

OAJIS

Open Access
Journal of
Information
Systems

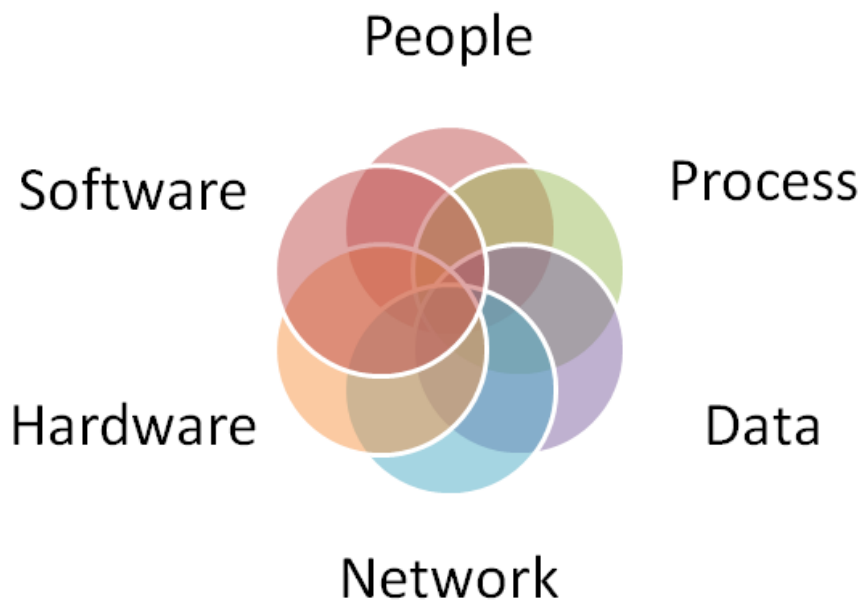
is.its.ac.id/pubs/oajis/

ISSN 1979-3979



jurnal sisfo

Inspirasi Profesional Sistem Informasi





Pimpinan Redaksi

Sholiq (Institut Teknologi Sepuluh Nopember)

Dewan Redaksi

Reny Nadlifatin (Institut Teknologi Sepuluh Nopember)

Mudjahidin (Institut Teknologi Sepuluh Nopember)

Tining Haryanti (Universitas Muhammadiyah Surabaya)

Faizal Mahananto (Institut Teknologi Sepuluh Nopember)

Rizal Risnanda Utama (Institut Teknologi Sepuluh Nopember)

Radityo Prasetyanto Wibowo (Institut Teknologi Sepuluh Nopember)

Monica Wideasri (Universitas Surabaya)

Anjik Sukmaaji (Universitas Dinamika)

Devi Septiani (Universitas Brawijaya)

Tata Pelaksana Usaha

Heppy Nuryanti (Institut Teknologi Sepuluh Nopember)

Sekretariat

Departemen Sistem Informasi – Fakultas Teknologi Elektro dan Informatika Cerdas

Institut Teknologi Sepuluh Nopember (ITS) – Surabaya

Telp. 031-5999944 Fax. 031-5964965

Email: editor@jurnalsisfo.org

Website: <http://jurnalsisfo.org>

Jurnal SISFO juga dipublikasikan di *Open Access Journal of Information Systems* (OAJIS)

Website: <http://is.its.ac.id/pubs/oajis/index.php>



Mitra Bestari

Prof. Erma Suryani, S.T., M.T., Ph.D. (Institut Teknologi Sepuluh Nopember)

Prof. Dr. Wiwik Anggraeni, S.Si., M.Kom. (Institut Teknologi Sepuluh Nopember)

Tony Dwi Susanto, S.T., M.T., Ph.D. (Institut Teknologi Sepuluh Nopember)

Yogantara Setya Dharmawan, S.Kom, M.BusProcessMgt. (Institut Teknologi Sepuluh Nopember)

Arif Wibisono, S.Kom., M.Sc., Ph.D. (Institut Teknologi Sepuluh Nopember)

Dr. Bambang Setiawan, S.Kom., M.T. (Institut Teknologi Sepuluh Nopember)

Dr. Muhammad Ainul Yaqin, S.T., M.Kom. (Universitas Islam Negeri Maulana Malik Ibrahim)

Taufik, S.T., M.Kom. (Universitas Airlangga)

Dr. Apol Pribadi Subriadi, S.T., M.T. (Institut Teknologi Sepuluh Nopember)

Muhammad Amirul Haq, S.T., M.Sc. (Universitas Muhammadiyah Surabaya)

Dhiani Tresna Absari, S.T., M.Kom. (Universitas Surabaya)

Dr. Mudjahidin, S.T., M.T. (Institut Teknologi Sepuluh Nopember)



Daftar Isi

Visualisasi Representasi Pengetahuan berbasis Ontologi untuk Memodelkan Mahasiswa Cumlaude Jenjang Sarjana <i>Nur Khofifah, Nur Laila, Sholikah Desi Purwanti, Amalinda Jayanty, Retno Aulia Vinarti</i>	1
Implementasi Metode Agile pada Pengembangan Sistem Informasi Manajemen Masjid Berbasis Website <i>Ridho Aulia Rahman, Rigen Ferdian Saputra, M. Ainul Yaqin</i>	11
Representasi Pengetahuan Berbasis Ontologi sebagai Panduan Berwisata dengan Aman <i>Muhammad Rhakan, Naufal Firjatullah Fano, Sang Intan Risqi Adi, Ziaul Haq Al Karimi, Retno Aulia Vinarti</i>	26
Impact of Digital Supply Chain in Agriculture: A Systematic Literature Review <i>Muhammad Syamil Fadlillah, Rahmatika Jagad Pramundito</i>	36
Penyusunan Dokumen SOP Sistem Manajemen Keamanan Aset Informasi Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kab. Sumenep Menggunakan Framework COBIT 5 dan ISO 27001:2013 <i>Yogantara Setya Dharmawan, Rizqi Amrullah Wildan Yani, Alif Millati Putri</i>	53
Penerapan Metodologi Agile Scrum dalam Pengembangan Situs Web AutomATEEs untuk Pembuatan Desain Kaos Berbasis AI <i>Darrell Valentino, Frans Nicklaus Gusyanto, Jhoni Ananta Sitepu, Dzaky Purnomo Rifa'i, Viera Tito Virgawan, Sholiq</i>	62
Analisis Penerapan Prinsip SOLID pada Tugas Proyek Mahasiswa UIN Malang <i>Alfred Rajendra Wijaya, Ela Ilmatul Hidayah, M. Ainul Yaqin</i>	85
Analisis Pengaruh Fitur Iklan Pada Media Sosial Terhadap Intensi Pembelian Pelanggan dengan Menggunakan Structural Equation Modelling (Studi Kasus: Instagram) <i>Andre Parvian Aristio, Mudjahidin, Made Puspa Wedanthi</i>	95

OAJIS

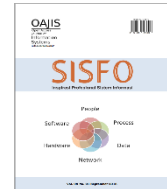
Open Access
Journal of
Information
Systems
is.its.ac.id/pubs/oajis/

jurnal sisfo

Jurnal Sisfo Vol. 11 No. 2 (2024)



Halaman ini sengaja dikosongkan



Penyusunan Dokumen SOP Sistem Manajemen Keamanan Aset Informasi Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kab. Sumenep Menggunakan Framework COBIT 5 dan ISO 27001:2013

Yogantara Setya Dharmawan^{a,*}, Rizqi Amrullah Wildan Yani^a, Alif Millati Putri^b

¹Departemen Sistem Informasi, Fakultas Teknologi Elektro dan Informatika Cerdas, Institut Teknologi Sepuluh Nopember

²Departemen Sistem Informasi, Fakultas Teknologi Informasi dan Kreatif, Universitas Internasional Semen Indonesia

Abstract

The Department of Tourism, Culture and Sports of the Sumenep Regency is a regional apparatus as the organizer of the implementation of regional government, led by the Head of the Service who is under and responsible to the Regent in carrying out some government affairs in Sumenep Regency. However, one government in Sumenep district, namely the Youth and Sports Tourism Office, has not implemented procedures on information asset security so that there are often problems with deletion of goods, loss of data and damage to computers which result in less than optimal public services. Therefore, it is necessary to make improvements from internal parties in building a quality service process management according to the standards set. In this study, the final result obtained is the preparation of a standard procedure in the form of a SOP (Standard Operating Procedure) document on information asset security management for the Tourism Office, Culture, Youth and Sports using the COBIT 5 and ISO 27001:2013 framework.

Keywords: Information Technology, Department of Tourism, Culture, Youth and Sports, COBIT 5, ISO 27001:2013

Abstrak

Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep merupakan perangkat daerah sebagai unsur pelaksana penyelenggaraan pemerintahan daerah, dipimpin oleh Kepala Dinas yang berada di bawah dan bertanggung jawab kepada Bupati dalam menyelenggarakan sebagian urusan pemerintahan di bidang Kepariwisata, Kebudayaan, Kepemudaan dan Keolahragaan di Kabupaten Sumenep. Akan tetapi, pada salah satu organisasi pemerintahan di Kabupaten Sumenep yaitu di Dinas Pariwisata Kebudayaan Pemuda dan Olahraga belum menerapkan prosedur atau aturan tentang keamanan aset informasi sehingga sering terjadi permasalahan mengenai penghapusan barang, kehilangan data dan kerusakan pada komputer yang mengakibatkan layanan publik yang kurang optimal. Pada penelitian ini, hasil akhir yang diperoleh yaitu penyusunan sebuah standar prosedur berupa dokumen SOP (Standard Operating Procedure) tentang manajemen keamanan aset informasi bagi Dinas Pariwisata Kebudayaan Pemuda dan Olahraga menggunakan kerangka kerja COBIT 5 dan ISO 27001:2013.

Kata Kunci: Teknologi Informasi, Dinas Pariwisata Kebudayaan Pemuda dan Olahraga, COBIT 5, ISO 27001:2013

*Corresponding Author

Email address: yogantara@its.ac.id (Yogantara S. Dharmawan)

<https://doi.org/10.24089/j.sisfo.2024.06.005>

© 2024 Jurnal SISFO.

Histori Artikel: Disubmit 21-03-2024; Direvisi 05-09-2024; Diterima 10-09-2024; Tersedia online 30-06-2024

1. Pendahuluan

Teknologi informasi saat ini sangat berkembang begitu pesat di seluruh garis kehidupan khususnya di kalangan bisnis. Pada suatu organisasi pemerintahan saat ini, kunci keberhasilan teknologi informasi merupakan faktor utama dalam seluruh proses kegiatan untuk menerima, mengirimkan informasi dan hal yang utama yaitu dapat mengoptimalkan sebuah layanan agar dapat digunakan secara tepat sesuai dengan kebutuhan dunia. Tantangan utama yang dihadapi termasuk ancaman dari negara-negara adidaya yang berusaha mencuri informasi intelijen atau mengganggu stabilitas nasional melalui serangan siber seperti spionase dan DDoS [1]. Terlebih, pada isu terkini terkait keamanan data yang kini muncul di Indonesia dengan adanya serangan *hacking* terhadap Pusat Data Nasional [2] [3] membuat lembaga pemerintahan harus lebih waspada dalam mengelola keamanan aset informasi mereka. Selain itu, arahan dari Pemerintah melalui peraturan Badan Siber dan Sandi Negara (BSSN) no 4 tahun 2021 terkait layanan SPBE (Sistem Pemerintahan Berbasis Elektronik) yang juga mengharuskan pengamanan terhadap data dan informasi yang disimpan didalamnya [4].

Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep yang disingkat dengan DISPARBUDPORA merupakan perangkat daerah sebagai unsur pelaksana penyelenggaraan pemerintahan daerah yang melayani bidang pariwisata, kebudayaan, pemuda dan olahraga di kabupaten Sumenep akan tetapi pada pemerintahan, keamanan aset informasi tidak diperhatikan setiap dilakukan proses sinkronisasi aset setiap 3 bulan sekali yang pencatatannya dilakukan pada website SIVA (Sistem Validasi Aset) dikarenakan masih terdapat permasalahan pada penghapusan barang, belum adanya aturan atau prosedur internal terkait sistem manajemen keamanan aset informasi. Hal tersebut didukung dalam peraturan tentang kedudukan, susunan organisasi, tugas fungsi dan tata kerja unit pelaksana teknis Dinas Pariwisata Kebudayaan Pemuda dan Olahraga sesuai dengan Peraturan Bupati Kab. Sumenep No. 30 Tahun 2018 [5]. Hal ini menjadi motivasi utama dalam mendukung Peraturan Bupati dan pengamanan data SPBE serta mencegah ancaman keamanan informasi tidak terjadi. Kabupaten Sumenep dipilih dikarenakan adanya kebutuhan dan permintaan Lembaga kepada tim peneliti untuk membantu mewujudkan prosedur untuk Sistem Manajemen Keamanan Aset Informasi.

Sistem Manajemen Keamanan Aset Informasi (SMKI) dapat dicapai dengan penerapan tata Kelola dan manajemen Teknologi Informasi yang memadai. Salah satunya yakni SMKI berbasis SNI/ISO 270001 yang telah ditetapkan oleh SNI. Selain itu, kebutuhan akan Tata Kelola terkait keamanan informasi juga meningkat mengakibatkan penyusunan SOP saja tidak cukup mengacu pada SNI/ISO saja, kerangka kerja Tata Kelola IT diperlukan untuk menjawab hal tersebut. Kerangka kerja COBIT 5 dipilih karena terdapat domain yang berkaitan dengan permasalahan keamanan informasi yang dikategorikan dalam *domain Align, Plan and Organise* (APO) dan *domain Decision, Support and System* (DSS). Sedangkan SNI/ISO 27001:2013 menyediakan 14 klausa, 35 Objektif, dan 114 kontrol (detail lihat pada sub bab 2.8) bagaimana cara membangun sistem manajemen keamanan informasi yang merupakan dokumen standar sistem manajemen keamanan informasi atau yang biasa disebut SMKI yang memberikan kerangka tata kelola keamanan informasi. Sehingga, tim penulis mengintegrasikan dua kerangka kerja COBIT dan SNI/ISO 270001 untuk memberikan Gambaran rinci bagaimana Prosedur Pengamanan Aset Informasi.

Dari permasalahan yang telah ditemukan oleh peneliti saat melakukan observasi, sebaiknya perlu diterapkan Manajemen Keamanan Aset Informasi dengan kerangka kerja COBIT 5 *for information security* (*Control Objective for Information and related Technology*) dan ISO 27001. COBIT 5 *for information security* yaitu dengan menggunakan ISO 27001:2013 sebagai standar manajemen keamanan informasi. Dari proses

penggabungan kerangka kerja tersebut diharapkan dapat mendukung penelitian penyusunan SOP (*Standard Operating Procedure*) manajemen keamanan aset informasi.

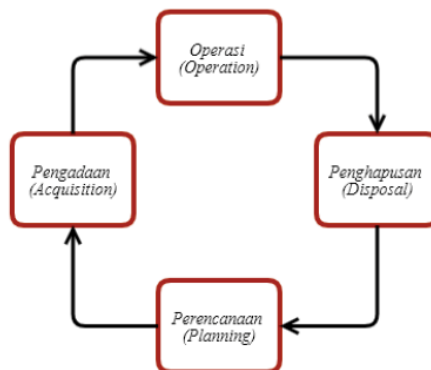
2. Tinjauan Pustaka/ Penelitian Sebelumnya

2.1 Aset

Sebagai hasil dari peristiwa transaksi, aset adalah keuntungan ekonomi yang akan diterima di masa depan atau yang akan dikelola oleh lembaga pemerintah. Aktiva (*Assets*) ialah barang berharga seperti uang tunai, produk, tanah, bangunan, dan peralatan yang dimiliki oleh instansi pemerintah. Aset merupakan sumber daya yang dikendalikan entitas sebagai akibat dari peristiwa masa lalu dan dari mana entitas mengharapkan untuk mendapatkan keuntungan ekonomi di masa depan [6].

2.2 Manajemen Aset

Manajemen aset merupakan pendekatan sistematis untuk memelihara, memperbarui, dan mengoperasikan aset dengan cara yang hemat biaya. Aset memiliki masa manfaat dan nilai uang. Manajemen aset juga berfungsi sebagai kerangka kerja untuk perencanaan jangka pendek dan jangka panjang yang merupakan suatu siklus (lihat Gambar 1) [7]. Tujuan manajemen aset adalah untuk membantu entitas (organisasi) mencapai tujuannya dalam memberikan layanan secara efektif dan efisien.



Gambar 1. Siklus Hidup Aset. Dikutip dari [7].

2.3 Aset Informasi

Aset informasi merupakan suatu informasi yang didefinisikan, disimpan dengan bermacam metode yang tidak gampang untuk ditukar, keahlian, waktu, sumber daya serta kombinasinya dan diakui selaku suatu yang berharga untuk suatu lembaga. Suatu sistem informasi mempunyai suatu komponen yang dibentuk berdasarkan pendukung yang meliputi sumber daya manusia (*people*), perangkat keras (*hardware*), perangkat lunak (*software*), data dan jaringan (*network*) [8].

2.4 Keamanan Informasi

Keamanan Informasi menurut ISACA dapat didefinisikan sebagai “*Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)*”. Keamanan sistem informasi merupakan perlindungan terhadap informasi dari 3 aspek yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan), dan perlindungan terhadap sistem serta perangkat keras yang digunakan untuk menyimpan informasi melalui penerapan kebijakan teknologi [9].

2.5 Tata Kelola Teknologi Informasi

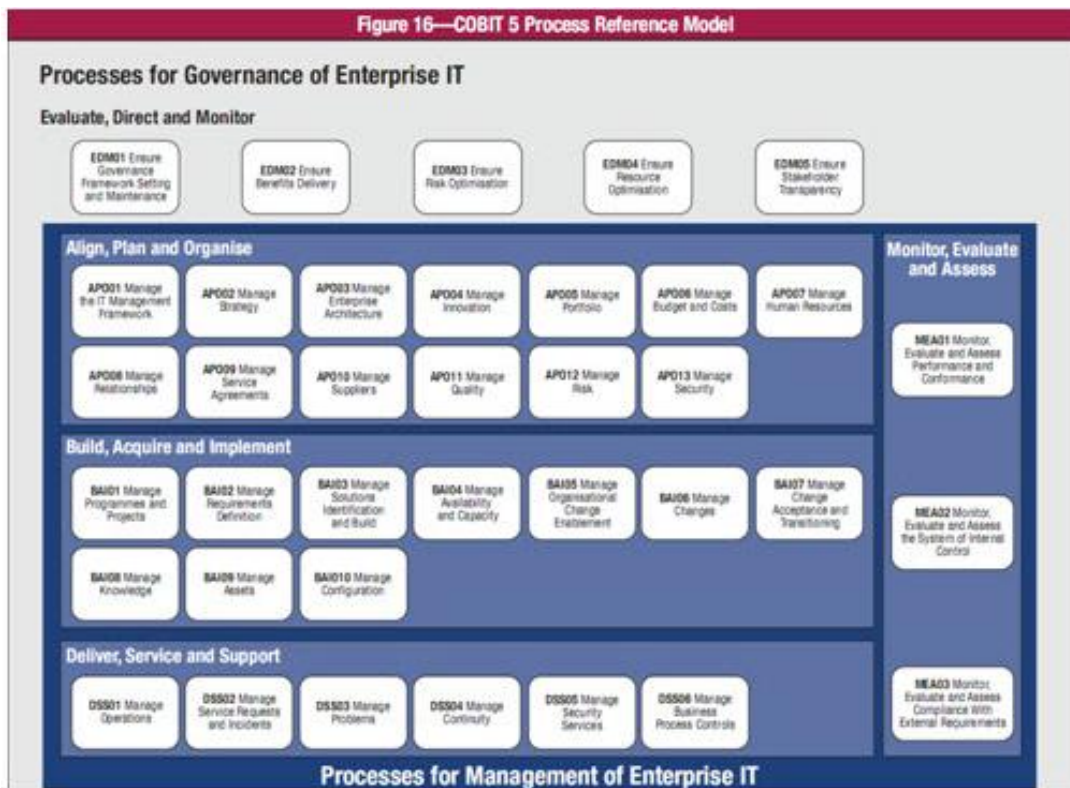
Tata kelola merupakan sebagai struktur kerangka kerja yang spesifik untuk membantu dalam mengambil sebuah keputusan secara akuntabel yang dapat mendorong perilaku yang diinginkan dalam penggunaan TI. Tata kelola teknologi informasi juga merupakan sebuah proses untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis dapat tercapai, namun tidak hanya pengelolaan proses saja tetapi juga memastikan sumber daya TI secara optimal untuk tujuan bisnis [10].

2.6 Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) atau yang disebut juga *Information Management Security System (ISMS)* merupakan suatu pendekatan yang sistematis untuk membangun, mengimplementasi, mengoperasikan, serta memantau, menjaga dan meningkatkan keamanan informasi yang berisi panduan keamanan informasi yang menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan informasi agar tetap aman yang mencakup kerahasiaan, keutuhan, dan ketersediaan untuk memenuhi tujuan perusahaan [11].

2.7 COBIT 5 For Information Security

Control Objective for Information and Related Technology (COBIT) pada Gambar 2 berikut merupakan kerangka kerja komprehensif yang dapat membantu perusahaan dalam mencapai tujuan untuk tata kelola dan manajemen perusahaan IT. Cobit dikembangkan oleh *IT Governance Institute (ITGI)* yang merupakan bagian dari *Information Systems Audit and Control Association* [12]. Berikut keseluruhan model referensi proses pada COBIT 5 sebagai berikut:



Gambar 2. Model Referensi Proses COBIT 5. Dikutip dari [12].

2.8 ISO 27001:2013 Untuk Keamanan Informasi

ISO 27001 terbit pada tahun 2013 yang merupakan hasil dari revisi SNI/IEC 27001:2009. ISO 27001:2013 menyediakan bagaimana cara membangun sistem manajemen keamanan informasi yang merupakan dokumen standar sistem manajemen keamanan informasi atau yang biasa disebut SMKI [11]. Keamanan informasi pada sebuah organisasi adalah dokumen standar sistem manajemen keamanan informasi yang dapat membagikan gambaran umum tentang hal yang harus dilaksanakan. Kontrol ISO/IEC 27001:2013 sebagai syarat untuk memenuhi persyaratan risiko yang teridentifikasi.

Kerangka kerja COBIT 5 dan ISO 27001:2013 dipilih karena mencakup unsur tata Kelola dan Manajemen yang telah dipetakan (lihat Tabel 3) dan memberikan kemudahan dalam Menyusun SOP keamanan asset informasi. Kerangka kerja lain seperti NIST (*National Institute of Standards and Technology*) atau CIS (*Critical Security Controls*) juga memberikan acuan kerangka pengamanan asset informasi yang detail dan spesifik namun lebih fokus pada keamanan siber. Jika dibandingkan COBIT 5 dan ISO 27001: 2013, kedua kerangka kerja terakhir ini lebih mampu memberikan esensi dan lingkup yang lebih luas serta dapat mencakup unsur Tata Kelola dan juga Manajemen Teknologi Informasi [13].

2.9 SOP (Standard Operating Procedure)

Penyusunan dokumen SOP (*Standard Operating Procedure*) didasarkan pada format SOP yang telah disusun. Namun ketidakkakuan format SOP menyebabkan organisasi dapat menyusun dokumen SOP sesuai dengan kebutuhannya masing-masing. Format SOP dipengaruhi oleh tujuan pembuatan SOP. Sehingga apabila tujuan pembuatan SOP maka format SOP juga dapat berbeda [13]. SOP dalam pemerintahan ini mengacu pada

3. Metodologi

Pada metodologi ini menjelaskan tentang langkah-langkah pada proses penelitian dalam menyusun dokumen SOP (*Standard Operating Procedure*) tahap pra-analisis, analisis, penyusunan dokumen SOP.

3.1 Pra Analisis

Pra-Analisis merupakan tahap dalam memulai pembuatan pada penelitian yang terdiri dari tiga tahapan sebagai berikut, studi literatur, observasi, metode pengumpulan data, dan perumusan masalah.

3.2 Analisis

Tahap analisis merupakan tahap dalam melihat kondisi aktual hingga pemetakan *best practice* COBIT 5 dan ISO 27001:2013 sebagai berikut, wawancara, penilaian risiko, pemetakan *best practice* COBIT 5 dan ISO 27001:2013

3.3 Penyusunan Dokumen SOP

Tahap dalam penyusunan dokumen SOP (*Standard Operating Procedure*) menggunakan kerangka kerja COBIT 5 dan ISO 27001:2013 dengan rincian tahapan pada tabel 1 sebagai berikut:

Tabel 1. Tahap Penyusunan SOP

Input	Proses	Output
<ul style="list-style-type: none"> • Pengendalian risiko untuk mengetahui risiko manajemen keamanan informasi yang memiliki prioritas tertinggi • Pemetakan risiko dengan kontrol ISO 27001:2013 • Validasi kontrol 	<ul style="list-style-type: none"> • Penyusunan bagian SOP • Penyusunan dokumen SOP sistem manajemen keamanan aset informasi menggunakan <i>framework</i> COBIT 5 dan ISO 27001:2013 	Dokumen SOP (<i>Standard Operating Procedure</i>) sistem manajemen keamanan aset informasi

4. Hasil dan Pembahasan

4.1 Pengumpulan Data dan Informasi

Pengumpulan data dan informasi seperti yang tertera pada Tabel 2 dibawah pada penelitian ini bertujuan untuk mengidentifikasi dan menilai risiko yang berkaitan tentang keamanan aset informasi pada Dinas Pariwisata Kebudayaan Pemuda Dan Olahraga Kabupaten Sumenep. Saat pengumpulan data, wawancara dilakukan dengan wawancara menggunakan *interview* dan observasi dengan Kasubbag.

Tabel 2. Pengumpulan Data dan Informasi

Nama Proses	Pengumpulan Data dan Informasi
Teknik	Wawancara, proses memperoleh data untuk penelitian melalui pertanyaan dan tanggapan tatap muka antara pewawancara dengan narasumber. Wawancara dilakukan dengan sistematis, terencana, dan sesuai dengan tujuan penelitian.
Objek	Keamanan Aset Informasi pada Dinas Pariwisata Kebudayaan Pemuda Dan Olahraga Kabupaten Sumenep.
Strategi Pelaksanaan	Saat melakukan wawancara, langkah selanjutnya adalah menyusun strategi pelaksanaan agar tidak ada hambatan yang dihadapi saat acara wawancara berlangsung. Strategi wawancara adalah sebagai berikut: <ul style="list-style-type: none"> • Menentukan tujuan wawancara • Membuat interview protocol • Menetapkan narasumber

4.2 Analisis

Pengumpulan daftar aset bersumber pada data yang ada pada Dinas Pariwisata Kebudayaan Pemuda Dan Olahraga Kabupaten Sumenep [14][15]. Identifikasi Kebutuhan Keamanan Aset Informasi melakukan identifikasi kebutuhan keamanan aset informasi pada Dinas Pariwisata Kebudayaan Pemuda dan Olahraga merupakan sebuah bentuk perlindungan atas ancaman yang mungkin terjadi pada proses bisnis atau atau upaya untuk meminimalisir risiko pada layanan. Yang dikelompokkan menjadi tiga kategori dalam melakukan identifikasi kebutuhan keamanan yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*).

4.3 Analisis Risiko

Analisis risiko dilakukan berdasarkan pada hasil identifikasi kebutuhan keamanan dan ancaman. Hal yang dilakukan pertama kali dalam menganalisis risiko yaitu melakukan identifikasi potensial mode kegagalan dan potensi penyebab kegagalan dalam setiap risiko. Setelah daftar risiko beserta penyebabnya. Penilaian risiko dilakukan secara keseluruhan pada seluruh komponen sistem informasi yaitu data, *hardware*, *software*, sumber daya manusia dan jaringan sehingga pada tahap analisis risiko akan diperoleh sesuai acuan yang digunakan dalam penelitian ini yaitu COBIT 5 dan ISO 27001:2013.

4.4 Prosedur Berdasarkan Hasil Rekomendasi Pengendalian Risiko

Berdasarkan hasil analisis risiko, dapat disimpulkan bahwa dalam mengelola risiko keamanan aset informasi dengan prioritas tertinggi pada Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep diperlukan prosedur yang berfungsi untuk memastikan bahwa risiko yang ada tidak dapat terjadi kembali dengan melakukan standar proses dan meminimalkan pelaksanaan suatu kegiatan operasional. Tabel 3 dibawah menjelaskan bagaimana hasil Rekomendasi Pengendalian Risiko dengan kerangka kerja COBIT 5 dan ISO 27001: 2013 yang telah dipetakan berdasarkan kebutuhan Prosedur yang dihasilkan.

Tabel 3. Hasil Rekomendasi Pengendalian Risiko


Jenis Aset	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kerangka Kerja Domain COBIT 5	Kerangka Kerja ISO 27001:2013	Prosedur Yang Dihadirkan
Data	Pengelolaan risiko tidak terdokumentasi dengan baik	Tidak terdapat dokumentasi <i>risk register</i> dan rencana pengelolaan risiko yang dimiliki DISPARBUDPORA	APO12.01 <i>Collect Data</i>	8.2 Penilaian risiko keamanan informasi 8.3 Perawatan risiko keamanan informasi	Prosedur Klasifikasi Pengelolaan Gangguan Permasalahan Aset
	Ketidakpastian penyelesaian risiko yang akan terjadi tentang aset atau layanan yang dimiliki	Tidak terdapat penerapan penilaian risiko	APO12.06 <i>Respond to Risk</i>	8.2 Penilaian risiko keamanan informasi	
	Ketidaksesuaian data pada inventaris dan <i>real</i>	Belum terdapat prosedur dan kebijakan yang dimiliki oleh DISPARBUDPORA	APO12.05 <i>Define a Risk Management Action Portfolio</i>	8.2 Penilaian risiko keamanan informasi 8.3 Perawatan risiko keamanan informasi	
	Penanganan tentang klasifikasi aset yang tidak sesuai	Tidak terdapat klasifikasi aset	BA109.01 <i>Identity and Record Current Assets</i>	A.8.2.1 Klasifikasi aset	
	Penanganan tentang klasifikasi aset yang tidak sesuai	Tidak terdapat klasifikasi aset	BA109.01 <i>Identity and Record Current Assets</i>	A.8.2.1 Klasifikasi aset	

4.5 Hasil Penyusunan Dokumen Prosedur

Berikut contoh prosedur klasifikasi pengelolaan gangguan permasalahan secara detail beserta pemetaan kontrol COBIT 5 yang dijabarkan pada Gambar 3 dibawah.

4.6 Validasi

Prosedur yang telah disusun, maka tahap selanjutnya sebelum dilakukan pembukuan dokumen *Standard Operating Procedure* (SOP) manajemen keamanan aset informasi yaitu dilakukan validasi untuk menjamin bahwa dokumen dapat diproses sesuai dengan kondisi yang ada pada Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep.

 <p>Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Jl. Gotong Royong No. 1 Sumenep Telp. 0328-667617</p>	Nomor SOP		No Aktivitas Pengurus Pengguna Barang Pelaksana Koordinator Pengurus Barang Kasubag Umum Dokumen Terkait
	Tanggal Pembuatan		
	Tanggal Revisi		
	Tanggal Efektif		
Disahkan Oleh		Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep	
Prosedur Klasifikasi Pengelolaan Gangguan Permasalahan Aset			
Deskripsi SOP Klasifikasi pengelolaan gangguan permasalahan merupakan pengurus aset yang dapat menerapkan pemantauan dan pengendalian yang sesuai agar dapat menghindari terjadinya gangguan permasalahan aset.	Kualifikasi Pelaksana 1. Staff pengelola gangguan permasalahan aset DISPARBUDPORA Kabupaten Sumenep 2. Memiliki wewenang pengelolaan gangguan permasalahan DISPARBUDPORA Kabupaten Sumenep 3. Memahami prosedur klasifikasi pengelolaan gangguan permasalahan aset DISPARBUDPORA Kabupaten Sumenep		4 Melakukan klasifikasi dan pencatatan gangguan permasalahan aset dalam formulir catatan gangguan permasalahan
Keterkaitan COBIT 5 ~ APO12.01 <i>Collect Data</i> , APO12.06 <i>Respond to Risk</i> , APO12.05 <i>Define a Risk Management Action Portfolio</i> ; BA109.01 <i>Identify and Record Current Assets</i> . ISO 27001:2013 ~ 8.2 Penilaian risiko keamanan informasi 8.3 Perawatan risiko keamanan informasi; A.8.2.1 Klasifikasi aset.	Peralatan/Perlengkapan Formulir Catatan Gangguan Permasalahan		11 2) Penerapan inisiasi tindakan pencegahan (<i>preventive</i>) yang memiliki potensi rentan pada gangguan permasalahan
Peringatan Apabila prosedur tidak dilaksanakan maka pengelolaan aset tidak sesuai dengan tupoksi yang telah ditetapkan	Pencatatan dan Pendataan Klasifikasi dan mencatat hasil gangguan permasalahan yang ada DISPARBUDPORA Kabupaten Sumenep		12 Apakah penyelesaian gangguan permasalahan berhasil? No Yes
			13 Jika berhasil, koordinator pengurus barang melaporkan laporan penyelesaian gangguan permasalahan pada aset 14 Jika tidak berhasil, melaporkan kepada koordinator pengurus barang untuk melakukan penanganan lebih lanjut 15 Selesai

Gambar 3. Contoh hasil penyusunan SOP Keamanan Aset Informasi

5. Kesimpulan

5.1 Simpulan

Berikut adalah kesimpulan yang diperoleh dari tahap analisis terhadap penyusunan dokumen dan validasi *Standard Operating Procedure (SOP)*:

- 1) COBIT 5 digunakan karena terdapat domain terkait masalah keamanan informasi yang dikategorikan dalam domain APO (*Align, Plan, and Organize*) dan DSS (*Decision, Support, and System*) untuk mengintegrasikan ke dalam proses bisnis pada setiap aspek manajemen dan operasi dan ISO 27001:2013 sebagai standar manajemen keamanan informasi yang memberikan kerangka tata kelola keamanan informasi. Hasil pemetaan COBIT 5 dan ISO 27001:2013 memberikan kerangka kerja standar dalam Menyusun SOP keamanan aset dan telah dirasa sesuai dengan kebutuhan dari Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep berdasarkan hasil wawancara dengan pihak terkait.
- 2) Hasil penyusunan dokumen SOP manajemen keamanan aset informasi menggunakan kerangka kerja COBIT 5 for information security dan ISO 27001:2013 pada Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep telah diterima dan diajukan untuk disahkan untuk diimplementasikan pada lingkungan Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep.

5.2 Saran

Untuk prosedur dapat diterapkan secara tepat dan teratur serta dimonitor secara berkala untuk menjamin dokumen SOP (*Standard Operating Procedure*) agar dapat mengurangi terjadinya risiko keamanan aset informasi pada Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep. Serta, untuk formulir dapat diterapkan oleh seluruh pelaksana di Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep agar dapat dikembangkan supaya dapat mengurangi risiko keamanan aset informasi.

6. Daftar Rujukan

- [1] CSIRT, "Teknokrat," Februari 2024. [Online]. Available: <https://csirt.teknokrat.ac.id/cyber-security-di-pemerintahan-tantangan-dan-inovasi-terbaru/>. [Accessed September 2024].
- [2] L. Septiani, "Kata Data Digital," *Kata Data*, 4 Juli 2024. [Online]. Available: <https://katadata.co.id/digital/teknologi/66862b8b7f375/kronologi-pusat-data-nasional-diretas-hingga-pejabat-kominfo-mundur>. [Accessed 1 September 2024].
- [3] Y. P. Mikhaangelo Fabialdi Nurhapy, "Tekno Kompas," *Kompas.com*, 26 Juni 2024. [Online]. Available: <https://tekno.kompas.com/read/2024/06/25/08450017/pusat-data-nasional-diserang-ransomware-hacker-minta-tebusan-rp-131-miliar>. [Accessed 31 Agustus 2024].
- [4] Badan Siber dan Sandi Negara (BSSN), "Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 4 Tahun 2021 mengatur tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik," BSSN, Jakarta, 2021.
- [5] Pemerintah Kabupaten Sumenep, "Peraturan Bupati tentang Kedudukan Susunan Organisasi, Tugas Fungsi Dan Tata Kerja Dinas Pariwisata, Kebudayaan Pemuda Dan Olahraga Kab. Sumenep," Pemerintah Kabupaten Sumenep, Sumenep, 2018.
- [6] S. V. S. R. W. A. F. E. T. T. H. Dwi Martani, *Akuntansi Keuangan Menengah Berbasis PSAK*, Jakarta: Salemba Empat, 2012.
- [7] M. Hidayat, *Manajemen Aset (Privat dan Publik)*, Yogyakarta: Laks Bang PressIndo, 2012.
- [8] J. O. George Marakas, *Introduction to Information Systems*, United States: McGraw-Hill, 2013.
- [9] H. J. M. Michael E. Whitman, *Principles of Information Security*, Cengage Learning, 2021.
- [10] J. W. R. Peter Weill, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, 2004.
- [11] SMKI Indonesia, "Implementasi SMKI dengan ISO 27001," *SMKI Indonesia*, 12 01 2021. [Online]. Available: <https://smki.or.id/implementasi-smki-dengan-iso27001/>. [Accessed 08 2024].
- [12] ISACA, *COBIT 5, ISA*, 2012.
- [13] F. H. Y. S. Diah Sulistyowati, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," *International Journal of Informatics Visualisation*, vol. 4, no. 4, 2020.
- [14] Kementerian Pendayagunaan Aparatur Sipil Negara dan Reformasi Birokrasi, "Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 35 Tahun 2012 Tentang Penyusunan SOP Administrasi Pemerintahan," *KemenPAN RB*, Jakarta, 2012.
- [15] Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kabupaten Sumenep, "Berkas Inventaris Barang," Sumenep, 2021.

