JURNAL UPI

Manajerial:
Jurnal Manajemen dan Sistem Informasi

Journal homepage: http://ejournal.upi.edu/index.php/ manajerial

Integrasi Framework dalam Penyusunan Prosedur Pengelolaan Keamanan informasi

Syarifah Norahanum Hanifah, Muhammad Andik Izzuddin, Nita Yalina

UIN Sunan Ampel Surabaya

*Correspondence: E-mail: hanifahhanum3@gmail.com, andik@uinsby.ac.id, nitayalina@uinsby.ac.id

ABSTRAK

Peningkatan kualitas layanan dewasan ini diperankan oleh adopsi TIK dalam berbagai lingkup, sehingga aspek yang muncul adalah perihal keamanan informasi dalam penyelenggaraan tata kelola. Penelitian ini bertujuan untuk menyusun panduan pengelolaan keamanan informasi dengan integrasi 3 framework yang meliputi COBIT 5, ITIL V3 dan ISO/IEC D27001:2013. Objek penelitian adalah Dinas Komunikasi dan Informasi Kabuaten Jombang. Tahapan penelitian ada 3 yaitu penyusunan pedoman, verifikasi, validasi dan perbaikan. Hasil dari tahap pertama didapatkan dari masing-masing framework dimulai dari COBIT 5 menggunakan APO13 dengan 10 aktifitas, ITIL V3 service design sub domain Information Security Management dengan 7 aktifitas, dan ISO/IEC 27001:2013 kalusul A.11 15 aktifitas. Sub domain COBIT 5 APO13.01 dipetakan dengan 9 kalusul ISO/IEC 27001:2013 dan 3 aktifitas ITIL, APO13.02 dipetakan dengan 4 klausul ISO/IEC 27001:2013 dan 1 aktifitas ITIL, APO13.03 dipetakan dengan 2 klausul ISO/IEC 27001:2013 dan 3 aktifitas ITIL. Hasil verifikasi menunjukan 66,7% narasumber menilai panduan secara bahasa dan istilah cukup jelas, mudah dipahami dan dilaksanakan. Sedangkan 100% narasumber menilai pembagian peran telah sesuai dan mampu menjawab kebutuhan instansi. Hasil validasi *expert judgement* panduan yang disusun dinyatakan valid.

ARTICLE INFO

Article History:
Submitted/Received Aug 2023
First Revised 10 Aug 2023
Accepted 10 Nov 2023
First Available online 01 Dec 2023
Publication Date 01 Dec 2023

Kata Kunci:
COBIT 5, ITIL V3, ISO 27001, Keamanan Informasi, Panduan Pengelolaan Keamanan Informasi

1. PENDAHULUAN

Dewasa ini teknologi informasi menjadi kebutuhan dalam setiap strategi bisnis baik dalam lingkup organisasi atau instansi. TIK berperan penting dalam peningkatan layanan yang diberikan. Dalam hal pelayanan publik terdapat faktor yang penting yaitu pada aspek keamanan informasi. Kinerja dalam suatu organisasi atau instansi akan terganggu apabila memiliki masalah pada keamanan informasi dikarenakan hal ini menyangkut kerahasiaan , ketersediaan dan kebutuhan (Lenawati et al., 2017).

The IT Government Institut (IT GI) mendefinisikan tata kelola IT ialah lingkup dalam tata kelola organisasi atau instansi yang meliputi struktur organisasi dan kepemimpinan yang bertujuan memastikan organisasi dapat mencapai tujuan dan strategi (Pratama & Perdana kusuma, 2018). Tata Sutabri berpendapat bahwa informasi dapat diartikan sebagai data yang telah diproses dan memiliki *value* yang penting serta berguna dalam pengambilan suatu keputusan, dan keamanan informasi diartikan sebagai tindakan dalam menjaga atau mengamankan aset IT dari berbagai ancaman dari berbagai arah (Widya, 2016). Dalam penerapannya terdapat komponen yang harus diperhatikan yang meliputi integritas, ketersediaan dan kerahasiaan (Nurul et al., 2022).

Berdasarkan pada peraturan Pemerintah Republik Indonesia Tahun 2016 Nomor 4 tentang manajemen pengamanan informasi , dimana semua penyelenggara sistem elektronik diharuskan menyiapkan strategi dalam menjaga keamanan terhadap informasi yang dimiliki. Sehingga dapat diketahui bahwa keamanan informasi sangat penting dalam rangka memenuhi kewajiban dalam memenuhi peraturan tersebut.

Berdasarkan surat dari Dinas Komunikasi dan Informatika Kabupaten Jombang Nomor 470/232/415.23/2020 tentang keharusan dalam melakukan penelitian yang berkaitan dengan keamanan informasi, sehingga dilakukan penelitian dengan mengintegrasikan beberapa *framework* TI menjadi pedoman dalam pengelolaan keamanan informasi. Dengan adanya dokumem pengelolaan keamanan informasi diharap mendapatkan padangan yang komperhensif sekaligus sistematis dalam hal keamanan informasi.

2. KAJIAN PUSTAKA

Teknologi informasi diartikan sebagai peralatan elektornik yang dapat mengkorelasikan antara pekerjaan dengan informasi yang berkaitan dengan tugas proses informasi (Haaq dan Kee), sehingga tidak hanya berkaitan dengan komputer sebagai media penyimpan namun dapat mencakup bagaimana pengiriman informasi (Tampang, 1907). Tekonologi informasi digunakan untuk pengolahan data yang meliputi pengambilan, pemrosesan, penyusunan, penyimpanan dan manipulasi informasi (Tampang, 1907). Sehingga adopsi teknologi informasi dalam lingkup organisasi atau perusahaan menjadi strategi dalam meningkatkan daya saing(Sulaiman Naibaho, 2017).

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

Tata kelola menjadi bagian dalam pengelolaan organisasi yang terintergrasi dan mencakup proses, struktur dan kepemimpinan organisasi dan instansi (Pribadi, 2013). Implementasi Tata kelola dalam perusahaan kana memiliki dampak positif pada kinerja dan meningkatnya nilai perusahaan (Noviarti & Yosi Stefhani, 2022). Hal ini bertujuan untuk dapat memperluas strategi dan optimis mempertahankan suatu tujuan organisasi (Afrianto et al., 2014) . Dalam IT Governance Institute, mendefinisikan tata kelola TI adalah tanggungjawab manajemen level atas atau dewan direksi (Ernawati & Santoso, 2016).

Keamanan Informasi adalah suatu usaha dalam menjaga informasi penting dari ancaman yang diperkirakan akan terjadi . Keamanan informasi selanjutnya diharapkan dapan menjamin kelanjutan strategi, meminimalisir risiko yang timbul dan optimal dalam hal *value* investasi. Keamanan informasi menjadi hal yang penting dalam melindungi informasi dan aset pada suatu organisasi atau perusahaan (Nurul et al., 2022). Menurut Whitman & Mattord ada beberapa jenis keamanan informasi sebagaimana berikut (Akraman & Priyadi, 2018):

1. *Security Physical*
2. *Security Personal*
3. *Security Operasional*
4. *Security Communication*
5. *Security Network*

COBIT dikembangkan pada tahun 1996 oleh ITGI dan merupakan *framework* yang biasa diimplementasikan dalam *IT Governance* dikarenakan dapat membantu dalam manajemen, auditor dan *user* untuk merelasikan antara kebutuhan kontrol terhadap risiko strategi bisnis dan masalah lainnya (Milkovich, 2012). COBIT saat ini dianggap sebagai *framework* yang konfeherensif yang sangat membantu dalam hal membantu suatu organisasi atau perusahaan dalam mencapai tujuan bisnis dengan manajemen TI dan tata kelola TI (Moonda & Norita, 2020). COBIT 5 telah di integrasikan dengan praktik tata kelola TI dengan tujuan dapat memudahkan dalam pemahaman, pengelolaan risiko, keamanan dan segala sesuatu yang berkaitan dengan TI (Andry et al., 2022). COBIT memiliki 5 prinsip dasar (Tambotoh et al., 2015) sebagaimana terlihat pada Gambar 1 berikut.

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

Gambar 1. Lima Prinsip COBIT 5 (Milkovich, 2012)

ITIL dikembangkan oleh Office of Government Commerce (OGC), dan menyimpulkan ITIL memuat praktek terbaik yang dapat menjadi pedoman/acuan dalam ITSM (Handoko, 2017). Salah satu *best practice* dari ITSM dalam bidang teknologi informasi ialah ITIL (Taylor et al., n.d.). Memiliki tujuan menyelaraskan kebutuhan bisnis dan layanan TI. Konsep ITIL digunakan untuk mengelola, mengembangkan dan mengoperasikan TI (Taylor et al., n.d.). ITIL Versi 3 menjadi update terbaru. Siklus hidup ITIL meliputi 5 *service* yaitu *service strategy(SS), service design (SD), service transition (ST), service operation (SO) dan continual service improvement (CSI)* (Wibowo, n.d.).

Gambar 2. Lifecycle ITIL V3 (Taylor et al., n.d.)

International Organization for Standardization meluncurkan standar mengenai cara melindungi sistem manajemen keamanan informasi (SMKI) yaitu ISO/IEC 27001:2013 (Afrianto et al., 2014). Sistem manajemen keamanan informasi adalah pendekatan yang digunakan untuk mengelola informasi penting atau sesitif agar tetap aman. ISO/IEC 27001 adalah standar audit keamanan pada sebuah sistem informasi yang sekaligus menjadi acuam dalam penyusunan dokumen rekomendasi (pedoman) (Bakri & Irmayana, 2017). ISO/IEC 27001:2013 dirancang untuk dapat disesuaikan dalam lingkup kecil, menengah dan besar dan

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

dalam sektor apapun (Fdis, 2013). ISO/IEC 27001:2013 memiliki 14 kalusul, *security control*, *objective control*, dan 14 *control* (Pratiwi, 2019).

Adapun klausul dari ISO/IEC 27001:2013 adalah sebagai berikut :

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 Asset 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

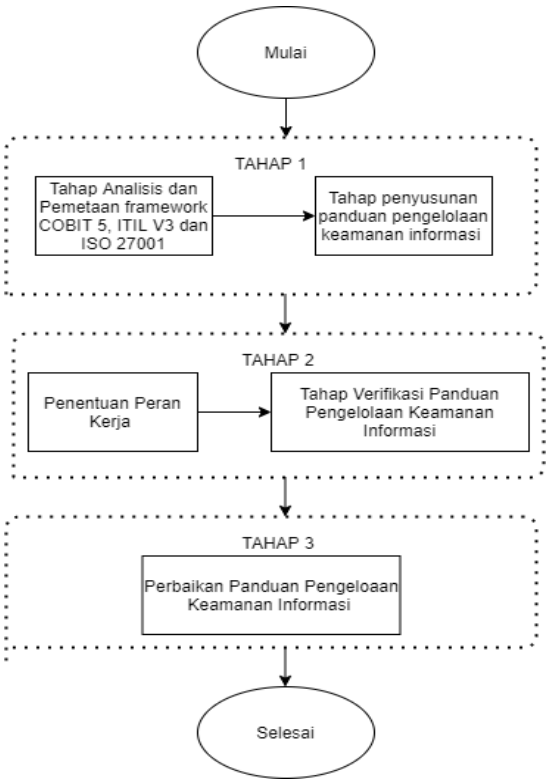
13. Klausul A.17 Information Security Aspects of Business Continuity Management

14. Klausul A.18 Compliance (Fdis, 2013)

Dinas Komunikasi dan Informatika Kabupaten Jombang yaitu organisasi perangkat daerah (OPD) yang membidangi komunikasi, informasi, statistik, humas dan persandian. Pada awalnya tugas-tugas yang diemban oleh Dinas Komunikasi dan Informatika menjadi tanggungjawab Kantor Perpustakaan, Arsip dan PDE (Pengelolaan Data Elektronik). Sehingga Dinas KOMINFO telah berdiri selama 4 tahun dengan 43 tenaga kerja. Saat ini panduan dalam bidang keamanan masih dalam tahap pemula dan belum memiliki SOP.

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

3. METODE PENELITIAN



Gambar 3. Flowchart Penelitian

3.1. Tahap Pertama

Terdapat 3 tahapan dalam penyusunan prosedur pengelolaan keamanan informasi ini yaitu:

a. Melakukan analisa proses pada *framework* COBIT 5, ITIL V3 dan ISO/IEC 27001:2013 untuk selanjutnya proses pemetaan pada ketiga *framework* dengan penyesuaian aktivitas yang saling berkaitan.
b. Pemetaan *framework* : pembuatan panduan pengelolaan keamanan yang ada pada ISO 27001 (Klausul A.11) dan ITIL V3 (Service Design) ke COBIT5 (APO13). Menentukan klausul A.11 (ISO/IEC 27001:2013) dan Service Design (ITIL V3) yang bersesuaian dengan APO13 (COBIT5).
c. Penyusunan Panduan : dari hasil pemetaan akan disusun panduan/acuan pengelolaan keamanan.

3.2. Tahap Kedua

a. Penentuan peran kerja berdasarkan RACI *Chart* dari *framework* COBIT 5
b. Verifikasi prosedur panduan pengeloaan keamanan informasi dilakukan dengan mengimplementasikan pada instansi. Pelaksanan verifikasi adalah Dinas KOMINFO Kab. Jombang. Responden ditentukan berdasarkan RACI *Chart* yang dipetakan dalam struktur organisasi Dinas.

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

3.3. Tahap Ketiga

Perbaikan panduan apabila terdapat kekurangan yang ada berdasarkan proses verifikasi dan validasi *expert judgement.*

4. HASIL DAN PEMBAHASAN

4.1. Penyusunan Prosedur Pengelolaan Keamanan Informasi

Analisis dan Pemetaan *Farmework*

Analisis dilakukan pada 3 *framework* yang telah dipilih dalam penelitian ini yaitu framewor COBIT5 , ITIL V3 dan ISO/IEC 27001:2013. Berikut adalah rincian dari masing-masing proses dan aktivitas dalam domain terpilih. Rincian sub domain dan aktifitas APO13 pada COBIT 5 adalah sebagaimana terlihat pada Tabel 1 berikut:

Tabel 1. Key Practice Domain AP013 Manage Security

Key Practice	***Name practice***	***Activity Code***
APO13.01	Menetapkan dan memelihara informasi sistem manajemen keamanan informasi (SMKI)	APO13.01-1, APO13.01-2, APO13.01-3, APO13.01-4, APO13.01-5, APO13.01-6, APO13.01-7
APO13.02	Menentukan dan Mengelolah rencana perawatan risiko keamanan informasi	APO13.01-1, APO13.01-2, APO13.01-3, APO13.01-4, APO13.01-5, APO13.01-6, APO13.01-7
APO13.03	Memantau dan meninjau sistem manejemen keamanan informasi (SMKI)	APO13.03-1, APO13.03-2, APO13.03-3, APO13.03-4, APO13.03-5

Rincian *framework* ITIL V3 domain *Service Design* sub domain *Information Security Management* terlihat pada Tabel 2 berikut :

Tabel 2. Aktivitas Information Security Management, Service Design ITIL V3

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

Proses *Information Security management*	Kode aktivitas
Produksi, peninjauan, dan revisi Kebijakan Keamanan Informasi secara keseluruhandan serangkaian kebijakan khusus yang mendukung	ISM01
Komunikasi , implementasi dan penegakan kebijakan keamanan Penilaian dan klasifikasi semua aset informasi dan dokumentasi	ISM02
Penilaian dan klasifikasi semua aset informasi dan dokumentasi	ISM03
Implementasi, peninjauan, revisi, dan peningkatan satu set keamanan kontrol dan penilaian risiko serta respons	ISM04
Pemantauan dan pengelolaan semua pelanggaran keamanan dan keamanan besar insiden	ISM05
Analisis, pelaporan, dan pengurangan volume dan dampak keamanan pelanggaran dan insiden.	ISM06
Jadwalkan dan selesaikan ulasan keamanan, audit, dan uji penetrasi	ISM07

Sedangkan rincian Kalusul A.11 *Physical and Enviromental Security* ISO/IEC 27001:2013 adalah pada Tabel 3 berikut :

Tabel 3. *Control Objective* Klausul A.11 ISO/IEC, 2013

Klausul	*Objective Control*	*Security Control*
A.11 *Physical and Enviromental Security*	*A.11.1 Secure Areas*	*A.11.1.1 Physical security perimeter* *A.11.1.2 Physical entry controls* *A.11.1.3 Securing offices, rooms and facilities* *A.11.1.4 Protecting against external and environmental threats* *A.11.1.5 Working in secure areas* *A .11.1.6 Delivery and loading areas*
	A.11.2 Equipment	*A.11.2.1 Equipment siting and protection* *A.11.2.2 Supporting utilities* *A.11.2.3 Cabling security* *A.11.2.4 Equipment maintance* *A.11.2.5 Removal of assets* *A.11.2.6 Security of equipment and assets off-premises* *A.11. 2.7 Secure disposal or reuse of equipment* *A.11.2.8 Unattended user* *A.11.2.9 Clear desk and clear screen policy*

Pemetaan *Framework*

Pemetaan dilakukan pada ISO/IEC 27001:2013 kalusul A.11 dan sub domai service design ITIL V3 yang memiliki kesinambungan dengan key practice COBIT 5 Sub Domain APO13 Manage Security . Adapun hasil dari pemetaan adalah sebagaimana Tabel 4 berikut:

Tabel 4. Hasil Pemetaan

COBIT 5	Hasil Pemetaan dengan ISO & ITIL
APO 13.01	A.11.1.1, A.11.1.3, A.11.2.1, A.11.2.2, A.1 1.2.5, A.11.2.4, A.11.1.2, A.11.1.6, A.11.2.9, ISM01, ISM02& ISM03

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

APO 13.02	A.11.1.6, A.11.1.5, A.11.1.4, A.11.2.3, ISM04
APO 13.03	A.11.2.7, A.11.2.8, ISM05, ISM06 & ISM07

Penyusunan Panduan

Penyusunan panduan berdasarkan pada hasil pemetaan Tabel 4 yang dibuat berupa langkah kerja. Hasil penyusunan panduan sebagaimana terlihat pada Tabel 7.

4.2. Penentuan Peran dan Verifikasi Hasil Panduan

Peran dan Tanggungjawab

Dalam menentukan peran dan tanggungjawab mengacu pada RACI *Chart* COBIT 5. Berikut adalah Gambar 4 RACI *Chart* domain APO13 COBIT 5.

APO13 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO13.01 Establish and maintain an ISMS.		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Define and manage an information security risk treatment plan.		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Monitor and review the ISMS.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Gambar 4. RACI Chart APO13 COBIT 5

Penentuan tanggungjawab yaitu data yang tingkat tanggungjawab *responsible* atau memiliki lambang R. hal ini dikarenakan peran *responsible* dinilai lebih menguasai proses terkait domain dan proses TI yang ada. Berikut Tabel 5 adalah hasil pemetaan peran dan tanggungjawab:

Tabel 5 Hasil Pemetaan Struktur Organisasi

Strutur Organisasi RACI COBIT 5	Struktur Organisasi KOMINFO JOMBANG
Chief Information Officer	Bidang Teknologi Informasi dan Komunikasi
Head IT. Administration	Seksi Pengeloaan Data dan Integritas Sistem Informasi
Information Security Manager	Seksi Infrastruktur, Keamanan Informasi dan Telekomunikasi

Verifikasi Panduan Pengelolaan Keamanan Informasi

Verifikasi panduan bertujuan untuk mengetahui kesesuaian panduan, apakah mudah dipahami dan kesesuaian terhadap implementasi pada suatu instansi atau organisasi.

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

Verifikasi dilakukan dengan menggunakan form penilaian yang akan diisikan oleh narasumber terkait. Adapun pihak atau narasumber yang terpilih sebagaiman pada Tabel 5. Adapun indikator pertanyaan adalah menurut penulis sendiri yang disusun dan dirasa dapat menjawab terkait verifikasi.

Tabel 6. Rekapitulasi Jawaban Narasumber

No	Indikator Penilaian	Jawaban	Hasil
1	Bagaimana bahasa yang digunakan dalam panduan prosedur	Tidak Jelas	0%
		Cukup Jelas	33,30%
		Jelas	66,70%
		Sangat Jelas	0%
2	Apakah panduan prosedur yang telah dibuat mudah untuk dilaksanakan?	Sulit dilaksanakan	0%
		Cukup mudah dilaksanakan	66,70%
		Mudah dilaksanakan	33,30%
		Sangat mudah dilaksanakan	0%
3	Apakah istilah yang terdapat panduan prosedur mudah untuk dipahami?	Sulit dipahami	0%
		Cukup mudah dipahami	66,70%
		Mudah dipahami	33,30%
		Sangat mudah dipaham	0%
4	Dalam panduan prosedur terdapat pembagian peran kerja, apakah sudah sesuai dengan fungsional Struktur Organisasi Diskominfo?	Tidak sesuai	0%
		Cukup sesuai	0%
		Sesuai	100%
		Sangat sesuai	0%
5	Apakah panduan prosedur yang telah dibuat bisa menjawab kebutuhan keamanan informasi instansi?	Ya	100%
		Tidak	0%

Berdasarkan hasil verifikasi didapatkan infromasi bahwa 66 ,7% narasumber menilai secara bahasa dan istilah dalam panduan dinilai jelas dan cukup mudah dipahami. Sebanyak 66 ,7% narasumber menilai bahwa panduan cukup mudah dilaksanakan , lalu 100% narasumber menilai bahwa pembagian peran telah sesuai . Persentasi 100% narasumber menyatakan bahwa panduan prosesur telah menjawab kebutuhan instansi.

4.3. Perbaikan Panduan Prosedur dan Validasi *Expert Judgement*

Validasi *Expert Judgement*

Validasi dibubuhkan untuk menguji pedoman operasional telah sesuai menurut ahli tahap validasi dilakukan mulai dari tahap awal, proses penelitian, pengolahan data hingga terbentuknya panduan operasional.

Perbaikan Panduan Prosedur

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

Perbaikan panduan operasional dilakukan berdasarkan dari hasil verifikasi narasumber dan validasi *Expert Judgement* . Adapun perbaikan adalah sebagai berikut:

a) Perlu adanya kebijakan dan persiapan terkait implementasi panduan prosedur agar berguna secara optimal
b) Dalam hal pengertian masing-masing indikator, sub indikator dan tata bahasa kurang mendalam. Maka diperlukan perbaikan:

- Memperjelas masing-masing indikator
- Memperbaiki tata bahasa

Berikut adalah hasil dari penyusunan pedoman prosedur yang telah diverifikasi pihak instansi terkait, divalidasi oleh *Expert Judgement* dan telah di perbaiki sesuai dengan hasil penilaian (Tabel 7).

4.4. Panduan Prosedur pengelolaan Keamanan informasi

Unit Penanggung jawab:

1. *Chief Information Officer*
2. *Head IT Administration*
3. *Information Security Manage*r

Tabel 7. Panduan Prosedur Pengelolaan Keaanan Inforasi

Proses	No	Langkah Kerja
Menetapkan dan memelihara informasi sistem manajemen keamanan informasi (SMKI)	1.	Menetapkan Ruang lingkup a) Organisasi dapat menetapkan ruang lingkup dalam hal karakteristik perusahaan , organisasi, lokasi, aset dan teknologi b) Membuat batas bat as keamana n untuk melindungi area yang menggandung informasi atau kriris fasilitas pengelolahan .
	2.	Menentukan kebijakan manajemen keamanan informasi: 1. Tentukan SMKI sesuai dengan kebijakan yang ada pada organisasi atau perusahaan selaras dengan organisasi, perusahaan , lokasi , aset dan teknologi 2. Rancang dan tetapkan keamanan fisik untuk kantor, k amar dan fasilitas 3. Adopsi kebij akan m eja ya ng jelas unt uk kertas dan media penyimpanan yang bisa dilepas serta keb ijakan layar yang jelas untuk fasi litas pemros esan informa si 4. keamanan yang diterapkan pada aset diluar lokasi harus mempertimbangkan berbagai risiko bekerja diluar gedung organisasi 5. Produksi serangkaian kebijakan khusus yang mendukung
	3.	Melakukan peninjauan secara keseluruan: a) sejajarkan ISM dengan pendekatan perusahaan secara keseluruhan pada manajemen keamanan b) Lakukan peninjauan, dan revisi kebijakan keamanan informasi secara keseluruhan
	4.	Mengimplementasi SMKI: a) Dapatkan otorisasi manajemen untuk mengimplemtasikan, mengoperasikan dan mengubah

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

Proses	No	Langkah Kerja
		SMKI b) Lakukan implementasi dan penilaian terhadap semua klasifikasi aset dan dokumentasi
	5.	Memelihara Perangkat: a) Siapkan dan pelihara pernyataan penerapan yang menggambarkan ruang lingkup b) Letakkan dan lindungi peralatan guna mengurangi risiko yang bisa menyebabkan ancaman dan bahaya lingkungan juga peluang akses yang tidak sah c) Lindungi peralatan dari kegagalan daya dan gangguan lain yang disebabkan oleh kegagalan dalam utilitas pendukung d) Tidak diperbolehkan membawa keluar perangkat lunak atau peralatan informasi dari lokasi tanpa adanya otorisasi sebelumnya e) Pelihara perangkat dengan benar untuk memastikan kelanjutan ketersediaan dan integritas. f) Penilaian dan klasifikasi semua aset informasi dan dokumentasi
	6.	Menetapkan dan mengkomunikasikan peran dan tanggung jawab manajemen keamanan informasi: a) Lindungi area aman dengan kontrol entri yang sesuai agar dapat memastikan bahwa hanya personel yang berwenang saja yang diizinkan mengakses b) Kendalikan jalur akses seperti area pengiriman, pemuatan dan titik lainnya dimana orang-orang yang tidak berwenang dapat memasuki tempat tersebut c) Isolasi pemrosesan informasi jika memungkinkan untuk menghindari akses yang tidak sah d) Lakukan Komunikasi, implementasi dan penegakan kebijakan keamanan
	7.	Komunikasikan pendekatan Sistem Manajemen keamanan Informasi (SMKI), implementasi dan penegakan kebijakan keamanan penialaian dan klasifikasi semua aset informasi dan dokumentasi
Menentukan dan Mengelolah rencana perawatan risiko keamanan informasi	1.	Identifikasi Manajemen Keamanan Informasi: a) Identifikasi praktik manajemen yang tepat dan optimal b) Identifikasi solusi keamanan dengan sumber daya, tanggung jawab dan prioritas terait pengelolaan risiko keamanan informasi
	2.	Mengelolah rencana perawatan risiko: a) pertahankan bagian dari arsitektur perusahaan inventarisasi komponen solusi yang tersedia untuk mengelola risiko terkait keamaman b) Rancang dan tetapkan prosedur untuk bekerja di daerah aman c) Implementasikan, tinjau, revisi dan peningkatan satu set keamanan kontrol.
	3.	Perawatan risiko a) kembangkan proposal untuk rencana perawatan risiko b) Implementasikan rencana perawatan risiko keamanan informasi yang didukung oleh kasus-kasus yang sesuai. Meliputi pertimbangan pendanaan dan alokasi peran serta tanggung jawab

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

Proses	No	Langkah Kerja
	4.	Mengembangkan solusi perawatan risiko a) Berikan masukan untuk desain praktik manajemen kemanan informasi. b) Berikan masukan untuk pengembangan solusi yang dipilih dari rencana perawatan risiko kemanan informasi c) Rancang dan terapkan perlindungan fisk terhadap bencana alam, serangan jahat atau kecelakaan d) Lindungi kabel listrik dan telekomunikasi yang membawa data atau layanan informasi pendukung dari intesepsi ganguan dan kerusakan e) Berikan penilaian risiko serta respons
	5.	Tetapkan bagaimana mengukur efektivitas pratik manajemen terpilih menghasilan hasil yang sebanding dan dapat direproduksi
	6.	Rekomendasikan pelatian keamanan informasi dan program kesadaran
	7.	Integrasikan antara perencanaan, desain, implementasi dan pemantauan informasi
Memantau dan meninjau sistem manejemen keamanan informasi (SMKI)	1.	Membuat Hasil Audit a) Buat hasil akun audit keamanan, insiden, hasil dari pengkuran efektivitas, sarandan juga umpan balik dari semua pihak yang berkepentingan b) Selesaikan ulasan keamanaan audit dan uji penetrasi
	2.	Melakukan Audit a) Lakukan audit ISMS internal pada interval yang direncanakan b) Buat jadwal keamanan keamanan audit
	3.	Meninjau SMKI a) Lakukan tinjauan pada sistem manajemen keamanan informasi secara teratur untuk memastikan bahwa ruang lingkup tetap memadai b) Lakukan identifikasi perbaikan dalam proses SMKI c) Verifikasi semua ite m pera latan yang mengandung m edia penyimpanan untu k memastikan bahwa data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa dengan aman sebelum dibuang ataupun digunakan lagi d) Semua pelanggaran keamanan dan insiden harus dipantau dan ditinjau e) Lakukan analisis , pelaporan dan pengurangan dampak dan volume keamanan, pelangaran serta insiden
	4.	Berikan masukan untuk pemeliharaan rencana keamanan guna memperhitungkan temuan kegiatan pemantauan dan peninjauan
	5	Catat dan awasi semua tindakan a) Catat tindakan dan peristiwa yang berdampak pada efektivitas atau kinerja b) Pengguna harus memastikan bahwa peralatan tanpa pengawasan sudah sesuai perlindungan

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

5. KESIMPULAN

Integrasi *framework* untuk menyusun panduan prosedur pengelolaan keamanan informasi ini menggunakan COBIT 5, ITIL V3 dan ISO/IEC 27001:2013. Pada tahap pertama analisis aktifitas pada masing-masing domain yang meliputi 3 sub domain (*Key Practice*) APO13 dari COBIT 5, 7 aktifitas dalam sub domain *Information Security Management* dari ITIL V3 dan 15 aktifitas pada kalusul A.11 ISO/IEC 27001:2013. Hasil pemetaan menunjukan sub domain COBIT 5 APO13.01 dipetakan dengan 9 kalusul ISO/IEC 27001:2013 dan 3 aktifitas ITIL, APO13.02 dipetakan dengan 4 klausul ISO/IEC 27001:2013 dan 1 aktifitas ITIL, APO13.03 dipetakan dengan 2 klausul ISO/IEC 27001:2013 dan 3 aktifitas ITIL.

Proses penentuan peran kerja mengacu pada RACI *Chart, Chief Information Officer* diperankan oleh Bidang Teknologi Informasi dan Komunikasi, *Head IT. Administration* oleh Seksi Pengeloaan Data dan Integritas Sistem Informasidan *Information Security Manager* oleh Seksi Infrastruktur ,Keamanan Informasi danTelekomunikasi.

6. SARAN

Dari hasil verifikasi diketahui bahwa 66,7% narasumber menilai dari segi bahasa dan istilah yang dituangkan dalam prosedur jelas dan cukup mudah dipahami. Dari segi pelaksanaan panduan dinilai cukup mudah dilaksanakan dengan persentase 66,7%, dan 100% responden menilai pembagian peran panduan prosedur dan dapat menjawab kebutuhan organisasi Dinas KOMINFO Kabupaten Jombang. Tahap akhir setelah dilakukan perbaikan hasil verifikasi dilakukan penilaian oleh *expert judgement,* panduan prosedur pengelolaan keamanan informasi yang disusun dinyatakan valid.

7. DAFTAR PUSTAKA

Afrianto, I., Suryana, T., & Sufa'atin. (2014). *Pengukuran Keamanan Informasi pada Aplikasi dan Sistem Informasi Pendukung Akademik Menggunakan SNI ISO/IEC 27001:2009* (p. 7). Unikom.

Akraman, R., & Priyadi, Y. (2018). *Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia*. *02*, 115–122.

Andry, J. F., Lee, F. S., Darma, W., Rosadi, P., & Ekklesia, R. (2022). Audit Sistem Informasi Menggunakan Cobit 5 Pada Perusahaan Penyedia Layanan Internet. *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi*, *8*(1), 17. https://doi.org/10.24014/rmsi.v8i1.14761

Bakri, M., & Irmayana, N. (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001. *Jurnal Tekno Kompak*, *11*(2), 41. https://doi.org/10.33365/jtk.v11i2.162

Ernawati, L., & Santoso, H. B. (2016). Tata Kelola Teknologi Informasi Di Lingkungan Perguruan Tinggi: Hambatan, Tantangan, Dan Peluang. *Seminar Nasional APTIKOM (SEMNASTIKOM)*, *2*(1), 806–811.

Fdis, I. E. C. (2013). *INTERNATIONAL STANDARD ISO / IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. *2013*.

Handoko, Y. (2017). Pemanfaatan ITIL v3 untuk Mengatasi Masalah Layanan TI pada Sistem Terintegrasi di Perguruan Tinggi Using ITIL v3 to Solve IT Service Problem in Integration System at Universities. *Prosiding SAINTIKS FTIK UNIKOM*, *2*.

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

Milkovich, A. (2012). *A Business Framework for the Governance and Management of Enterprise IT*.

Moonda, P. A., & Norita, B. (2020). Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 (Studi Kasus : PT. Jamkrida Provinsi Jawa Tengah). *Jurnal Masyarakat Informatika*, *11*(1), 1–21. https://doi.org/10.14710/jmasif.11.1.31449

Noviarti, & Yosi Stefhani. (2022). Analisis Tata Kelola Perusahaan, Dan Nilai Perusahaan. *Jurnal Manajemen*, *6*(2), 73–82. https://doi.org/10.54964/manajemen.v6i2.205

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)*, *Vol. 3*(No. 5), 564–573.

Pratama, E. R., & Perdana kusuma, A. R. (2018). *Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001*. *2*(11), 5911–5920.

Pratiwi, W. A. (2019). *Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 pada Kominfo Provinsi Jawa Timur*. 1–168. https://repository.dinamika.ac.id/id/eprint/3310/1/14410100156-2019-STIKOMSURABAYA.pdf

Pribadi, M. R. (2013). Penerapan Tata Kelola Teknologi Informasi Dengan Menggunakan Cobit Framework 4.1 (Studi Kasus Pada Pt. Vaksincom). *Jurnal Eksplora Informatika*, *1*(November), 115–124. http://digilib.esaunggul.ac.id/UEU-Undergraduate-200883091/408

Sulaiman Naibaho, R. (2017). *PERANAN DAN PERENCANAAN TEKNOLOGI INFORMASI DALAM PERUSAHAAN*. *April*. https://media.neliti.com/media/publications/290731-peranan-dan-perencanaan-teknologi-inform-ad00d595.pdf

Tambotoh, J. J., Augie David Manuputty, M., & Kristen Satya Wacana Salatiga, U. (2015). *Pengukuran Tingkat Kapabilitas Tata kelola TI Menggunakan Kerangka kerja COBIT 5 (Studi Kasus: PT. PDA. Net Kota Cirebon) Artikel Ilmiah Peneliti: Rininta Ayunigdiah (682011607)*. *5*.

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570

Tampang, B. L. (1907). *PERAN TEKNOLOGI INFORMASI DALAM PENGEMBANGAVOKASI PENDIDIKAN TINGGI*. 415–422.

Taylor, S., Lloyd, V., & Rudd, C. (n.d.). *ITIL Version 3 Service Design*. OGC.

Wibowo, A. M. (n.d.). *Service Design IT Infrastructure Library Versi 3*.

Widya, D. R. (2016). PENGARUH FAKTOR PENDIDIKAN, PELATIHAN DAN PENGUASAAN KOMPUTER STAF BAGIAN KEUANGAN TERHADAP KUALITAS PENYAJIAN INFORMASI AKUNTANSI. In *http://repository.unpas.ac.id/*.

DOI: https://doi.org/10.17509/manajerial.v22i2
ISSN: 1412-6613 & E-ISSN: 2527-4570