, sanitation, and waste disposal services in urban areas of Nepal. *Utilities Policy*, *62*(2020), 100996.

Heba, A., Eman, S. M. (2020). Co-sensitization of mesoporous ZnS with CdS and polyaniline for efficient photocatalytic degradation of anionic and cationic dyes. *Colloid and Interface Science Communications, 39*(2020), 100330.

Bencheikh, I, Azoulay, K., Mabrouki, J., Hajjaji, S. E., Moufti, A., and Labjar, N. (2021). The use and the performance of chemically treated artichoke leaves for textile industrial effluents treatment. *Chemical Data Collections*, *31*(2021), 100597.

Stewart, E. J. (2012). Growing unculturable bacteria. *Journal of bacteriology*, *194*(16), 4151-4160.

Kim, Y. K., Yoo, K., Kim, M. S., Han, I., Lee, M., Kang, B. R., and Park, J. (2019). The capacity of wastewater treatment plants drives bacterial community structure and its assembly. *Scientific Reports*, *9*(1), 1-9.

Sadasivuni, K. K., Panchal, H., Awasthi, A., Israr, M., Essa, F. A., Shanmugan, S., and Khechekhouche, A. (2020). Ground water treatment using solar radiation-vaporization

and condensation-techniques by solar desalination system. *International Journal of Ambient Energy*, 1-7 (*Accepted Manuscript*).