J-ICON, Vol. 10 No. 2, Oktober 2022, pp.122~128
DOI: 10.35508/jicon.v10i2.7985

INTEGRASI *FRAMEWORK* ISO 27001 DAN COBIT 2019 PADA KEAMANAN INFORMASI *SMART TOURISM* PT. YoY MANAJEMEN INTERNASIONAL

Muhammad Nawir[1], Irfan AP[2] dan Farid Wajidi[3]

[1,2,3]Program Studi Teknik Informatika, Universitas Sulawesi Barat, Jl. Prof. Dr. Baharuddin, S.H
[1]Email: muhammad.nawir0909@gmail.com
[2]Email: irfan_ap@unsulbar.ac.id
[3]Email: faridwajidi@unsulbar.ac.id

ABSTRAK

Teknologi informasi yang berkembang pesat menjadi ancaman terhadap sistem informasi menjadi sangat tinggi. PT. YoY Manajemen Internasional yang akan mengelola Aplikasi *smart tourism* berbasis lokasi perlu melakukan perlindungan terhadap informasi perusahaan, agar terhindar dari gangguan dan ancaman yang dapat merugikan perusahaan. Pada penelitian ini dilakukan analisis terhadap tata kelola teknologi informasi (IT) menggunakan *framework* COBIT 2019, dengan cara menyelaraskan strategi dan tujuan dari perusahaan ke dalam proses-proses yang ada pada COBIT 2019 yang kemudian dipetakan ke dalam ISO 27001 untuk manajemen keamanan informasinya. Tujuan penelitian ini untuk melakukan tata kelola terhadap keamanan informasi dengan menggunakan *framework* COBIT 2019 dan standar ISO 27001:2013. Metode penelitian yang digunakan pada penelitian ini adalah deskriptif kualitatif. Hasil yang didapatkan pada penelitian ini berupa beberapa rekomendasi kebijakan-kebijakan dalam mengelola keamanan informasi pada aplikasi *smart tourism* sesuai dengan standar COBIT 2019 dan ISO 27001:2013.
Kata kunci: COBIT 2019, ISO 27001, Keamanan Informasi, PT. YoY Manajemen Internasional

ABSTRACT

Information technology that is growing rapidly becomes a very high threat to information systems. PT. YoY Management Internasional which will manage the location-based smart tourism application so that it is necessary to protect company information, in order to avoid interference and threats that can harm the company. In this study, an analysis of information technology (IT) governance was carried out using the COBIT 2019 framework, by aligning the company's strategies and goals into existing processes in COBIT 2019 which were then mapped into ISO 27001 for information security management. The purpose of this research is to manage information security using the COBIT 2019 framework and the ISO 27001:2013 standard. The research method used in this research is descriptive qualitative. The results obtained in this study are in the form of several recommendations for policies in managing information security in smart tourism applications in accordance with the COBIT 2019 and ISO 27001:2013 standards.
Keywords: COBIT 2019, ISO 27001, Information Security, PT. YoY International Management

1. PENDAHULUAN

Teknologi informasi mempunyai peranan penting dalam aktivitas manusia, terutama pada kegiatan-kegiatan bisnis dan memberikan peran besar terhadap perubahan-perubahan yang mendasar, seperti struktur, operasi maupun manajemen teknologi informasi. Karena semakin meningkatnya penggunaan teknologi membuat keamanan informasi menjadi hal yang harus diperhatikan dan perlu dilindungi dengan baik agar terhindar dari serangan.

Sangat penting untuk menjaga informasi, karena merupakan aspek yang sangat mempengaruhi teknologi informasi. Keamanan informasi merupakan perlindungan terhadap informasi dari berbagai ancaman, untuk menjamin kelangsungan suatu instansi maupun bisnis dan mendapatkan hasil yang maksimal dalam bisnis [1].

Ancaman keamanan sistem informasi dapat menghambat kinerja operasional sehingga merugikan suatu instansi. Untuk itu diharapkan para *stakeholder* untuk lebih memperhatikan masalah terhadap keamanan informasi agar meminimalisir kerugian yang terjadi [2]. Begitu pula pada aplikasi *smart tourism*, perlu dilakukan tata kelola terhadap keamanan informasinya agar terhindar dari ancaman yang bisa merugikan.

Aplikasi *smart tourism* merupakan aplikasi pariwisata yang dapat merekomendasikan tempat dan fasilitas wisata sesuai dengan lokasi (*location based service*) serta preferensi wisatawan yang dapat merekomendasikan bukan hanya tempat wisata yang sudah terkenal tetapi juga tempat dan fasilitas wisata yang memiliki potensi tinggi namun masih kurang dikenal. Aplikasi *smart tourism* ini nantinya akan

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (online)

terintegrasi dengan tempat-tempat wisata dan fasilitas pendukung pariwisata, sehingga memungkinkan wisatawan untuk melakukan transaksi secara *real time*.

Seperti yang kita ketahui bahwa kerusakan informasi dapat mempengaruhi perusahaan maupun bisnis. Maka pada aplikasi *smart tourism*, PT. YoY Manajemen Internasional mempunyai kewajiban untuk melindungi data pelanggan beserta asetnya, sehingga terhindar dari serangan/ancaman yang dapat merusak proses bisnis dari *smart tourism*. Untuk itu perlu dilakukan tata kelola terhadap sistem keamanan informasi pada aplikasi ini, agar pengguna aplikasi *smart tourism* tidak takut dalam melakukan transaksi maupun hal-hal lain yang berkaitan dengan informasi. Dalam melakukan tata kelola teknologi informasi terdapat banyak standar dan *framework* yang dapat digunakan, dan yang paling sering digunakan yaitu ISO/IEC 27001 dan COBIT 2019.

ISO/IEC 27001 merupakan standar internasional yang telah disiapkan dan menyediakan persyaratan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (SMKI) [3]. ISO/IEC 27001 menerapkan proses manajemen risiko serta memberikan keyakinan kepada pihak yang berkepentingan bahwa risiko sudah dikelola sesuai dengan standar yang telah ditetapkan. Implementasi sistem manajemen keamanan informasi diharapkan dapat ditingkatkan sesuai dengan kebutuhan organisasi [4]. COBIT merupakan kerangka tata kelola IT yang berfokus dalam menetapkan suatu tata kelola TI bisa berjalan dengan lancar. Dalam COBIT juga sediakan struktur, perlengkapan serta tutorial dalamvmenggapai tingkat maupun tingkatan yang di harapkan dari kinerja proses TI yang diguanakan untuk penuhi kebutuhan bisnis [5].

2. MATERI DAN METODE

Teknologi Informasi

Teknologi informasi adalah teknologi yang tidak hanya terbatas pada komputer (perangkat lunak dan perangkat keras) yang digunakan untuk menyimpan data maupun infomasi tetapi juga mencakup bagaimana untuk mengirimkan informasi.

Disisi lain teknologi informasi dan komunikasi mempunyai lingkup yang besar, karena mencakup semua jenis perangkat teknis yang dipergunakan untuk mengirimkan serta memproses informasi. Ada dua aspek teknologi informasi dan komunikasi (TIK), yaitu teknologi informasi dan teknologi komunikasi, yang saling terkait dan tidak bisa dipisahkan. Artinya, pengertian luas dari teknologi informasi dan komunikasi mencakup semua prosedur yang berkaitan dalam proses pengelolaan, transmisi dan manipulasi data-data dan informasi ke media lain [6].

COBIT 2019

COBIT ialah singkatan dari *Control Objective for Information and related* yang secara universal digunakan buat mengimplementasikan IT *Governance*, *framework* yang bermanfaat untuk membantu terpaut manajemen, auditor serta user dalam menghubungkan antara kebutuhan kontrol terhadap resiko strategi bisnis serta pula kasus yang terdapat. *Framework* COBIT bisa digunakan pada seluruh tipe organisasi serta tidak memandang terhadap kecil ataupun besarnya suatu organisasi. COBIT ialah lingkup bagian dari ISACA.

COBIT 2019 adalah prinsip tata kelola ada untuk memastikan bahwa kebutuhan *stackholder* dievaluasi dan disepakati berdasarkan tujuan perusahaan, untuk menetapkan arah melalui pembuatan prioritas dan pengambilan keputusan, dan untuk memantau kinerja dan kepatuhan terhadap arah dan tujuan yang ditetapkan [7].

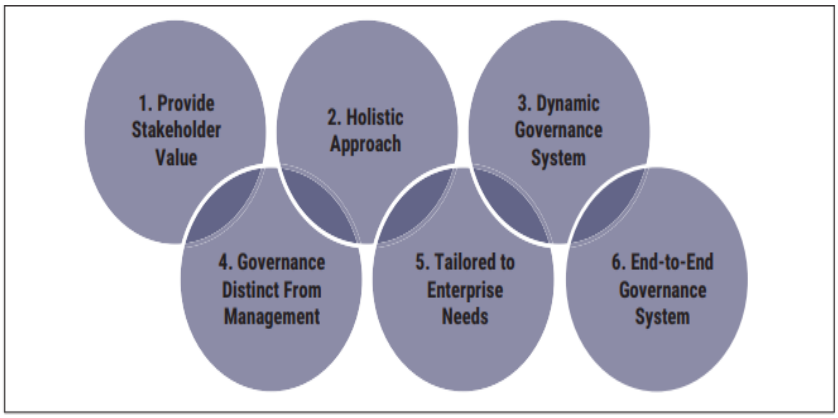
COBIT 2019 dikembangkan berdasarkan dua set prinsip:

1. Prinsip-prinsip yang dapat menggambarkan persyaratan mendalam dari sistem tata kelola untuk informasi dan teknologi bagi perusahaan. Terdapat 6 prinsip dan dapat dilihat pada gambar 1.
   Enam prinsip untuk sistem tata kelola adalah:
   a. Tiap industri memerlukan sistem tata kelola guna penuhi kebutuhan pemangku kepentingan (*stackholder*) serta untuk menciptakan nilai dari pemakaian teknologi informasi. Nilai ini mencerminkan penyeimbang antara utilitas, resiko, sumber energi, serta industri membutuhkan strategi yang bisa ditindaklanjuti dari sistem tata kelola buat mewujudkan nilai ini.
   b. Tata kelola sistem dalam IT industri dibentuk dari beberapa komponen yang didapat dari bermacam tipe serta yang bekerja sama secara holistik.
   c. Sistem tata kelola pasti dinamis. Ini berarti kalau tiap kali satu ataupun lebih aspek desain berganti (misalnya, pergantian strategi ataupun teknologi), akibat dari pergantian ini pada

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (online)

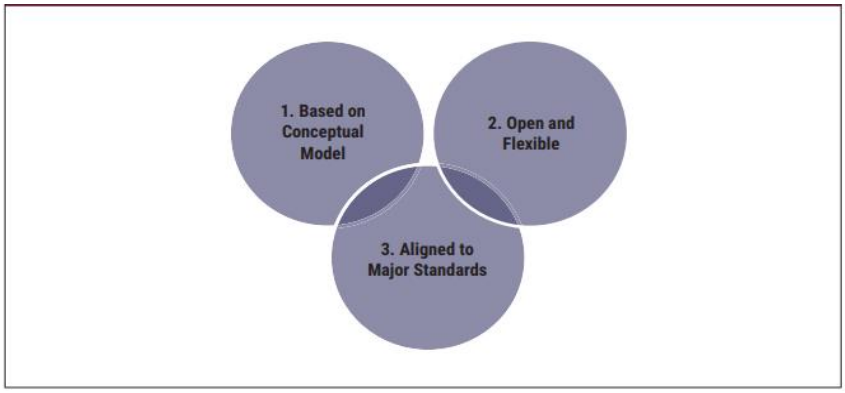
sistem *Enterprise Governance of IT* (EGIT) wajib dan dipertimbangkan. Pemikiran dinamis tentang EGIT hendak menuju pada sistem EGIT yang layak serta tahan di masa depan.

d. Sistem tata kelola secara jelas membagi dan membedakan antara aktivitas serta struktur tata kelola serta pengelolaan.
e. Sistem tata kelola seharusnya diselaraskan dengan kebutuhan industri, dengan memakai serangkaian aspek desain selaku parameter untuk membiasakan serta memprioritaskan komponen sistem tata kelola.
f. Sistem tata kelola mewajibkan mencakup industri secara merata, dengan fokus tidak cuma pada peranan TI namun pada seluruh teknologi serta pemrosesan data yang dicoba industri buat menggapai tujuannya.



Gambar 1. Prinsip sistem tata kelola

2. Prinsip-prinsip untuk kerangka kerja tata kelola yang bisa digunakan dalam membangun suatu sistem tata kelola untuk perusahaan. Terdapat 3 prinsip dan dapat dilihat pada gambar 2.



Gambar 2. Prinsip kerangka kerja

Tiga prinsip kerangka tata kelola adalah:

a. Kerangka kerja tata kelola wajib didasarkan dalam model konseptual, mengenali komponen utama serta ikatan antar komponen, guna mengoptimalkan konsistensi serta mengizinkan otomatisasi.
b. Kerangka tata kelola wajib terbuka serta fleksibel. Harus membolehkan akumulasi konten baru serta keahlian untuk menanggulangi permasalahan baru dengan metode yang sangat fleksibel, dan mempertahankan integritas serta konsistensi.
c. Kerangka tata kelola mesti selaras dengan suatu standar, kerangka kerja, serta peraturan yang baik dan relevan.

ISO 27001

Standar ISO 27001 yang diterbitkan pada tahun 2013 merupakan hasil perbaikan dari ISO/ IEC 27001: 2009. ISO 27001: 2013 berisi tentang membangun SMKI. Dalam keamanan data yang menggambarkan dokumen standar sistem manajemen keamanan data yang mampu membagikan cerminan secara universal mengenai sebagian tentang yang wajib dilakukan oleh suatu organisasi [8]. Pengendalian serta kontrol dalam ISO/ IEC 27001: 2013 dimaksudkan guna penuhi persyaratan yang teridentifikasi oleh resiko yang ada, kemudian diperlukan perencanaan yang matang untuk pemilihan secara rinci dari kontrol

yang hendak digunakan. Kontrol yang menggambarkan pendefinisian dari manajemen keamanan data dalam menunjang implementasi pada kontrol.

ISO/IEC mempunyai 14 klausul, kontrol keamanan, 35 objektif serta 114 kontrol. Berikut ialah penjabaran dari klausul yang terdapat ke dalam ISO 27001:2013 [9].

1. Klausul A.5 *Information Security Policies.*
2. Klausul A.6 *Organization of Information Security*
3. Klausul A.7 *Human Resource Security*
4. Klausul A.8 *Aset Management*
5. Klausul A.9 *Access Control*
6. Klausul A.10 *Cryptography*
7. Klausul A.11 *Physical and Enviromental Security*
8. Klausul A.12 *Operations Security*
9. Klausul A.13 *Comunications Security*
10. Klausul A.14 *System Acquisition, Development and Maintence*
11. Klausul A.15 *Supplier Relationships*
12. Klausul A.16 *Information Security Incident Management*
13. Klausul A.17 *Information Security Aspects of Business Continuity Management*
14. Klausul A.18 *Compliance*

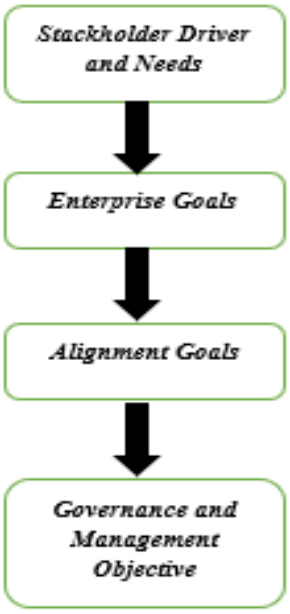
Metode Penelitian

Penelitian ini menggunakan pendekatan deskriptif kualitatif. Metode deskriptif merupakan suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran ataupun suatu kelas peristiwa pada masa sekarang. Kualitatif merupakan sebagai suatu prosedur penelitian yang bisa mendapatkan data deskriptif yang berupa kata-kata tertulis atau dari lisan orang-orang maupun para perilaku yang bisa diamati.

3. HASIL DAN PEMBAHASAN

Analisis *Framework* COBIT 2019

Di tahap ini dilakukan analisis dengan melakukan proses pemetaan dari tujuan organisasi yang dimiliki oleh PT. YoY Manajemen Internasional. Pemetaan dilakukan mulai dari memetakan tujuan organisasi PT. YoY Manajemen Internasional dengan *Enterprise Goals*, kemudian dilanjutkat pemetaan *Enterprise Goals* dan *IT- Related Goals* (*Alignment Goals*) hingga mendapatkan IT proses hasil dari pemetaan *IT-Related Goals dengan Governance and Management Objective*. Adapun tahapan pada gambar 3.



Gambar 3. Tahapan COBIT 2019

a. Pemetaan Tujuan Organisasi dengan *Enterprise Goals* COBIT 2019

Untuk melakukan pemetaan tujuan organisasi dengan *Enterprise Goals* COBIT 2019, maka diperlukan data untuk memetakannya [10]. Data yang digunakan diperoleh dari lapangan, dengan

melakukan wawancara kepada salah satu *owner* PT. YoY Manajemen Internasional serta observasi. Selanjutnya data diolah dan disesuaikan dengan standar kerangka kerja COBIT 2019, sehingga pemetaan tujuan organisasi PT. YoY Manajemen Internasional dengan *Enterprise Goals* COBIT 2019.

Hasil pemetaan tujuan organisasi diambil dari hasil wawancara dan visi misi yang dimiliki PT. YoY Manajemen Internasional untuk mencapai tujuan organisasi, kemudian akan disesuikan dengan *enterprise goals* COBIT 2019 dengan hasil pemetaan tujuan orgnisasi PT. YoY Manajemen Internasional dengan *Enterprise Goals* COBIT 2019 seperti pada gambar 3 dan dirangkum pada tabel 1.

Tabel 1. Pilihan *Enterprise Goals*

Tujuan PT. YoY Manajemen Internasional	**BSC *Dimension***	**No**	***Enterprise Goals***
Referensi tata kelola perusahaan yang terpercaya, Transparansi, akuntabel dan profesional.	*Financial*	02	*Manage Bussines Risk*
	Customer	06	*Business service continuity and availability*
	Customer	07	*Quality of management information*

Berdasarkan hasil rangkuman tujuan organisasi pada tabel 1, maka *Enterprise Goals* yang paling sesuai yaitu *Business service continuity and availability. Business service continuity and availability* (kesinambungan dan ketersediaan layanan bisnis) harus menjadi yang utama dalam pikiran semua orang saat ini karena situasi pandemi yang sedang berlangsung. Penting untuk mengidentifikasi komponen kritis yang perlu dievaluasi untuk menilai kesiapan organisasi terhadap kelangsungan dan ketersediaan layanan bisnis.

b. Pemetaan *Enterprise Goals* dan *Alignment Goals*

Setelah pemetaan tujuan organisasi kedalam *Enterprise Goals* COBIT 2019, selanjutnya akan dilakukan pemetaan *Enterprise Goals* terhadap *Alignment Goals.*

Tabel 2. Pemetaan *IT Goals*

Alignment Goals	***Description***	***Priority***
AG07	*Security of information, processing infrastructure and applications, and privacy*	P

Pada tabel 2 dapat diketahui bahwa hasil pemetaan *Enterprise Goals* terhadap *Alignment Goals* diperoleh data cell P (*Primary*) yaitu *Security of information, processing infrastructure and applications, and privacy* (keamanan informasi, infrastruktur pemrosesan dan aplikasi, serta privasi).

c. Pemetaan *Alignment Goals* dan *Governance and Management Objective*

Tahapan selanjutnya yaitu memetakan *Alignment Goals* yang telah diperoleh kedalam *Governance and Management Objective* (IT Proses).

Tabel 3. Pemetaan IT proses

Governance and Management Objective	***Description***	***Priority***
EDM03	*Ensured risk optimization*	P
APO12	*Managed risk*	P
APO13	*Managed security*	P
BAI10	*Managed configuration*	P
DSS04	*Managed continuity*	P
DSS05	*Managed securty services*	P

Dari tabel 3 dapat diketahui bahwa hasil pemetaan AG07 "*Security of information, processing infrastructure and applications, and privacy*" kedalam IT proses yang ada pada cobit, terdapat 6 IT proses yang berhubungan Primary (P) dengan AG07, yaitu EDM03 (*Ensured risk optimization*), APO12 (*Managend risk*), APO13 (*Managed security*), BAI10 (*Managed configuration*), DSS04 (*Managed continuity*) dan DSS05 (*Managed security services*).

Hasil pemetaan tersebut akan disesuaikan lagi dengan kondisi dan keinginan dari PT. YoY Manajemen Internasional untuk menentukan IT proses yang akan digunakan. Oleh karena itu pada penelitian ini akan menggunakan domain IT proses yaitu APO13 *managed security* (mengelola keamanan), karena di dalamnya terdapat pembahasan tentang SMKI. Selanjutnya APO13 ini akan dipetakan kedalam ISO 27001.

APO13-*Managed Security* akan mendefinisikan, mengoperasikan dan mengawasi sistem manajemen keamanan informasi. Tujuannya adalah untuk menjaga agar dampak dari insiden keamanan informasi masih berada pada level yang bisa diterima perusahaan.

Pemetaan COBIT 2019 dengan ISO 27001

Setelah mendapatkan domain IT proses COBIT 2019 yaitu APO13, selaniutnya akan dipetakan ke dalam ISO 27001 seperti pada tabel 4.

Tabel 4. Integrasi COBIT dan ISO

Proses COBIT 2019		Kontrol keamanan ISO 27001:2013
APO 13	**Mengelola Keamanan**	
APO 13.01	Menetapkan dan memelihara informasi sistem manajemen keamanan informasi (SMKI)	8.1.1 Inventaris Aset 8.1.2 Kepemilikan Aset 8.2.1 Klasifikasi Informasi 12.3.1 *Backup* Informasi 16.1.5 Respon terhadap insiden keamanan informasi 16.1.6 Belajar dari insiden Keamanan Informasi
APO 13.02	Menentukan dan Mengelolah rencana perawatan risiko keamanan informasi	7.2.1 Tanggung Jawab Manajemen 12.2.1 Kontrol terhadap *malware*
APO 13.03	Menamtau dan meninjau sistem manejemen keamanan informasi (SMKI)	9.1.2 Akses ke Jaringan dan Layanan 16.1.2 Pelaporan Peristiwa keamanan informasi

Dari hasil pemetaan pada tabel 4, maka selanjutnya akan di terapkan pada aplikasi *smart toursm* yang akan di kelola oleh PT. YoY Manajemen Internasional.

Pemilihan Keebijakan/Kontrol Keamanan

Bersarkan hasil pemetaan pada tabel 4, maka kebijakan/kontrol yang akan dipilih dan sesuai dengan kondisi pada PT. YoY Manajemen Internasional dalam mengelola keamanan informasi pada aplikasi *smart toursm*.

Tabel 5. Kebijakan/Kontrol Keamanan

NO	KEBIJAKAN/KONTROL KEAMANAN
1	Tanggung Jawab Manajemen
2	Inventaris Aset
3	Kepemilikan Aset
4	Klasifikasi Informasi
5	Akses ke Jaringan dan Layanan
6	Kontrol terhadap *malware*
7	*Backup* Informasi
8	Pelaporan Peristiwa keamanan informasi
9	Respon terhadap insiden keamanan informasi
10	Belajar dari insiden Keamanan Informasi

Tabel 5 merupakan kebijakan yang penulis rekomendasikan untuk PT. YoY Manajemen Internasional. Dari beberapa rekomendasi pada tabel 5 diharapkan dapat menjadi bahan pertimbangan bagi PT. YoY Manajemen Internasional untuk menerapkan SMKI pada aplikasi *smart tourism*.

4. KESIMPULAN DAN SARAN

Analisis framework COBIT 2019 yang dilakukan dengan menyelaraskan tujuan dari industri PT. YoY Manajemen Internasional ke dalam proses yang ada pada COBIT 2019. Sehingga didapatkan IT proses APO13 Ensured Risk (mengelola keamanan), kemudian dari APO13 akan dipetakan ke dalam klausul dan kontrol keamanan yang ada pada standar ISO 27001:2013.

Dari klausul tersebut, terdapat beberapa kontrol keamanan didalamnya dan akan digunakan sebagai acuan untuk membuat rekomendasi kebijakan untuk PT. YoY Manajemen Internasional dalam mengelola keamanan informasinya..

Terdapat kekurangan dalam penelitan ini, seperti hanya menggunakan 1 domain APO13 *Ensured Risk*, diharapkan pada penelitian selanjutnya dapat menggunakan domain yang lainnya seperti EDM03, APO12, BAI10, DSS04 dan DSS05.

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (online)

DAFTAR PUSTAKA

[1] Sholikhatin, S. A., Setyanto, A., & Luthfi, E. T. 2019. Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto). It Cida, 4(1), 1–9. http://journal.amikomsolo.ac.id/index.php/itcida/article/view/75

[2] Steve G Watkins,. 2008. An Introduction to Information Security and ISO 27001 : IT Publising.United Kingdom

[3] Lenawati, M., Winarno, W. W., & Amborowati, A. (2017). Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT 5. *Sentra Penelitian Engineering Dan Edukasi*, *9*(1), 44–49. http://speed.web.id/jurnal/index.php/speed/article/view/220

[4] Iec, I. S. O., & Iec, I. S. O. (2019). INTERNATIONAL STANDARD ISO / IEC Security techniques — Extension to. 2019.

[5] Masduki. 2020. Introduction and Methodology. In Palgrave Series in Asia and Pacific Studies. https://doi.org/10.1007/978-981-15-7650-8_1

[6] Riyana, C. 2010. Teknologi Informasi dan Komunikasi. Pusat Perbukuan Kementrian Pendidikan Nasional, 1(April), 1–302.

[7] INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION – ISACA. (2018). Governance and Management Objectives. In COBIT® 2019 Framework. https://www.isaca.org/resources/cobit

[8] Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System. In *Implementing an Information Security Management System*. https://doi.org/10.1007/978-1-4842-5413-4

[9] International Organization for Standardization. 2013. INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements. Information Technology — Security Techniques — Information Security Management Systems — Requirements, 2014(ISO/IEC 27001:2013), 38.

[10] Fathoni, Simbolon, N., & Yunika Hardiyanti, D. (2019). Security audit on loan debit network corporation system using cobit 5 and iso 27001: 2013. *Journal of Physics: Conference Series*, *1196*(1). https://doi.org/10.1088/1742-6596/1196/1/012033

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (online)