

# Pengukuran Implementasi *Information Assurance* Pada Dinas Kependudukan dan Pencatatan Sipil Menggunakan *Framework* IAFEG

1<sup>st</sup> Kimberly Kailla  
Fakultas Informatika  
Universitas Telkom  
Bandung, Indonesia

kkailla@students.telkomuniversity  
.ac.id

2<sup>nd</sup> Rahmat Yasirandi  
Fakultas Informatika  
Universitas Telkom  
Bandung, Indonesia

batanganhita@telkomuniversity.ac  
.id

3<sup>rd</sup> Rio Guntur Utomo  
Fakultas Informatika  
Universitas Telkom  
Bandung, Indonesia

riogunturutomo@telkomuniversity  
.ac.id

**Abstrak-**Pemanfaatan teknologi informasi pada pemerintahan di Indonesia telah diterapkan pada berbagai lembaga pemerintahan, tidak terkecuali lembaga pemerintahan yang berorientasi pada bidang pelayanan publik. Implementasi teknologi informasi yang telah diterapkan pada pemerintahan Indonesia yaitu *e-Government* atau *electronic government*. Dalam *e-Government* diperlukan adanya jaminan keamanan informasi dalam mendukung proses bisnis. *Information Assurance* (IA) atau jaminan informasi merupakan sebuah praktik untuk mengelola resiko terkait informasi dan langkah-langkah yang diperlukan untuk sistem informasi. Dengan kata lain, IA berfokus pada perlindungan dan jaminan sistem layanan informasi. IA perlu diukur untuk mengetahui sejauh mana penerapannya agar mengetahui hal-hal apa saja terkait instansi yang sudah baik implementasi IA nya atau yang membutuhkan perbaikan. Instrumen pengukuran IA menggunakan framework IAFEG yang mengadopsi metode Goal Question Metric (GQM) akan membagi instrumen pengukuran IA dalam 3 kategori yaitu *Organisational Management*, *Implementation Management* dan *Social Management*. Kategori-kategori tersebut mempunyai faktor item pengukuran dengan pertanyaan instrumen yang berbeda sebagai acuan dalam pengukuran implementasi IA. Hasil dari pengukuran berupa skala pengukuran atau metric yang akan menunjukkan status implementasi IA pada lembaga pemerintah.

**Kata kunci** - *pelayanan publik*, *E-Government*, *information assurance*, *goal question metric*, *framework IAFEG*

**Abstract-***The use of information technology in government in Indonesia has been applied to various government institutions, including government institutions that are oriented to the field of public services. The implementation of information technology that has been applied to the Indonesian government is e-Government or electronic government. In e-Government, it is necessary to guarantee information security in supporting business processes. Information Assurance (IA) is a practice to manage risks related to information and the steps required for information systems. In other*

*words, IA focuses on the protection and assurance of information service systems. IA needs to be measured to find out the extent of its implementation in order to find out what things are related to institutions that have good IA implementation or need improvement. The IA measurement instrument using the IAFEG framework which adopts the Goal Question Metric (GQM) method will divide the IA measurement instrument into 3 categories, namely Organizational Management, Implementation Management and Social Management. These categories have measurement item factors with different instrumental questions as a reference in measuring IA implementation. The results of the measurement are in the form of a measurement scale or metric that will show the status of IA implementation in government institutions.*

**Keywords-** *public service, E-Government, information assurance, goal question metric, framework IAFEG.*

## I. PENDAHULUAN

Penggunaan teknologi digital dalam sistem pemerintahan seperti *e- Government* telah memperluas kesempatan terjadinya komunikasi dua arah antara pemerintah dan masyarakat melalui jaringan internet dalam penyebaran informasi dan pelayanan pemerintah kepada masyarakat [1]. *E-Government* dinilai dapat memberikan manfaat dalam meningkatkan kinerja instansi pemerintah dan interaksi dengan masyarakat [2]. Di Indonesia, implementasi *e-Government* diatur pada Peraturan Pemerintah (PP) Nomor 71 Tahun 2019, mengenai penyelenggaraan dan transaksi elektronik [3]. Dan Peraturan Presiden (Perpres) Nomor 95 Tahun 2018, tentang Sistem Pemerintahan Berbasis Elektronik [11].

Dalam PP Nomor 71 Tahun 2019, disebutkan bahwa perangkat keras yang digunakan oleh penyedia *e-Government* harus memenuhi aspek

keamanan, interoperabilitas dan kompatibilitas dengan sistem yang digunakannya serta memiliki dukungan teknis, pemeliharaan, dan layanan kontinuitas layanan. Perangkat lunak yang digunakan oleh penyedia *e-Government* harus beroperasi dengan aman dan andal, memastikan kesinambungan layanan [3]. Dan dalam Perpres Nomor 95 Tahun 2018, menyebutkan bahwa sistem pemerintahan berbasis elektronik harus meliputi; tata kelola, manajemen, layanan, infrastruktur, aplikasi, keamanan, dan audit teknologi informasi dan komunikasi [11].

Dalam hal ini, jaminan informasi atau *Information Assurance* (IA) dapat dijadikan sebagai mekanisme untuk melindungi dan mengamankan sistem dan layanan informasi [2], karena IA adalah praktik melindungi dan mempertahankan sistem informasi dengan memastikan ketersediaan, kerahasiaan, integritas, otentikasi, dan non-penyangkalan dan dapat memberikan organisasi kemampuan untuk melindungi informasi [4], serta menyediakan cara yang efektif dan efisien untuk melindungi sistem informasi. Beberapa manfaat IA yang efektif antara lain manfaat operasional, manfaat taktis, manfaat strategis, dan manfaat organisasi [2].

Instansi pemerintah yang akan menjadi objek kajian penelitian adalah Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil) Kota Bandar Lampung. Pertimbangan instansi dijadikan objek kajian karena Disdukcapil merupakan instansi pemerintah yang telah menerapkan *e-Government*, dimana bidang kerja yang ada pada instansi tersebut mencakup pengelolaan informasi, termasuk sistem informasi administrasi kependudukan, pengolahan dan penyajian data, pemanfaatan data dan dokumen kependudukan, serta tata kelola dan sumber daya manusia teknologi informasi dan komunikasi, sehingga membutuhkan pengukuran terhadap jaminan perlindungan informasi atau IA, agar patuh terhadap Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 dan Peraturan Presiden (Perpres) Nomor 95 Tahun 2018.

Kajian terhadap implementasi dari manajemen keamanan informasi pada sistem *e-Government*, dapat dilakukan menggunakan berbagai instrumen pengukuran keamanan informasi, seperti framework COBIT 5, ISO/IEC 27001, *Information Assurance For E-Government* (IAFEG) dan lainnya. Pada penelitian ini, akan berfokus menggunakan framework IAFEG karena framework IAFEG adalah framework yang dibangun untuk mengukur penerapan IA pada sistem *e-Government* di Indonesia. Sedangkan IA merupakan sebuah rumpun keilmuan yang mana merupakan superset dari keamanan informasi. IA mencakup *scope* yang lebih luas daripada keamanan informasi, seperti kebijakan, organisasi,

dan juga lainnya. Maka dari itu, proses dari IA yang mendukung tata kelola perusahaan dapat meningkatkan penerapan *e-Government* yang ada pada Disdukcapil Bandar Lampung, karena IA bertujuan untuk meningkatkan efektivitas, efisiensi, dan kualitas layanan.

Tujuan dari penelitian ini adalah untuk dapat mengetahui sejauh mana status implementasi IA pada Disdukcapil Bandar Lampung, dengan mengukur setiap faktor-faktor IA nya. Lebih jauh, penelitian ini juga akan memberikan rekomendasi kontrol berdasarkan hasil status pengukuran implementasi IA, dengan mengacu pada setiap kontrol ISO/IEC 27002:2013. Hasil dari rekomendasi tersebut dapat digunakan sebagai pedoman dalam perbaikan atau peningkatan faktor-faktor IA pada Disdukcapil Bandar Lampung.

Dengan adanya pengukuran IA pada *e-Government* di Disdukcapil Bandar Lampung, dan rekomendasi kontrol berdasarkan ISO/IEC 27002, diharapkan dapat menjadi pedoman Disdukcapil Bandar Lampung dalam mengetahui apa saja hal-hal terkait instansi yang belum sesuai terhadap implementasi IA dan yang memerlukan perbaikan atau peningkatan pada kinerja setiap praktik, agar penyelenggaraan *e-Government* sesuai dengan tujuan penyelenggaraan *e-Government* yang ada pada Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 dan Peraturan Presiden (Perpres) Nomor 95 Tahun 2018.

#### A. Topik dan Batasannya

Pada tugas akhir ini, akan berfokus pada evaluasi dan kajian pengukuran implementasi IA di Disdukcapil, dengan mengacu pada framework IAFEG. Pengukuran implementasi IA dilakukan berdasarkan hasil kuesioner yang telah dibagikan kepada staf Disdukcapil Bandar Lampung pada bidang pengelolaan informasi administrasi kependudukan, meliputi staf dari seksi sistem informasi administrasi kependudukan, seksi pengolahan dan penyajian data dan seksi tata kelola dan sumber daya manusia teknologi informasi dan komunikasi. Hasil kuesioner akan menentukan status IA dan rekomendasi kontrol yang mengacu pada ISO/IEC 27002.

#### B. Tujuan

Adapun tujuan yang ingin dicapai pada penelitian ini adalah:

1. Mengukur kondisi dari implementasi *information assurance* pada Disdukcapil Bandar Lampung
2. Mengevaluasi dan mengkaji hasil pengukuran implementasi *information assurance* pada Disdukcapil Bandar Lampung.

3. Memberikan rekomendasi untuk peningkatan implementasi *information assurance* berdasarkan hasil pengukuran dan analisis.

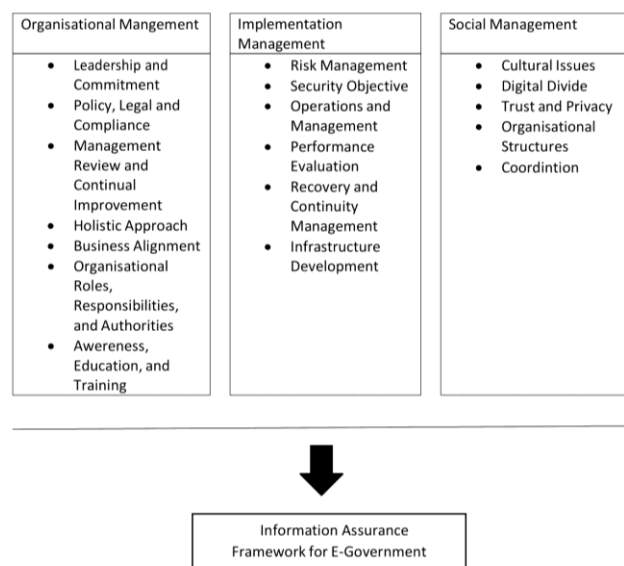
## II. KAJIAN TEORI

### A. Information Assurance

*Information Assurance* (IA) adalah sebuah proses untuk menjaga dan mempertahankan informasi dengan memastikan kerahasiaan, integritas dan ketersediaan untuk melindungi hak-hak orang dan organisasi. IA mengacu pada pertimbangan yang dapat memberi organisasi kemampuan untuk melindungi hak mereka serta memberi organisasi kemampuan untuk melindungi hak-hak pihak lain yang mendukung dan berinteraksi dengan mereka [4]. Dengan kata lain, IA merupakan masih berkaitan dengan keamanan informasi, tetapi IA berfokus pada mekanisme perlindungan dan jaminan sistem dan layanan informasi [2].

Tahapan awal dari proses IA yaitu enumerasi dan klasifikasi aset informasi yang akan dilindungi. IA akan melakukan penilaian risiko kerentanan atas aset informasi yang ada. Penilaian IA akan mempertimbangkan probabilitas dan dampak dari ancaman yang mengeksploitasi kerentanan dalam suatu aset dengan dampak yang biasanya diukur dalam hal biaya bagi pemangku kepentingan aset tersebut [6].

### B. Framework IAFEG



GAMBAR 1.  
PEMODELAN IAFEG (RIO GUNTUR UTOMO, 2020)

Pada gambar diatas, terlihat bahwa framework dibagi menjadi 3 kategori

Information Assurance Framework for E-Government (IAFEG) adalah sebuah framework yang dibangun untuk mengukur penerapan IA pada sistem *e-Government* di Indonesia dengan kerangka kerja yang terdiri dari 18 faktor yang dibagi menjadi 3 kategori yang telah dikonfirmasi, yaitu; *Organisational Management*, *Implementation Management*, dan *Social Management*. Faktor-faktor tersebut disusun dengan melibatkan 8 ahli pada bidang *e-Government*, *information assurance*, dan keamanan informasi yang mampu dan memiliki kapabilitas dalam mengkaji IA untuk *e-Government*.

Kerangka kerja yang telah dikonfirmasi akan dikembangkan untuk digunakan sebagai instrumen penelitian untuk mengukur proses implementasi IA pada *e-Government*. Instrumen akan dikembangkan dengan melakukan pendekatan *Goals Question and Metric (GQM)*. *Goals* merupakan faktor item dari kerangka IA, sedangkan *question* adalah pengembangan dari instrumen-instrumen IA yang telah disempurnakan menjadi pertanyaan instrumen, yang mewakili komponen dari masing-masing faktor. *Metric* adalah skala yang dikembangkan untuk organisasi dalam menjawab setiap pertanyaan instrumen untuk menilai tingkat IA nya. Framework IAFEG juga mengadopsi Process Assessment Model COBIT 5 yang didasarkan pada ISO/IEC 15504-2:2003 dalam mengukur proses implementasi IA yang menghasilkan status dan skor tiap kategori IA. Berikut adalah ilustrasi dari framework IAFEG:

berdasarkan ruang lingkup. Yang pertama yaitu kategori *Organisational Management* (OM),

pada kategori tersebut terdapat 7 faktor instrumen pengukuran yang didasarkan pada tujuh faktor dari kategori OM. Yang kedua yaitu kategori *Implementation Management* (IM), terdapat 6 faktor instrumen pengukuran berdasarkan 6 faktor dari kategori IM. Dan yang ketiga yaitu kategori *Social Management* (SM) mempunyai 5 faktor instrumen pengukuran berdasarkan 5 faktor dari kategori SM. Faktor-faktor dari framework IAFEG sangat signifikan secara statistik sehingga dapat mempengaruhi implementasi IA untuk *e- Government* di Indonesia [7].

### C. Goal Questions and Metric (GQM)

*Goal Questions and Metric* (GQM) adalah sebuah teknik untuk membantu menentukan kekuatan dan kelemahan dari proses yang dijalankan saat ini, dan memberikan alasan untuk mengadopsi atau menyempurnakan teknik, untuk mengevaluasi kualitas dan dampak dari proses tertentu. *Goal* adalah level konseptual yang ingin dicapai. Sasaran dari *goal* harus spesifik, terukur, dapat dicapai, relevan/realistis dan tepat waktu. *Questions* berfokus pada tingkat operasional, seperti menggunakan serangkaian pertanyaan untuk menentukan apa yang ingin di pelajari. Sedangkan *metric* adalah untuk menyelaraskan bagaimana mengukur jawaban atas pertanyaan, sehingga membuat setiap pertanyaan lebih terukur [8].

### D. COBIT 5 Process Assessment Model

COBIT 5 PAM (*Process Assessment Model*) adalah model penilaian kemampuan proses berbasis ISO/IEC 15504 yang menggabungkan COBIT 5 sebagai model referensi proses untuk persyaratan dasar dan ISO/IEC 15504 sebagai dasar kerangka pengukuran untuk menentukan tingkat kemampuan. COBIT 5 memungkinkan perusahaan untuk membangun tata kelola dan manajemen kerangka kerja yang efektif, serta memungkinkan teknologi informasi terkait untuk diatur dan dikelola secara holistik untuk seluruh perusahaan, dengan mempertimbangkan kepentingan terkait TI dari pemangku kepentingan internal maupun eksternal [9]. COBIT 5 PAM membagi setiap kemampuan proses dari tingkat nol hingga tingkat lima, dimana tingkat nol yang berarti proses tidak lengkap hingga level lima dimana proses telah berjalan optimal. Penilaian dari COBIT 5 PAM akan mengevaluasi seberapa baik atribut proses tertentu untuk setiap tingkat proses tercapai, dan memberikan tingkat keyakinan pada hasil penilaian yang menunjukkan kemampuan keseluruhan proses manajemen. Peringkat

tersebut didasarkan oleh bukti objektif dan tervalidasi untuk setiap atribut proses. Tingkat kemampuan suatu proses ditentukan berdasarkan pencapaian atribut proses tertentu menurut ISO/IEC 15505, yaitu apakah atribut proses pada tingkat tersebut sudah tercapai dan apakah atribut proses untuk tingkat yang lebih rendah telah tercapai sepenuhnya [9].

### E. ISO/IEC 27002:2013

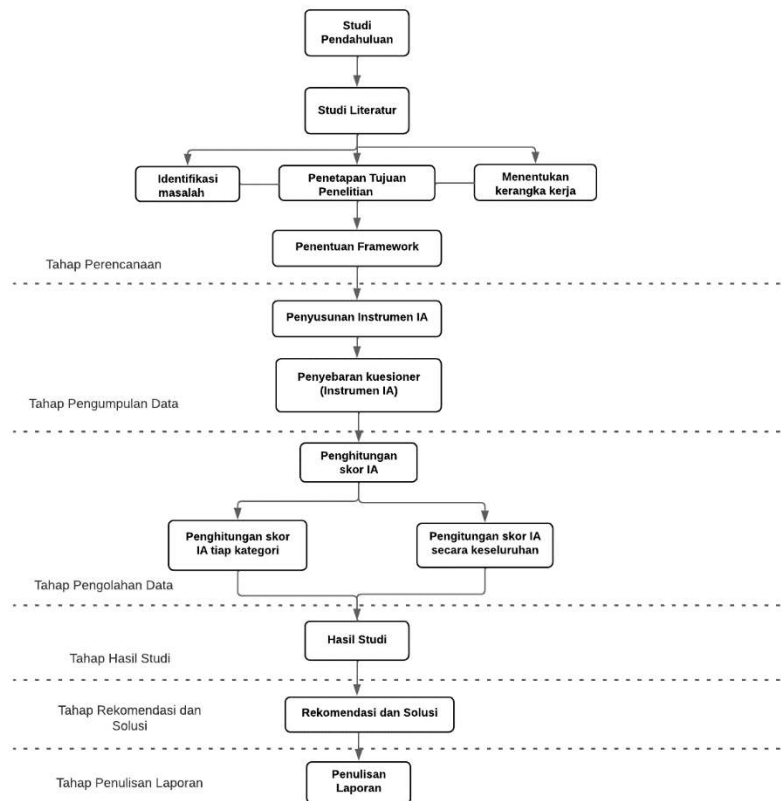
ISO (*the International Organization for Standardization*) dan IEC (*the International Electrotechnical Commission*) adalah standar internasional dalam bidang keamanan informasi yang dirancang untuk digunakan oleh organisasi sebagai rekomendasi dalam memilih kontrol proses penerapan Sistem Manajemen Keamanan Informasi (SMKI). ISO/IEC 27002 terdiri dari 14 klausul kategori utama keamanan (*main security categories*), yang menyediakan best practice untuk organisasi sebagai kontrol keamanan informasi dan peningkatan keamanan informasi yang diterima secara umum. Keamanan informasi dicapai dengan menerapkan seperangkat kontrol yang sesuai, termasuk kebijakan, proses, prosedur, struktur organisasi dan fungsi perangkat lunak dan perangkat keras. Kontrol ini perlu ditetapkan, diterapkan, dipantau, ditinjau, dan ditingkatkan, jika perlu, untuk memastikan bahwa tujuan keamanan dan bisnis spesifik organisasi terpenuhi. Adapun 14 klausul utama keamanan dari ISO/IEC 27002:2013 [10], yaitu:

1. *Information Security Policy* (Kebijakan Keamanan Informasi)
2. *Organizing Information Security* (Keamanan Informasi Organisasi)
3. *Human Resources Security* (Keamanan Sumber Daya Manusia)
4. *Asset Management* (Pengelolaan Aset)
5. *Access Control* (Kontrol Akses)
6. *Cryptography* (Kriptografi)
7. *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan)
8. *Operations Security* (Keamanan Operasional)
9. *Communication Security* (Keamanan Komunikasi)
10. *System Acquisition, Development and Maintenance* (Akuisisi, Pengembangan dan Pengelolaan Sistem)
11. *Supplier Relationships* (Hubungan dengan Supplier)
12. *Information Security Incident Management* (Pengelolaan Insiden Keamanan Informasi)



13. *Information Security Aspects of Business Continuity Management* (Keamanan Informasi dari Aspek Pengelolaan Keberlangsungan Bisnis)
14. *Compliance* (Kepatuhan)

### III. METODE



GAMBAR 2.  
METODOLOGI PENELITIAN

#### A. Tahap Perencanaan

Dalam proses perencanaan penelitian, dilakukan studi pendahuluan, yaitu dengan melakukan studi literatur terhadap penelitian-penelitian terkait yang sudah ada sebelumnya. Kegiatan ini berguna untuk menentukan rumusan masalah dan tujuan yang akan dicapai dari penelitian dan juga untuk mengetahui data yang dibutuhkan untuk mendukung proses pengumpulan data sehingga dapat menentukan framework yang tepat.

#### B. Tahap Pengumpulan Data

Dalam pengumpulan data dilakukan dengan menggunakan kuesioner. Kuesioner berisikan pertanyaan instrumen dari masing-masing faktor item pada IA yang telah dikonfirmasi dalam framework IAFEG. Instrumen ini disusun berdasarkan pendekatan *Goals Question and Metric* (GQM) untuk membantu mengukur proses implementasi IA dalam sebuah

Pada bab ini telah disusun metodologi penelitian yaitu langkah pengerjaan tugas akhir secara sistematis yang dijabarkan menggunakan *flowchart*. Metodologi penelitian ini akan menjadi acuan dalam proses pengerjaan tugas akhir.

organisasi dengan menjawab pertanyaan terkait dengan kinerja setiap praktik. Kuesioner akan dijawab dengan penilaian skala 0 hingga 5 yang nantinya akan menjadi sumber data dalam proses penelitian.

#### 1. Penyusunan Instrumen IA

Dalam pengumpulan data dilakukan dengan menggunakan kuesioner. Kuesioner berisikan pertanyaan instrumen dari masing-masing faktor item pada IA yang telah dikonfirmasi dalam framework IAFEG. Instrumen ini disusun berdasarkan pendekatan *Goals Question and Metric* (GQM) untuk membantu mengukur proses implementasi IA dalam sebuah organisasi dengan menjawab pertanyaan terkait dengan kinerja setiap praktik. Kuesioner akan dijawab dengan penilaian skala 0 hingga 5 yang nantinya akan menjadi sumber data dalam proses penelitian:

TABEL 1.  
INSTRUMEN PENGUKURAN IA

Kategori Item	Faktor Item	Pertanyaan Instrumen
Organisational Management (OM)	Leadership and Commitment	Pimpinan dewan direksi untuk implementasi IA? Komitmen direksi untuk implementasi IA?
	Policy, Legal, and Compliance	Ketersediaan kebijakan untuk memberikan arah dan dukungan manajemen untuk IA sesuai dengan business requirements?
		Ketersediaan aspek hukum untuk mengidentifikasi kewajiban hukum organisasi (undang-undang, peraturan, dan kontrak)?
		Ketersediaan yang sesuai prosedur untuk memastikan kepatuhan dengan aspek hukum yang berlaku untuk organisasi?
	Management Review and Continual Improvement	Tinjauan berkala (mengenai kesesuaian, kecukupan, dan efektivitas) dari kebijakan IA oleh manajemen senior?
		Perbaikan berkelanjutan atas kebijakan IA oleh manajemen senior?
	Holistic Approach	Perbaikan IA sebagai kombinasi dari keamanan fisik, prosedural, personel, dan keamanan teknis?
	Business Alignment	Keselaran antara implementasi IA dan kebutuhan bisnis organisasi?
	Organisational Roles, Responsibilities, and Authorities	Manajemen senior menugaskan dan mengkomunikasikan peran organisasi yang relevan dengan IA?
		Manajemen senior memberikan tanggung jawab untuk memastikan IA sesuai dengan kebijakan?
		Manajemen senior menugaskan otoritas untuk mengkonfirmasi IA sesuai dengan kebijakan?
	Awareness, Education, and Training	Kesadaran semua karyawan dalam organisasi tentang kontribusinya terhadap penerapan IA?
Pendidikan semua karyawan dalam organisasi yang relevan dengan fungsi pekerjaan?		
Pelatihan semua karyawan di organisasi yang relevan dengan fungsi pekerjaan mereka?		
Implementation Management (IM)	Risk Management	Penerapan strategi manajemen risiko dari implementasi IA?
	Security Objectives	Relevansi tujuan keamanan informasi dengan fungsi dan level?
	Operations and Management	Rencana keamanan informasi mematuhi kebijakan keamanan informasi?
		Implementasi dari keamanan informasi sesuai dengan kebijakan keamanan informasi?
	Performance Evaluation	Kontrol keamanan informasi mematuhi kebijakan keamanan informasi?
	Recovery and Continuity Management	Evaluasi kinerja (berkaitan dengan efektivitas dan pemeliharaan) dari implementasi IA?
		Pengadopsian rencana pemulihan bencana dari implementasi IA?
Infrastructure Development	Pengadopsian rencana kelangsungan bisnis jika terjadi kegagalan besar?	
	Teknologi dan infrastruktur yang dibutuhkan relevan dengan implementasi IA?	
Social Management (SM)	Cultural Issues	Teknologi dan infrastruktur yang dibutuhkan relevan dengan implementasi IA?
	Digital Divide	Pertimbangan masalah budaya dalam organisasi selama implementasi IA?
	Trust and Privacy	Pertimbangan masalah literasi digital dalam organisasi selama implementasi IA?
		Terjalinnnya kepercayaan antara pemerintah dan warga?
	Perlindungan mengenai privasi informasi?	
	Organisational Structures	Pembentukan divisi untuk mengontrol penanganan masalah keamanan informasi?
Coordination	Koordinasi antara institusi terkait tugas masing-masing institusi?	

## 2. Penyebaran Kuesioner

Pada penelitian ini, penulis akan membagikan kuesioner kepada staf instansi pada bidang kerja yang berkaitan dengan keamanan informasi. Kriteria responden yang dibutuhkan untuk menjawab kuesioner ini adalah staf Disdukcapil yang berasal dari bidang pengelolaan informasi administrasi kependudukan, meliputi staf dari seksi sistem informasi administrasi kependudukan, seksi pengolahan dan penyajian data dan seksi tata kelola dan sumber daya manusia teknologi informasi dan komunikasi, yang memiliki pengalaman bekerja diatas 6 tahun dan memahami pengetahuan dasar mengenai keamanan informasi dan *information assurance*. Pengukuran dilakukan dengan menyebarkan

kuesioner secara online yang dapat diakses dengan mudah oleh para staf instansi.

## C. Tahap Pengolahan Data

### 1. Penghitungan Skor IA

Dalam pengolahan data dilakukan penghitungan skor dari tiap kategori IA dan skor IA secara keseluruhan. Pengolahan data dalam penelitian ini menggunakan metric untuk menjabarkan respon dari pertanyaan instrumen. Metric diadaptasi dari Process Assessment Model dari COBIT 5 yang didasarkan pada ISO/IEC 15504-2:2003 yang menjabarkan skor pengukuran IA berdasarkan skala penilaian enam tingkat. Untuk memastikan penilaian yang lebih jelas akan dijabarkan sebagai berikut:

- a. Level 0 - Non-Existent Process: Proses tidak diadopsi atau tidak diimplementasikan. Hal ini dikategorikan "Area kritis dan diperlukan tindakan yang serius". Skor nya adalah 0%
- b. Level 1 - Initial Process: Proses tidak diimplementasikan dengan baik, dan/atau gagal mencapai tujuannya. Akibatnya, proses nya informal dan tidak terkoordinasi. Hal ini dikategorikan "Area di bawah rata-rata dan diperlukan tindakan yang besar dan mendesak". Skor nya adalah 20%
- c. Level 2 - Defined Process: Proses diimplementasikan, didokumentasikan, dan dikomunikasikan secara sederhana; mencapai tujuan proses. Hal ini dikategorikan "Area sedang dan diperlukan perbaikan sedang". Skor nya adalah 40%
- d. Level 3 - Managed Process: Proses yang ditentukan telah diimplementasikan dengan cara yang terkelola (direncanakan, dipantau, dan disesuaikan). Hal ini dikategorikan "Area diatas rata-rata dan peningkatan kecil diperlukan". Skor nya adalah 60%
- e. Level 4 - Established Process: Proses yang terkelola telah diimplementasikan menggunakan definisi proses yang mampu mencapai hasil prosesnya dan produk kerja diukur, dikendalikan, dan dipelihara dengan tepat. Hal ini dikategorikan "Area solid dan perbaikan kecil mungkin diperlukan". Skor nya adalah 80%
- f. Level 5 - Optimised Process: Proses yang ditetapkan telah ditingkatkan terus-menerus dan best practice diikuti untuk memenuhi tujuan bisnis. Hal ini dikategorikan "Area tepat/sepurna tidak diperlukan perbaikan apapun". Skor nya adalah 100%

Setelah penjabaran skala penilaian enam tingkat dilakukan, tahapan selanjutnya menentukan skor faktor (skor kategori sebelum pembobotan) dan skor IA keseluruhan yang kemudian akan menghasilkan nilai pengukuran implementasi IA pada instansi.

## 2. Penghitungan Skor IA Tiap Kategori

- a. Organisational Management (OM) weight =  $(F1 \text{ score} + \dots + F7 \text{ score}) / \text{No. of factor}(7)$
- b. Implementation Management (IM) weight =  $(F1 \text{ score} + \dots + F6 \text{ score}) / \text{No. of factor}(6)$
- c. Social Management (SM) weight =  $(F1 \text{ score} + F2 \text{ score} + F5 \text{ score}) / \text{No. of factor}(5)$

Proses penilaian akhir akan dibagi menjadi enam skala yang ditunjukkan sebagai berikut:

- a. Skor dari 0% ke 12% : Level 0 status - Perbaikan serius dan kritis diperlukan
- b. Skor dari 12,50% ke 37% : Level 1 status - Perbaikan besar dan mendesak dibutuhkan
- c. Skor dari 37,50% ke 50% : Level 2 status - Perbaikan sedang diperlukan
- d. Skor dari 50,50% ke 62% : Level 3 status - Perbaikan kecil diperlukan
- e. Skor dari 62,50% ke 87% : Level 4 status - Perbaikan kecil mungkin diperlukan
- f. Skor dari 87,50% ke 100% : Level 5 status - Tidak dibutuhkan tindakan

## b. Penghitungan Skor IA Secara Keseluruhan

Setelah menentukan skor tiga kategori (OM, IM, SM) selanjutnya mengidentifikasi bobot akhir penilaian IA yang dilakukan dengan tahapan berikut:

1. Dengan membagi seluruh No. of Factor dengan 100.  
 $\text{Bobot faktor} = 100 / (\text{No. of Faktor tiap kategori: } 7+6+5) = 100/18 = 5,56$
2. Menghitung bobot total tiap kategori:  
 $\text{Bobot total tiap kategori} = \text{Bobot faktor}(5,56) * \text{No. of Factor tiap kategori}$   
 $\text{Bobot total kategori OM} = 5,56 * \text{No. of factor}(7) = 38,9\%$   
 $\text{Bobot total kategori IM} = 5,56 * \text{No. of factor}(6) = 33,3\%$   
 $\text{Bobot total kategori SM} = 5,56 * \text{No. of factor}(5) = 27,8\%$
3. Setelah itu, bobot masing-masing tiap kategori dalam institusi dapat dihitung. Tahap ini dilakukan dengan mengalikan bobot kategori penuh dengan skor akhir kategori tersebut dan dibagi dengan angka 100.  
 Contoh:  $\text{Bobot kategori OM di institusi} = \text{Bobot kategori OM } (38,9) * \text{skor akhir kategori OM di institusi} / 100$
4. Lalu dapat disimpulkan bahwa nilai akhir IA pada institusi adalah bobot nilai tiap kategori pada institusi.  
 $\text{Nilai akhir IA pada institusi} = \text{Bobot OM institusi} + \text{Bobot IM institusi} + \text{Bobot SM institusi}$

## IV. HASIL DAN PEMBAHASAN

Pengumpulan data dan informasi pada penelitian ini berdasarkan hasil dari jawaban kuesioner yang telah dibagikan pada responden yaitu para staf dari bidang pengelolaan informasi administrasi kependudukan di Disdukcapil. Ada 8 responden yang bersedia untuk mengisi kuesioner, yang masing-masing berasal dari seksi sistem informasi administrasi kependudukan, seksi pengolahan dan penyajian data dan seksi tata kelola dan sumber daya manusia teknologi informasi dan komunikasi. Tabel dibawah ini merupakan hasil dari

pengumpulan data yang dikategorikan berdasarkan level status faktor.

TABEL 2.  
HASIL PENGUMPULAN DATA BERDASARKAN STATUS FAKTOR

Kategori	Nama Faktor	Status Fakor
SM	Trust and privacy	Level 4 (80%)
SM	Coordination	
OM	Leadership and Commitment	Between Level 3 (60%) and Level 4 (80%)
OM	Policy, Legal, and Compliance	
OM	Management review and continual improvement	
OM	Organisational roles, responsibilities, and authorities	
OM	Awareness, education, and training	
IM	Operations and management	
IM	Recovery and Continuity Management	
OM	Holistic Approach	Level 3 (60%)
OM	Business Alignment	
IM	Risk Management	
IM	Security Objective	
IM	Performance evaluation	
IM	Infrastructure Development	
SM	Cultural Issues	
SM	Digital Divide	
SM	Organisational Structures	

**Kategori Level 4 status (Skor dari 62,50% ke 87%)**

1. *Organisational Management* **65,71%**
2. *Implementation Management* **62,77%**
3. *Social Management* **68%**

**Hasil dari keseluruhan skor IA adalah sebagai berikut:**

Bobot kategori OM di institusi =  $38,9\% \times 65,71\% / 100 = 25,56\%$

Bobot kategori IM di institusi =  $33,3\% \times 62,77\% / 100 = 20,90\%$

Bobot kategori SM di institusi =  $27,8\% \times 68\% / 100 = 18,90\%$

Dengan menjumlahkan seluruh bobot kategori, total keseluruhan skor IA yang didapatkan adalah **65,36%** pada status level 4.

A. Rekomendasi Kontrol Berdasarkan ISO/IEC 27002

Berdasarkan hasil pengukuran implementasi IA, dapat dilihat bahwa skor kategori IA dan skor keseluruhan IA berada pada level 4 yang berarti “perbaikan kecil mungkin diperlukan”. Pada kasus seperti ini, pengembangan rekomendasi kontrol diperlukan untuk area yang membutuhkan perbaikan. ISO/IEC 27002 merupakan standar dalam bidang keamanan informasi yang menerapkan seperangkat kontrol yang sesuai, termasuk kebijakan, proses, prosedur, struktur organisasi dan fungsi perangkat lunak dan perangkat keras, agar memastikan tujuan keamanan dalam instansi dapat mencapai prosesnya. Rekomendasi pemilihan



kontrol untuk faktor-faktor IA dapat dilihat pada tabel berikut.

TABEL 3.  
REKOMENDASI KONTROL UNTUK KATEGORI OM

No	Faktor Item	ISO 27002	Kontrol
1	Leadership and Commitment	Sub Kontrol 7.2.1 Management responsibilities	Manajemen mewajibkan seluruh karyawan dan kontraktor untuk mengimplementasikan keamanan informasi yang relevan terhadap kebijakan dan prosedur yang telah dipatenkan oleh organisasi.
2	Policy, Legal, and Compliance	Sub Kontrol 5.1.1 Policies for information security	Serangkaian kebijakan keamanan informasi wajib ditetapkan, diakui oleh manajemen, diterbitkan dan disampaikan ke karyawan dan pihak eksternal yang relevan.
3	Management review and continual improvement	Sub Kontrol 5.1.2 Review of the policies for information security	Kebijakan keamanan informasi harus ditinjau pada interval yang direncanakan atau ketika ada perubahan signifikan untuk memastikan relevansi, kecukupan dan efektivitasnya.
4	Holistic Approach	Sub Kontrol 11.2.1 Equipment siting and protection	Aset yang ada wajib diposisikan dan dipelihara untuk meminimalisir risiko dari adanya akses ilegal.
5	Business Alignment	Sub Kontrol 8.2.1 Classification of information	Informasi wajib diklasifikasikan menurut kapasitas hukum, nilai, materialitas, dan kemungkinan atau perubahan yang ilegal.
6	Organisational roles, responsibilities, and authorities	Sub Kontrol 6.1.1 Information security roles and responsibilities	Seluruh responsibilitas keamanan informasi harus ditetapkan dan didistribusikan.
7	Awareness, education, and training	Sub Kontrol 7.2.2 Information security awareness, education and training	Seluruh karyawan organisasi dan, jika berlaku, kontraktor wajib memperoleh pelatihan untuk kesadaran terkait keamanan informasi dan pelatihan yang sesuai serta pembaruan rutin kebijakan dan prosedur organisasi yang relevan dengan fungsi mereka.

TABEL 4.  
REKOMENDASI KONTROL UNTUK KATEGORI IM

No	Faktor Item	ISO 27002	Kontrol
1	Risk Management	Sub Bab 15.1.3 Information and communication technology supply chain	Kontrak pemasok wajib meliputi ketentuan risiko keamanan informasi yang mencakup layanan teknologi informasi dan komunikasi serta rantai pasokan produk.
2	Security Objective	Sub Kontrol 17.1.3 Verify, review and evaluate information security continuity	Organisasi wajib secara berkala meninjau kontrol kesinambungan keamanan informasi yang sudah ditentukan dan diterapkan agar tetap efektif dalam keadaan yang merugikan.
3	Operations and management	Sub Kontrol 14.1.1 Information security requirements analysis and specification	Persyaratan keamanan informasi wajib disertakan persyaratan untuk sistem informasi yang terbaru atau perluasan dari sistem informasi yang telah ada.
4	Performance evaluation	Sub Kontrol 15.2.1 Monitoring and review of supplier services	Organisasi wajib secara terus-menerus meninjau, dan mengaudit penyampaian layanan pemasok.
5	Recovery and Continuity Management	Sub Kontrol 17.1.1 Planning information security continuity	Organisasi harus meninjau persyaratan keamanan informasi mereka dan kontrol keamanan informasi saat ini dalam situasi yang merugikan, misalnya selama krisis atau bencana.

6	Infrastructures Development	Sub Kontrol 13.1.1 Network controls	Jaringan wajib dikelola dan terkendali dengan baik dalam melindungi informasi sistem dan aplikasi.
---	-----------------------------	-------------------------------------	--

TABEL 5.  
REKOMENDASI KONTROL UNTUK KATEGORI SM

No	Faktor Item	ISO 27002	Kontrol
1	Cultural Issues	Sub Kontrol 7.2.3 Disciplinary process	Metode pendisiplinan formal dikomunikasikan dan wajib dilakukan tindakan lebih lanjut pada karyawan yang berbuat pelanggaran dalam hal keamanan informasi
2	Digital Divide	Sub Kontrol 7.2.2 Information security awareness, education and training	Karyawan dan kontraktor (jika terdapat kontraktor), wajib memperoleh penataran yang sesuai serta pembaruan rutin terkait kebijakan dan prosedur organisasi yang setara dengan bidang kerjanya.
3	Trust and Privacy	Sub Kontrol 14.2.6 Secure development environment	Organisasi harus membangun dan mengamankan zona pengembangan yang terjaga dalam pengembangan sistem dan cara integrasi terhadap semua siklus hidup pengembangan sistem.
4	Organisational Structures	Sub Kontrol 7.1.2 Implementing information security continuity	Organisasi wajib menentukan, mencadangkan, mempraktikkan, dan memelihara proses, prosedur, dan kontrol untuk menyediakan tingkat kontinuitas yang dibutuhkan dalam keamanan informasi saat terjadi keadaan yang merugikan.
5	Coordination	Sub Kontrol 6.1.5 Information security in project management	Terlepas dari jenis proyek, manajemen proyek harus menangani keamanan informasi.

#### B. Feedback Analisis

Analisis umpan balik (*feedback*) diperlukan untuk memvalidasi penelitian ini. Hasil *feedback* analisis didapatkan dengan melakukan *interview* terhadap 4 orang *expert judgement* yang berasal dari kepala sub bagian umum dan kepegawaian, kepala

seksi sistem informasi administrasi kependudukan, kepala seksi pengolahan dan penyajian data dan kepala seksi tata kelola dan sumber daya manusia teknologi informasi dan komunikasi.. *Interview* juga dilakukan dengan menjawab beberapa pertanyaan tambahan untuk mempermudah penilaian.

TABEL 7.  
FEEDBACK ANALISIS

Pertanyaan	Respon
Q1. Organisational Management, 65,71%	Sangat setuju
Q4. Skor keseluruhan IA 65,36%	
Q2. Implementation Management, 62,77%	Setuju
Q3. Social Management, 68%	

Skor kategori OM instansi yang didapatkan adalah 65,71% dan *experts* sepenuhnya setuju dengan hasilnya. *Experts* juga menambahkan bahwa setiap divisi pada instansi memiliki seorang kepala departemen yang berperan serta dalam melaksanakan tugas sesuai dengan bidang pekerjaannya. Instansi juga telah memiliki kebijakan hukum untuk melindungi informasi dan aset di dalam nya. Selain itu,

tinjauan berkala dan perbaikan dilakukan sesuai dengan kepentingan instansi.

Skor kategori IM instansi yang didapatkan adalah 62,77%, *experts* sepakat bahwa pengukuran ini mencerminkan kondisi nyata dari adopsi IA. Instansi juga telah menerapkan manajemen risiko dengan lumayan baik dan telah perencanaan pemanfaatan aset dengan benar untuk memenuhi kebutuhan instansi tersebut. Tujuan keamanan informasi juga cukup relevan dengan

fungsi dan kebutuhan keamanan informasi pada instansi. Rencana, implementasi dan kontrol dari keamanan informasi telah diterapkan dengan baik sesuai dengan kebijakan yang berlaku. Selain itu, peninjauan dan evaluasi berkala terhadap kinerja pegawai juga dilakukan sesuai dengan proses. Instansi juga telah mengadopsi pencadangan dan pemulihan jika terjadi insiden yang tak terduga, baik insiden yang disebabkan oleh manusia maupun bencana alam. Infrastruktur teknologi informasi dalam instansi sudah cukup baik untuk mendukung proses implementasi IA.

Skor kategori SM di instansi yang didapatkan adalah 68%, *experts* setuju dengan hasilnya. Kebijakan mengenai masalah budaya, perilaku individu dan kesenjangan terhadap teknologi informasi telah diterapkan, namun masih membutuhkan peningkatan dalam implementasinya. Selain itu, kepercayaan masyarakat terhadap instansi pelayanan publik ini berjalan dengan cukup baik walaupun belum dikatakan sempurna. Instansi tersebut juga telah mempunyai divisi untuk menangani permasalahan keamanan informasi sehingga masing-masing tugas tiap pegawai terkoordinasi dengan baik.

Terakhir, *experts* sangat setuju dengan hasil pengukuran keseluruhan dari implementasi IA yang berada pada status level 4 dengan skor 65,36%, dimana instansi sudah mengimplementasikan IA dengan baik dan terkelola serta dapat mencapai hasil proses, walau masih ada perbaikan kecil yang perlu ditingkatkan.

## V. KESIMPULAN

Dari penelitian yang telah dilakukan, terkait pengukuran implementasi *information assurance* pada Disdukcapil, penulis dapat menarik kesimpulan bahwa implementasi IA pada Disdukcapil telah mencapai level yang cukup baik, walaupun belum semua faktor mencapai skor yang sempurna. Skor IA pada kategori *organisational management* adalah 65,71%, kategori *implementation management* adalah 62,77%, dan kategori *social management* adalah 68%, artinya keseluruhan kategori IA telah mencapai “*Established Process*” atau proses yang telah ditetapkan. Namun, belum ada faktor IA yang nilainya telah mencapai level yang tidak membutuhkan perbaikan. Rata-rata nilai tiap faktor IA pada Disdukcapil berada pada rentang 60% hingga 80% yang artinya pada kasus ini, proses telah diimplementasikan dengan cara yang terkelola, menggunakan definisi proses dan mampu mencapai hasil prosesnya, namun masih memerlukan peningkatan kecil pada area yang memiliki kekurangan, sehingga perbaikan kecil pada area tertentu mungkin diperlukan. Nilai total keseluruhan

skor IA juga mendapatkan hasil status “*Established Process*”, sehingga implementasi dari keseluruhan faktor-faktor IA pada Disdukcapil masih memerlukan perbaikan kecil.

## REFERENSI

- [1] Dhevina Ihsanira. (2018, April 4). E-Government: Inovasi dalam Strategi Komunikasi. Retrieved from SetNeg: [https://www.setneg.go.id/baca/index/e\\_government\\_inovasi\\_dalam\\_strategi\\_komunikasi](https://www.setneg.go.id/baca/index/e_government_inovasi_dalam_strategi_komunikasi)
- [2] Utomo, R G. (2021). Studi Kasus Pengukuran Implementasi Information Assurance untuk e-Government menggunakan Metode Goal Question Metric. Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK. 15(1).
- [3] Peraturan Pemerintah no.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. (Tambahan Lembar Negara RI Nomor 6400).
- [4] Boyce Joseph. Jennings W. (2002). Information Assurance: Managing Organizational IT Security Risk Woburn: British Library.
- [5] Dinas Kependudukan dan Pencacatan Sipil. (2020). Survey Kepuasan Masyarakat
- [6] Kumar Arun. (2018). Information Assurance and Security. Deepublish: jeyalakshmi publication. Retrieved from academia.edu: [https://www.academia.edu/42194126/Chapter\\_1\\_Information\\_Assurance\\_and\\_Security](https://www.academia.edu/42194126/Chapter_1_Information_Assurance_and_Security)
- [7] Utomo, R.G., (2020). Information assurance framework for eGovernment in Indonesia (Doctoral dissertation, University of Southampton).
- [8] Overview of the GQM (Goal, Question, Metric). (2020). Retrieved from IntraHealth International: <https://www.mhero.org/sites/mhero/files/gqm.pdf>
- [9] “Prosess Model Assessment (PAM): Menggunakan COBIT 5” ISACA. (2013) Available: <https://pdfcoffee.com/5-cobit5-process-assessment-modelenid-pdf-free.html>
- [10] “ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls.” Iso.org. (October 10, 2013). Available: <https://www.iso.org/standard/54533.html>
- [11] Peraturan Presiden no.95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik