CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 6, No. 1, Mei 2023, hlm. 12 of 17

ANALISA KEAMANAN INFORMASI PADA *E-GOVERNMENT* MENGGUNAKAN *COBIT 5 FRAMEWORK*

Fanny Novianto

Program Studi Informatika
Fakultas Sains dan Teknologi, UIN Sunan Kalijaga
Email : fannynovianto@yahoo.co.id

Abstrak

Pemerintah saat ini mengimplementasikan sistem *e-government (e-gov)* di Indonesia. *E-gov* adalah sistem pemerintahan yang berbasis teknologi informasi. Pada prinsipnya inovasi *e-gov* ini adalah untuk meningkatkan kualitas proses pelayanan dari lembaga pemerintah kepada masyarakat melalui pelayanan publik secara online. Dalam implementasi *e-gov*, keamanan informasi menjadi hal terpenting dalam penggunaan teknologi informasi yang diterapkan. Keamanan informasi dan data pemerintah, khususnya informasi yang dapat diakses dan ditampikan melalui sebuah web aplikasi ternyata sangat rawan untuk diretas. Divisi Pemasyarakatan Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia Daerah Istimewa Yogyakarta pada saat ini menerapkan e-*gov* dalam proses bisnis internal dan layanan publik sejalan berupa Sistem Informasi Pemasyarakatan Yogyakarta (sipasta). Data dan informasi dalam sipasta beberapa bersifat terbatas dalam hal akses dan rahasia. Pengguna sipasta adalah masyarakat dan Aparatur Sipil Negara (ASN) Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia Daerah Istimewa Yogyakarta. Hal ini berdampak berdampak pada banyaknya pertukaran informasi dimana informasi tersebut ada yang bersifat penting, rahasia dan terbatas hak aksesnya hanya ditujukan bagi pengguna tertentu. Metode penelitian yang digunakan menggunakan COBIT5 framework dengan fokus domain APO13 dan DSS05. Hasil analisa Process Capability Model berada pada level 2 atau managed process. Hal ini dikarenakan capaian rating pada performance management dan work product management domain APO13 dan DSS05 adalah Largely Achieved. Untuk dapat dinilai pada level berikutnya proses tersebut harus mencapai kategori Fully achieved (F).

Kata kunci: *keamanan informasi, e-government, COBIT5*

INFORMATION SECURITY ANALYSIS OF E-GOVERNMENT USING COBIT5 FRAMEWORK

Abstract

The government is currently implementing the e-government (e-gov) system in Indonesia. E-gov is a government system based on information technology. In principle, this e-gov innovation is to improve the quality of the service process from government agencies to the public through online public services. In the implementation of e-gov, information security is the most important thing in the use of applied information technology. Government information and data security, especially information that can be accessed and displayed through a web application, is prone to being hacked. The Correctional Division of the Regional Office of the Ministry of Law and Human Rights of the Special Region of Yogyakarta is currently implementing e-gov in internal business processes and public services in line with Sistem Informasi Pemasyarakatan Yogyakarta (Sipasta). Some data and information in private sector are limited in terms of access and confidentiality. Private users are the public and the Aparatur Sipil Negara (ASN) Regional Office of the Ministry of Law and Human Rights of the Special Region of Yogyakarta. This has an impact on the number of exchanges of information where the information is important, confidential and has limited access rights that are only intended for certain users. The research method used is the COBIT5 framework with a focus on the APO13 and DSS05 domains. The results of the Process Capability Model analysis are at level 2 or managed process. This is because the rating achievements in the performance management and work product management domains of APO13 and DSS05 are Largely Achieved. To be assessed at the next level the process must reach the Fully achieved (F) category.

Keywords: *information security, e-government, COBIT5*

1. PENDAHULUAN

Indonesia dewasa ini selalu meningkatkan kualitasnya sebagai sebuah bangsa. Mulai dari pembangunan infrastruktur hingga peningkatan kekuatan ekonomi. Tak mau ketinggalan, sektor pemerintahan juga ikut berinovasi.

Pemerintah kini sedang mengiemplementasikan sistem *e-government (e-gov)* di Indonesia. *E-gov* adalah sistem pemerintahan yang berbasis teknologi informasi. Pada prinsipnya inovasi *e-gov* ini adalah untuk meningkatkan kualitas proses pelayanan dari lembaga pemerintah kepada masyarakat melalui pelayanan publik secara online(N, 2018).

United Nations (UN) e-Government Survey 2020 menempatkan Indonesia pada peringkat 88 atas pengembangan dan pelaksanaan *e-gov*. Hasil di tahun 2020 yang dirilis pada bulan Juli, menunjukkan kenaikan 19 peringkat dibandingkan tahun 2018 yang berada di urutan 107 dan urutan 116 di tahun 2016 (Sari, 2020).

Dalam Instruksi Presiden Nomor 3 Tahun 2003 terdapat enam strategi yang harus dilakukan dalam pengembangan *e-gov*, strategi pertama mengembangkan sistem pelayanan yang handal dan terpercaya, serta terjangkau oleh masyarakat luas. Kedua menata sistem dan proses kerja pemerintah dan pemerintah daerah otonom secara holistik. Strategi ketiga yaitu memanfaatkan teknologi informasi dan komunikasi secara optimal. Strategi keempat adalah meningkatkan peran serta dunia usaha dan mengembangkan industri telekomunikasi dan teknologi informasi dalam negeri. Strategi kelima adalah meningkatkan kapasitas sumber daya manusia disertai dengan meningkatkan elektronifikasi masyarakat, dan strategi keenam adalah melaksanakan pengembangan secara sistematis melalui tahapan yang realistik dan terukur (Presiden RI, 2003).

Dalam implementasi *e-gov*, keamanan informasi menjadi hal terpenting dalam penggunaan teknologi informasi yang diterapkan. Keamanan informasi dan data pemerintah, khususnya informasi yang dapat diakses dan ditampikan melalui sebuah web aplikasi ternyata sangat rawan untuk diretas. Berdasarkan data dari Badan Siber dan Sandi Negara, terdeteksi lebih dari 360 juta serangan siber pada periode bulan Januari hingga Oktober tahun 2020. serangan terbanyak adalah *Phising*, *DDOS*, dan *Ransomware(Anon., n.d.).(-, Riadi and Ananda, 2019)*

Divisi Pemasyarakatan Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia Daerah Istimewa Yogyakarta pada saat ini menerapkan e-*gov* dalam proses bisnis internal dan layanan publik sejalan berupa Sistem Informasi Pemasyarakatan Yogyakarta (sipasta). Hal ini sejalan dengan program Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia dalam mengembangkan *e-gov* yaitu implementasi revolusi digital pelayanan publik. Penerapan *e-gov* diharapkan mampu memberikan pelayanan yang efektif serta efisien terhadap masyarakat.

Sipasta merupakan inovasi pelayanan publik berbasis teknologi informasi yang dibangun oleh sumber daya manusia yang dimiliki oleh Divisi Pemasyarakatan Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia Daerah Istimewa Yogyakarta dalam rangka pelayanan perizinan online, monitoring pelaksanaan bimbingan terhadap klien pemasyarakatan, dan berbagai informasi tentang pemasyarakatan.

Data dan informasi dalam sipasta beberapa bersifat terbatas dalam hal akses dan rahasia. Pengguna sipasta adalah masyarakat dan Aparatur Sipil Negara (ASN) Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia Daerah Istimewa Yogyakarta. Hal ini berdampak berdampak pada banyaknya pertukaran informasi dimana informasi tersebut ada yang bersifat penting, rahasia dan terbatas hak aksesnya hanya ditujukan bagi pengguna tertentu.

Dengan pemanfaatan teknologi informasi dan semakin banyaknya informasi yang disajikan oleh pemerintah sebagai bagian dari pelayanan publik semakin besar pula kerentanan terhadap keamanan dan kerahasiaan sistem informasi itu sendiri(Wijaya, 2019).

Sebuah organisasi tidak hanya fokus dalam pengembangan tata kelola teknologi informasi, akan tetapi juga harus mempertahankan dan meningkatkan kualitas keamanan informasi organisasi tersebut. Keamanan informasi meliputi *confidentiality, integrity dan availability(Aritonang, Udayanti and Iksan, 2018).*

Ruang lingkup dalam penelitian ini adalah dengan melakukan evaluasi tingkat kematangan keamanan informasi sipasta di lingkungan Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia Daerah Istimewa Yogyakarta untuk menjaga keberlanjutan dari proses bisnis yang ada. Metode penelitian yang digunakan adalah dengan melakukan analisa terhadap domain APO13 (mengelola keamanan) dan DSS05 (mengelola layanan keamanan) pada COBIT5 *framework.*

2. TINJAUAN PUSTAKA

2.1 *e-government (e-gov)*

E-gov adalah penggunaan information and communication technology (ICT) untuk meningkatkan hubungan antara pemerintah dengan pihak-pihak lain. Penggunaan ICT ini kemudian menghasilkan hubungan bentuk baru, seperti G2C (government to citizen), G2B (government to business) dan G2G (inter agency relationship)(Choiri, 2020).

Penerapan *e-gov* merupakan bentuk dari implementasi penggunaan teknologi informasi bagi pelayanan pemerintah kepada publik yaitu bagaimana pemerintah memberikan informasi kepada pemangku kepentingan (*stakeholder*) melalui sebuah portal web. Alasan utama mengimplementasikan e-government(Indrayani, 2020) :

a. *e-gov* meningkatkan efisiensi;
b. *e-gov* memperbaiki kualitas pelayanan;
c. *e-gov* membantu mencapai keluaran kebijakan yang lebih baik;
d. *e-gov* berkontribusi dalam mencapai tujuan ekonomi;
e. *e-gov* dapat menjadi kontributor utama dalam pelaksanaan reformasi;
f. *e-gov* membangun kepercayaan antara pemerintah dan warga negara.

2.2 Keamanan Informasi

Informasi merupakan aset yang sangat berharga bagi sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha. Oleh karena itu maka perlindungan terhadap informasi (keamanan informasi) merupakan hal yang mutlak harus diperhatikan secara sungguh-sungguh oleh segenap jajaran pemilik, manajemen, dan karyawan organisasi yang bersangkutan. Keamanan informasi yang dimaksud menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman terhadapnya sehingga dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup organisasi.

Prinsip Keamanan adalah sebagai berikut (NKD, 2021) :

a. Kerahasiaan : memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya;
b. Integritas : melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif;
c. Ketersediaan : memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

Gambar 1. Prinsip keamanan informasi

2.3 *COBIT5 framework*

Control Objective for Information and Related Technology (COBIT) 5 adalah kerangka panduan tata kelola TI dan atau bisa juga disebut sebagai *toolset* pendukung yang bisa digunakan untuk menjembatani gap antara kebutuhan dan bagaimana teknis pelaksanaan pemenuhan kebutuhan tersebut dalam suatu organisasi. COBIT memungkinkan mengembangan kebijakan yang jelas dan sangat baik digunakan untuk IT kontrol seluruh organisasi, membantu meningkatkan kualitas dan nilai serta menyederhanakan pelaksanaan alur proses sebuah organisasi dari sisi penerapan IT(Anon., 2023b)

COBIT 5 mendorong setiap perusahaan untuk menyesuaikan konten COBIT dengan prioritas dan keadaan perusahaan sendiri. Namun, di antara proses yang direkomendasikan COBIT 5 memiliki 3 hal yang sangat sesuai dengan sistem keamanan perusahaan dan terdapat metrik yang disarankan, yaitu :

1. Sistem mempertimbangkan dan secara efektif menangani persyaratan keamanan informasi perusahaan. Ini tampak menyeluruh, dan langkah-langkah yang disarankan mencakup jumlah peran keamanan yang telah didefinisikan secara jelas dan jumlah insiden terkait dengan keamanan. Sebagian besar perusahaan ingin menambahkan tindakan lain ke dalam daftar sesuai dengan situasi mereka sendiri.
2. Rencana keamanan yang telah ditetapkan, diterima dan dikomunikasikan ke seluruh perusahaan. Disini COBIT 5 melihat tingkat kepuasan pemangku kepentingan dengan *security plan*, jumlah solusi keamanan yang menyimpang dari rencana yang disepakati dan jumlah solusi keamanan yang menyimpang dari infrastruktur keamanan perusahaan. Infrastruktur dengan jelas mengkompromikan poin risiko dengan 2 cara: dengan membuat celah keamanan dan memperpanjang waktu untuk memperbaiki masalah keamanan atau kepatuhan.
3. Solusi keamanan informasi diterapkan di seluruh perusahaan. Disini metrik COBIT 5 melihat jumlah layanan dan solusi yang sesuai dengan rencana keamanan bersamaan dengan insiden keamanan yang disebabkan oleh ketidakpatuhan terhadap *security plan*. Ini semua adalah metrik yang baik untuk dilacak dan memberikan contoh ilustrasi yang berguna.

COBIT 5 didasari oleh 5 prinsip kunci dalam menjalankan governance dan management suatu IT enterprise. Kelima prinsip tersebut yaitu(Anon., 2023a):

1. *Meeting stakeholder needs*
   COBIT 5 terdiri atas proses-proses dan enabler untuk mendukung penciptaan nilai bisnis melalui penerapan IT. Sebuah perusahaan dapat menyesuaikan COBIT 5 dengan konteks perusahaan tersebut .
2. *Covering the enterprise end-to-end*

COBIT 5 mengintegrasikan pengelolaan IT perusahaan terhadap tatakelola perusahaan. Hal ini dimungkinkan karena :

a. COBIT 5 mencakup seluruh fungsi dan proses yang ada di perusahaan.COBIT 5 tidak hanya fokus pada fungsi IT, tapi menjadi teknologi dan informasi tersebut sebagai aset yang berhubungan dengan aset-aset lain yang dikelola semua orang di dalam sebuah perusahaan.
b. COBIT 5 mempertimbangkan seluruh enabler dari governance dan management terkait IT dalam sudut pandang perusahaan dan end-to-end. Artinya COBIT 5 mempertimbangkan seluruh entitas di perusahaan sebagai bagian yang saling mempengaruhi.

3. *Applying a single, integrated framework*
   COBIT 5 selaras dengan standar-standar terkait yang biasanya memberi panduan untuk sebagian dari aktivitas IT. COBIT 5 adalah framework yang membahas high level terkait governance dan management dari IT perusahaan. COBIT 5 menyediakan panduan high level dan panduan detailnya disediakan oleh standar-standar terkait lainnya.
4. *Enabling a holistic approach*
   Governance dan management IT perusahaan yang efektif dan efisien membutuhkan pendekatan yang bersifat menyeluruh, yaitu mempertimbangkan komponen yang saling berinteraksi.COBIT 5 mendefiniskan sekumpulan enabler untuk mendukung implementasi governance dan management sistem IT perusahaan secara komprehensif.
5. *Separating governance from management*
   COBIT 5 memberikan pemisahan yang jelas antara management dan governance. Kedua hal ini meliputi aktivitas yang berbeda,membutuhkan struktur organisasi yang berbeda dan melayani tujuan yang berbeda.

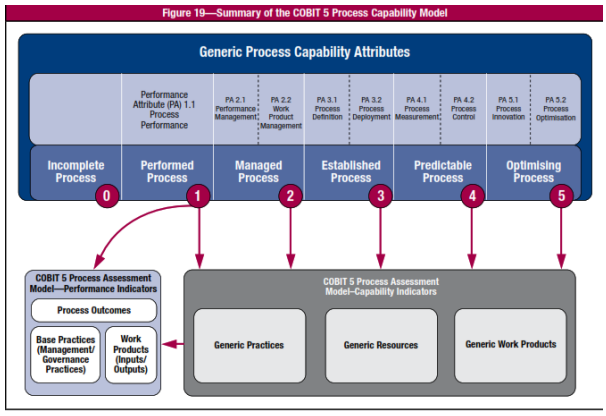
2.4 Domain COBIT 5

Domain dalam COBIT 5 yang digunakan dalam penelitian ini adalah(Anon., 2012, p.5) :

1. APO13 : *Manage Security*
   Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. Tujuan proses ini adalah menjaga dampak dan kejadian terkait insiden keamanan infomasi.
   a. APO13.01 : *Establish and maintain an information security management system* (ISMS).
   b. APO13.02 : *Define and manage an information security risk treatment plan*.
   c. APO13.03 : *Monitor and review the ISMS.*
2. DSS05 : *Manage Security Services*
   Melindungi informasi perusahaan untuk mempertahankan tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. Membangun dan memelihara peran keamanan informasi dan hak akses serta melakukan monitoring keamanan. Tujuan proses ini adalah memperkecil dampak bisnis dari kerentanan keamanan informasi operasional dan insiden terkait.

Process Capability Model dalam COBIT 5 adalah penilaian dalam COBIT 5 didasarkan pada ISO / IEC 15504 yang menggarisbawahi keselarasan yang kuat dari kerangka kerja ini dengan praktik terbaik dan standar yang paling diterima secara umum. Enam tingkat Process Capability Model dalam COBIT 5 adalah :

1. Level 0 : Incomplete process
   Proses tidak diimplementasikan atau gagal untuk mencapai tujuan prosesnya. Pada level ini tidak ada bukti dari setiap pencapaian sistematis tujuan proses.
2. Level 1 : Performed process
   Proses diimplementasikan mencapai tujuan prosesnya.
3. Level 2 : Managed process
   Proses yang dilakukan sekarang diimplementasikan dengan cara dikelola (direncanakan, dimonitor, dan disesuaikan) dan produk kerjanya secara tepat ditetapkan, dikontrol, dan dipelihara.
4. Level 3 : Established process
   Proses yang dikelola sekarang diimplementasikan menggunakan proses definisi yang mana mampu mencapai hasil prosesnya.
5. Level 4 : Predictable process
   Proses yang didirikan sekarang beroperasi dalam batas-batas yang didefinisikan untuk mencapai hasil prosesnya.
6. Level 5 : Optimising process.
   Proses diprediksi yang terus ditingkatkan untuk memenuhi arus yang relevan dan tujuan bisnis proyek.



Gambar 2. *Process Capability Model*

Setiap atribut dinilai menggunakan skala penilaian standard yang terdefinisi dalam standard ISO/IEC 15504 (ISACA, 2012).

Tabel 1. ISO/IEC Rating

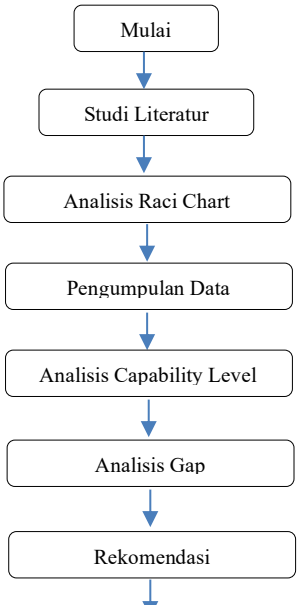
N	Not Achieved	0 - 15% achievement
P	Partially Achieved	>15%-50% achievement
L	Largely Achieved	>50%-85% achievement
F	Fully Achieved	>85%-100% achievement

Suatu proses cukup meraih kategori Largely achieved (L) atau Fully achieved (F) untuk dapat dinyatakan bahwa proses tersebut telah meraih suatu level kapabilitas tertentu, namun proses tersebut harus meraih kategori Fully achieved (F) untuk dapat melanjutkan penilaian ke level kapabilitas berikutnya, misalnya bagi suatu proses untuk meraih level kapabilitas 3, maka atribut pada level 1 dan 2 proses tersebut harus mencapai kategori Fully achieved (F), sementara level kapabilitas 3 cukup mencapai kategori Largely achieved (L) atau Fully achieved (F).

2.5 Analisis Gap

Analisis gap atau analisis kesenjangan adalah analisis kinerja yang melibatkan perbandingan kinerja aktual dengan kinerja potensial atau yang diinginkan. Analisis gap digunakan sebagai alat evaluasi bisnis yang menitikberatkan pada kesenjangan kinerja perusahaan saat ini dengan kinerja yang sudah ditargetkan sebelumnya.

3. METODOLOGI PENELITIAN



Gambar 3. Metode Penelitian

Tahapan dalam penelitian ini adalah studi literatur dengan menelaah dan mempelajari teori-teori yang mendukung penelitian ini melalui buku, jurnal dan artikel dari internet, menentukan responden yang akan mengisi kuesioner berdasarkan RACI *Chart*, pengumpulan data dilakukan melalui penyebaran kuesioner dengan pernyataan tentang tingkat kapabilitas yang harus dijawab oleh responden.

4. HASIL DAN PEMBAHASAN

Yang menjadi populasi pada penelitian ini adalah ASN pada Divisi Pemasyarakatan Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia Daerah Istimewa Yogyakarta sejumlah 30 orang. Sampel diperoleh dari populasi yang ada dengan menggunakan analisa RACI (Responsibility, Accountable, Consulted, Informed) untuk mengidentifikasi pihak-pihak yang memiliki keterkaitan dengan pengelolaan web aplikasi sipasta. Penentuan sampel pada penelitian ini menggunakan teknik purposive sampling, yaitu peneliti secara sengaja memilih langsung memilih para responden yang memenuhi persyaratan untuk dijadikan sebagai sampel, kemudian diberikan kuesioner.

Tabel 2. *RACI*

RACI Roles	*Organisation Roles*
Chief Executive Officer	Kadiv Pemasyarakatan
Head of Human Resources	Kabid Pembinaan
Head Development	Kasubbid Keamanan
Head IT Operation	Kasubbid TI

Tabel 3 memperlihatkan hasil dari kuesioner :

Tabel 3. Atribut Kapabilitas

Level	Attribute		APO13		DSS05	
			%	Rating	%	Rating
Level 0			85,59%	F	88,24%	F
Level 1	Process Performance	PA 1.1	85,29%	F	85,67%	F
Level 2	Performance Management	PA 2.1	78,39%	L	74,25%	L
	Work Product Management	PA 2.2	77,45%	L	77,63%	L
Level 3	Process Definition	PA 3.1	26,67%	P	47,62%	P
	Process Deployment	PA 3.2	23,53%	P	44,59%	P
Level 4	Process Measurement	PA 4.1	34,23%	P	33,65%	P
	Process Control	PA 4.2	35,12%	P	37,45%	P
Level 5	Process Innovation	PA 5.1	42,67%	P	41,59%	P
	Process Optimisation	PA 5.2	40,78%	P	48,63%	P

Dari tabel diatas, Process Capability Model berada pada level 2 atau managed process. Hal ini dikarenakan capaian rating pada performance management dan work product management domain APO13 dan DSS05 adalah Largely Achieved. Untuk dapat dinilai pada level berikutnya proses tersebut harus mencapai kategori Fully achieved (F).

Target level yang diharapkan oleh organisasi adalah level 3. untuk mencapainya, pada domain APO13 PA 2.1 masih ada gap 6,62% dan 7,56% untuk mencapai kondisi Fully achieved (F). Pada

domain DSS05 masih ada gap 10,76% dan 7,38% untuk mencapai kondisi Fully achieved (F).

Rekomendasi yang diberikan untuk mencapai kondisi Fully achieved (F) adalah :

a. Melakukan perbaikan pengelolaan keamanan informasi melalui Information Security Management System (ISMS)
b. Melakukan audit keamanan informasi secara berkala
c. Meningkatkan kompetensi ASN terkait keamanan informasi
d. Melakukan monitoring terhadao infrastruktur terkait pencegahan dan penanganan insiden keamanan

5. KESIMPULAN

Berdasarkan uraian dari hasil dan pembahasan, dapat diambil kesimpulan sebagai berikut :

a. Process Capability Model berada pada level 2 atau managed process. Hal ini dikarenakan capaian rating pada performance management dan work product management domain APO13 dan DSS05 adalah Largely Achieved. Untuk dapat dinilai pada level berikutnya proses tersebut harus mencapai kategori Fully achieved (F).
b. Untuk mencapai kondisi Fully achieved (F) pada level 2 atau managed process, Divisi Pemasyarakatan Kanwil Kementerian Hukum dan HAM Daerah Istimewa Yogyakarta dapat melakukan perbaikan pengelolaan keamanan informasi melalui Information Security Management System (ISMS), melaksanakan audit keamanan informasi secara berkala, meningkatkan kompetensi ASN terkait keamanan informasi dan melakukan monitoring terhadap infrastruktur terkait pencegahan dan penanganan insiden keamanan

DAFTAR PUSTAKA

-, S., RIADI, I. AND ANANDA, P., 2019. Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework. International Journal of Advanced Computer Science and Applications, [online] 10(11). https://doi.org/10.14569/IJACSA.2019.0101118.

ANON. 2012. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. COBIT® 5. [online] ISACA. Available at: <https://books.google.co.id/books?id=1iLKVlOIg9EC>.

ANON. 2023a. 5 Prinsip Yang Mendasari COBIT 5 - PROXSISGROUP. [online] Available at: <https://proxsisgroup.com/5-prinsip-yang-mendasari-cobit-5/> [Accessed 3 August 2023].

ANON. 2023B. Framework COBIT Sebagai Pengendali Perusahaan - ITGID. [online] Available at: <https://itgid.org/framework-cobit/> [Accessed 3 August 2023].

ANON. N.D. BSSN: Kedaulatan Data dan Keamanan di Ruang Siber Merupakan Bagian Integral dari Kemerdekaan Bangsa Indonesia yang Tidak Bisa Dikompromikan | bssn.go.id. Available at: <https://bssn.go.id/bssn-kedaulatan-data-dan-keamanan-di-ruang-siber-merupakan-bagian-integral-dari-kemerdekaan-bangsa-indonesia-yang-tidak-bisa-dikompromikan/> [Accessed 3 August 2023].

ARITONANG, I.J., UDAYANTI, E.D. AND IKSAN, N., 2018. Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (APO13). *ITEJ (Information Technology Engineering Journals)*, 3(2), pp.6–10.

CHOIRI, E.O., 2020. *Pengertian E-Government, Model Serta Kelebihan & Kekurangan*. [online] Qwords. Available at: <https://qwords.com/blog/pengertian-e-government/> [Accessed 3 August 2023].

INDRAYANI, E., 2020. *e-Government : Konsep,* Implementasi *dan Perkembangannya di Indonesia*.

N, S., 2018. *Penerapan Sistem E-government di Indonesia*. [online] Available at: <https://www.goodnewsfromindonesia.id/2018/01/23/penerapan-sistem-e-government-di-indonesia> [Accessed 3 August 2023].

NKD, F., 2021. Definisi Keamanan Informasi dan 3 Aspek di Dalamnya (CIA Triad). *Web developer LOGIQUE's Blog*. Available at: <https://www.logique.co.id/blog/2021/02/18/keamanan-informasi/> [Accessed 3 August 2023].

PRESIDEN RI, 2003. *Instruksi Presiden RI No.3* tahun *2003, "Kebijakan dan Strategi Nasional Pengembangan E-Government,"*.

SARI, N.P., 2020. *Hasil Survei PBB, 'e*-Government' *Indonesia Naik Peringkat*. [online] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. Available at: <https://menpan.go.id/site/berita-terkini/hasil-survei-pbb-e-government-indonesia-naik-peringkat> [Accessed 3 August 2023].

WIJAYA, A., 2019. Information Security Strategy To Counter Cyber Threats in Electronic Procurement Systems (Study of Hacker Attacks in. *vol*, 5, pp.71–86.