Jurnal Sistem Informasi, Teknik Komputer dan Teknologi Pendidikan (JUSTIKPEN)
Volume 5, Nomor 1 September 2025, Page 165-172
ISSN 2828-7924 (media online) | DOI: https://doi.org/10.55338/justikpen.v5i1.332

Audit Sistem Informasi Tata Kelola Keamanan Pada Layanan Website Online Single Submission Mengggunakan COBIT 2019

Audrey Muthia Vasya[1], Khoirun Nisa[2]
[1,2]Sistem Informasi, Universitas Nusa Mandiri, Jakarta, Indonesia
Email Penulis : [1]11211477@nusamandiri.ac.id, [2]khoirun.khn@nusamandiri.ac.id

Abstrak−Pemerintahan Indonesia sedang bertransformasi menuju era digital untuk meningkatkan efisiensi, transparansi, dan akuntabilitas melalui sistem terintegrasi. *Online Single Submission Risk Based Approach* (OSS RBA) Adalah salah satu platform digital terintegrasi yang berfungsi sebagai layanan perizinan usaha diseluruh Indonesia, menuntut tata kelola keamanan yang efektif dikarenakan mengelola berbagai data sensitive pelaku usaha. Penelitian ini bertujuan untuk mengukur Tingkat kapabilitas tata kelola keamanan pada layanan OSS menggunakan framework COBIT 2019, dengan fokus pada domain DSS05 *(Manage Security Service)* dan MEA03 (*Managed Compliance with External Requirements*). Metode yang digunakan Adalah deskriptif kualitatif dengan pengumpulan data melalui wawancara, obeservasi dan kuesioner yang disebarkan kepada responden yang sesuai dengam kriteria. Hasil evaluasi menunjukan bahwa Tingkat kapabilitas tata kelola keamanan pada peran pengelola (administrator) berada pada level 3-*Established*, sementara untuk peran pengguna project (contributor) mencapai level 4-*Predictable*. Terdapat kesenjangan 1 poin pada pengelola yang mengindikasi bahwa meskipun proses telah terdokumentasi dengan baik, tetapi masih diperlukannya perbaikan untuk mencapai Tingkat kematangan yang lebih tinggi. Berdasarkan temuan, diperlukannya penguatan sistematis pada pemantauan rutin dan pengembangan prosedur terstruktur guna meningkatkan efektivitas tata kelola keamanan layanan OSS.

Kata kunci: Tata Kelola Keamanan, OSS, COBIT 2019, Keamanan Informasi, Audit Sistem Infomasi

Abstract−The Indonesian government is entering the digital age to increase productivity through efficiency, transparency, and accountability. The Online Single Submission Risk Based Approach (OSS RBA) is an integrated digital system that serves to process business licenses throughout Indonesia. OSS is a crucial digital platform for business licensing services, which processes sensitive data, thus requiring effective security governance. This study aims to monitor security and measure the level of security governance capabilities in OSS services using the COBIT 2019 framework, specifically in the DSS05 (Manage Security Service) and MEA03 (Monitor, Evaluate and Assess Compliance with External Requirements) domains. The research method used is descriptive qualitative, with data collection through interviews, observations, and questionnaires distributed to respondents actively involved in the management, development, and supervision of the OSS system. Purposive sampling was used for questionnaire distribution, with content validity validation through expert judgment from internal experts at PT Telkom. The evaluation results indicate that the level of information governance capability and compliance of the administrator role is at level 3-Established, indicating that security processes are documented and standardized. Meanwhile, the contributor role is at level 4-Predictable, indicating that processes are monitored, measured, and consistently predictable. The gap analysis confirmed a 1-point gap in some sub-domains.

Keyword: Security Governance,OSS, COBIT 2019, Information Security, System Information Audit

1. PENDAHULUAN

Perkembangan globalisasi dan revolusi industri 4.0, telah mendorong transformasi digital, menjadikan sebagai aspek krusial dan strategis dalam pelayanan publik [1]. Untuk meningkatkan produktivitas, dalam Upaya meningkatkan efisiensi, trasnparansi serta pertanggung jawaban. *Online Single Submission Risk Based Approach* OSS RBA merupakan platform terintegrasi yang difungsikan untuk proses perizinan berusaha di seluruh Indonesia. Seiring meningkatnya ketergantungan pada teknologi digital, teknologi dan komunikasi menjadi suatu keharusan bagi Lembaga yang memberikan pelayanan kepada Masyarakat. Jika pemanfaatan layanan teknolgi tidak dijalankan secara optimal dapat menimbulkan persoalan seperti pembekakan biaya operasional, control pelayanan yang butuh, pemanfaatan asset yang tidak efektif, serta pengambilan Keputusan yang salah [2].

Transformasi digital dalam pelayanan publik juga mencakup digitalisasi proses bisnis secara menyuluruh termasuk peralihan dari proses sistem manual ke digital yang memanfaatkan kecerdasan buatan, otomatisasi, waktu respons yang lebih cepat, lebih sedikit kesalahan manusia, dan peningkatan efisiensi secara keseluruhan [3]. Pelaku usaha dari berbagai bidang dapat mengajukan dan mengelola perizinan secara online melalui sistem OSS, sehingga dapat mempercepat proses birokrasi dan meningkatkan kemudahan berusaha.

Sebagai penyedia infrastuktur digital yang memiliki peran strategis dalam mendukung layanan publik PT Telkom Indonesia turut berkontribusi dalam pengembangan dan pengelolaan sistem OSS. Sebagai sistem informasi skala nasional yang menyimpan data sensitive terkait perizinan dan identitas pelaku usaha, OSS sangat rentan terhadap ancaman keamanan informasi. Dalam studi OSS masih belum memiliki pengautran khusus yang tertanam sehingga belum dapat terjaminan perllindungan data yang tertanam dalam sistem. Meskipun terdapat keterlibatan Kepolisian Republik Indonesia, regulasi terkait perlindungan data pribadi pelaku usaha masih belum tersedia secara jelas [4]. Perlindungan data pribadi pengguna masih mengacu pada ketentuan umum pada UU ITE

Submitted: **04/08/2025**; Accepted: **29/08/2025**; Published: **29/09/2025**

Jurnal Sistem Informasi, Teknik Komputer dan Teknologi Pendidikan (JUSTIKPEN)
Volume 5, Nomor 1 September 2025, Page 165-172
ISSN 2828-7924 (media online) | DOI: https://doi.org/10.55338/justikpen.v5i1.332

dan undang-undang informasi, tanpa adanya pengaturan khusus yang dipakai langsung dalam mekanisme OSS itu sendiri Kondisi ini menunjukkan adanya *gap* regulasi dan implementasi yang berpotensi menimbulkan risiko kebocoran data[5].

Maka dari itu sangat penting unutk memastikan bahwa sistem OSS memiliki control keamanan yang memadai, seperti pengelolaan akses pengguna yang ketat, sistem pencadangan data yang handal, serta pemantauan sistem yang dilakukan secara berkala. Melalui audit ini, tidak hanya menganalisa sejauh mana penerapan monitoring pada aspek keamanan informasi dilakukan, tetapi juga untuk pengukuran Tingkat kapabilitas dari proses-proses yang di audit.

Secara khusus, penelitian ini menjawab dua rumusan masalah utama, yaitu:

a. Bagaimana efektivitas sistem monitoring keamanan informasi yang diterapkan pada layanan OSS dalam menjaga kerahasiaan dan ketersediaan data pelaku usaha?
b. Sejauh mana kondisi tata kelola keamanan informasi pada sistem OSS yang dapat diidentifikasi melalui audit, serta bagaimana posisi serta tingkat kapabilitas keamanan informasi saat ini?

Luaran penelitian ini diharapkan mampu memberikan gambaran mengenai Tingkat kapabilitas tata Kelola yang telah diterapkan. Dan mampu memberkan kontribusi sebagai dasar pertimbangan masukan stategis dalam memndorong kepatuhan terhadap setandar perlindungan informasi, memperkuat keandalan sistem, serta meningkatkan kepercayaan pelaku usaha dalam layanan OSS.

Proses audit menggunakan *framework* COBIT 2019, dengan focus domain dan subdomain yang relvan dengan keamanan informasi[6]:

a. DSS05 *(Manage Security Service)* mengevaluasi dan mengaudit pengelolaan layanan TI untuk melindungi aset informasi dari ancaman.
    1. DSS05.01–Menyediakan pengawasan terhadap serangan digital, termasuk malware.
    2. DSS05.02–Melakukan pengawasan terhadap keamanan jaringan serta kestabilan koneksi.
    3. DSS05.03–Menjamin keamanan perangkat milik pengguna.
    4. DSS05.04–Menangani pengelolaan identitas pengguna serta akses logis.
    5. DSS05.06–Menjaga keamanan dokumen sensitif dan perangkat keluaran.
    6. DSS05.07–Mengelola kerentanan dan pemantauan infrastruktur yang berkaitan dengan keamanan.
b. MEA03 (*Managed Compliance With External Requirements)* evaluasi dan kepatuhan terhadap aturan keamanan serta regulasi yang berlaku.
    1. MEA03.01–Menyusun dan mengenali kewajiban persyaratan kepatuhan yang harus dipenuhi.
    2. MEA03.02–Mengoptimalkan respon terhadap persyaratan kebutuhan.
    3. MEA03.03–Melakukan evaluasi terhadap kesesuaian praktik dengan persyaratan dari pihak eksternal.
    4. MEA03.04–Memperoleh jaminan kepatuhan eksternal.

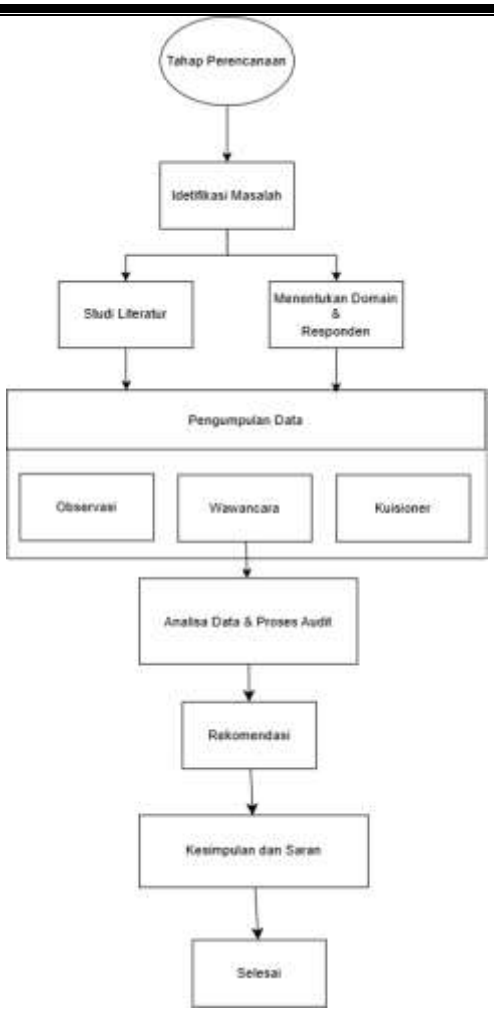
2. METODOLOGI PENELITIAN

2.1. Tahapan Penelitian

Metode penelitian ini merupakan jenis penelitian deskripsif kualitatif yang mengungkapkan suatu fenomena dengan cara mendeskripsikan data dan fakta melalui kata-kata secara menyeluruh terhadap subjek penelitian [7]. Tujuannya adalah untuk mengevaluasi tata Kelola keamanan pada sistem *online single submission* (OSS) dengan menggunakan framework COBIT 2019, khususnya pada domain DSS05-*Manage Security Services*, MEA03-*Managed Compliance with External Requirements.* Pendekatakan kualitatif digunakan untuk memperoleh pemahaman mengenai implmeentasi proses tata kelola melalui teknik pengumpulan data berupa wawancara, dan observasi langsung kepada pihak yang terlibat dalam pengelolaan sistem OSS [7]. Proses ini digunakan untuk melengkapi perspektif, pengalaman, dan praktik yang terjadi di lapangan secara kontekstual. Teknik sampling yang digunakan Adalah *purposive sampling* dengan pendekatan *content validity* di mana responden dipilih berdasarkan peran aktif dalam pengelolaan, pengembangan, atau pengawasan keamanan informasi. Validasi instrument dilakukan melalui *expert judgment* dari pihak internal Telkom[8].

Submitted: **04/08/2025**; Accepted: **29/08/2025**; Published: **29/09/2025**

Jurnal Sistem Informasi, Teknik Komputer dan Teknologi Pendidikan (JUSTIKPEN)
Volume 5, Nomor 1 September 2025, Page 165-172
ISSN 2828-7924 (media online) | DOI: https://doi.org/10.55338/justikpen.v5i1.332



Gambar 1. Metodologi Penelitian

Tahapan penelitian ini dimula dari perencanaan, pengumpulan data hingga analisis data. Prosedur penelitian ini mengacu pada metodologi yang dijelaskan dalam COBIT 2019 Framework: Introduction and Methodology [6].

a. Tahapan perencanaan: Tahapan ini mencakup studi literatur mendalam terkait audit sistem informasi COBIT 2019, dan konsep keamanan informasi. Tujuannya adalah untuk membangun kerangka kerja sebagai landasan penelitian.
b. Identifikasi masalah : Mengkaji permasalahan utama terkait pengelolaan keamanan informasi pada sistem OSS, khususnya pengendalian akses, perlindungan data dan kepatuhan terhhadap kebijakan internal maupun eskternal.
c. Studi literatur: memahami refrensi yang relevan terkait sistem OSS, tata Kelola TI dan penerapan COBIT 2019, termasuk teori *governance* dan kerangka kerja audit sistem informasi.
d. Identifikasi domain COBIT 2019: menentukan domain yang relevan terhadap onjek penelitian, peneliti menentukan dua domain yaitu (*Manage Security Services*) dan MEA03 (*Managed Compliance With External Requirements*).
e. Penetuan responden : dalam menentukan responden yang sesuai untuk pengisian kuesioner, penelitian ini dibantu dengan RACI Chart untuk mengidentifikasi peran dan tanggung jawab individu dalam proses pengelolaan sistem OSS.
f. Tahapan pengumpulan data: pengumpulan data dilakukan dengan tiga metode yaitu:
    1. Observasi: Metode ini melibatkan pengamatan langsung terhadap proses dan aktivitas operasional terkait keamanan OSS di lingkungan kerja PT Telkom Indonesia. Dengan pengumpulan data yang mencakup catatan lapangan, dokumentasi visual dari praktif-praktif keamanan yang telah diterapkan.
    2. Wawancara; wawancara semi terstruktur dilakukan dengan narasumber dari PT Telkom Indonesia yang terlibat langsung dalam perancangan dan pengelolaan sistem OSS. Wawancara ini bertujuan untuk menggali informasi kualitatif mengenai perspektif, dan praktik-praktik tata kelola keamanan yang tidak tercatat dalam dokumen formal.

Submitted: **04/08/2025**; Accepted: **29/08/2025**; Published: **29/09/2025**

Jurnal Sistem Informasi, Teknik Komputer dan Teknologi Pendidikan (JUSTIKPEN)
Volume 5, Nomor 1 September 2025, Page 165-172
ISSN 2828-7924 (media online) | DOI: https://doi.org/10.55338/justikpen.v5i1.332

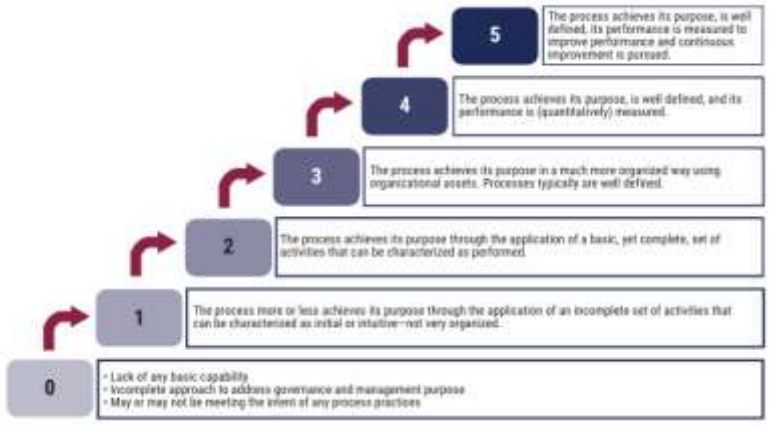
3. Kuesioner disusun berdasarkan proses dan indicator dari COBIT 2019, khususnya DSS05 dan MEA03. Disebarkan secara daring menggunakan *Google Form* kepada responden yang berperan sebagai administrator dan kontributor sistem OSS.

g. Tahap Analisis Data: Data yang terkumpul direkapitulasi dan dianalisis untuk menghasilkan nilai kapabilitas pada masing-masing *sub-domain*. Penilaian analisis kapabilitas ini mengikuti skala penilaian yang merujuk pada metodologi yang dijelaskan dalam COBIT 2019 [6].

2.2. Metode Audit Sistem Informasi

Metode audit dilakukan mengacu pada framework COBIT 2019, menggunakan skala kapabilitas. Domain yang difokuskan Adalah DSS05 (*Manage Security Services*) Berfokus pada pengelolaan layanan keamanan untuk melindungi asset TI. MEA03 (*Monitor, Evaluate and Assess Compliance with External Requirements*): Berfokus pada evaluasi kepatuhan terhadap regulasi eksternal dan kebijakan internal. COBIT 2019 digunakan untuk mengendalikan teknologi informasi dan pengendalian internal yang membantu para manjer, penggguna dan audiot dalam memamhami dan mneginterprestasikan sistem teknologi infiormasi di unit mereka untuk mengembangkan tata Kelola di dalamnya[9].

Tingkat kapabilitas ini diukur berdasarkan hasil rata-rata skor dari kuesioner yang disebarkan kepada responden[10]



Gambar 2. Capability Level

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil dari audit sistem informasi yang dilakukan pada layanan website OSS. Data yang diolah berasal dari kuesioner, observasi, dan wawancara.

3.1 Pengukuran Tingkat Kapabilitas

Berdasarkan hasil pengolahan data kuesioner, diperoleh nilai rata-rata untuk setiap domain dan peran responden

Table 1. *DSS05 Administrator*

No.	Perhitungan per- capability	Skor per-capability	Hasil per-subdomain
1.	DSS05.01-CL2	3	3,02
2.	DSS05.01-CL3	2,91	
3.	DSS05.01-CL4	3,16	
4.	DSS05.02-CL2	3,75	3,43
5.	DSS05.02-CL3	3,16	
6.	DSS05.02-CL4	3,375	
7.	DSS05.03-CL2	3,625	3,52
8.	DSS05.03-CL3	3,41	
9.	DSS05.04-CL2	4	3,52
10.	DSS05.04-CL3	3,5	
11.	DSS05.04-CL3	3,08	
12.	DSS05.06-CL2	2,75	2,87
13.	DSS05.06-CL2	3	
14.	DSS05.07-CL1	3,75	3,41
15.	DSS05.07-CL2	3,25	

Submitted: **04/08/2025**; Accepted: **29/08/2025**; Published: **29/09/2025**

Jurnal Sistem Informasi, Teknik Komputer dan Teknologi Pendidikan (JUSTIKPEN)
Volume 5, Nomor 1 September 2025, Page 165-172
ISSN 2828-7924 (media online) | DOI: https://doi.org/10.55338/justikpen.v5i1.332

16.	DSS05.07-CL3	3,25	
Rata-rata Domain			3,276

Table 2. *DSS05 Kontributor*

No.	Hasil perhitungan per- capability	Skor per-capability	Hasil per-subdomain
1.	DSS05.01-CL2	4,42	4
2.	DSS05.01-CL3	3,78	
3.	DSS05.01-CL4	4,14	
4.	DSS05.03-CL2	3,57	4
5.	DSS05.03-CL3	4,14	
6.	DSS05.04-CL2	4,28	4
7.	DSS05.04-CL3	4,23	
8.	DSS05.04-CL4	3,85	
9.	DSS05.06-CL2	3,2	3,5
10.	DSS05.06-CL3	3,76	
Rata-rata Domain			3,90

Table 3. Domain DSS05

Domain	Skor rata-rata	*Level Kapabilitas*
DSS05 Administrator	3,276	*Established (Level 3)*
DSS05 Kontributor	3,90	*Predictable (Level 4)*

Berdasarkan hasil perhitungan domain DSS05 tersebut menunjukan bahwa setiap peran mempunyai levelnya masing-masing. Peran administrator berada pada level 3 dengan skor 3,276, yang artinya proses kepatuhan IT sudah stabil dan terukur namun masih bisa ditingkatkan kembali, sedangkan kontributor berada pada level 4 dengan skor 3,90, menunjukan bahwa proses pengelolaan pengguna project sudah termonitor secara rutin dan dievaluasi secara sistematis.

Table 4. *MEA03 Administrator*

No.	**Hasil perhitungan per- capability**	**Skor per-*capability***	**Hasil per-subdomain**
1.	MEA03.01-CL2	3,25	3,33
2.	MEA03.01-CL3	3	
3.	MEA03.02-CL3	3,33	3
4.	MEA03.03-CL3	3,25	3,25
5.	MEA03.03-CL4	3,25	
6.	MEA03.03-CL5	3,25	
7.	MEA03.04-CL2	3,125	3,125
8.	MEA03.04-CL3	3,125	
9.	MEA03.04-CL4	3,125	
Rata-rata domain			3,20

Table 5. *MEA03 Kontributor*

No.	**Perhitungan per- *capability***	**Skor per-*capability***	**Hasil per-subdomain**
1.	MEA03.02-CL3	3,82	3,82
2.	MEA03.03-CL3	4,07	3,97
3.	MEA03.03-CL4	4	
4.	MEA03.03-CL5	3,85	
Rata-rata domain			3,90

Table 6. Domain MEA03

Domain	Skor rata-rata	Level Kapabilitas
MEA03 Kontributor	4,04	*Predictable (Level 4)*

Submitted: **04/08/2025**; Accepted: **29/08/2025**; Published: **29/09/2025**

Jurnal Sistem Informasi, Teknik Komputer dan Teknologi Pendidikan (JUSTIKPEN)
Volume 5, Nomor 1 September 2025, Page 165-172
ISSN 2828-7924 (media online) | DOI: https://doi.org/10.55338/justikpen.v5i1.332

MEA03 Administrator	3,20	*Established (Level 3)*

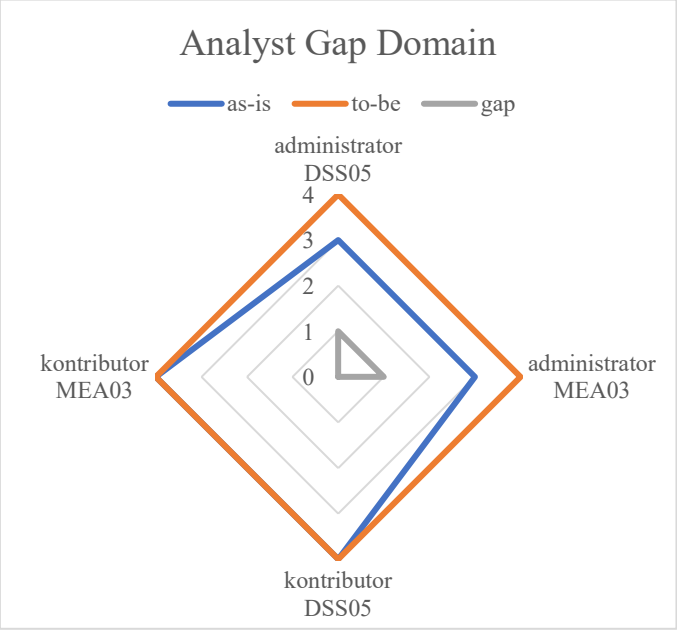
Berdasarkan hasil perhitungan rata-rata skor pada domain MEA03 bisa dilihat bahwa setiap peran mempunyai levelnya masing-masing. Peran contributor sudah mencapai pada level 4 dengan skor 3,90 yang artinya kepatuhan keamanan sudah ada pada tahap yang terukur dan dipantau secara konsisten. Sedangkan administrator berada pada level 3 dengan skor 3,20. Yang menunjukan bahwa pengelolaan kepatuhan sistem OSS sudah dijalankan secara konsisten dan terdokumentasi. Namun masih bisa terus ditingkatkan.

3.2 Analisis GAP

Analisis *gap* dilakukan untuk membandingkan tingkat kapabilitas saat ini (*as-is*) dengan tingkat kapabilitas yang ditargetkan (*to-be*).

Table 7. Analisis GAP

Domain	as-is	to-be	gap
administrator DSS05	3	4	1
administrator MEA03	3	4	1
kontributor DSS05	4	4	0
kontributor MEA03	4	4	0



Gambar 3 Gap Analisis

Berdasarkan hasil dari anlisa gap pada domain DSS05 dan MEA03 pada Table 3 Analisis GAP dan Gambar 3 Gap Analisis, dapat disimpulkan bahwa peran contributor telah sepenuhnya selaras dengan Tingkat kapabilitas yang ditargetkan, sehingga tidak ditemukan adanya gap. Sementara itu, administrator terdapat gap sebesar 1 poin, baik dari penemuan keamanan informasi (DSS05) maupun kepatuhan internal eksternal (MEA03), yang mengindikasi perlunya peningkatan dalam praktik tata Kelola keamanan informasi.

3.3 Temuan dan Rekomendasi

Berdasarkan Analisa yang didapatkan dari kuesioner, observasi dan wawancara terdapat beberapa penemuan kunci sebagai berikut:

a. Sistem kemmanan teknis sudah memadai dengan adanya protocol keamanan kredensial SHA256, penggunaan URL open-source terverifikasi dan koneksi melalui VPN. Menunjukan bahwa praktik keamanan yang optimal dan terdapat prosedur jelas mengenai tools tambahan untuk memastikan berasal dari sumber terverifikasi.
b. Kepatuhan audit eksternal yang dilakukan secra berkala oleh BSSN (Badan Siber dan Sandi Nasional) yang mencakup vulnerability & Penetration testing. Hal ini menunjukan adanya Upaya kepatuhan dari pihak krtiga dan komitmen peningkatan kepatuhan.

Submitted: **04/08/2025**; Accepted: **29/08/2025**; Published: **29/09/2025**

c. Kesenjangan pada administrator meskipun praktik keamanan dasar sudah diterapkan namun peran administrator yaitu pengelola dan pengawasan infrastruktur masih berasa pada level 3, menunjukan bahwa proses pemantauan dan evaluasi belum sepenuhnya termonitor secara sistematis.

Bedasarkan temuan tersebut, rekomendasi yang dapat diberikan adalah:

a. Memperkuat prosedur tinjauan rutin terhadap log keamanan dan aktivitas sistem OSS untuk mendeteksi anomali atau serangan secara proaktif
b. Memastikan seluruh prosedur dan kebijakan keamanan terdokumentasi dan mudah diakses oleh seluruh pihak terkait.
c. Perlu dilakukan sinkonisasi dan transparansi hasil audit untuk menyamakan persepsi dan pemahaan terhadap proses audit, temuan dan tindak lanjut kepatuhan.
d. Mengembangkakn *dashboard* interaktif untuk mendapatkan informasi keamanan yang akurat dan *real-time*
e. Membuat platform atau mekanisme komunikasi yang efisiensi untuk menyinkronkan hasil audit.

Dengan demikian, temuan ini mengindikasi adanya konsistensi pada aspek kepatuhan eksternal dan internal. Hal ini sejalan dengan latar belakang yang telah dijelaskan pada pendahuluan, dimana OSS sebagai sistem skala nasional masih menghadapi gap regulasi dan risiko kebocoran data [4]. Menunjukan bahwa meskipun masih terdapat gap yang masih diperlukan peningkatan, namun aspek kepatuhan eksternal telah terjamin.

4. KESIMPULAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan terhadap audit sistem informasi layanan Online single submission menggunakan framework COBIT 2019, dapat ditarik beberapa Kesimpulan utama. Permasalahan yang melatarbelakangi penelitian ini adalah kurangnya tata kelola keamanan yang optimal pada layanan OSS yang menyimpan data sensitive, yang berpotensi menimbulkan risiko kebocoran data dan penyalahgunaan. Oleh karena itu, diperlukan evaluasi mendalam terhadap tata Kelola keamanan informasi, khususnya pada aspek pengelolaan akses pengguna, pemantauan sistem, dan kesiapan menghadapi ancaman dengan fokus pada domain DSS05 *(Manage Security Service)* dan MEA03 (*Managed Compliance With External Requirements)*.

Hasil penelitian ini menunjukan bahwa tingkat kapabilitas untuk peran contributor berada pada Level 3-*Established* dengan rata-rata skor 3,20 pada MEA03 dan 3,276 pada DSS05. Hal ini menunjukan bahwa proses telah dimonitor terukur dan dapat diprediksi secara konsisten. Sedangkan peran contributor berada pada Level 4-*Predictable* dengan rata-rata skor 3,90. Hal ini menunjukan proses keamanan telah terukur, dimonitor secara rutin dan dapt diprediksi secara konsisten. Hasil analisis gap yang dilakukan mengonfirmasi adanya kesenjangan sebesar 1 poin pada peran administrator, mengindikasi bahwa proses keamanan masih perlu ditingkatkan agar mendapatkan tingkat kematangan yang lebih tinggi. Dengan demikian, audit ini bisa memberikan gambaran objektif mengenai Tingkat kematangan proses TI saat ini pada layanan website OSS dan menjadi dasar unutk perumusan rekomendasi perbaikan yang berkelanjutan.

UCAPAN TERIMAKASIH

Terima kasih kepada seluruh pihak yang telah mendukung terlaksannya penelitian ini, terutama dosen pembimbing dan pembimbing perususahaan yang telah memberikan araha dan bimbingan, serta terima kasih kepada PT Telkom yang telah memberikan data dan kesempatan rist.

REFERENCES

[1] H. Syamsuddin, Muhammad Nur, Mas'ud, "Strategi Manajerial dalam Meningkatkan Efektivitas Pelayanan Perizinan dengan Sistem Online Single Submission pada Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Bima," vol. 5, no. 4, 2024.

[2] I. N. R. W. Kesuma, I. Hermadi, and Y. Nurhadryani, "Evaluasi Tata Kelola Teknologi Informasi di Dinas Pertanian Gianyar Menggunakan COBIT 2019," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 3, pp. 513–522, 2023, doi: 10.25126/jtiik.20231026565.

[3] S. M. Anggara, A. Hariyanto, Suhardi, A. A. Arman, and N. B. Kurniawan, "The Development of Digital Service Transformation Framework for The Public Sector," *IEEE Access*, vol. 12, no. October, pp. 146160–146189, 2024, doi: 10.1109/ACCESS.2024.3406571.

[4] A. E. Rahmadani, Y. Pangestu, and N. Halizhah, "Analisis Penerapan Perizinan Berusaha Melalui Sistem Online Single Submission (OSS)," vol. 2, no. 4, 2024.

[5] T. Lestariningtyas and M. Roqib, "Perlindungan Data Pribadi Pengguna Sistem Layanan Perizinan Berusaha Terintegrasi Secara Elektronik Oss 1.1 Dan Oss Rba (Risk Basic Approach)," *J. Jendela Huk.*,

Submitted: **04/08/2025**; Accepted: **29/08/2025**; Published: **29/09/2025**

vol. 8, no. 2, pp. 25–34, 2021.
[6] ISACA, *COBIT 2019 Framework - Introduction and Methodology*. 2019.
[7] Mouwn Erland, *Metodologi Penelitian Kualitatif. In Metodologi Penelitian Kualitatif*, no. March. 2020.
[8] A. Akbar and M. Barni, *Metodologi Penelitian Bidang Pendidikan*, vol. 12, no. 1. 2022. doi: 10.18592/jtipai.v12i1.6774.
[9] M. M. Jawad, M. H. Ali, A. A. Khaleel, and M. F. Hasan, "Evaluating the performance of IT management under the implementation of the COBIT 2019 framework," *Eximia*, vol. 12, pp. 18–36, 2023, doi: 10.47577/eximia.v12i1.331.
[10] COBIT 2019, *Governance and Management Objectives*. 2019.

Submitted: **04/08/2025**; Accepted: **29/08/2025**; Published: **29/09/2025**