Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Kepedulian Keamanan Informasi di Pemerintahan: Praktik Manajemen dan Dampaknya

Bemy Fachriandi[1], **Teduh Dirgahayu**[2]
[1,2]Program Studi Magister Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia, Yogyakarta, Indonesia
e-mail: [1]17917105@students.uii.ac.id

Abstrak

Dalam sebuah organisasi pentingnya meningkatkan praktik kepedulian keamanan informasi menjadi prioritas utama yang dilakukan oleh manajemen dengan cara menerapkan praktik manajemen keamanan informasi meskipun praktik yang dilakukan tidak selalu berdampak pada perubahan perilaku anggota organisasi. Berbagai praktik keamanan informasi dilakukan namun ada saja kendala yang terjadi seperti minimnya kesadaran keamanan informasi, perilaku kerja, budaya kerja serta kurangnya sumber daya manusia yang ada. Banyak praktik keamanan informasi yang telah dilakukan oleh manajemen namun apakah anggota organisasi peduli terhadap praktik tersebut. Dengan demikian maka dilakukan penelitian dengan tujuan untuk mengetahui apakah praktik kepedulian keamanan informasi yang diterapkan oleh manajemen berdampak bagi anggota organisasi khususnya organisasi itu sendiri. Fokus penelitian pada organisasi pemerintah dengan menggunakan metode interpretif kualitatif dan kuantitatif sebagai proses pengumpulan data di tiga organisasi pemerintahan. Dengan memanfaatkan model SAP-LAP maka diketahui berbagai praktik yang diterapkan oleh manajemen di organisasi pemerintahan dan hasil survei menunjukkan dampak positif artinya anggota organisasi memiliki kepedulian yang tinggi terhadap praktik keamanan informasi yang diterapkan.

Kata kunci: *Keamanan Informasi; Kepedulian Keamanan Informasi; Praktik Manajemen Keamanan Informasi; SAP-LAP; Organisasi Pemerintah*

Abstract

In an organization, the importance of increasing the practice of information security concern is a top priority carried out by management by implementing information security management practices even though the practices carried out do not always have an impact on changes in the behavior of members of the organization. Various information security practices are carried out but there are obstacles that occur such as a lack of awareness of information security, work behavior, work culture and a lack of human resources. Many information security practices have been carried out by management, but whether members of the organization care about these practices. Thus, a research was carried out with the aim of finding out whether the information security concern practices implemented by management had an impact on members of the organization, especially the organization itself. The research focuses on government organizations using qualitative and quantitative interpretive methods as a data collection process in three government organizations. By utilizing the SAP-LAP model, it is known that the various practices implemented by management in government organizations and the survey results show a positive impact, meaning that organizational members have a high level of concern for the implemented information security practices.

Keywords: *Information Security; Information Security Concerns; Information Security Management Practices; SAP-LAP; Government Organization*

1. Pendahuluan

Organisasi mempunyai tanggung jawab dalam meningkatkan keamanan informasi bagi semua anggota organisasi yang terlibat tentu dengan pengelolaan dan pemanfaatan informasi yang baik. Praktik keamanan informasi dapat digunakan oleh organisasi guna meminimalisir terjadinya resiko dan kendala. Kendala yang bisa terjadi adalah lemahnya tingkat kepedulian terhadap keamanan informasi baik dari manajemen dan anggota organisasi sebagai pengguna akhir. Ada beberapa praktik yang dilakukan oleh manajemen seperti membuat Standar Operasional Prosedur (SOP), penggunaan standar manajemen keamanan informasi seperti ISO, melakukan bimbingan teknis dan pelatihan tentang keamanan informasi kepada *stakeholder* atau anggota organisasi, serta mensosialisasikan kebijakan tersebut secara massal. Penelitian [1] tentang keamanan informasi pada organisasi pemerintahan di Indonesia untuk mengukur tingkat kematangan sistem informasi pada lembaga pemerintahan dan menentukan kesenjangan dalam mencapai sertifikasi ISO/IEC 27001:2013. Penelitian menggunakan analisis GAP dan *Capability Maturity Model for Integration* (CMMI) hasil menunjukkan bahwa keamanan informasi yang diterapkan tidak sesuai standar ISO/IEC 27001:2013 dan tingkat kematangan pada berada pada tingkat 1 (*initial*). Penelitian lain oleh [2] mengukur tingkat kesadaran keamanan informasi bagi Pegawai Negeri Sipil (PNS) menggunakan metode kuantitatif dengan analisis *Multiple Criteria Decision Analy*sis (MCDA). Pada penelitian ditemukan tingkat kesadaran keamanan informasi secara keseluruhan di pemerintahan tersebut berada pada level sedang sehingga perlu adanya *monitoring* sebagai pembenahan. Penelitian [3] mengenai praktik manajemen keamanan informasi pada dua organisasi swasta di India. Analisa deskriptif menggunakan kerangka kerja *Situation, Actor, Process - Learning, Action, Performance* (SAP-LAP) dilakukan melalui wawancara untuk mendapatkan data kepada para ahli. Hasil menunjukkan perlunya dukungan dari manajemen secara konsisten, budaya keamanan informasi bagi organisasi dan sistem pemantauan yang tepat untuk efektivitas manajemen keamanan informasi. Penelitian lain [4] dilakukan pada organisasi pemerintahan di India menggunakan model SAP-LAP untuk menyajikan konteks berkaitan dengan tata kelola keamanan informasi dan implementasi kebijakan Teknologi Informasi (TI) untuk mendukung proyek-proyek *e-Governance*. Hasil temuan, yaitu peningkatan kapasitas dan memberikan edukasi yang berhubungan dengan aplikasi *Information And Communications Technology* (ICT) dan *e-Governance* secara totalitas.

Faktanya organisasi dapat mengembangkan kebijakan keamanan informasi untuk membimbing dan menilai perilaku anggota, mencegah yang tidak diinginkan, serta kejadian yang mungkin disebabkan oleh insiden pelanggaran terhadap keamanan informasi [5]. Hal ini diungkapkan saat wawancara bersama pihak manajemen pada organisasi yang diteliti. Saat ini praktik keamanan informasi telah dilakukan oleh pihak manajemen di organisasi pemerintah. Namun apakah anggota organisasi peduli terhadap praktik tersebut. Oleh karena itu, dilakukan penelitian dengan tujuan untuk mengetahui praktik kepedulian keamanan informasi yang telah diterapkan oleh manajemen apakah berdampak bagi anggota organisasi khususnya organisasi itu sendiri. Penelitian ini menggunakan model SAP-LAP[6] untuk menganalisis praktik keamanan informasi manajemen secara inkuiri. Pemilihan model SAP-LAP diharapkan dapat membantu pihak manajerial dalam pemecahan masalah mengenai praktik keamanan informasi ataupun kendala lain pada organisasi serta digunakan sebagai pedoman untuk implementasi perumusan sebuah kebijakan TI.

Di Indonesia belum ditemukan penelitian tentang praktik keamanan informasi yang diterapkan oleh manajemen apakah berdampak bagi anggota organisasi. Dengan demikian, penelitian ini merujuk pada penelitian yang pernah dilakukan tentang praktik manajemen

keamanan informasi [3], [4]. Pentingnya dilakukan penelitian ini agar efektivitas terhadap praktik keamanan informasi diketahui dan kepedulian keamanan informasi dapat meningkat seiring dengan berkembangnya TI. Metode pada penelitian ini, yaitu interpretif kualitatif dan kuantitatif dengan studi kasus di tiga organisasi pemerintahan yakni pada Dinas Komunikasi dan Informatika (Diskominfo) Kab/Kota DI Yogyakarta. Organisasi ini merupakan organisasi pemerintah yang mengelola TI. Teknik analisis menerapkan model SAP-LAP sebagai analisis kualitatif. Pemilihan model SAP-LAP dapat digunakan oleh pihak manajerial dalam pemecahan masalah tentang praktik keamanan informasi yang telah diterapkan oleh organisasi serta sebagai pedoman untuk perumusan kebijakan TI. Selain itu, untuk analisis kuantitatif memanfaatkan analisis korelasi agar diketahui hubungan antara praktik keamanan informasi dan kepedulian keamanan informasi.

2. Kajian Pustaka

2.1 Keamanan informasi

Keamanan informasi dalam panduan COBIT 5, yaitu sebuah kepastian bahwa setiap informasi di organisasi terlindungi dari pengungkapan terhadap pengguna yang tidak sah (*confidentiality* - kerahasiaan), perubahan yang tidak layak (*integrity* - integritas) dan non akses bila diperlukan (*availability* - ketersediaan) [7]. Para peneliti dan profesional dalam bidang keamanan informasi banyak menggunakan dengan istilah *Confidentiality, Integrigrity, Availability* (CIA).

2.2 Manajemen Keamanan Informasi

Fungsi dari manajemen keamanan informasi, yaitu melindungi informasi dari banyaknya ancaman untuk memastikan bisnis dapat berlangsung dengan baik, meminimalkan risiko bisnis, dan memaksimalkan laba atas investasi organisasi [8]. Prosedur tentang manajemen keamanan informasi bisa dilakukan melalui praktik yang tepat dengan memanfaatkan pedoman standar manajemen keamanan informasi [9]. Pedoman manajemen keamanan informasi yang banyak diterapkan organisasi antara lain BS7799, ISO 17799, ataupun ISO/IEC 27000, dan turunannya. Standar tersebut dapat menjadi panduan mengenai kebijakan serta aturan yang bisa diimplementasikan oleh manajerial maupun praktisi keamanan informasi organisasi [8].

2.3 Praktik Manajemen keamanan informasi dan Kepedulian Keamanan Informasi

Pelaksanaan praktik manajemen keamanan informasi adalah untuk mengidentifikasi risiko keamanan yang muncul serta merancang dan menerapkan aspek kontrol dari praktik tersebut. Menurut [10] keberhasilan pelaksanaan praktik keamanan informasi memerlukan dukungan dan kepemimpinan dari manajemen. Keamanan informasi tidak hanya menjadi masalah TI yang harus ditangani oleh manajemen ataupun bagian TI dalam organisasi namun harus dianggap sebagai kewajiban bersama untuk melindungi informasi dan infrastruktur organisasi [11].

Setiap manajemen organisasi menginginkan data dan informasi terjamin kerahasiaan, integritas, dan ketersediaannya. Kepedulian terhadap keamanan informasi sangat penting karena kebijakan keamanan informasi atau prosedur dapat disalahgunakan, disalahtafsirkan atau tidak digunakan oleh pengguna akhir sehingga tingkat kepedulian terhadap keamanan informasi secara jelas tidak hilang manfaatnya [12].

3. Metode Penelitian

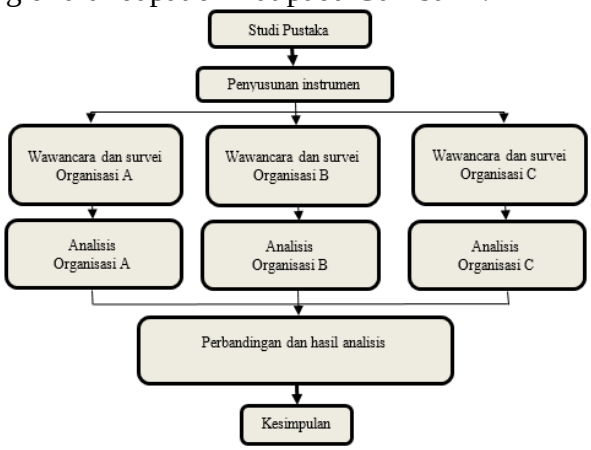
Metode penelitian ini menggunakan interpretif kualitatif dan kuantitatif. Data dikumpulkan dalam dua tahap, yaitu tahap pertama wawancara kepada pihak manajemen dan tahap kedua survei kepada anggota organisasi. Lokasi penelitian dilakukan pada tiga organisasi pemerintah, yakni lingkup Diskominfo Kabupaten/Kota di DIY. Organisasi yang diteliti meliputi :

1. Organisasi A, yaitu pada DiskominfoKabupaten Sleman,
2. Organisasi B, yaitu pada Diskominfo Kabupaten Bantul, dan
3. Organisasi C, yaitu pada Diskominfo DI Yogyakarta.

Sasaran penelitian dilakukan pada organisasi tersebut karena merupakan salah satu organisasi pemerintah yang mengelola TI di pemerintahan dan memiliki struktur organisasi bidang keamanan informasi.

3.1 Tahapan Penelitian

Tahapan penelitian digunakan untuk mempermudah proses penelitian yang dilakukan maupun penulisan artikel agar menjadi lebih terarah dan sistematis. Secara garis besar, tahapan penelitian yang dilalui dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Berbagai tahapan dilakukan dari awal hingga akhir penelitian. Penjelasan lebih rinci terkait dengan tahapan tersebut, yaitu:

3.1.1 Studi Pustaka

Tahap awal dalam penelitian dengan mencari referensi dan mengumpulkan berbagai literatur membahas tentang keamanan informasi pada organisasi dari makalah, jurnal ilmiah, dan media *online*. Proses yang dilakukan, yaitu menganalisis literatur berdasarkan tujuan, fokus, metode serta analisa penelitian sehingga diperoleh referensi yang tepat.

3.1.2 Penyusunan Instrumen

Pembuatan dan penyusunan instrumen penelitian diolah dari beberapa sumber penelitian. Instrumen terdiri dari dua bagian, yaitu instrumen wawancara dan kuesioner survei. Instrumen wawancara penelitian ini bersumber dari penelitian yang dilakukan oleh [3]. Dalam instrumen tersebut terdapat pertanyaan seputar praktik keamanan informasi. Selanjutnya, untuk instrumen kuesioner dalam penelitian ini juga didapat dari beberapa sumber. Kuesioner dibagi dalam dua variabel antara praktik keamanan informasi dan kepedulian keamanan informasi. Dari masing-masing variabel memiliki indikator atau

pertanyaan menyangkut survei penelitian pada anggota organisasi dengan catatan menyesuaikan hasil wawancara dengan pihak manajemen. Indikator pertanyaan kuesioner bersumber dari penelitian oleh [2], [11], [13], [14], [15], [16], [17], dan beberapa indikator untuk pengembangan penelitian.

3.1.3 Wawancara dan Survei

Tahap ini peneliti melakukan pengumpulan data di setiap organisasi pemerintahan yang diawali dengan wawancara secara langsung kepada pihak manajemen kemudian survei pada setiap anggota organisasi.

3.1.4 Analisis

Pada tahap analisis dilakukan menggunakan dua tahapan. Tahap yang pertama menganalisis data kualitatif hasil wawancara menggunakan model SAP-LAP. Tahap kedua, yaitu hasil dari data kuantitatif dianalisis dan pengujian menggunakan analisis korelasi yang dijalankan memalui aplikasi SPSS.

3.1.5 Perbandingan, hasil analisis dan kesimpulan

Pada tahap ini peneliti membandingkan kesamaan praktik dan hasil analisis antar organisasi pemerintahan. Tahap akhir dari penelitian berupa kesimpulan hasil dari penelitian.

3.2 Penelitian kualitatif

Penelitian kualitatif merupakan tahap pertama untuk mendapatkan data dari pihak manajemen. Adapun tahap pengumpulan data pada penelitian kualitatif, yaitu:

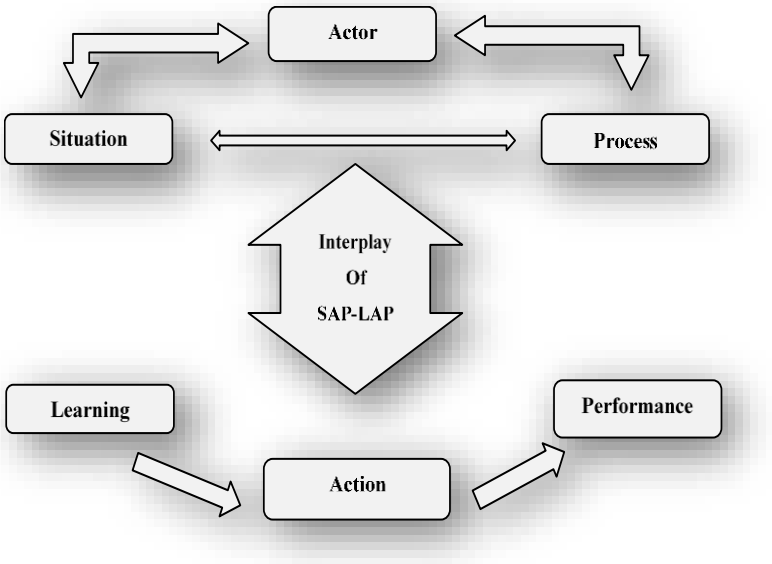
3.2.1 Wawancara

Aawancara dilakukan untuk mendapatkan data mengenai bagaimana praktik manajemen meningkatkan kepedulian keamanan informasi bagi anggota organisasi khususnya dan organisasi pada umumnya. Responden wawancara ialah pejabat yang ahli dibidangnya dan berwenang mengelola keamanan informasi pada organisasi. Dalam instrumen pertanyaan untuk wawancara mengkaji penelitian [3], terdapat 12 faktor tentang standar praktik manajemen keamanan informasi seperti kebutuhan keamanan informasi, dukungan manajemen puncak, kebijakan keamanan informasi, pelatihan keamanan informasi, kesadaran keamanan informasi, budaya keamanan informasi, audit keamanan informasi, praktik terbaik manajemen keamanan informasi, manajemen asset, manajemen insiden keamanan informasi, kepatuhan peraturan keamanan informasi, dan efektivitas manajemen keamanan informasi.

3.2.2 Model SAP-LAP

Model SAP-LAP merupakan metode yang dapat digunakan untuk menganalisis praktik dari keamanan informasi manajemen secara inkuiri. Model ini digunakan secara terstruktur untuk menganalisis kasus berdasarkan situasi, aktor yang terlibat, berbagai proses, pengetahuan, aksi, dan tindakan sesuai peranan dari keamanan informasi manajemen organisasi [3]. Situasi mencirikan keadaan sekarang dalam organisasi. Aktor adalah bagian yang terlibat baik secara individu atau berkelompok. Proses adalah konversi dari mengatur masukan menjadi keluaran yang diinginkan guna terpenuhinya tujuan organisasi. Diperolehnya pengetahuan akan mengarahkan aksi yang barangkali akan diterima untuk

menangani situasi kedepannya [6]. Hal tersebut akan menghasilkan tindakan yang tersistem. Dengan pengetahuan serta perubahan terbaru pada tindakan maka situasi, aktor, dan proses akan menyesuaikan. Situasi dapat mengaitkan aktor untuk melakukan berbagai proses yang terjadi dalam organisasi. Pengaruh dan kombinasi SAP menuju ke berbagai kegiatan LAP sehingga SAP saling mempengaruhi LAP. Model ini memuat sekumpulan pertanyaan sebagai pemecahan masalah yang secara *general* digunakan untuk menganalisa model SAP-LAP. Bentuk model SAP-LAP dapat dilihat pada Gambar 2.



Gambar 2. Model SAP-LAP [12]

3.2.3 Teknik Analisis

Analisis desktiptif metode inkuiri digunakan untuk menganalisis praktik manajemen keamanan informasi menggunakan kerangka kerja SAP-LAP. Data hasil dari wawancara dijelaskan secara deskripsi sehingga mudah dimengerti.

3.3 Penelitian Kuantitatif

Penelitian kuantitatif merupakan tahap kedua untuk mendapatkan data dari anggota organisasi. Adapun tahap pengumpulan data untuk penelitian kuantitatif pada penelitian ini, yaitu:

3.3.1 Survei

Survei dilaksanakan secara *online* kepada seluruh anggota organisasi. Kuesioner penelitian dirancang menggunakan *google form* dan memberikan *link* kuesioner kepada organisasi. Kuesioner menerapkan skala likert disusun menggunakan lima alternatif jawaban yang dinilai dari Sangat Setuju-Sangat Tidak Setuju. Total pertanyaan untuk survei sebanyak 46 item yang terbagi dalam variabel praktik keamanan informasi sebanyak 29 item dan variabel kepedulian keamanan informasi sebanyak 17 item.

3.3.2 Populasi dan Sampel

Populasi pada penelitian ini, yaitu seluruh anggota organisasi di Diskominfo Kabupaten/Kota DI Yogyakarta. Total populasi dapat dilihat pada Tabel 1.

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Tabel 1. Jumlah Populasi

No	Organisasi	Jumlah	Total Pegawai
1	Dinas Kominfo Kab. Sleman	PNS : 37 Non PNS : 36	73
2	Dinas Kominfo Kab. Bantul	PNS : 43 Non PNS : 27	70
3	Dinas Kominfo DIY	PNS : 48 Non PNS : 20	68
	Total Populasi		211

Sampel untuk penelitian ini diambil sampel acak dari populasi berdasarkan teknik sampel penelitian yang ditentukan dan harus bersifat representatif. Sampel dalam penelitian ini ditentukan 30 orang yang dibagi dari 3 organisasi sehingga masing-masing organisasi diambil sampel 10 orang. Ukuran sampel 30 dan kurang dari 500 sesuai untuk hampir seluruh penelitian [18]. Teknik sampling penelitian ini menerapkan teknik *probability sampling* berupa *proporsionate stratified random sampling*. Menurut [19] *Probability sampling* adalah teknik pengambilan sampel yang mana bagi setiap anggota populasi diberikan kemungkinan yang sama untuk terpilih menjadi anggota sampel.

3.3.3 Hipotesis

Dalam penelitian ini hipotesis yang digunakan adalah hipotesis hubungan atau hipotesis asosiatif. Apakah ada korelasi antara praktik keamanan informasi dengan kepedulian keamanan informasi. Adapun hipotesis yang dalam penelitian ini adalah

H0 = Praktik keamanan informasi tidak memiliki hubungan signifikan terhadap kepedulian keamanan informasi

Ha = Praktik keamanan informasi memiliki hubungan yang signifikan terhadap kepedulian keamanan informasi

3.3.4 Teknik Analisis

Teknik analisis menggunakan analisis korelasi untuk mengetahui hubungan antara praktik keamanan informasi terhadap kepedulian keamanan informasi. Analisis ini memanfaatkan korelasi *pearson* untuk pengujian validitas dan reliabilitas dari instrumen serta uji koefisien korelasi dan hipotesis. Selain itu, analisis uji korelasipun digunakan agar diketahui hubungan antara dua variabel antara variabel bebas dengan variabel terikat. Yang termasuk dalam variabel bebas (*Independent Variable*), yaitu praktik keamanan informasi (X) sedangkan variabel terikat (*Dependent Variable*), yaitu kepedulian keamanan informasi (Y). Keeratan hubungan dari kedua variabel tersebut dapat diketahui dari hasil analisis berdasarkan nilai koefisien korelasi seperti pada Tabel 2.

Tabel 2. Nilai Koefisien Korelasi

Nilai Koefisien Korelasi	**Keeratan Hubungan**
0,00	Tidak ada korelasi
0,10 – 0,20	Korelasi Sangat rendah/lemah sekali
0,21 – 0,40	Korelasi Rendah/lemah tapi pasti
0,41 - 0,70	Korelasi Cukup berarti/sedang
0,71 - 0,90	Korelasi Tinggi/kuat
0,91 - 1,00	Korelasi Sangat tinggi/kuat sekali
1	Korelasi sempurna.

Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

4. Hasil dan Pembahasan

4.1 Analisis Kualitatif

Analisi ini diuraikan secara deskripsi dari wawancara yang dilakukan pada masing-masing organisasi. Model analisis SAP-LAP disajikan berbentuk tabel agar diketahui perbandingan kesamaan praktik yang telah diterapkan. Analisis studi kasus dapat dilihat pada Tabel 3. Adapun Hasil pengamatan penelitian pada masing-masing organisasi, yaitu :

4.1.1 Organisasi A

Organisasi A adalah Diskominfo Kabupaten Sleman yang merupakan organisasi Perangkat Daerah (OPD) hasil pembenahan kelembagaan pada tahun 2016 dan beroperasi pada tahun 2017. Organisasi ini menyatukan urusan komunikasi dan informatika yang sebelumnya digabung di Dinas Perhubungan, Komunikasi dan Informatika, urusan data statistik yang wewenang sebelumnya berada di Badan Perencanaan Pembangunan Daerah dan sebagian urusan kehumasan yang sebelumnya ada di Sekretariat Daerah. Sumber data tersebut dikutip dari laman Dinas Kominfo https://kominfo.slemankab.go.id/sejarah. Kegiatan keamanan informasi pada Dinas Kominfo Kabupaten Sleman berada di Bidang Layanan *e-Government* dan Persandian.

Pada organisasi A hasil analisis SAP-LAP menunjukkan manajemen *concern* terhadap keamanan informasi namun belum sepenuhnya *aware* tentang keamanan informasi walaupun memiliki kebijakan yang telah diatur secara spesifik. Adapun kebijakan keamanan informasi tertuang dalam Peraturan Bupati, Keputusan Kepala Dinas, SOP serta ISO 27001. Organisasi selalu melakukan audit setiap tahun baik ekternal maupun internal. Organisasi masih minim SDM sehingga masih terdapat anggota yang merangkap jabatan pada bidang tertentu ataupun tugas pokok tidak sesuai dengan latar belakang pendidikan. Hal tersebut mungkin akan menambah beban tambahan pekerjaan bagi anggota organisasi. Kemungkinan lain yang terjadi karena lemahnya kesadaran keamaan informasi oleh manajemen dan anggota serta anggaran terbatas dapat menjadi perhatian utama.

4.1.2 Organsiasi B

Organisasi B adalah Diskominfo Kabupaten Bantul merupakan OPD baru yang dibentuk pada tahun 2016. Organisasi ini menyelenggarakan aspek komunikasi dan informatika, statistik dan persandian yang sebelumnya merupakan gabungan dan bagian dari beberapa OPD yaitu Pengolahan Data Telematika, sebagian dari Bagian Humas Sekretariat Daerah, sebagian dari Bagian Umum Sekretarian Daerah, dan sebagian dari Dinas Perhubungan. Sumber data tersebut dikutip dari laman Diskominfo https://diskominfo.bantulkab.go.id/hal/sejaran-pembentukan. Kegiatan keamanan informasi pada Diskominfo Bantul berada pada bidang infrastruktur teknologi informasi, keamanan informasi dan persandian.

Analisis SAP-LAP pada organisasi B menunjukkan organisasi mulai sadar pentingnya keamanan informasi. Saat ini manajemen akan menerapkan kebijakan dengan standar keamanan informasi yaitu ISO 27001 selain kebijakan yang telah digunakan seperti Peraturan Bupati dan SOP keamanan informasi dengan menyesuaikan kondisi. Semua aplikasi maupun layanan online yang ada di server harus melalui uji keamanan informasi, *assessment*, *security assesment*. Organisasi memiliki mekanisme kontrol akses terhadap sistem dan layanan TI. Dukungan dari manajemen tetap diberikan dan menjadi prioritas untuk tujuan keamanan informasi namun tetap memperhatikan kegiatan yang lebih *urgent* menyesuaikan situasi dan kondisi. Hal yang mempengaruhi lemahnya kesadaran keamanan

informasi dapat dikarenakan minimnya pengetahuan anggota tentang keamanan informasi, budaya dan perilaku kerja serta kurangnya SDM menyebabkan adanya rangkap jabatan dan akhirnya tidak fokus pada pekerjaan utama.

4.1.3 Organisasi C

Organisasi C adalah Diskominfo DIY merupakan gabungan dari 2 (dua) bidang yakni dari Dinas Perhubungan Komunikasi dan Informatika DIY pada bidang pemberdayaan masyarakat informasi dan bidang layanan teknologi manajemen informatika serta UPTD Plaza informasi. Organisasi ini berdiri pada tahun 2016 dan bertugas membantu Gubernur dalam melaksanakan urusan pemerintahan bidang komunikasi dan informatika serta urusan pemerintahan bidang persandian. Sumber data tersebut dikutip dari laman diskominfo DIY https://diskominfo.jogjaprov.go.id/sejarah-dinas. Kegiatan keamanan informasi pada Dinas Kominfo DIY berada di Bidang Keamanan Informasi dan persandian.

Pada organisasi C hasil temuan dari analisis SAP-LAP menunjukkan manajemen memiliki *awareness* dan *support* yang cukup tinggi terhadap keamanan informasi. Dari sisi SDM terpenuhi sehingga tidak ada anggota organisasi yang merangkap jabatan. Organisasi saat ini mempunyai kebijakan keamanan informasi seperti Peraturan Gubernur dan SOP sesuai standar ISO 27001. Organisasi memiliki data center yang terintegrasi menjadi praktik terbaik yang diterapkan. Data dan informasi apapun selalu di *backup* dan melalui proses backup yang sesuai dengan standar layanan SLA (*Service Level Agreement*). Adaptasi pola kerja akan terjadi ketika adanya bencana sehingga harus meningkatkan keamanan informasi pada infrastruktur yang ada.

Tabel 3. Analisis SAP-LAP

SAP-LAP	**Organisasi A**	**Organisasi B**	**Organisasi C**
Situation. • Bagaimana saat ini? • Apa yang terjadi sekarang? • Apa yang diharapkan terjadi?	• Keamanan informasi untuk aplikasi dan server. • Kebijakan diatur secara spesifik dalam Keputusan Kepala Dinas dan SOP • Memiliki standar keamanan informasi seperti ISO 27001. • Ada dukungan dan *concern* dari manajemen	• Keamanan informasi untuk validitas data dan informasi • Kebijakan tertuang dalam Peraturan Bupati dan SOP • Baru menerapkan ISO 27001 • Ada dukungan dari manajemen puncak	• Keamanan informasi untuk mengamankan seluruh aset informasi • Kebijakan tertuang dalam SOP dan Peraturan Gubernur sesuai ISO • Memiliki standar keamanan informasi ISO 27001 • Ada dukungan dan *awareness* dari pimpinan
Actor • Manajemen yang terlibat	• Kepala seksi Persandian	• Kepala seksi keamanan informasi dan persandian	• Kepala Bidang Keamanan Informasi dan Persandian
Process • Apa yang dilakukan? • Mengapa dilakukan? • Bagaimana itu dilakukan?	• Selalu melakukan audit dan monev. • Ada proses untuk meninjau kebijakan, pedoman, dan prosedur keamanan informasi.	• Proses audit dilakukan untuk evaluasi • Penggunaan tanda tangan digital sejauh data atau informasi digital.	• Selalu ada audit serta monev secara berkala • Ada *master plan*, *blueprint* mengarah pada penataan sumber daya dan memenuhi

			kebutuhan keamanan informasi.
Learning • Apa masalah utama terkait situasi? • Apa masalah utama terkait aktor? • Apa masalah utama terkait proses?	• Belum ada mekanisme penggunaan lisensi legal • Minim sumber daya, kesadaran keamanan informasi oleh manajemen dan staf • Masih terjadi rangkap jabatan • Keterbatasan anggaran	• Minimnya SDM • Masih terjadi rangkap pekerjaan. • Masih lemahnya kesadaran dari SDM yang ada.	• Keamanan informasi menjadi pembiasaan namun budaya kerja organisasi, perilaku kerja, SDM, dapat membawa dampak yang menyebabkan kerugian. • Ketersediaan anggaran menyesuaikan kemampuan keuangan daerah.
Action • Apa yang harus dilakukan dalam meningkatkan situasi? • Apa yang dapat dilakukan untuk meningkatkan aktor? • Apa yang harus dilakukan untuk meningkatkan / mengimplementasikan proses?	• Melakukan *security testing* • Selalu update firewall, melakukan backup harian, mingguan, dan bulanan serta mencatat segala asset yang ada. • Sistem *ticketing* untuk pelaporan insiden • Pelatihan keamanan informasi dilakukan satu sampai dua kali setiap tahun	• Sistem informasi dan aplikasi dibangun dengan *secure by design*. • Aplikasi maupun sistem online harus melalui tahapan uji keamanan informasi • Ada mekanisme kontrol akses terhadap sistem dan layanan TI • Melakukan pelacakan jika terindikasi penyalahgunaan hak akses. • Pelatihan keamanan informasi dilakukan rutin sesuai kebutuhan	• Perlindungan aplikasi sesuai standar manajemen keamanan informasi • Rutin melakukan backup data • Mempunyai *mirorring backup* pada data center. • Beberapa ruangan yang sensitif dilengkapi dengan *door access* menggunakan *finger*. • Rutin memberikan pelatihan
Performance • Apa dampaknya terhadap situasi? • Bagaimana aktor akan terpengaruh? • Bagaimana kinerja proses terpengaruh?	• Jika terjadi insiden perlu respon dan penanganan yang cepat • Manajemen diharapkan memberikan dukungan penuh terkait masalah keamanan informasi • Menyiapkan SDM dan anggaran sesuai kebutuhan praktik keamanan informasi	• Belum memiliki mekanisme kontrol untuk patuh terhadap penggunaan perangkat lunak yang sah. • Manajemen harus memberikan dorongan penuh kepada anggota tentang kesadaran keamanan informasi • Ketersediaan anggaran dan SDM dapat dijadikan prioritas guna	• Adanya perubahan pola kerja ketika terjadi perubahan situasi • Ketika semua kegiatan kerja dilakukan secara online maka keamanan informasi harus ditingkatkan • Tingkat *awareness* akan jauh lebih baik karena sesuai sistem manajemen keamanan informasi dan tata kelola TIK .

		peningkatan praktik keamanan informasi	

4.1.4 Kesamaan Praktik

Dari studi kasus di atas, setiap organisasi memiliki beberapa kesamaan mengenai praktik keamanan informasi. Semua organisasi menyatakan bahwa keamanan informasi penting untuk mengamankan data dan informasi karena informasi merupakan sebuah aset. Organisasi A menyatakan keamanan informasi tidak hanya mengamankan informasi namun penting untuk mengamankan infrastruktur yang ada. Organisasi B menyatakan keamanan informasi sangat penting untuk menjaga keutuhan ketersediaan dan validitas data atau informasi. Organisasi C menyatakan keamanan informasi sangat penting karena selain mengamankan aset informasi yang dimiliki, organisasi juga bertugas mengamankan aset informasi yang ada di organisasi yang lebih luas, yaitu pada pemerintahan secara umum.

Setiap organisasi mendapatkan dukungan dari manajemen puncak namun belum maksimal dan tidak semua kegiatan dapat direalisasikan. Dukungan keamanan informasi dari manajemen organisasi A masih terlihat minim namun sudah mulai peduli pada keamanan informasi. Dukungan keamanan informasipun diberikan oleh pihak manajemen pada Organisasi B namun tidak selalu mendapat dukungan penuh karena menyesuaikan situasi dan kondisi yang terjadi. Hal yang sama terjadi pada organisasi C bahwa manajemen puncak selalu memberikan dukungan penuh tetapi menyesuaikan situasi, kondisi, dan kemampuan organisasi.

Setiap organisasi memiliki kebijakan keamanan informasi yang tertuang dalam Peraturan Gubernur, Peraturan Bupati, Keputusan Kepala Dinas, SOP dan ISO 27001. Pada organisasi A kebijakan keamanan informasi secara jelas dan spesifik sudah diatur dalam SOP serta Keputusan Kepala Dinas yang telah ditinjau secara berkala dan sejalan dengan tujuan organisasi. Kebijakan keamanan informasi pada organisasi B tertuang dalam Peraturan Bupati serta SOP dan akan menerapkan ISO 27001. Selain menerapkan SOP yang sesuai standar ISO 27001, organisasi C juga memiliki kebijakan yang tertuang dalam Peraturan Gubernur dan Peraturan Bupati.

Pelatihan keamanan informasi selalu diberikan secara reguler satu atau dua kali dalam setahun menyesuaikan kebutuhan serta anggaran yang telah disediakan. Organisasi melakukan pelatihan yang bermanfaat, *up to date*, dan relevan dengan pekerjaan untuk menambah pengalaman serta pengetahuan. Organisasi A menyatakan pelatihan keamanan informasi diberikan bagi anggota organisasi untuk menambah pengetahuan namun dilakukan sesuai kebutuhan. Hal yang sama terjadi pada organisasi B pelatihan dilakukan oleh pihak organisasi sendiri ataupun dengan mengundang pihak *IT Training* untuk dapat meningkatkan *skill* para anggota organisasi. Begitu pula pada organisasi C pelatihan diberikan setiap tahun secara reguler baik sosialisasi, bimbingan teknis, mengikuti *workshop* dan *training* bagi tim teknis baik pada organisasi sendiri atau di tempat lain.

4.2 Analisis Kuantitatif

Seperti yang disampaikan pada point 3.2.3 di atas, penelitian ini menggunakan analisis korelasi. Adapun proses analisis dilakukan melalui beberapa tahap, yaitu:

4.2.1 Demografi Responden

Responden merupakan semua anggota organisasi tidak hanya pada bidang keamanan informasi namun pada unit lain yang masuk dalam struktur organisasi. Karakteristik data yang dianalisis hanya ditujukan bagi anggota yang tidak memiliki jabatan seperti Kepala

Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Dinas, Kepala Bidang, ataupun Kepala Seksi. Tahap evaluasi menjadi langkah setelah terkumpulnya data yaitu dengan mengamati dan meneliti data dari kesalahan pengisian ataupun duplikasi. Rekapitulasi dari data yang tidak memenuhi syarat tersebut tidak disertakan dalam proses analisis. Seluruh demografi responden dirangkum dalam Tabel 4.

Tabel 4. Demografi Responden

Kelompok		N=30	Persentase
Jenis Kelamin	Laki - Laki	18	60%
	Perempuan	12	40%
Usia	17-25	1	3%
	26-35	12	40%
	36-45	9	30%
	46-55	5	17%
	>55	3	10%
Pendidikan Terakhir	Setingkat SMA	5	17%
	Diploma (D3)	5	17%
	Sarjana (S1)	18	60%
	Magister (S2)	2	7%
	Doktor (S3)	0	0%
Jurusan Pendidikan Terkahir	TI	19	63%
	Non IT	11	37%
Masa Kerja	< 1 Tahun	1	3%
	1 - 4 Tahun	16	53%
	> 4 Tahun	13	43%

Analisis menggunakan aplikasi SPSS untuk uji validitas, uji reliabilitas, dan uji koefisien korelasi dari data hasil penelitian. Data yang tepat dipilih untuk diukur validitas datanya sehingga dapat dianalisis lebih lanjut.

4.2.2 Uji Validitas

Teknik korelasi pearson digunakan sebagai uji validitas. Tolak ukur yang digunakan yaitu apabila nilai koefisien korelasi (rhitung) bernilai positif dan lebih besar dari rtabel maka item penelitian dinyatakan valid. Dengan N=30 dan $\alpha = 0{,}05$ maka didapat nilai rtabel sebesar 0,361. Hasil pengujian validitas instrumen disajikan dalam Tabel 5. Hasil uji validitas instrumen membuktikan bahwa semua item mempunyai koefisien korelasi (rhitung) yang bernilai positif dan lebih besar dari rtabel=0,361 yang berarti valid.

Tabel 5. Hasil Uji Validitas

Variabel	Item	rhitung	rtabel 5% (N=30)	Sig.	Kriteria	Variabel	Item	rhitung	rtabel 5% (N=30)	Sig.	Kriteria
X	A1	,608**	0,361	0,000	Valid	**Y**	I1	,567**	0,361	0,001	valid
	A2	,805**	0,361	0,000	Valid		I2	,490**	0,361	0,006	valid
	A3	,788**	0,361	0,000	Valid		I3	,716**	0,361	0,000	valid
	A4	,631**	0,361	0,000	Valid		I4	,770**	0,361	0,000	valid
	B1	,739**	0,361	0,000	Valid		I5	,768**	0,361	0,000	valid
	B2	,841**	0,361	0,000	Valid		J1	,752**	0,361	0,000	valid
	B3	,845**	0,361	0,000	Valid		J2	,566**	0,361	0,001	valid
	B4	,855**	0,361	0,000	Valid		J3	,615**	0,361	0,000	valid
	B5	,798**	0,361	0,000	Valid		J4	,480**	0,361	0,007	valid
	C1	,825**	0,361	0,000	Valid		K1	,758**	0,361	0,000	valid
	C2	,810**	0,361	0,000	Valid		K2	,768**	0,361	0,000	valid
	C3	,856**	0,361	0,000	Valid		K3	,658**	0,361	0,000	valid
	C4	,737**	0,361	0,000	Valid		K4	,670**	0,361	0,000	valid
	C5	,719**	0,361	0,000	Valid		K5	,620**	0,361	0,000	valid
	D1	,719**	0,361	0,000	Valid		L1	,670**	0,361	0,000	valid
	D2	,843**	0,361	0,000	Valid		L2	,544**	0,361	0,002	valid
	D3	,789**	0,361	0,000	Valid		L3	,394*	0,361	0,031	valid
	E1	,741**	0,361	0,000	Valid						
	E2	,641**	0,361	0,000	Valid						

Variabel	Item	rhitung	rtabel 5% (N=30)	Sig.	Kriteria	Variabel	Item	rhitung	rtabel 5% (N=30)	Sig.	Kriteria
	F1	,785**	0,361	0,000	Valid						
	F2	,696**	0,361	0,000	Valid						
	F3	,790**	0,361	0,000	Valid						
	F4	,748**	0,361	0,000	Valid						
	G1	,815**	0,361	0,000	Valid						
	G2	,857**	0,361	0,000	Valid						
	G3	,797**	0,361	0,000	Valid						
	H1	,676**	0,361	0,000	Valid						
	H2	,722**	0,361	0,000	Valid						
	H3	,559**	0,361	0,001	Valid						

4.2.3 Uji reliabilitas

Teknik analisis *Cronbach Alpha* digunakan untuk uji reliabilitas. Kuesioner dapat dikatakan reliabel jika alpha > 0,6. Hasil uji reliabilitas disajikan pada tabel 6. Seluruh pertanyaan dalam kuesioner mempunyai nilai alpha > 0,6 sehingga dapat disimpulkan bahwa alat ukur tersebut dinyatakan reliabel.

Tabel 6. Uji Reliabilitas

Variabel	Alpha	Kriteria
X	0,972	Reliabel
Y	0,904	Reliabel

4.2.4 Uji koefisien korelasi

Analisis korelasi pearson digunakan untuk uji koefisien korelasi. Hasil uji korelasi disajikan pada tabel 7. Diketahui nilai r = 0,850 artinya nilai korelasi berada diantara 0,71 - 0,90 yang menyatakan adanya hubungan yang positif dan tingkat keeratan hubungan korelasi tinggi atau memiliki hubungan kuat antara praktik keamanan informasi dengan kepedulian keamanan informasi.

Tabel 7. Hasil Uji Korelasi

Correlations			
		Praktik keamanan informasi	**Kepedulian keamanan informasi**
Praktik keamanan informasi	Pearson Correlation	1	,850**
	Sig. (2-tailed)		,000
	N	30	30
Kepedulian keamanan informasi	Pearson Correlation	,850**	1
	Sig. (2-tailed)	,000	
	N	30	30
**. Correlation is significant at the 0.01 level (2-tailed).			

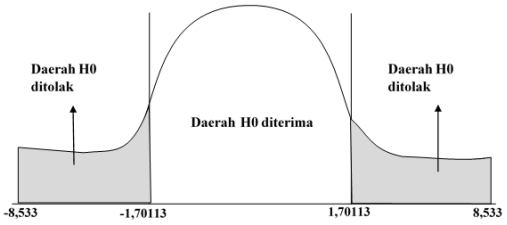
4.2.5 Uji hipotesis

Untuk mengetahui signifikan tidaknya hubungan antar variabel yang sedang diselidiki maka perlu adanya uji hipotesis terhadap koefisien korelasi dengan menggunakan persamaan 1. Pengujian ini menggunakan t – test dengan tingkat signifikan 5%. Titik kritis dicari melalui tabel –t (*t distribution*) yang mana nilai t-tabel ditentukan berdasarkan penggunaan tingkat signifikansi (α) dan derajat bebas atau *degree of freedom* (df), dimana df=n-2, besaran nilainya tergantung pada jumlah sampel (n). Nilai t-hitung < t-tabel pada α 0,05 atau t- hitung pada p-value>0,05 maka H0 diterima dan Ha ditolak. Sebaliknya jika nilai t-hitung > t-tabel pada α 0,05 atau t- hitung pada p-value<0,05 maka H0 ditolak dan Ha diterima.

$$t = \frac{4{,}497}{0{,}527} = 8{,}533 \qquad (1)$$

Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

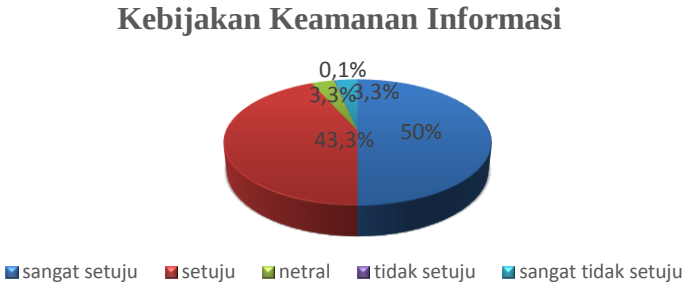
Berdasarkan perhitungan diatas maka diketahui H0 ditolak dan Ha diterima, pernyataan tersebut sangat jelas karena t hitung (t=8,533) lebih besar dari t tabel (t=1,70113). Untuk mengetahui daerah penolakan H0 dapat dilihat pada Gambar 3.



Gambar 3. Uji t 2 sisi

4.3 Pembahasan

Hasil pengujian hipotesis ditemukan bahwa adanya korelasi antara praktik keamanan informasi dan kepedulian keamanan informasi. Hal ini terbukti karena thitung (t=8,533) lebih besar dari t tabel (t=1,70113). Hal tersebut juga menunjukkan bahwa praktik keamanan informasi berhubungan positif dan signifikan dengan kepedulian keamanan informasi. Diketahui dari hasil analisis tentang praktik keamanan informasi pada organisasi, pihak manajemen menyatakan bahwa keamanan informasi penting dilakukan untuk mengamankan aset informasi. Hasil survei menunjukkan terdapat 53,3% menyatakan sangat setuju dan terdapat 43,3% yang setuju tentang pentingnya keamanan informasi namun ada 3,3% menyatakan sangat tidak setuju. Berkaitan dengan kebijakan keamanan informasi yang diterapkan, setiap manajemen menyatakan organisasi memiliki kebijakan dan aturan tentang keamanan informasi yang tertuang dalam SOP, Peraturan Gubernur, Peraturan Bupati, serta Keputusan Kepala Dinas.



Gambar 4. Grafik kebijakan Keamanan informasi

Pada gambar 4 diketahui hasil survei terdapat 50% yang menyatakan sangat setuju dan 43,3% yang setuju dengan pernyataan di atas. Namun ada pula yang menjawab netral yaitu 3,3% dan sangat tidak setuju ada 3,3%. Kebijakan yang telah diterapkan merupakan hasil rapat antara manajemen dan staf dilingkup masing-masing organisasi. Untuk pernyataan tersebut diketahui dari hasil survei yang menjawab sangat setuju ada 26,7% dan ada pula yang menjawab setuju yaitu 63,35%. Tetapi ada 2 responden yang menjawab netral dengan 6,7% dan sangat tidak setuju 3,3%. Pihak manajemen menyatakan praktik keamanan informasi di organisasi diterapkan bagi semua staf. Respon dari hasil survei ada yang sagat setuju dengan presentase 30%, selain itu ada 46,7% menyatakan setuju dengan hal tersebut. Namun ada beberapa responden yang menjawab netral yaitu 13,3%, tidak setuju ada 6,7%, dan sangat tidak setuju ada 3,3%. Manajemen puncak memberikan pelatihan secara rutin setiap tahun untuk staf baik sosialisasi, bimbingan teknis, ataupun *workshop* tentang

keamanan informasi. Terdapat 56,7% dari hasil survei menyatakan setuju dengan pernyataan tersebut artinya bahwa pelatihan selalu diberikan kepada anggota organisasi untuk menambah pengetahuan dan pengalaman dibidang keamanan informasi.

Dari perspektif kepedulian keamanan informasi oleh anggota organisasi. Berkaitan dengan kepatuhan regulasi keamanan informasi, anggota organisasi melindungi privasi data yang ada di organisasi. Hasil survei menunjukkan terdapat 43,3% yang sangat setuju, 50% setuju, 3,3% menjawab netral dan 3,3% mengatakan tidak setuju. Selain itu, anggota organisasi mematuhi dan mengikuti kebijakan keamanan informasi yang telah ditetapkan. Dari hasil survei terhadap pernyataan tersebut 33,3% sangat setuju, 60% setuju, 3,3% netral dan 3,3% tidak setuju. Dari sisi kesadaran keamanan informasi, anggota organisasi menyadari kebijakan dan pedoman yang diberikan oleh organisasi. Hasil survei terhadap anggota ada 33,3% sangat setuju, 56,7% setuju, 10% memilih netral. Anggota sadar terhadap hukuman maupun tindakan disiplin karena melanggar pedoman keamanan informasi. Dari data hasil survei yang menyatakan sangat setuju ada 30%, 60% setuju, 6,7% netral, dan terdapat 3,3% yang tidak setuju.

5. Kesimpulan

Manajemen organisasi telah menerapkan praktik keamanan informasi agar menjamin terciptanya keamanan informasi di masing-masing organisasi khususnya pada bidang keamanan informasi. Praktik keamanan informasi memiliki efektivitas yang cukup tetapi ada kalanya berbanding terbalik karena menyesuaikan keadaan sekarang. Perlunya dukungan yang tinggi dari pimpinan dan manajemen puncak merupakan suatu harapan agar mempengaruhi tingkat kepedulian keamanan informasi bagi anggota. Jika anggota organisasi enggan ataupun kurang peduli terhadap keamanan informasi maka akan berdampak pada munculnya resiko yang tidak diinginkan dan kerugian bagi organisasi. Dari hasil uji hipotesis dengan taraf signifikansi 5% maka diketahui H0 ditolak dan Ha diterima. Pernyataan ini diperkuat melalui hasil analisis korelasi yang telah diuji dengan nilai 0,850. Nilai tersebut menyatakan hubungan positif dan tingkat keeratan hubungan korelasi tinggi antar variabel. Hal tersebut dapat diartikan bahwa dampak yang diberikan oleh anggota organisasi juga bernilai positif sehingga anggota organisasi memiliki kepedulian yang tinggi terhadap praktik keamanan informasi oleh manajemen. Dari analisis SAP-LAP diketahui praktik keamanan informasi oleh organisasi telah diterapkan dengan baik walaupun masih belum sepenuhnya maksimal karena menyesuaikan situasi dan kondisi organisasi.

Ucapan Terima Kasih

Terima kasih kepada Allah SWT., terima kasih kepada para responden, yaitu Diskominfo Kab/Kota DIY, yakni Diskominfo Kab. Sleman, Diskominfo Kab. Bantul, dan Diskominfo DIY serta terima kasih kepada pihak yang membantu penulis dalam menyelesaikan penelitian ini.

Daftar Pustaka

[1] A. Z. Maingak and L. D. Harsono, "*Information Security Assessment Using Iso / Iec 27001 : 2013 Standard*," vol. 17, no. 1, pp. 28–37, 2018.

[2] M. Amin, "Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda)," vol. 5, no. 1, pp. 15–24, 2014.

[3] A. N. Singh and M. P. Gupta, "*Information Security Management Practices: Case Studies from India*," *Glob. Bus. Rev.*, vol. 20, no. 1, pp. 253–271, 2017.

[4] R. Anand, S. Medhavi, V. Soni, C. Malhotra, and D. Kumar Banwet, "*Information &*

Computer Security Transforming Information Security Governance in India (A SAP-LAP based Case Study of Security , IT Policy and e-Governance)," *Transform. Inf. Secur. Gov. India*, 2016.

[5] M. I. Merhi and P. Ahluwalia, "*Examining the impact of deterrence factors and norms on resistance to Information Systems Security*," *Comput. Human Behav.*, vol. 92, no. October 2018, pp. 37–46, 2019.

[6] Sushil, "SAP-LAP models of inquiry," *Manag. Decis.*, vol. 38, no. 5, pp. 347–353, 2000.

[7] R. Lepofsky, "COBIT® 5 for Information Security," *Manag. Guid. to Web Appl. Secur.*, pp. 133–145, 2014.

[8] S. E. Chang and C. B. Ho, "*Organizational factors to the effectiveness of implementing information security management*," *Ind. Manag. Data Syst.*, vol. 106, no. 3, pp. 345–361, 2006.

[9] K. A. Barton, G. Tejay, M. Lane, and S. Terrell, "*Information system security commitment: A study of external influences on senior management*," *Comput. Secur.*, vol. 59, pp. 9–25, 2016.

[10] G. P. Z. Montesdioca and A. C. G. Maçada, "*Measuring user satisfaction with information security practices*," *Comput. Secur.*, vol. 48, pp. 267–280, 2015.

[11] A. N. Singh, M. P. Gupta, and A. Ojha, "*Identifying factors of 'organizational information security management*," *J. Enterp. Inf. Manag.*, vol. 27, no. 5, pp. 644–667, 2014.

[12] M. T. Siponen, "*A conceptual foundation for organizational information security awareness . Information Management & Computer Security A conceptual foundation for organizational information security awareness*," vol. 8, no. January, pp. 31–41, 2016.

[13] S. E. Chang and C. S. Lin, *Exploring organizational culture for information security management*, vol. 107, no. 3. 2007.

[14] H. N. Chua, S. F. Wong, Y. C. Low, and Y. Chang, "*Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations*," *Telemat. Informatics*, vol. 35, no. 6, pp. 1770–1780, 2018.

[15] S. Sharma and M. Warkentin, "*Do I really belong?: Impact of employment status on information security policy compliance*," *Comput. Secur.*, vol. 87, p. 101397, 2019.

[16] C. H. Au and W. S. L. Fung, "*Integrating knowledge management into information security: From audit to practice*," *Int. J. Knowl. Manag.*, vol. 15, no. 1, pp. 37–52, 2019.

[17] N. S. Safa and R. Von Solms, "*An information security knowledge sharing model in organizations*," *Comput. Human Behav.*, vol. 57, pp. 442–451, 2016.

[18] U. Sekaran, *Research and Markets: Research Methods for Business - A Skill Building Approach*. 2003.

[19] Sugiyono, "Statistika untuk Penelitian," in *Statistika untuk Penelitian,* Alfabeta Bandung, 2019, p. 63.