Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa

Khairunnisak Nur Isnaini[1], Guti Julias Nofita Sari[2], Adam Prayogo Kuncoro[3]
Informatika, Sistem Informasi, Informatika
Universitas Amikom Purwokerto
Purwokerto, Indonesia
e-mail: [1]nisak@amikompurwokerto.ac.id, [2]gutijulias22@gmail.com, [3]adam@amikompurwokerto.ac.id

Diajukan: 12 Februari 2022; Direvisi: 17 Juli 2023; Diterima: 24 Agustus 2023

Abstrak

Risiko keamanan informasi dapat terjadi sewaktu-waktu di sebuah instansi, hal tersebut juga dapat terjadi di kantor pemerintahan Desa Cingebul. Peluang risiko yang dapat timbul antara lain hilangnya data/kebocoran data dan adanya pihak yang tidak memiliki akses dapat mengakses sistem. Tujuan penelitian ini adalah mengetahui dan menilai risiko keamanan informasi di kantor Desa Cingebul menggunakan ISO 27005:2019 pada aplikasi Sistem Pelayanan Desa. Metode pengumpulan data yang yang dilakukan adalah wawancara, observasi, studi pustaka dan dokumentasi. Kontrol ISO 27005:2019 digunakan sebagai acuan dalam penilaian risiko tersebut. Hasil yang diperoleh menunjukkan bahwa risiko yang didapatkan dari aplikasi Simpel Desa yang paling tinggi yaitu ketika ancaman risiko yang terjadi server down. Risiko tersebut dapat diminimalisir dengan menerapkan kontrol rekomendasi information backup (A. 12.3.1) dengan melakukan backup data secara berkala dengan lokal backup maupun dengan cloud backup. Maka dapat disimpulkan bahwa kontrol ISO 27005 dapat digunakan sebagai standar atau acuan dalam menilai risiko keamanan informasi terutama pada bagian hasil penilaian risiko. Saran yang perlu dipertimbangkan untuk meningkatkan keamanan aplikasi simpel desa pada kantor Desa Cingebul yaitu dengan menerapkan rekomendasi keamanan untuk mengurangi kemungkinan risiko yang terjadi.

Kata kunci: *Analisis risiko, ISO 27005:2019, Simpel Desa.*

Abstract

Cingebul Village Office has one of the information systems, namely the Village Management and Service Information System (Simpel Desa) which is integrated with android so that it makes it easier to intercation administration, services and village businesses between the government and the village community. The Simpel Desa application contains important data, because users in doing access need to use the Population Master Number (PMN) and phone number as a condition for registering so that it must be maintained and protected by security. During the use of the application, various threats or risks may arise such as data leaks and parties who do not have access to them. This research aims to conduct information security risk analysis in village management and service information system (Simpel Desa) applications using ISO 27005:2019. The results obtained show that the risk obtained from the Simple Village application is the highest when the risk threat that occurs server down. These risks can be minimized by implementing information backup recommendation control (A. 12.3.1) by backing up data with local backup or cloud backup periodically. It can then be concluded that ISO 27005 controls can be used as a standard or reference in assessing information security risks, especially in the risk assessment results section. The advice to consider to improve the security of simple village applications at the Cingebul Village office is to implement security recommendations to reduce the possibility of risks that occur.

Keywords*: Risk analysis, ISO 27005:2019, Simpel Desa.*

1. Pendahuluan

Desa Cingebul merupakan salah satu desa yang terletak di Kecamatan Lumbir, Kabupaten Banyumas. Dalam menjalankan kegiatan di pemerintahan Desa Cingebul terdapat sistem informasi yang digunakan salah satunya yaitu Sistem Informasi Manajemen dan Pelayanan Desa (Simpel Desa). Sistem Informasi Manajemen dan Pelayanan Desa (Simpel Desa) adalah aplikasi yang berbasis web (*dashboard*)

yang terintegrasi dengan aplikasi (*android*) untuk mempermudah melakukan interaksi administrasi, pelayanan dan usaha desa antara pemerintahan dengan masyarakat desa [1]. Aplikasi ini merupakan salah satu aplikasi yang diimplementasikan dalam program *Smart Village* Nusantara dalam mengembangkan aspek pembangunan desa digital yang mencakup tata kelola pemerintahan desa, tata niaga desa dan tata sosial desa dengan memanfaatkan teknologi informasi dan komunikasi. *Smart Village* Nusantara merupakan salah satu wujud dukungan PT Telkom Indonesia terhadap pemerintah dalam membangun Indonesia dari potensi di desa-desa dengan mendukung pengembangan ekosistem desa digital demi ekonomi desa yang berkelanjutan dan bekerjsama dengan lembaga kementerian desa serta pemerintah desa di wilayah setempat. Salah satu anak perusahaan PT Telkom Indonesia yang menjalankan dan mengelola kegiatan usaha jasa aplikasi simpel desa yaitu PT Hannan Idea Indonesia. Aplikasi simpel desa memudahkan perangkat desa dalam mengerjakan administrasi dan pelayanan terhadap masyarakat, terutama pada layanan pembuatan surat. Aplikasi ini berisi beberapa informasi salah satunya seperti layanan informasi publik yang dapat diakses oleh penduduk desa, informasi tentang pembangunan atau pemberdayaan antar warga dan memberikan berita yang bermanfaat kepada masyarakat baik urusan pemerintah, kesehatan dan teknologi.

Dalam melakukan akses aplikasi simpel desa menggunakan data yang penting yaitu Nomor Induk Kependudukan (NIK) dan nomor telepon yang aktif digunakan agar dapat menerima konfirmasi *OTP* (*One Time Password)*. Berdasarkan hasil wawancara yang dilakukan kepada Bapak M. Showabi Ihsan selaku kaur keuangan yang bertanggung jawab di bidang teknologi informasi, bahwa terdapat permasalahan dalam menjalankan aplikasi simpel desa yaitu jaringan atau sinyal kurang memadai dan jaringan internet tidak dapat digunakan. Berkaitan dengan hal tersebut juga mempengaruhi aksesibiltas terhadap server jika diakses oleh banyak pengguna secara bersamaan pada awal aplikasi tersebut digunakan oleh masyarakat desa. Selain hal tersebut server yang *down* akibat server *load* menyebabkan aplikasi tidak dapat menjalankan permintaan dari pengguna [2]. Dampak dari permasalahan tersebut yaitu kebutuhan masyarakat menjadi terganggu karena terhambatnya permintaan kebutuhan ke desa melalui sistem informasi tersebut. Karena sistem informasi ini sudah terkomputerisasi namun selama penggunaan aplikasi ini belum pernah dilakukan evaluasi keamanan informasi untuk mengetahui peluang terjadinya risiko yang mengancam data pengguna aplikasi maupun proses bisnis aplikasi secara menyeluruh [3].

Risiko adalah peluang terjadinya sesuatu yang menimbulkan dampak atau mengakibatkan terganggunya proses bisnis organisasi sampai menyebabkan gagalnya tujuan bisnis organisasi. Risiko diukur berdasarkan dampak yang ditimbulkan terhadap kemungkinan terjadinya risiko [4]. Risiko merupakan suatu kejadian yang tidak diinginkan dimana dihasilkan dari sebuah kejadian atau peristiwa sehingga berdampak merugikan dan hasilnya tidak pasti [5]. Ketika suatu sistem informasi diserang atau terancam, maka proses sistem yang sedang berjalan akan terganggu terutama pada aspek keamanan informasi. Aspek keamanan informasi yang dimaksud yaitu kerahasiaan (*confidentiality*), integritas *(integrity)* dan ketersediaan *(availability*) [6]. Keamanan informasi merupakan suatu hal yang perannya sangat penting untuk menjaga informasi pada suatu perusahaan maupun organisasi. Ketika keamanan informasi pada suatu lembaga pemerintahan tidak diolah dengan baik, maka dapat menimbulkan risiko pada keberlangsungan penggunaan sistem informasi. Dengan adanya analisis risiko keamanan ini dapat dimanfaatkan untuk mengetahui berbagai macam ancaman dan risiko yang kemungkinan terjadi pada aplikasi simpel desa [7]. Analisis manajemen keamanan informasi dilakukan untuk melindungi aset informasi pada sebuah aplikasi dari berbagai ancaman yang kemungkinan terjadi seperti kebocoran data dan pihak yang tidak memiliki akses dapat mengakses aplikasi tersebut.

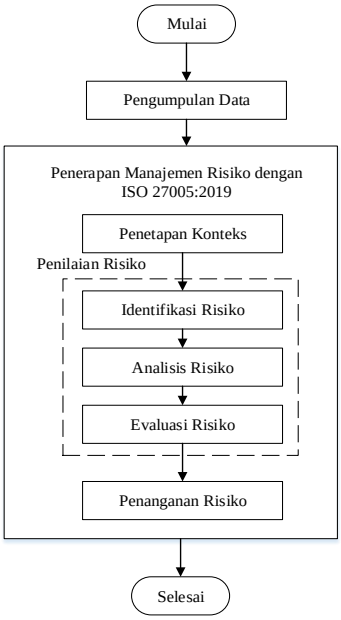
Metode-metode yang dapat digunakan dalam melakukan manajemen risiko keamanan informasi di antaranya yaitu Octave, NIST 800-30, ISO 27005 dan yang lainnya. Dalam pemilihan metode dapat disesuaikan dengan kebutuhan organisasi. Untuk pengembangan manajemen keamanan informasi bagi penyelenggaraan publik di Indonesia dihimbau menggunakan ISO 27000 [8]. Salah satu seri dari ISO 27000 yaitu ISO 27005 yang merupakan panduan atau pedoman untuk melakukan manajemen risiko keamanan informasi. ISO 27005 adalah pendekatan sistematis untuk manajemen risiko keamanan informasi diperlukan untuk mengidentifikasi persyaratan organisasi terkait dengan keamanan informasi dan menciptakan Sistem Manajemen Keamanan Informasi (SMKI) yang efektif [9]. Pada ISO 27005 menyediakan pedoman untuk manajemen risiko keamanan informasi, sehingga dapat membantu merancang manajemen keamanan informasi dengan mengetahui terlebih dahulu risikonya. Setelah mengetahui risikonya maka dilakukan analisis dengan tujuan agar dapat mengendalikan risiko yang telah diketahui [10]. Pemilihan ISO 27005 sebagai standar yang digunakan karena dianggap memudahkan dalam pengelolaan keamanan informasi aplikasi simpel desa pada tahap selanjutnya yaitu dalam tahap pengembangan aplikasi [8].

Berdasarkan penelitian sebelumnya yang dilakukan oleh [11] manajemen keamanan informasi dievaluasi dengan mengacu pada standar COBIT dan ISO/IEC 27001. Pada penelitian yang dilakukan oleh [12] keamanan informasi digunakan dalam melindungi data atau informasi agar tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak maka dilakukan perlindungan data dan informasi dengan melakukan enkrispi dan deskripsi *file* dokumen. Penelitian yang dilakukan oleh [13] dalam meningkatkan keamanan sistem pada *financial technology* menggunakan *One Time Password* pada akun pengguna layanan. Penelitian yang dilakukan oleh [14] analisis risiko digunakan pada aplikasi *service desk* dengan tujuan untuk melakukan perancangan manajemen keamanan informasi dan penerapan keamanan informasi pada aplikasi tersebut. Penelitian yang dilakukan oleh [15] analisis keamanan informasi diterapkan pada aplikasi *e-office* yang dikelola oleh PT Telkom Indonesia menggunakan standar ISO/IEC 27005:2018 untuk melakukan analisis manajemen risiko keamanan informasi dengan tujuan setiap risiko yang kemungkinan terjadi dapat ditangani dengan baik dan menjadi bahan evaluasi untuk pengembangan aplikasi.

Penelitian ini bertujuan untuk melakukan analisis risiko keamanan informasi menggunakan ISO 27005:2019 pada aplikasi simpel desa. Fokus penelitian ini hasil analisis risiko keamanan informasi menggunakan ISO 27005: 2019 digunakan sebagai bahan rekomendasi untuk tahap pengembangan aplikasi maupun sebagai bahan literasi bagi pengguna yaitu masyarakat Desa Cingebul.

2. Metode Penelitian

Proses analisis risiko keamanan informasi pada aplikasi simpel desa di kantor Desa Cingebul dilakukan menggunakan standar ISO 27005:2019. ISO 27005:2019 yang merupakan standar internasional yang menyediakan pedoman untuk melakukan proses manajemen risiko keamanan informasi [16]. Data yang digunakan dalam penelitian ini adalah hasil wawancara dengan pihak yang bertanggung jawab dalam pengelolaan aplikasi simpel desa. Langkah penelitian yang dilakukan disajikan pada Gambar 1.



Gambar 1. Tahapan Penelitian

Tahapan pertama dari penelitian ini dimulai dari pengumpulan data melalui wawancara, observasi, studi pustaka dan dokumentasi. Wawancara dan observasi dilakukan kepada pihak yang bertanggung jawab di bidang teknologi informasi. Tahap kedua dengan melakukan penetapan konteks dengan membahas pertimbangan umum dan kriteria dasar aplikasi simpel desa. Tahap ketiga melakukan penilaian risiko yang terdiri dari identifikasi risiko, analisis risiko dan evaluasi risiko. Identifikasi risiko yang terdiri dari beberapa proses yaitu identifikasi aset, identifikasi ancaman, identifikasi *existing control* dan identifikasi *vulnerabilities*. Perlu melakukan identifikasi untuk setiap aset yang dimiliki agar dapat diketahui *responsibility dan accountability*. Identifikasi ancaman memiliki potensi yang dapat membahayakan aset yang dimiliki, dengan ancaman yang mungkin timbul dapat berasal dari alam atau manusia, dan baik disengaja atau tidak disengaja. Selain itu, ancaman juga dapat timbul dari luar atau dalam suatu organisasi. Identifikasi *existing control* dilakukan untuk menghindari pengeluaran biaya yang tidak perlu dan tahap ini

mengindentifikasi kontrol yang ada dimana suatu pemeriksaan dilakukan dengan memastikan terlebih dahulu bahwa kontrol bekerja dengan benar. Identifikasi *vulnerabilities* menggambarkan adanya suatu kerentanan dari sebuah ancaman dipengaruhi pada kontrol yang dilaksanakan. Dengan adanya suatu penerapan kontrol yang tidak tepat dapat menimbulkan adanya kerentanan. Kemudian melakukan analisis risiko dalam tahap ini meliputi analisis kualitatif dengan melakukan penentuan kategori kemungkinan ancaman dan kategori dampak risiko serta menentukan level risiko. Pada tahap evaluasi risiko pada aplikasi simpel desa terdiri dari sebuah daftar risiko dengan tingkat dan nilai untuk melakukan perbandingan tingkat risiko dan kriteria dalam penanganan risiko. Selain itu juga akan diurutkan level risiko mulai dari yang tertinggi ke yang terendah. Tahap keempat dilakukan penanganan risiko dengan membandingkan penilaian risiko dan kriteria penerimaan risiko untuk membuat keputusan dalam mendapatkan hasil penanganan risiko, yang terdiri dari modifikasi risiko, mempertahankan risiko, menghindari risiko dan membagi risiko.

3. Hasil dan Pembahasan

Penelitian ini menggunakan ISO 27005:2019 untuk manajemen risiko keamanan informasi pada aplikasi simpel desa di kantor Desa Cingebul. Dalam melakukan proses penilaian risiko diawali dengan melakukan identifikasi terlebih dahulu lalu dilakukan tahap analisis risiko yang kemungkinan terjadi sehingga dapat muncul hasil evaluasi yang dibutuhkan.

3.1. Penetapan Konteks

Tahapan manajemen risiko yang dilakukan mengacu pada kerangka kerja ISO 27005:2019 dengan batasam konsep penelitian mulai dari penetapan konteks, penilain risiko dan penanganan risiko. Dengan kriteria dampak risiko yang ditetapkan yaitu dampak ancaman dan dampak kemungkinan terjadinya ancaman.

3.2. Penilaian Risiko

Proses penilaian risiko keamanan informasi pada aplikasi simpel desa di kantor Desa Cingebul dilakukan melalui tiga tahapan yaitu identifikasi risiko, analisis risiko dan evaluasi risiko.

3.2.1. Identifikasi Risiko

Identifikasi risiko terdiri dari beberapa proses di antaranya identifikasi aset, identifikasi ancaman dan identifikasi *existing control* & identifikasi *vulnerabilities*. Identifikasi aset yang dimiliki kantor Desa Cingebul dalam menjalankan aplikasi terdiri dari aset utama berupa aplikasi Simpel Desa dan aset pendukung berupa perangkat keras dan perangkat lunak.

Identifikasi ancaman terhadap aset TI yang dimiliki kantor Desa Cingebul, ancaman dapat berasal dari alam dan *human error* yang disajikan pada Tabel 1.

Tabel 1. Identifikasi ancaman

No	Aset	Kode Aset	Ancaman
1	*Hardware*	H1	Petir
		H2	Kebakaran
		H3	Bencana alam
		H4	Debu/kotoran
		H5	Listrik padam
		H6	Koneksi jaringan terputus
		H7	Kegagalan/rusaknya *hardware*
		H8	*Human error*
		H9	*Server down*
		H10	Banyak virus yang terdapat di PC
2	*Software*	S1	Hilangnya data/kebocoran data
		S2	Akses data oleh pihak yang tidak berhak
		S3	Serangan virus
		S4	Gangguan pada sistem operasi
		S5	Kesalahan penggunaan perangkat
		S6	*Bruteforce login/ login* secara paksa
		S7	Serangan DDoS

Pada Tabel 1 berisi tentang hasil identifikasi ancaman yang terdiri dari beberapa ancaman yang mungkin terjadi. Identifikasi ancaman dibagi menjadi dua jenis yaitu yang berasal dari alam dan *human error*. Ancaman pada aset yang dimiliki diberikan kode dengan tujuan untuk mempermudah identifikasi dan analisis pada proses selanjutnya.

Identifikasi *existing control* dilakukan untuk mengetahui kontrol yang diterapkan pada aset untuk menghindari pengeluaran biaya yang tidak perlu. Identifikasi *vulnerabilities* menggambarkan adanya suatu kerentanan dari yang dapat terjadi pada aset yang dimiliki. Identifikasi *existing control* & identifikasi *vulnerabilities* disajikan pada Tabel 2.

Tabel 2. Identifikasi *existing control* & identifikasi *vulnerabilities*

Nama Aset	***Existing controls*** **(Kontrol yang ada)**	***Vulnerabilities*** **(Kerentanan)**
Hardware	Memasang penangkal petir	Kabel penyalur arus petir belum memadai
	Menyediakan APAR (Alat Pemadam Api Ringan)	Tidak berhati – hati dalam menggunakan api di lingkungan sekitar kantor
	Menyiapkan tempat dengan memperhatikan dan mempertimbangkan keamanannya	Perangkat diletakkan di tempat yang rawan bencana
	Membersihkan secara berkala	Berada di lokasi terbuka
	Menggunakan bantuan *genset*	Jaringan listrik tidak stabil
	Perbaikan/penggantian perangkat atau menghubungi pihak ketiga	Koneksi jaringan di kantor Desa Cingebul tidak stabil
	Melakukan pengecekan *hardware* secara berkala	Kurangnya pemeliharaan (*maintenance)* dan perangkat keras sudah melampaui batas akhir penggunaan
	Adanya pembagian tugas	Kurangnya pengetahuan dalam penggunaan sistem
	Melakukan pemeliharaan dan pembaruan secara berkala	Banyak proses yang berjalan
	Melakukan instal antivirus	Tidak adanya antivirus
Software	Melakukan kontrol secara berkala pada *software* yang berjalan	Banyaknya proses yang berjalan
	Melakukan autentikasi terhadap akses	Modifikasi disengaja atau manipulasi perangkat lunak yang mengarah pada data yang salah dan tindakan yang curang
	Menambah *bandwith*	Banyak yang mengakses jaringan secara bersamaan
	Update antivirus secara berkala	Gangguan terhadap layanan akibat serangan virus yang tidak terdeteksi oleh antivirus yang tidak *up to date*
	Mengganti dengan sistem operasi yang asli	Windows tidak berjalan dengan semestinya jika menggunakan OS bajakan
	Adanya pelatihan secara berkala terhadap penanggung jawab aplikasi	Kurangnya pelatihan terhadap penanggung jawab aplikasi
	Otorisasi *password* hak akses kepada user yang menggunakan	Tidak ada batasan akses sehingga mudah diakses oleh orang yang tidak berwenang
	Meningkatkan keamanan menggunakan *firewall*, anti spam, *Virtual Private Network* (VPN) serta sistem keamanan lainnya	Meningkatnya lalu lintas jaringan internet

Tabel 2 berisi tentang identifikasi *existing control* dan identifikasi *vulnerabilities* yang berisi tentang kontrol yang ada terhadap ancaman atau kerentanan yang muncul pada kegiatan maupun aktivitas yang ada berdasarkan masing-masing aset yang dimiliki kantor Desa Cingebul. Dari aspek *hardware* dan *software* dapat dijabarkan bahwa kerentanan yang paling spesifik dan difokuskan adalah yang berkaitan dengan aplikasi simpel desa.

3.2.2. Analisis Risiko

Pada tahap ini akan dilakukan penilaian risiko yang mungkin telah diidentifikasi sebelumnya. Penentuan nilai ini akan dilakukan berdasarkan kemungkinan dari ancaman dan kategori dampak terjadinya risiko. Dengan kategori kemungkinan ancaman mulai dari *very unlikely* (1), *unlikely* (2), *possible* (3), *likely* (4) dan *frequent* (5), dengan nilai kategori mulai dari 1 sampai 5. Kategori dampak terjadinya risiko mulai dari dampak yang tidak signifikan hingga dampak yang sangat signifikan dan menimbulkan gangguan pada pelayanan. Kategori dari dampak mulai dari *very low* (1), *low* (2), *medium* (3), *high* (4) dan *very high* (5), dengan nilai dampak mulai dari yang sangat rendah dengan nilai 1 sampai dampak yang paling tinggi dengan nilai 5. Berikut analisis risiko berdasarkan nilai ancaman dan nilai dampak dengan kode H untuk aset *hardware* dan kode S untuk aset *software*, dapat dilihat pada tabel di bawah ini:

Tabel 3. Analisis risiko

Nama Aset	Kode	*Existing controls* (Kontrol yang ada)	*Vulnerabilities* (Kerentanan)	Nilai Ancaman	Nilai dampak
Hardware	H1	Memasang penangkal petir	Kabel penyalur arus petir belum memadai	*Unlikely*	*Medium*
	H2	Menyediakan APAR (Alat Pemadam Api Ringan)	Tidak berhati – hati dalam menggunakan api di lingkungan sekitar kantor	*Unlikely*	*Medium*
	H3	Menyiapkan tempat dengan memperhatikan dan mempertimbangkan keamanannya	Perangkat diletakkan di tempat yang rawan bencana	*Unlikely*	*High*
	H4	Membersihkan secara berkala	Berada di lokasi terbuka	*Unlikely*	*Low*
	H5	Menggunakan bantuan *genset*	Jaringan listrik tidak stabil	*Possible*	*Medium*
	H6	Perbaikan/penggantian perangkat atau menghubungi pihak ketiga	Koneksi jaringan di kantor Desa Cingebul tidak stabil	*Unlikely*	*Medium*
	H7	Melakukan pengecekan *hardware* secara berkala	Kurangnya pemeliharaan dan perangkat keras sudah melampaui batas akhir penggunaan	*Unlikely*	*Medium*
	H8	Adanya pembagian tugas	Kurangnya pengetahuan dalam penggunaan sistem	*Unlikely*	*Medium*
	H9	Melakukan pemerliharaan dan pembaruan secara berkala	Banyaknya proses yang berjalan	*Possible*	*Low*
	H10	Melakukan *install* antivirus	Tidak adanya antivirus	*Possible*	*Low*
Software	S1	Melakukan kontrol secara berkala pada *software* yang berjalan	Banyaknya proses yang berjalan	*Possible*	*Low*
	S2	Melakukan autentikasi terhadap akses	Modifikasi disengaja atau manipulasi perangkat lunak yang mengarah pada data yang salah dan tindakan yang curang	*Unlikely*	*Medium*
	S3	Menambah *bandwith*	Banyak yang mengakses jaringan secara bersamaan	*Unlikely*	*Medium*
	S4	Mengganti dengan sistem operasi yang asli	Windows tidak berjalan dengan semestinya jika menggunakan OS bajakan	*Possible*	*Medium*
	S5	Adanya pelatihan secara berkala terhadap penanggung jawab aplikasi	Kurangnya pelatihan terhadap penanggung jawab aplikasi	*Possible*	*High*
	S6	Otorisasi *password* hak akses kepada user yang menggunakan	Tidak ada batasan akses sehingga mudah diakses oleh orang yang tidak berwenang	*Possible*	*High*
	S7	Meningkatkan keamanan menggunakan *firewall*, anti spam, *Virtual Private Network* (VPN) serta sistem keamanan lainnya	Meningkatnya lalu lintas jaringan internet	*Possible*	*High*

Dalam bagian dari analisis risiko ini terdapat kategori penilaian risiko, dimana proses penilaian risiko ini dilakukan secara kualitatif dengan melakukan penaksiran ancaman dan risiko yang kemungkinan terjadi. Sedangkan penelitian kuantitatif mendapatkan hasil risiko yang dinilai dalam bentuk angka dikategori analisis risiko. Kategori penilaian risiko itu berasal dari hasil perkalian antara nilai kemungkinan terjadinya ancaman dan nilai dampak ancaman. Matriks penilaian risiko dibagi menjadi tiga kategori level risiko yaitu risiko rendah (*low risk),* risiko sedang (*medium risk)* dan risiko tinggi *(high risk)*.

Berdasarkan kemungkinan risiko yang sudah diidentifikasi dan dianalisis sebelumnya kemudian dibuat daftar prioritas risiko yang sesuai dengan nilai risiko yang disajikan pada Tabel 4.

Tabel 4. Hasil Penilaian Level Risiko

Kode	Nilai ancaman	Nilai dampak	Nilai Risiko	Level Risiko
H1	2	3	6	*Medium*
H2	2	3	6	*Medium*
H3	2	4	8	*Medium*
H4	2	2	4	*Low*
H5	3	3	9	*Medium*
H6	4	3	12	*Medium*
H7	2	3	6	*Medium*
H8	2	3	6	*Medium*
H9	4	5	20	*High*
H10	3	2	6	*Medium*
S1	3	2	6	*Medium*
S2	2	3	6	*Medium*
S3	2	3	6	*Medium*
S4	3	3	9	*Medium*
S5	3	4	12	*Medium*
S6	3	4	12	*Medium*
S7	3	4	12	*Medium*

Berdasarkan Tabel 4 pada penilaian level risiko mendapatkan hasil level risiko dengan rata-rata level risiko sedang atau medium (M), sedangkan pada poin H4 yang merupakan identifikasi ancaman yang berasal dari debu/kotoran dengan level risiko yang terendah atau *low* (L) dari sekian ancaman yang ada dan ancaman yang paling tinggi pada kode aset H9 yaitu ketika *server down.*

3.2.3. Evaluasi Risiko

Pada tahap ini dilakukan proses berdasarkan hubungan antara frekuensi terjadinya ancaman dan nilai dampak. Selain itu juga akan diurutkan level tertinggi ke yang terendah seperti pada Tabel 5 dan Tabel 6 di bawah ini:

Tabel 5. Matriks Penilaian Risiko

		Kemungkinan terjadinya ancaman				
		(1)	(2)	(3)	(4)	(5)
Dampak	(1)					
	(2)		H4	H10, S1		
	(3)		H1, H2,H7, H8, S2, S3,	H5, S4	H6	
	(4)		H3	S5, S6, S7		
	(5)				H9	

Keterangan warna
Hijau : risiko rendah (*low*)
Kuning : risiko sedang (*medium*)
Merah : risiko tinggi (*high*)

Dapat dikelompokkan menjadi satu, matriks dengan kategori penilaian risiko di atas menunjukkan bahwa hasil rata-rata risiko sedang atau *medium*. Terdapat satu risiko yang rendah yaitu pada kode H4 berdasarkan kategori ancaman pada *hardware* karena debu/kotoran dan satu risiko yang bernilai tinggi pada kode H9 akibat ancaman ketika *server down.*

Tabel 6. Daftar level risiko yang mungkin terjadi

Level Risiko	Kode Aset
Low (L)	H4
Medium (M)	H1, H2, H3, H5, H6, H7, H8, H10, S1, S2, S3, S4, S5, S6, S7
High (H)	H9

3.3. Penanganan Risiko

Pada tahap penilaian risiko dilakukan dengan pemilihan tindakan dalam penanganan risiko yang terdiri dari empat perlakuan meliputi modifikasi risiko (*Risk Modification/RM*), mempertahankan risiko (*Risk Retention/RR*), menghindari risiko (*Risk Avoidance/RA*) dan membagi risiko (*Risk Sharing/RS*). Hasil penilaian risiko disajikan pada Tabel 7.

Tabel 7. Hasil Penilaian Risiko

Kode	Level Risiko	Biaya Pemulihan	Penanganan Risiko	Keterangan
H1	*Medium*	*Low*	RM	Pengendalian risiko dengan memasang penangkal petir
H2	*Medium*	*Medium*	RM	Dengan menyediakan APAR
H3	*Medium*	*Medium*	RM	Mempertimbangkan keamanan penempatan perangkat keras
H4	*Low*	*Low*	RR	Dengan membersihkan secara berkala
H5	*Medium*	*Medium*	RM	Menggunakan *genset*
H6	*Medium*	*Medium*	RM	Pergantian perangkat
H7	*Medium*	*Medium*	RM	Kontrol *hardware* secara berkala
Kode	Level Risiko	Biaya Pemulihan	Penanganan Risiko	Keterangan
H8	*Medium*	*Medium*	RM	Pembagian tugas
H9	*High*	*High*	RA	Melakukan *backup* data secara berkala
H10	*Medium*	*Low*	RM	Instal antivirus
S1	*Medium*	*Low*	RM	Kontrol *software* yang berjalan
S2	*Medium*	*High*	RA	Autentikasi terhadap akses
S3	*Medium*	*Medium*	RM	Menambah *bandwith*
S4	*Medium*	*High*	RA	Penggantian sistem operasi
S5	*Medium*	*High*	RA	Pelatihan penggunaan aplikasi
S6	*Medium*	*High*	RA	Otorisasi *password* pada *user*
S7	*Medium*	*High*	RA	Menggunakan *firewall* dan VPN

Hasil penanganan risiko ini rata-rata *risk modification* (RM). Dalam penanganan risiko dengan kode risiko H4 dengan level risiko L (*low)* dan biaya pemulihan rendah atau *low* (L) mendapatkan penanganan risiko *risk retention* (RR). Pada aset kode H9 dengan level risiko *high* dan biaya pemulihan *high* maka penanganan risiko yang muncul *risk avoidance* (RA).

Berdasarkan hasil analisis penilaian risiko yang terdapat pada Tabel 4.8 maka rekomendasi yang tepat untuk penanganan risiko pada keamanan informasi aplikasi simpel desa berdasarkan ISO 27005:2019 yaitu:

1) Kontrol rekomendasi kode H1, H2, H3 dan H4 yaitu *equipment sitting and protection* (A.11.2.1) dengan memberikan peralatan perlindungan sesuai dengan ancaman pada masing-masing aset.
2) Kontrol rekomendasi pada kode H5 dan H6 yaitu *supporting utilities* (A.11.2.2) dengan menggunakan bantuan *genset* dan melakukan pergantian perangkat.
3) Kontrol rekomendasi kode H7 yaitu *equipment maintenance* (A.11.2.4) dengan melakukan perawatan perangkat keras secara berkala.
4) Kontrol rekomendasi kode H8 dan kode S5 yaitu *management responsibilities* (A.7.2.1) dengan melakukan pelatihan untuk perangkat desa agar bertanggung jawab dalam pembagian tugas yang ada.
5) Kontrol rekomendasi kode S3 dan H10 yaitu *cabling security* (A.11.2.3) dengan melakukan penggantian kabel yang rusak dengan kualitas yang tebal dan kuat agar tahan lama dan tidak mudah rentan.
6) Kontrol rekomendasi S4 dan S7 yaitu *installation of software on operational systems* (A.12.5.1) dengan mengganti sistem operasi yang ada dan meningkatkan keamanan menggunakan *firewall* & VPN.
7) Kontrol rekomendasi kode H9, S1, S2 dan S6 yaitu *information backup* (A.12.3.1) dengan melakukan *backup* data secara berkala.

4. Kesimpulan

Berdasarkan analisis risiko keamanan informasi pada aplikasi simpel desa yang ada di kantor Desa Cingebul menggunakan ISO 27005:2019 dapat disimpulkan bahwa terdapat 17 kemungkinan risiko yang dapat terjadi terdiri dari satu ancaman tingkat tinggi (*high*), 15 kemungkinan risiko tingkat sedang (*medium*)

dan terdapat satu kemungkinan ancaman dengan tingkat rendah (*low*). Rekomendasi untuk penanganan risiko keamanan informasi pada aplikasi simpel desa berdasarkan ISO 27005:2019 di antaranya yaitu dengan kontrol rekomendasi *equipment sitting and protection* (A.11.2.1), *supporting utilities* (A.11.2.2), *equipment maintenance* (A.11.2.4), *management responsibilities* (A.7.2.1), *Cabling Security* (A.11.2.3), *installation of software on operational systems* (A.12.5.1) dan *Information backup* (A.12.3.1). Saran untuk penelitian selanjutnya dapat melakukan analisis risiko keamanan informasi pada pusat aplikasi simpel desa untuk mengetahui risiko keamanan informasi secara lebih spesifik.

Daftar Pustaka

[1] "Simpel Desa," 2018.

[2] F. Apriliansyah, I. Fitri, and A. Iskandar, "Implementasi Load Balancing Pada Web Server Menggunakan Nginx," Jurnal Teknologi dan Manajemen Informatika, Vol. 6, No. 1, 2020, doi: 10.26905/jtmi.v6i1.3792.

[3] N. Matondanga, I. N. Isnainiyahb, and A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," Jurnal RESTI(Rekayasa Sistem dan Teknologi Informasi), Vol. vOL.2 nO.1, 2018.

[4] F. Nasher, "Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (LPSE) di Dinas Komunikasi dan Informatika Kabupaten Cianjur dengan Menggunakan SNI ISO/IEC 27001:2013," Media Jurnal Informatika, Vol. Vol.10 No., 2018.

[5] H. Ikhsan and N. Jarti, "Analisis Risiko Keamanan Teknologi Informasi Menggunakan Octave Allegro," Jurnal Responsive, Vol. Vol.2 No.1, 2018.

[6] S. A. Sholikhatin and K. N. Isnaini, "Analysis of Information Security Using ISO 27001 and Triangular Fuzzy Number Weighting," Jurnal Ilmiah Informatika, Vol. 6, No. 1, PP. 43–49, Jun. 2021, doi: 10.35316/jimi.v6i1.1224.

[7] R. L. Bawono, "Evaluasi Manajemen Risiko Keamanan Informasi Pada PT Hardo Soloplast Menggunakan Framework NIST SP 800-30 dan Perhitungan Maturity Level Keamanan Informasi Menggunakan ISO 27002:2005," 2020.

[8] Asriyanik and Prajoko, "Manajemen Risiko Keamanan Informasi Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," Jurnal Teknik Informatika dan Sistem Informasi, Vol. Vol.4, No., 2018.

[9] Jonny, A. Ambarwati, and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005," Jurnal Sistem Informasi (SISTEMASI), Vol. Vol 10 No, 2021.

[10] E. Nursetyawati, R. Fauzi, and R. A. Nugraha, "Perancangan Manajemen Keamanan Informasi Menggunakan Metode Analisis Risiko ISO 27005:2008 pada Dinas Komunikasi dan Informatika Jawa Barat," Vol. Vol.7 No.3, 2020.

[11] D. P. Agustino, "Information Security Management System Analysis Menggunakan ISO/IEC 27001 (Studi Kasus: STMIK STIKOM Bali)," Eksplora Informatika, Vol. 8, No. 1, P. 1, Sep. 2018, doi: 10.30864/eksplora.v8i1.130.

[12] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," Eksplora Informatika, Vol. 8, No. 1, P. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.

[13] G. Sitoresmi and W. Wijanarto, "Analisis Algoritma RSA Dan LSB pada One Time Password untuk Financial Technology," Eksplora Informatika, Vol. 8, No. 2, PP. 122–131, 2019, doi: 10.30864/eksplora.v8i2.157.

[14] E. Nursetyawati, R. Fauzi, and ..., "Perancangan Manajemen Keamanan Informasi Menggunakan Metode Analisis Risiko ISO 27005:2008 pada Dinas Komunikasi dan Informatika Jawa Barat," eProceedings …, Vol. 7, No. 2, PP. 7338–7347, 2020.

[15] S. Sahira, R. Fauzi, and I. Santosa, "Analisis Manajemen Risiko pada Aplikasi E-Office yang Dikelola oleh PT TELKOM Indonesia Menggunakan Standar ISO/IEC 27005:2018," Vol. Vol.7 No.2, 2020.

[16] A. Moura, "Abnt Nbr Iso," PP. 15–25, 2018.