JDBIM
(Journal of Digital Business and Innovation Management)

Volume 2, Issue 1, Juni 2023, 17-33
ISSN (Online): **2962-3898**
DOI: 10.1234/jdbim.v2i1.53366
https://ejournal.unesa.ac.id/index.php/jdbim

ANALISIS IMPLEMENTASI *DATA SECURITY, INTENTION FOR COMPLIANCE*, DAN KERANGKA COBIT DI PERUSAHAAN: TINJAUAN LITERATUR SISTEMATIS

Fadia Nur Rohmah[1]*, Siska Erliana [2], Abyan Haq 'Aisy Su'udi[3], Mohammad Masdarul Asrar[4]
[12345]Universitas Negeri Surabaya

Abstract

One way to protect organizational data is to comply with security standards set by regulations and industry standards. The purpose of this compliance is to ensure that the organization meets the security requirements set by the competent authorities and avoids the risk of penalties or sanctions for breaches of privacy and data security. COBIT (Control Objectives for Information and Related Technology) is an IT management framework used by organizations to ensure that data security and privacy are well maintained. The purpose of this research is to find out the forms of implementation of data security management, intention for compliance with the COBIT framework in companies over the last 10 years. This research is expected to provide a scientific contribution to the direction of research in the field of data security management and provide managerial contributions regarding the urgency and challenges of COBIT implementation as part of good IT governance.

Keywords: *data security, COBIT, intention for compliance, IT governance*.

Received: 24 Mei 2023; Accepted: 24 Juni 2023; Published: 30 Juni 2023.

*Corresponding author
Email: fadia.21049@mhs.unesa.ac.id

Abstrak

Salah satu cara untuk melindungi data organisasi adalah dengan mematuhi standar keamanan yang telah ditetapkan oleh regulasi dan standar industri. Tujuan dari kepatuhan ini adalah untuk memastikan bahwa organisasi telah memenuhi persyaratan keamanan yang ditetapkan oleh pihak yang berwenang dan menghindari risiko hukuman atau sanksi atas pelanggaran privasi dan keamanan data. COBIT (Control Objectives for Information and

To cite this document:
Nur Rohmah, Fadia., Erliana, Siska., Haq 'Aisy Su'udi, Abyan., Asrar, Mohammad Masdarul. Analisis Implementasi *Data Security, Intention For Compliance*, dan Kerangka Cobit di Perusahaan: Tinjauan Literatur Sistematis. *JDBIM (Journal of Digital Business and Innovation Management)*

JDBIM (Journal of Digital Business and Innovation Management)
Volume 2 Issue 1, Juni 2023
E-ISSN: **2962-3898**
Page 17-33

Related Technology) adalah kerangka kerja manajemen TI yang digunakan oleh organisasi untuk memastikan bahwa keamanan dan privasi data dijaga dengan baik. Tujua dari penelitian ini adalah untuk mengetahui bentuk-bentuk implementasi manajemen pengamanan data, intention for compliance dengan kerangka COBIT di perusahaan selama 10 tahun terakhir. Penelitian ini diharapkan dapat memberikan sumbangsih keilmuan terhadap arah penelitian di bidang manajemen keamanan data dan memberikan sumbangsih manajerial tentang urgensi dan tantangan implementasi COBIT sebagai bagian dari *good IT governance*.
***Kata kunci**: data security, COBIT, intention for compliance, tata keloloa TI*.

PENDAHULUAN

Dalam era digital saat ini, penggunaan teknologi informasi dan komunikasi semakin meluas dan memungkinkan organisasi untuk mengumpulkan, menyimpan, dan memproses data dengan lebih efisien. Namun, pengumpulan dan pengolahan data juga meningkatkan risiko keamanan informasi dan privasi yang berkaitan dengan kebocoran, penggunaan yang tidak sah, dan manipulasi data. Oleh karena itu, organisasi harus memastikan bahwa mereka memiliki sistem keamanan yang kuat untuk melindungi data mereka dari serangan dan pelanggaran keamanan (Andry & Hartono, 2017).

Salah satu cara untuk melindungi data organisasi adalah dengan mematuhi standar keamanan yang telah ditetapkan oleh regulasi dan standar industri. Tujuan dari kepatuhan ini adalah untuk memastikan bahwa organisasi telah memenuhi persyaratan keamanan yang ditetapkan oleh pihak yang berwenang dan menghindari risiko hukuman atau sanksi atas pelanggaran privasi dan keamanan data (Berrada dkk, 2021).

COBIT (Control Objectives for Information and Related Technology) adalah kerangka kerja manajemen TI yang digunakan oleh organisasi untuk memastikan bahwa keamanan dan privasi data dijaga dengan baik. COBIT mencakup berbagai prinsip dan praktik manajemen TI, termasuk keamanan data. COBIT memberikan panduan tentang bagaimana organisasi dapat memastikan bahwa mereka mematuhi persyaratan keamanan data dan meminimalkan risiko keamanan (Bunnel & Weistroffer, 2017).

Penelitian ini membahas tentang data security dan tujuan kepatuhan terhadap regulasi keamanan data, dengan fokus pada kerangka kerja COBIT. Beberapa kata kunci(keyword) yang digunakan adalah "data security" yaitu keamanan data yang meliputi konsep dan teknologi yang digunakan untuk melindungi data dari akses yang tidak sah, penggunaan yang tidak diizinkan, dan manipulasi data (Deysel, 2011); "intention for compliance" yaitu tujuan dari kepatuhan untuk memastikan bahwa organisasi memenuhi persyaratan keamanan yang ditetapkan oleh pihak

berwenang (Berrada dkk, 2021), dan "Cobit" yaitu kerangka kerja manajemen TI yang membahas berbagai prinsip dan praktik manajemen TI, termasuk keamanan data (Bruzza dkk, 2017).

Kerangka COBIT dalam Tata Kelola TI Perusahaan

Control Objectives for Information and Related Technology (COBIT) adalah sebuah kerangka kerja tata kelola yang komprehensif untuk memberikan panduan kepada manajer teknologi informasi dalam mengelola dan mengatur TI perusahaan (Mishra & Weistroffer, 2007). Berdasarkan hasil analisis 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 (Kam dkk, 2016). Analisis artikel ini juga menunjukkan bahwa artikel yang diterbitkan berada pada domain akuntansi. Namun, ruang lingkup COBIT telah meningkat selama beberapa tahun dan saat ini mencakup banyak area terkait IS (Gehrmann, 2012).

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 (maturity model) COBIT dapat digunakan untuk menilai perkembangan proses pengelolaan sumber daya teknologi informasi 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 di industri (Deysel, 2011).

Pengelolaan Teknologi Informasi dengan Cobit 5

Teknologi informasi (TI) merupakan bagian yang sangat penting bagi perusahaan atau institusi dan nilai investasi untuk membuat perusahaan atau institusi menjadi lebih baik. Perusahaan atau institusi menggunakan teknologi informasi untuk mendukung rencana strategis perusahaan dalam mencapai visi, misi, dan tujuan perusahaan atau institusi. Penerapan teknologi informasi di perusahaan atau institusi perlu diatur. Pengelolaan teknologi informasi memerlukan audit untuk mengevaluasi dan memastikan kepatuhan dalam hal pendekatan standar. Kerangka kerja

JDBIM (Journal of Digital Business and Innovation Management)
Volume 2 Issue 1, Juni 2023
E-ISSN: **2962-3898**
Page 17-33

COBIT 5 digunakan untuk audit, yang berfokus pada tujuan pengiriman layanan TI sesuai dengan kebutuhan bisnis (Bruzza dkk, 2017).

COBIT (Control Objectives for Information and Related Technology) adalah seperangkat dokumen dan panduan yang mengarahkan Tata Kelola TI dan Manajemen TI yang dapat membantu auditor, manajemen, dan pengguna (user) untuk menjembatani kesenjangan antara risiko bisnis, kebutuhan kontrol, dan masalah teknis. COBIT dikembangkan oleh institusi TI Institute Governance (ITGI), yang merupakan bagian dari Asosiasi Sistem Informasi dan Kontrol (ISACA). Pada versi COBIT 5, terdapat lima (5) prinsip utama dari tata kelola dan manajemen perusahaan TI (Andry & Hartono, 2017)

Evaluate, Direct and Monitor (EDM). Domain ini bertanggung jawab untuk memastikan bahwa strategi dan tujuan TI sejalan dengan tujuan bisnis. Hal ini juga mencakup pemantauan dan evaluasi kinerja proses dan layanan TI, serta memastikan kepatuhan terhadap persyaratan regulasi dan hukum.

Align, Plan and Organize (APO). Domain ini bertanggung jawab untuk menyelaraskan TI dengan kebutuhan bisnis, merencanakan dan mengorganisir sumber daya TI, serta memastikan bahwa proses dan layanan TI dirancang untuk memenuhi tujuan bisnis.

Build, Acquire and Implement (BAI). Domain ini bertanggung jawab untuk membangun dan mengimplementasikan solusi TI yang memenuhi persyaratan bisnis, mengelola perubahan pada proses dan layanan TI, serta memastikan bahwa proyek TI disampaikan tepat waktu, dalam anggaran, dan dengan kualitas yang dibutuhkan.

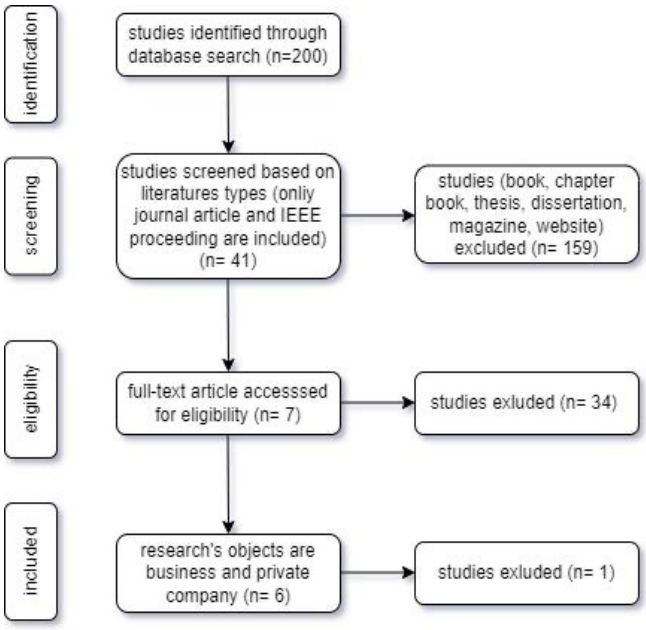
Deliver, Service and Support (DSS). Domain ini bertanggung jawab untuk menyampaikan dan mendukung layanan TI, mengelola operasi TI, serta memastikan bahwa layanan TI memenuhi kebutuhan dan harapan bisnis.

Monitor, Evaluate and Assess (MEA). Domain ini bertanggung jawab untuk memantau dan mengevaluasi kinerja proses dan layanan TI, menilai efektivitas tata kelola dan manajemen TI, serta memastikan peningkatan yang berkelanjutan. Setiap domain terdiri dari serangkaian proses, yang dijelaskan secara rinci dalam kerangka kerja COBIT 5. Proses-proses ini memberikan pemahaman yang jelas tentang aktivitas yang perlu dilakukan untuk mencapai tata kelola dan manajemen TI yang efektif. Sehingga artikel ini bertujuan untuk mengeksplorasi tentang 1) pengelolaan teknologi

informasi dengan Cobit 5; 2) integrasi Cobit 5 dengan SDLC dan pengembangan atestasi akses pengguna dan 3) praktik organisasi dalam pendidikan tinggi dan industri perbankan dengan IT governance (ITG), berdasarkan literatur yang selama 10 tahun terakhir (2012-2022) pada Scopus Database.

METODE

Metode penelitian adalah penelitian kualitatif dengan pendekatan studi literatur (PRISMA). 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:



Bagan 1 Kerangka Metode dengan PRISMA

HASIL

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; intention for compliance; cobit" pada 10 tahun terakhir yakni 2011 hingga 2022 dan terdapat 200 jurnal yang telah memiliki citation records dan patents.

JDBIM (Journal of Digital Business and Innovation Management)
Volume 2 Issue 1, Juni 2023
E-ISSN: **2962-3898**
Page 17-33

Analisis Data dengan VOSviewer

a. *Network Visualization*

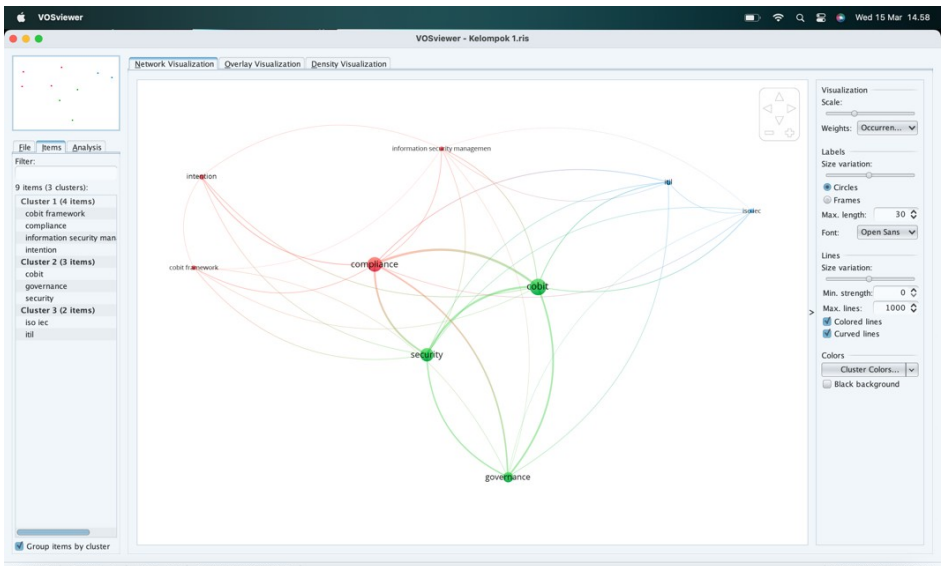
Network Visualization merupakan visualisasi jejaring dari analisis data. Analisis yang artikel ini lakukan menggunakan analisis normalization dengan metode association strength. Dari analisis yang artikel ini lakukan terdapat 3 warna yaitu merah, hijau, dan biru. Setiap warna mewakili masing – masing cluster seperti merah (cluster 1), hijau (cluster 2), dan biru (cluster 3). Dari analisis yang artikel ini lakukan tidak ada item yang masuk ke dalam 2 cluster secara bersamaan. Hasil analisis dari 200 jurnal pada VOSviewer terdapat *9 item, 3 clusters, 31 links*, dan *total links strength 518*.

Berikut merupakan hasil keterhubungan artikel VOSviewers dari network visualizaition dimana banyak penelitian yang membahas mengenai cobit, compliance, security, dan governance. Dari analisis yang artikel ini lakukan masih sedikit penelitian yang membahas mengenai cobit framework, information security management, ISO, IEC dan ITIL.

Tabel 1 Klusterisasi Artikel Berdasarkan VosViewer

Cluster	Item
Kluster 1 (4 items)	1) Cobit framework 2) Compliance 3) Information Security Management 4) Intention
Kluster 2 (3 items)	1) Cobit 2) Governance 3) Security
Kluster 3 (2 items)	1) ISO IEC 2) ITIL

Gambar 1 Network Visualization

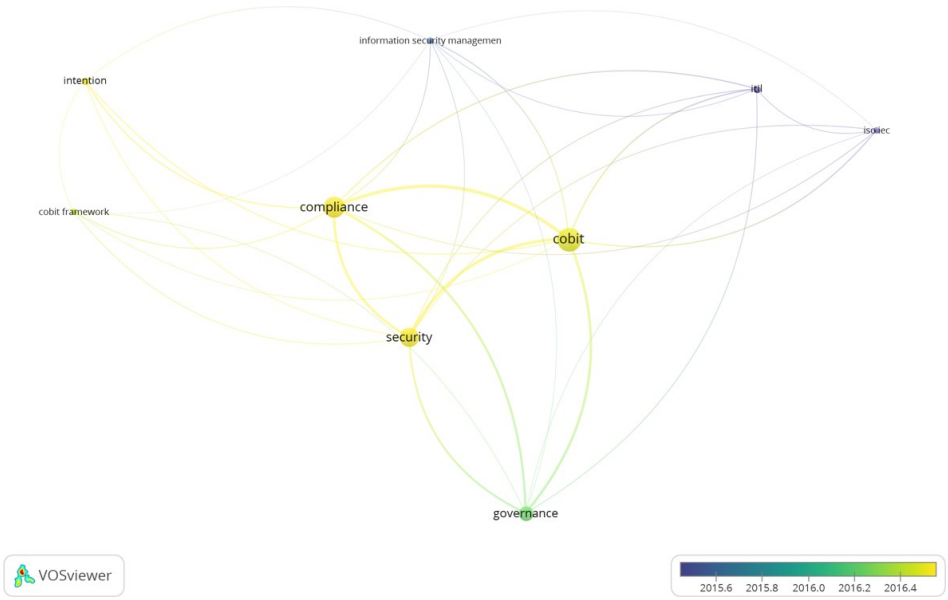


b. Overlay Visualization

Overlay Visualization merupakan visualisasi dari rentang waktu penelitian yang telah dilakukan. Dari hasil analisis yang artikel ini 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 cobit, *compliance, security, intention,* dan *cobit framework* diterbitkan pada tahun 2016 ke atas, lalu penelitian yang membahas mengenai governance diterbitkan pada tahun 2016, sementara penelitian yang membahas mengenai *information security management*, ITIL, ISO dan IEC yang diterbitkan pada tahun 2015 ke bawah.

Gambar 2 Network Visualization

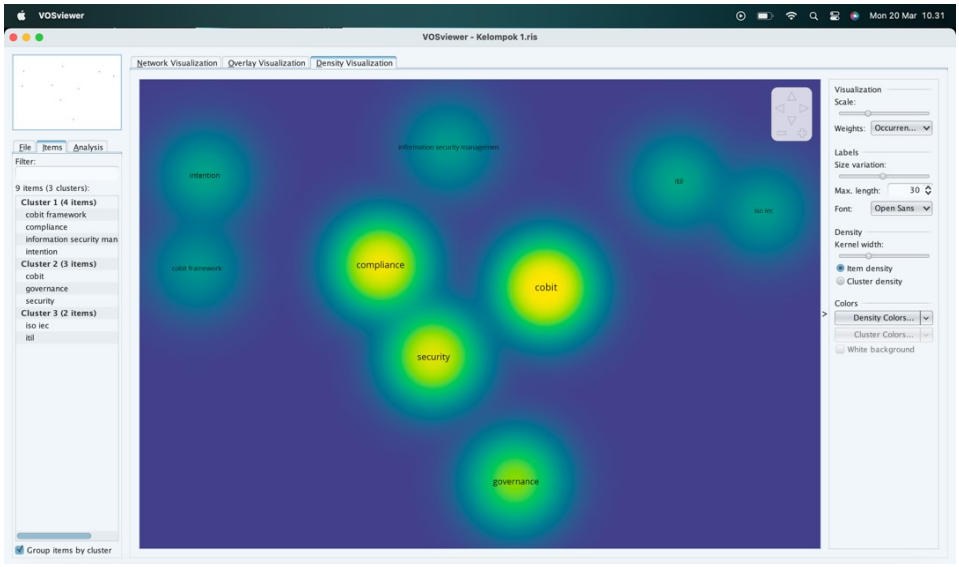
JDBIM (Journal of Digital Business and Innovation Management)
Volume 2 Issue 1, Juni 2023
E-ISSN: **2962-3898**
Page 17-33



Gambar 2 Overlay Visualization

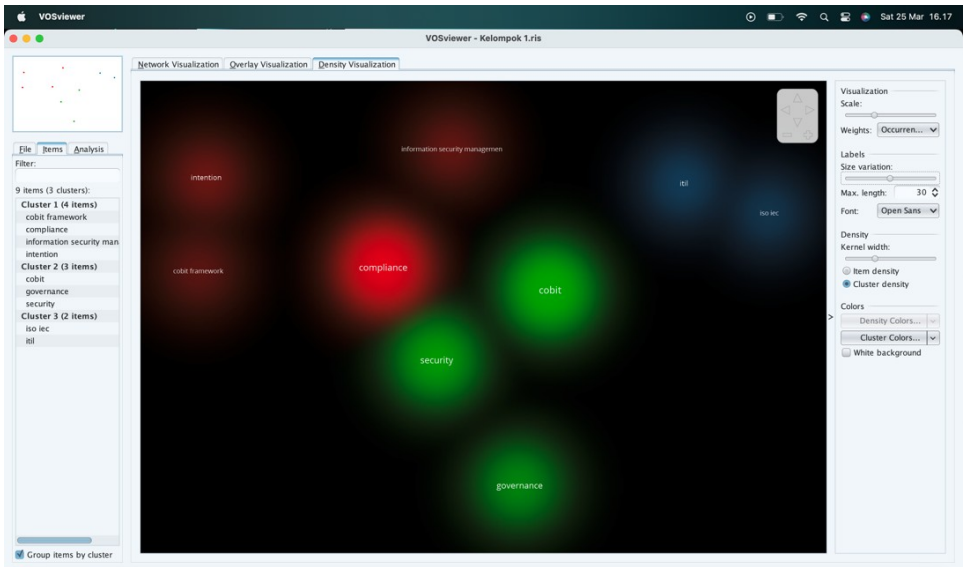
c. *Density Visualization*

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 artikel ini dapat dilihat pada gambar dibawah terlihat bahwa istilah *cobit, compliance, security*, dan *governance* memiliki kepadatan atau istilah – istilah tersebut sering muncul dalam suatu dokumen. Kepadatan dapat dipengaruhi oleh *cluster*. Dari hasil analisis artikel ini yang telah artikel ini lakukan dapat dilihat pada gambar dibawah terlihat bahwa masing – masing item sudah dikelompokkan berdasarkan clusternya. Cluster 1 terdiri atas *compliance, cobit framework, intention*, dan *information security management* lalu Cluster 2 terdiri atas *cobit, security*, dan governance, sementara Cluster 3 terdiri atas ITIL, ISO, dan IEC.



Gambar 3 Density Visualization

Kepadatan dapat dipengaruhi oleh cluster. Dari hasil analisis artikel ini yangtelah artikel ini lakukan dapat dilihat pada gambar dibawah terlihat bahwa masing–masing item sudah dikelompokkan berdasarkan clusternya. Cluster 1 terdiri atas *compliance, cobit framework, intention,* dan *information security management* lalu Cluster 2 terdiri atas *cobit, security*, dan *governance*, sementara Cluster 3 terdiri atas ITIL, ISO, IEC.



Gambar 4 Density Visualization by Cluster

Analisis Data dengan Excel

Dari hasil pencarian menggunakan Publish or Perish dengan keyword "data security; intention for compliance; cobit" pada 10 tahun terakhir yakni 2012 hingga 2022 dan terdapat 200 artikel yang telah memiliki *citation records* dan *patents*. Kemudian dari 200 data artikel tersebut, dilakukan identification dengan melakukan filter pada tipe file dengan hanya memilih jurnal *open access* dengan format pdf. Setelah dilakukan *identification* maka diperoleh 41 data artikel yang menggunakan tipe pdf. Selanjutnya adalah *screening* terhadap 41 artikel dengan hanya memilih publisher terindeks Scopus sehingga diperoleh 7 data jurnal. Tahap yang ketiga yakni *eligibility*, filter pada title jurnal yang sesuai dan berkaitan dengan kata kunci yang analisis sehingga diperoleh 6 artikel yang memiliki kesesuaian dengan topik.

PEMBAHASAN

Integrasi Cobit 5 dengan SDLC dan Pengembangan Atestasi Akses Pengguna

Seiring dengan meningkatnya pengawasan hukum dan regulasi yang dihadapi oleh organisasi karena undang-undang seperti SOX dan HIPPA, pengendalian teknologi informasi (TI) telah menjadi fokus kritis. Oleh karena itu, sangat penting bagi departemen yang bertanggung jawab atas tata kelola TI untuk memperhatikan secara khusus pengguna mana yang dapat memulai, mengotorisasi, memproses, menyimpan, dan melaporkan transaksi. Atestasi akses pengguna berkala, yang mengotorisasi penggunaan karyawan yang sesuai dengan artefak TI, adalah cara untuk memastikan bahwa pengendalian yang tepat dijaga. Aplikasi yang efisien biaya untuk mendukung pengelolaan akses pengguna TI yang sesuai diperlukan untuk memastikan kepatuhan regulasi. Sehingga COBIT diperlukan untuk memetakan siklus hidup pengembangan sistem (SDLC) untuk mengembangkan sistem atestasi akses pengguna menggunakan alat-alat in-house yang tersedia secara luas (Almuhammadi & Alsaleh, 2017).

Pada analisis di bidang tata kelola TI khususnya terkait pengembangan sistem, dengan memperkenalkan pendekatan yang efisien dalam hal waktu, sumber daya, dan biaya untuk mengembangkan sistem Atestasi Akses Pengguna (AtTest) dengan menggunakan alat pengembangan perangkat lunak yang tersedia luas.

Kerangka kerja COBIT 5 dapat diintegrasikan ke dalam SDLC dan menggambarkan tindakan penilaian COBIT 5 untuk memastikan ketaatan terhadap prinsip tata kelola TI dan kepatuhan peraturan. Alur kerja SDLC ke pemetaan COBIT 5 yang diperkenalkan oleh Mishra dan Weistroffer ke dalam kerangka kerja COBIT 5 baru dan menyediakan kerangka kerja bagi pengembang sistem untuk menggabungkan kontrol tata kelola TI dengan menggunakan pendekatan pengembangan yang beragam untuk sistem yang terkena masalah kepatuhan perundang-undangan dan peraturan (Mishra & Wesitroffer, 2007). Tujuan bisnis tidak dapat dinilai dengan sistem prototipe, tetapi implementasi penuh perencenaan dan penelitian lebih lanjut akan dapat menentukan apakah penggunaan sistem mencapai tujuan dan metrik serta mencapai penilaian prestasi model kemampuan proses COBIT 5 yang sepenuhnya tercapai.

Keamanan Informasi dengan COBIT

Organisasi semakin bergantung pada informasi mereka. Kompromi terhadap informasi ini dalam hal kehilangan, ketidaktepatan, atau akses yang tidak sah oleh pesaing dapat memiliki konsekuensi yang sangat merugikan bagi organisasi. Oleh karena itu, tata kelola keamanan informasi telah menjadi kekhawatiran utama bagi semua organisasi, besar maupun kecil. Tata kelola keamanan informasi didasarkan pada seperangkat kebijakan dan kontrol internal yang digunakan organisasi untuk mengarahkan dan mengelola keamanan informasinya. Program tata kelola keamanan informasi yang efektif harus didasarkan pada kerangka kerja yang diakui, seperti Control Objectives for Information and related Technology (COBIT). COBIT berfokus pada objektif kontrol apa yang harus dicapai untuk mengelola lingkungan teknologi informasi dengan efektif. Berdasarkan penelitian terdahulu, mayoritas organisasi menengah tidak menyadari pentingnya tata kelola keamanan informasi dan menyadari risikonya atau memilih untuk mengabaikan risiko tersebut karena mereka tidak memiliki keahlian atau sumber daya yang tersedia untuk memberikan jaminan bahwa perusahaan memiliki kontrol keamanan informasi yang tepat untuk melindungi organisasi mereka dari ancaman (Bicaku dkk, 2020; Budiarta dkk, 2016; Dunner & Weistroffer, 2017; Ukdive dkk, 2017; Ula dkk, 2011; Motii & Semma, 2017).

Audit TI menambahkan keamanan, keandalan, dan ketepatan pada sistem informasi yang integral bagi kehidupan manusia. Tanpa audit TI, tidak mungkin untuk berbelanja secara aman di internet atau mengontrol

identitas. Peran auditor TI mungkin tidak diketahui oleh kebanyakan orang tetapi hal ini berdampak pada kehidupan setiap orang. Namun, audit ini perlu didasarkan pada standar atau kerangka kerja yang sudah dikembangkan, yang dikenal oleh banyak organisasi. Kontrol terperinci dalam kerangka kerja COBIT mengatasi 'apa' yang harus dilakukan. Kontrol keamanan informasi mengatur aset – aset tersebut dan lapisan audit keamanan informasi memastikan kontrol yang tepat diterapkan (Bruzza dkk, 2017).

Proses keamanan informasi yang termasuk dalam model tersebut didukung oleh ISCAT (Information Security Control Audit Tool). Alat audit digunakan pertama kali untuk mengevaluasi status terkini organisasi. Selanjutnya, organisasi harus meninjau semua tanda peringatan yang diidentifikasi oleh alat audit dan mengembangkan serta menerapkan rencana tindakan untuk menyelesaikan masalah di area–area tersebut. Organisasi kemudian mengulang kembali melalui langkah–langkah ini sampai ISCAT menunjukkan status yang dapat diterima untuk semua proses TI dalam semua empat domain kerangka kerja COBIT. Status keamanan informasi yang dapat diterima atau memuaskan akan memberikan ketenangan pikiran bagi manajemen organisasi bahwa semua kontrol keamanan informasi yang diperlukan telah diterapkan. Namun, organisasi harus menyadari bahwa model ini harus diterapkan secara teratur untuk memastikan status keamanan informasi yang konsisten dan dapat diterima.

Implementasi COBIT di Industri Pendidikan dan Perbankan

Sebagian besar kerangka kerja pengelolaan TI membahas manajemen sistem informasi dalam pengaturan perusahaan yang mendukung manajemen dari atas ke bawah. Namun, hal ini mengabaikan beberapa pengaturan organisasi yang mendukung pendekatan dari bawah ke atas, seperti di bidang pendidikan tinggi. Untuk mengisi kesenjangan ini, studi ini membandingkan gaya manajemen dan praktik organisasi antara pendidikan tinggi dan industri perbankan untuk mengungkap faktor-faktor yang mendasari norma keamanan organisasi di kedua industri tersebut. Hasilnya mengungkapkan bahwa pendidikan tinggi beroperasi dalam lingkungan terbuka yang mendukung partisipasi karyawan dalam kepatuhan kebijakan. Di sisi lain, manajemen secara *topdown* memberlakukan kebijakan dan memfasilitasi partisipasi karyawan untuk

perlindungan keamanan informasi di industri perbankan. Oleh karena itu, studi ini menyarankan bahwa paradigma baru dari kerangka kerja IT Governance (ITG) diperlukan untuk mengatasi budaya unik di bidang pendidikan tinggi. Selain itu, pengelolaan TI dapat beroperasi dalam mode terdesentralisasi di industri perbankan untuk mendorong partisipasi karyawan dalam mendukung kepatuhan kebijakan informasi (Kam dkk, 2016)

Jika dibandingkan dengan industri perbankan, manajemen terbuka di perguruan tinggi lebih efektif dalam memfasilitasi partisipasi karyawan dalam pengambilan keputusan untuk kepatuhan ISP (Internet Service Protocol). Hal ini menyiratkan bahwa tata kelola bersama harus diperhatikan untuk mencapai kepatuhan ISP di perguruan tinggi. Meskipun hasil analisis menunjukkan bahwa manajemen yang kaku juga meningkatkan partisipasi karyawan di perguruan tinggi, artikel ini berpendapat bahwa manajemen yang kaku dengan fokus pada pemantauan yang ketat tidak dapat diterapkan di lingkungan pendidikan tinggi. Hal ini terutama karena pendidikan tinggi menganut konstruksi sosial, multikulturalisme, dan heterogenitas yang tidak dapat dicapai dengan pemantauan yang ketat. Pada manajemen yang kaku mendorong partisipasi karyawan dalam pengambilan keputusan di industri perbankan. Meskipun mempunyai struktur yang hierarkis, bank memfasilitasi partisipasi karyawan. Hal ini juga mendukung gagasan bahwa tata kelola TI dapat beroperasi dalam mode terdesentralisasi yang melibatkan sejumlah pembagian kekuasaan dengan manajemen (Okour, 2019).

Dikarenakan globalisasi dan digitalisasi dari sistem industri, kepatuhan standar semakin mendapatkan perhatian yang lebih. Untuk tetap bersaing dan bertahan dalam bisnis, berbagai sektor dalam industri diwajibkan untuk mematuhi banyak regulasi. Kepatuhan bertujuan untuk memenuhi regulasi dengan memasukkan semua tindakan yang diwajibkan oleh undang – undang dan standar. Setiap perangkat, aplikasi, atau layanan menerapkan beberapa teknologi pada banyak tingkat, dan standar mendukung interoperabilitas di antara mereka. Mereka membantu untuk menciptakan pasar global untuk industri dan memungkinkan pengembangan jaringan untuk menjadi sukses dan berkelanjutan. Pentingnya kepatuhan standar dan verifikasi kontinu dalam perangkat Internet of Things (IoT) dan mengimplementasikan kerangka pemantauan otomatis dan verifikasi kepatuhan standar. Model metrik dikembangkan sebagai dasar untuk informasi yang diperlukan untuk verifikasi kepatuhan,

termasuk persyaratan, standar, dan metrik. Model ini menyajikan prototipe kerangka pemantauan dan verifikasi kepatuhan standar yang digunakan untuk menunjukkan kepatuhan keamanan dari sebuah kasus penggunaan perangkat IoT (Tariq dkk, 2013; Putra dkk, 2017).

Digitalisasi produksi industri akan membawa tantangan baru bagi sistem manufaktur yang sudah ada. Meskipun begitu, aspek keamanan, keselamatan, dan organisasi, terutama kepatuhan terhadap standar dan peraturan digitalisasi yang sudah ada, tetap kritikal untuk keberhasilan implementasi. Standar tetap menjadi masalah untuk adopsi skala besar di lingkungan produksi. Deskripsi tingkat tinggi dari pendekatan dan arsitektur diberikan, di mana tiga komponen utama untuk membangun kerangka kerja kepatuhan otomatis: (a) agen pemantauan, (b) modul EGM (Expert Groyp Meeting), dan (c) modul kepatuhan diidentifikasi (Susanto dkk, 2011; Sheikhpour & Modiri, 2012).

Setelah mengidentifikasi komponen, kerangka kerja MSCV di platform cloud OpenStack, menggunakan check_mk, plugin yang sudah ada, dan skrip yang disesuaikan untuk agen pemantauan. Model metrik yang digunakan untuk mengidentifikasi persyaratan, standar, dan mengekstrak MIPs (Microprocessor without Interlocked Pipelined Stages). MIPs diklasifikasikan dalam MSIs, MSFIs, dan MOIs, dan informasi digunakan sebagai input untuk kerangka kerja MSCV. Pada kerangka kerja ini menyediakan kepatuhan komponen atau sistem berdasarkan standar yang dievaluasi dan MIPs yang diekstrak. Kerangka kerja ini mampu menghasilkan peringatan dan tindakan otomatis untuk memastikan kepatuhan dengan standar yang ditetapkan. Menunjukkan kepatuhan dari sebuah kasus penggunaan IoT berdasarkan persyaratan kontrol akses. Untuk menunjukkan kepatuhan keamanan, standar ISO 27002 dan IEC 62443-3-3 dievaluasi, dan seperangkat MSIs yang representatif diekstrak. MSIs dipantau dalam lima komponen kasus penggunaan dan kepatuhan keseluruhan dari sistem target ditunjukkan dalam dua skenario: (a) salah satu komponen memenuhi sebagian besar MSIs dan (b) komponen tidak memenuhi satu pun dari MSIs.

Kesimpulan

Dari hasil penelitian tersebut, data security merupakan hal yang sangat penting bagi organisasi di era digital saat ini, di mana penggunaan teknologi informasi dan komunikasi semakin meluas dan memungkinkan organisasi untuk mengumpulkan, menyimpan, dan memproses data

dengan lebih efisien. Namun, pengumpulan dan pengolahan data juga meningkatkan risiko keamanan informasi dan privasi yang berkaitan dengan kebocoran, penggunaan yang tidak sah, dan manipulasi data.

Untuk melindungi data organisasi, penting bagi organisasi untuk mematuhi standar keamanan yang telah ditetapkan oleh regulasi dan standar industri. Tujuan dari kepatuhan ini adalah untuk memastikan bahwa organisasi telah memenuhi persyaratan keamanan yang ditetapkan oleh pihak yang berwenang dan menghindari risiko hukuman atau sanksi atas pelanggaran privasi dan keamanan data.

COBIT adalah kerangka kerja manajemen TI yang dapat membantu organisasi dalam memastikan bahwa keamanan dan privasi data dijaga dengan baik. COBIT memberikan panduan tentang bagaimana organisasi dapat memastikan bahwa mereka mematuhi persyaratan keamanan data dan meminimalkan risiko keamanan. Implikasi manajerial penelitian ini adalah bagi organisasi untuk memahami pentingnya keamanan data dan tujuan kepatuhan, serta menggunakan kerangka kerja seperti COBIT untuk memastikan bahwa perusahaan memenuhi persyaratan keamanan yang ditetapkan dan melindungi data organisasi dari risiko keamanan.

DAFTAR PUSTAKA

Al-Ahmad, W., & Mohammad, B. (2012). Can a single security framework address information security risks adequately. *International Journal of Digital Information and Wireless Communications*, *2*(3), 222-230.

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, *7*(3), 51-62.

Andry, J. F., & Hartono, H. (2017). Performance Measurement of IT Based on COBIT Assessment: A Case Study. *Jurnal Sistem Informasi Indonesia*, *2*(1).

Berrada, H., Boutahar, J., & El Houssaïni, S. E. G. (2021). Simplified IT Risk Management Maturity Audit System based on "COBIT 5 for Risk". *International Journal of Advanced Computer Science and Applications*, *12*(8).

Bicaku, A., Tauber, M., & Delsing, J. (2020). Security standard compliance and continuous verification for Industrial Internet of Things. International Journal of Distributed Sensor Networks, 16(6), 1550147720922731.

Budiarta, K., Iskandar, A. P. S., & Sudarma, M. (2016). Audit Information System Development using COBIT 5 Framework. International Journal of Engineering and Emerging Technology, 1(1), 3-7.

Bunnell, L., & Weistroffer, H. R. (2017). Integration of the COBIT 5 Framework into the SDLC for Development of a User Access Attestation System. Integration, 3, 25-2017.

Bruzza, M., Tupia, M., & Rodríguez, F. (2017). An E-government implementation model for Peruvian state companies based on COBIT 5.0: definition and goals of the model. International Journal of Humanities and Social Sciences, 11(3), 675-682.

Deysel, N. (2011). A model for information security control audit for small to mid-sized organisations (Doctoral dissertation).

Gehrmann, M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. *Navus-Revista de Gestão e Tecnologia*, *2*(2), 66-77.

Kam, H. J., Katerattanakul, P., & Hong, S. (2016). IT Governance framework: one size fits all?. In AMCIS.

Mangalaraj, G., Singh, A., & Taneja, A. (2014, August). IT Governance Frameworks and COBIT-A Literature Review. In AMCIS.

Mishra, S., & Weistroffer, H. R. (2007). A framework for integrating Sarbanes-Oxley compliance into the systems development process. *Communications of the Association for Information Systems*, *20*(1), 44.

Motii, M., & Semma, A. (2017). Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament. *IJCSI International Journal of Computer Science Issues*, *14*(3), 49-58.

Okour, S. (2019). The Impact of the Application of IT Governance According to (COBIT 5) Framework in Reduce Cloud Computing Risks. *Mod. Appl. Sci*, *13*(7), 25.

Putra, I. N., Hakim, A., Pramono, S. H., & Tolle, H. (2017). Adopted COBIT-5 framework for system design of Indonesia navy IS/IT: An evaluation. *International Journal of Applied Engineering Research*, *12*(17), 6420-6427.

Tariq, M. I., Haq, D., & Iqbal, J. A. V. E. E. D. (2013). SLA based information security metric for cloud computing from COBIT 4.1

framework. *International Journal of Computer Networks and Communications Security*, *1*(3), 95-101.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23-29.

Sheikhpour, R., & Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Applications*, *6*(2), 13-28.

Ukidve, A., Smantha, D., & Tadvalka, M. (2017). Analysis of payment card industry data security standard [PCI DSS] compliance by confluence of COBIT 5 framework. *International Journal of Engineering Research and Applications*, *7*(01), 42-48.

Ula, M., Ismail, Z., & Sidek, Z. M. (2011). A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*, *2011*, 1-12.