EVALUASI TATA KELOLA KEAMANAN SISTEM INFORMASI MENGGUNAKAN *FRAMEWORK* COBIT 5 (STUDI KASUS: TSIRWAH INDONESIA)

Denny Rusdianto[1], Hanif Ibrahim[2]
[1,2]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Bale Bandung
[1]dennyrusdianto@gmail.com, [2] Ibrahimhanif207@gmail.com

Abstrak
Evaluasi tata kelola keamanan sistem informasi merupakan aspek penting dalam menjamin keamanan, efisiensi, dan efektivitas operasional organisasi, khususnya bagi perusahaan yang bergantung pada teknologi informasi. Tsirwah Indonesia sebagai perusahaan yang memanfaatkan sistem informasi dalam mendukung proses bisnisnya menghadapi tantangan dalam memastikan keamanan informasi secara optimal. Oleh karena itu, penelitian ini dilakukan untuk mengevaluasi tingkat kematangan tata kelola keamanan sistem informasi di Tsirwah Indonesia menggunakan framework COBIT 5, dengan fokus pada domain DSS05 (Manage Security Services).Metode penelitian yang digunakan adalah pendekatan kuantitatif melalui penyebaran kuesioner kepada para pemangku kepentingan yang terlibat dalam pengelolaan dan penggunaan sistem informasi. Data yang diperoleh dianalisis untuk mengukur tingkat kematangan pada subdomain DSS05, yang meliputi perlindungan terhadap malware, manajemen keamanan jaringan, pengelolaan identitas dan akses pengguna, serta pengendalian layanan keamanan lainnya. Hasil penelitian menunjukkan bahwa tingkat kematangan tata kelola keamanan sistem informasi di Tsirwah Indonesia berada pada level 3 (Established) hingga level 4 (Predictable). Hal ini mengindikasikan bahwa organisasi telah memiliki prosedur keamanan yang terdokumentasi dan diterapkan secara konsisten, namun masih terdapat kesenjangan untuk mencapai tingkat kematangan optimal (Optimized). Berdasarkan hasil gap analysis, disusun rekomendasi perbaikan yang mencakup peningkatan kompetensi sumber daya manusia, pembaruan kebijakan keamanan, serta penerapan teknologi perlindungan yang lebih memadai. Hasil penelitian ini diharapkan dapat menjadi dasar perbaikan tata kelola keamanan sistem informasi dan meningkatkan keandalan operasional Tsirwah Indonesia.
Kata Kunci: Tata kelola TI, Keamanan Sistem Informasi, COBIT 5, DSS05, Tingkat Kematangan

Abstract
The evaluation of information system security governance is a crucial aspect in ensuring the security, efficiency, and effectiveness of organizational operations, particularly for companies that rely heavily on information technology. Tsirwah Indonesia, as a company that utilizes information systems to support its business processes, faces challenges in achieving optimal information security governance. Therefore, this study aims to evaluate the maturity level of information system security governance at Tsirwah Indonesia using the COBIT 5 framework, with a specific focus on the DSS05 (Manage Security Services) domain. This research employs a quantitative approach through the distribution of questionnaires to

relevant stakeholders involved in the management and use of information systems. The collected data are analyzed to assess the maturity level of DSS05 subdomains, including malware protection, network security management, user identity and access management, and other security service controls. The results indicate that the maturity level of information system security governance at Tsirwah Indonesia is within level 3 (Established) to level 4 (Predictable). This finding suggests that the organization has implemented documented and consistently applied security procedures; however, improvements are still required to achieve the optimal level (Optimized). Based on the gap analysis, several strategic recommendations are proposed, including enhancing human resource competencies through training, updating security policies and procedures, and implementing more advanced security technologies. The results of this study are expected to contribute to the improvement of information system security governance and support more reliable organizational operations at Tsirwah Indonesia.
***Keywords** : IT governance, information system security, COBIT 5, DSS05, maturity leve*

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong organisasi untuk mengintegrasikan sistem informasi ke dalam hampir seluruh aktivitas operasional dan pengambilan keputusan. Pemanfaatan teknologi informasi memberikan berbagai manfaat, seperti peningkatan efisiensi proses bisnis, kemudahan akses informasi, serta peningkatan kualitas layanan. Namun, ketergantungan yang tinggi terhadap teknologi informasi juga menimbulkan berbagai risiko, khususnya yang berkaitan dengan keamanan sistem informasi. Ancaman seperti serangan malware, kebocoran data, penyalahgunaan akses, dan gangguan layanan dapat berdampak serius terhadap keberlangsungan operasional organisasi apabila tidak dikelola secara memadai.

Keamanan sistem informasi tidak hanya berfokus pada aspek teknis, tetapi juga memerlukan tata kelola yang baik agar pengelolaannya selaras dengan tujuan bisnis organisasi. Tata kelola keamanan sistem informasi berperan penting dalam memastikan bahwa kebijakan, prosedur, dan pengendalian keamanan diterapkan secara konsisten dan efektif. Evaluasi tata kelola keamanan informasi telah banyak dibahas dalam penelitian sebelumnya, di mana pendekatan berbasis COBIT 5 kerap digunakan untuk menilai tingkat kematangan pengelolaan keamanan dan memberikan rekomendasi perbaikan bagi organisasi. Sebagai contoh, studi pada perpustakaan daerah menggunakan COBIT 5 untuk menilai kematangan tata kelola keamanan informasi, menunjukkan efektivitas framework ini dalam mengukur praktik keamanan yang ada. (Fatimah, 2023)

Tsirwah Indonesia merupakan perusahaan yang bergerak di bidang teknologi informasi dan memanfaatkan sistem informasi sebagai bagian penting dalam mendukung proses bisnisnya. Penggunaan teknologi informasi di Tsirwah Indonesia bertujuan untuk meningkatkan kualitas layanan kepada para pemangku kepentingan, khususnya dalam penyediaan informasi pemberitaan online kepada masyarakat secara cepat, akurat, dan mudah diakses. Seiring dengan meningkatnya ketergantungan terhadap sistem informasi tersebut, diperlukan dukungan keamanan informasi yang memadai agar proses

penyampaian informasi dapat berjalan secara lancar, andal, dan berkelanjutan. Keamanan informasi menjadi faktor krusial untuk melindungi data dari ancaman seperti akses tidak sah, manipulasi informasi, serta gangguan layanan, sehingga kepercayaan masyarakat dan stakeholder terhadap layanan yang disediakan oleh Tsirwah Indonesia dapat tetap terjaga.

Dalam konteks evaluasi tata kelola keamanan, penelitian lain menggunakan kerangka kerja COBIT 2019 pada berbagai organisasi juga menunjukkan bahwa penilaian kapabilitas keamanan informasi penting untuk mengetahui posisi organisasi dalam pengelolaan risiko keamanan serta area yang memerlukan peningkatan (Jannah, 2025). Domain khusus seperti DSS05 (Manage Security Services) dianggap krusial karena berhubungan langsung dengan pelaksanaan layanan keamanan seperti pengelolaan identitas, proteksi jaringan, dan respon insiden (Ayu, 2025). Sejalan dengan hal tersebut, penelitian audit teknologi informasi menggunakan framework COBIT 5 pada institusi pendidikan menunjukkan bahwa pengukuran tingkat kematangan mampu mengidentifikasi kelemahan tata kelola TI dan menjadi dasar dalam penyusunan rekomendasi perbaikan yang berkelanjutan (Rosmalina., 2019). Selain itu, penerapan COBIT 5 pada sistem informasi berbasis web juga terbukti efektif dalam mengevaluasi tingkat kematangan tata kelola keamanan serta mengidentifikasi kesenjangan proses yang perlu ditingkatkan (Rosmalina & Alhabib, 2023).

Meskipun demikian, masih terdapat keterbatasan penelitian yang secara spesifik mengevaluasi tingkat kematangan tata kelola keamanan sistem informasi pada perusahaan berbasis teknologi informasi di Indonesia dengan fokus pada domain DSS05. Banyak organisasi telah menerapkan berbagai kontrol keamanan tetapi belum melakukan evaluasi formal untuk mengetahui tingkat kematangan tata kelola keamanan yang dimiliki serta kesenjangan antara kondisi saat ini dengan kondisi yang diharapkan. Hal ini menunjukkan adanya gap penelitian terkait evaluasi tata kelola keamanan sistem informasi yang terstruktur dan berbasis framework standar.

Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk mengevaluasi tingkat kematangan tata kelola keamanan sistem informasi di Tsirwah Indonesia menggunakan framework COBIT 5, khususnya pada domain DSS05 (Manage Security Services). Penelitian ini bertujuan untuk mengidentifikasi tingkat kematangan saat ini, menganalisis kesenjangan yang ada, serta memberikan rekomendasi perbaikan guna meningkatkan kualitas tata kelola keamanan sistem informasi. Kebaruan (novelty) dari penelitian ini terletak pada penerapan evaluasi domain DSS05 secara terfokus pada studi kasus Tsirwah Indonesia, sehingga diharapkan dapat memberikan kontribusi praktis bagi perusahaan serta memperkaya kajian empiris terkait tata kelola keamanan sistem informasi di Indonesia.

2. KAJIAN PUSTAKA

Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi (IT Governance) merupakan konsep yang menekankan pentingnya pengelolaan dan pengendalian teknologi informasi agar selaras dengan tujuan dan strategi bisnis organisasi. Tata kelola TI berfungsi untuk memastikan bahwa pemanfaatan teknologi informasi dapat memberikan nilai tambah bagi organisasi, sekaligus

mengelola risiko yang timbul dari penggunaan teknologi tersebut. Penerapan tata kelola TI yang baik memungkinkan organisasi untuk mengoptimalkan sumber daya TI, meningkatkan kinerja operasional, serta mendukung pengambilan keputusan yang lebih efektif (De Haes, 2020)

Keamanan Sistem Informasi

Keamanan sistem informasi merupakan aspek penting dalam tata kelola TI untuk melindungi aset informasi dari ancaman. Prinsip utama keamanan informasi adalah kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) atau CIA Triad, yang menjadi dasar pengendalian untuk mencegah akses tidak sah, menjaga keakuratan data, dan memastikan ketersediaan sistem bagi pengguna berwenang (Whitman, 2021). CIA Triad juga dianalisis dalam konteks keamanan jaringan modern dan ancaman digital terbaru (Chai, 2021) (Jones, 2025).

Manajemen Resiko TI

Dalam pengelolaan keamanan sistem informasi, manajemen risiko teknologi informasi memegang peranan penting. Manajemen risiko TI melibatkan proses identifikasi, analisis, dan evaluasi risiko yang dapat mempengaruhi keberlangsungan sistem informasi serta penentuan langkah mitigasi yang tepat. Pendekatan berbasis risiko membantu organisasi dalam memprioritaskan upaya pengamanan sesuai dengan tingkat dampak dan kemungkinan terjadinya ancaman, sehingga pengelolaan keamanan dapat dilakukan secara lebih efektif dan efisien (Susanto, 2021). Selain itu, strategi *IT risk management* mencakup identifikasi aset, ancaman, serta analisis dan perlakuan risiko secara sistematis untuk mendukung pengambilan keputusan yang tepat dan pengembangan kontrol keamanan yang responsif (Rahman, 2024). Penelitian tinjauan literatur terbaru menunjukkan bahwa manajemen risiko IT fokus pada identifikasi, evaluasi, dan pengelolaan risiko yang berkaitan dengan teknologi dan operasional TI untuk mendukung keberlanjutan bisnis dalam lingkungan digital yang kompleks (Akmal, 2024)

***Framework* COBIT 5**

Salah satu kerangka kerja yang banyak digunakan dalam tata kelola dan manajemen teknologi informasi adalah COBIT 5, yang menyediakan panduan komprehensif terkait prinsip, proses, dan praktik terbaik dalam pengelolaan TI. COBIT 5 dirancang untuk membantu organisasi mencapai tujuan bisnis melalui pengelolaan TI yang terstruktur, termasuk pengelolaan layanan keamanan informasi di bawah domain DSS05 (*Deliver, Service, and Support*). Penelitian-penelitian empiris terbaru menunjukkan bahwa domain DSS05 sangat relevan dalam menilai efektivitas pelayanan keamanan serta mengidentifikasi gap kematangan layanan keamanan di berbagai organisasi, termasuk layanan publik dan layanan akademis (Hadi, 2024)

Domain DSS05 (*Manage Security Services*) berfokus pada pengelolaan layanan keamanan sistem informasi, seperti perlindungan terhadap malware, manajemen keamanan jaringan, pengendalian identitas dan akses pengguna, serta pemantauan dan penanganan insiden keamanan. Penggunaan DSS05 sebagai indikator dalam penelitian-penelitian tersebut menunjukkan kemampuannya dalam memberikan gambaran status keamanan yang objektif melalui pengukuran tingkat

kematangan proses keamanan. (Putra, 2024)

Untuk mengukur tingkat penerapan tata kelola keamanan sistem informasi, model tingkat kematangan (maturity level model) digunakan sebagai alat ukur yang menggambarkan tahapan perkembangan pengelolaan proses dari level rendah (Incomplete) hingga level tinggi (Optimized). Model ini memungkinkan organisasi untuk mengidentifikasi kondisi saat ini, mengevaluasi gap, serta merumuskan rekomendasi perbaikan secara sistematis (Rahayu, 2025)

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi kasus**.** Pendekatan ini dipilih karena penelitian berfokus pada pengkajian secara mendalam terhadap kondisi aktual tata kelola keamanan sistem informasi yang diterapkan pada Tsirwah Indonesia. Evaluasi dilakukan menggunakan kerangka kerja COBIT 5**,** khususnya pada domain DSS05 (*Manage Security Services*)**,** yang berfungsi untuk menilai sejauh mana pengelolaan layanan keamanan sistem informasi telah diterapkan secara terstruktur dan efektif.

Objek dan Subjek Penelitian : Objek penelitian ini adalah tata kelola keamanan sistem informasi pada Tsirwah Indonesia, sedangkan subjek penelitian meliputi pihak-pihak yang terlibat langsung dalam pengelolaan dan penggunaan sistem informasi, seperti manajemen, staf teknologi informasi, serta pengguna sistem. Subjek tersebut dipilih karena memiliki pemahaman dan peran penting dalam penerapan kebijakan serta prosedur keamanan sistem informasi.

Teknik Pengumpulan Data: Teknik pengumpulan data dalam penelitian ini dilakukan melalui beberapa metode, yaitu:

1. Wawancara, untuk memperoleh informasi terkait kebijakan, prosedur, serta praktik keamanan sistem informasi yang diterapkan di Tsirwah Indonesia.
2. Observasi, untuk mengamati secara langsung penerapan pengamanan sistem informasi dalam aktivitas operasional perusahaan.
3. Studi dokumentasi, dengan menelaah dokumen pendukung seperti kebijakan keamanan informasi, prosedur operasional standar, serta laporan terkait keamanan sistem.

Selain itu, digunakan kuesioner yang disusun berdasarkan proses-proses pada domain DSS05 COBIT 5 untuk mengukur tingkat kematangan tata kelola keamanan sistem informasi

Tahapan penelitian diawali dengan identifikasi permasalahan, yaitu belum adanya evaluasi terstruktur terhadap tata kelola keamanan sistem informasi di Tsirwah Indonesia. Selanjutnya dilakukan studi literatur untuk memahami konsep tata kelola TI, keamanan sistem informasi, serta framework COBIT 5 domain DSS05. Tahap berikutnya adalah pengumpulan data melalui wawancara, observasi, dokumentasi, dan kuesioner.

Data yang diperoleh kemudian dianalisis dengan cara memetakan kondisi eksisting organisasi terhadap proses-proses yang terdapat dalam domain DSS05. Hasil pemetaan digunakan untuk mengukur tingkat kematangan (*maturity level*) setiap proses keamanan sistem informasi. Setelah itu dilakukan analisis kesenjangan (*gap analysis***)** antara tingkat kematangan saat ini dengan tingkat yang diharapkan. Tahap akhir adalah penyusunan rekomendasi perbaikan guna meningkatkan tata kelola keamanan sistem informasi secara berkelanjutan.

Teknik Analisis Data : Teknik analisis data dilakukan dengan menghitung nilai rata-rata hasil kuesioner untuk menentukan tingkat kematangan masing-masing proses DSS05 berdasarkan skala maturity level COBIT 5, yaitu dari level 0 (*Incomplete*) hingga level 5 (*Optimized)*. Hasil analisis disajikan dalam bentuk tabel dan grafik untuk mempermudah interpretasi, kemudian dianalisis secara deskriptif untuk menarik kesimpulan dan merumuskan rekomendasi

4. HASIL DAN PEMBAHASAN

Hasil Identifikasi Permasalahan

Tahap awal dilakukan dengan mengidentifikasi permasalahan keamanan sistem informasi di Tsirwah Indonesia. Berdasarkan observasi dan wawancara, ditemukan bahwa perusahaan sangat bergantung pada sistem informasi untuk mendukung layanan pemberitaan online kepada masyarakat. Ketergantungan ini menuntut tingkat keamanan sistem informasi yang tinggi, khususnya pada aspek ketersediaan layanan. Insiden *Distributed Denial of Service* (DDoS) Attack yang terjadi menunjukkan adanya kelemahan dalam pengelolaan layanan keamanan sistem informasi, sehingga diperlukan evaluasi tata kelola keamanan secara terstruktur menggunakan kerangka kerja yang standar.

Studi Literatur dan Penentuan Domain Evaluasi

Berdasarkan studi literatur yang telah dilakukan, framework COBIT 5 dipilih sebagai kerangka kerja evaluasi tata kelola teknologi informasi karena mampu memberikan panduan komprehensif dalam pengelolaan TI. Penelitian ini difokuskan pada domain DSS05 (*Manage Security Services*) karena domain tersebut secara langsung berkaitan dengan pengelolaan keamanan sistem informasi, meliputi perlindungan terhadap malware, manajemen keamanan jaringan, pengendalian identitas dan akses, serta penanganan insiden keamanan. Penentuan domain DSS05 dinilai relevan dengan permasalahan keamanan yang dihadapi oleh Tsirwah Indonesia.

Pengumpulan Data

Pengumpulan data dilakukan sesuai dengan tahapan metode penelitian melalui wawancara dengan pihak manajemen dan tim IT, observasi terhadap infrastruktur dan operasional sistem informasi, studi dokumentasi kebijakan keamanan, serta penyebaran kuesioner berbasis COBIT 5 domain DSS05. Data yang diperoleh mencerminkan kondisi aktual penerapan keamanan sistem informasi di Tsirwah Indonesia dan menjadi dasar dalam proses analisis tingkat kematangan tata kelola keamanan.

Pemetaan Proses DSS05

Berdasarkan data yang telah dikumpulkan, dilakukan pemetaan kondisi eksisting terhadap proses-proses pada domain DSS05. Hasil pemetaan menunjukkan bahwa Tsirwah Indonesia telah menerapkan beberapa praktik pengelolaan keamanan, seperti penggunaan firewall, pengaturan hak akses pengguna, serta mekanisme dasar penanganan insiden keamanan. Namun, sebagian besar proses tersebut belum sepenuhnya terdokumentasi secara formal dan belum dilengkapi dengan prosedur evaluasi berkala, sehingga konsistensi penerapannya masih perlu ditingkatkan.

Pengukuran Tingkat Kematangan

Tahap selanjutnya adalah pengukuran tingkat kematangan tata kelola keamanan sistem informasi berdasarkan hasil kuesioner. Pengukuran dilakukan dengan

mengacu pada model tingkat kematangan COBIT 5, yaitu level 0 (Incomplete) hingga level 5 (Optimized). Hasil pengukuran menunjukkan bahwa tingkat kematangan tata kelola keamanan sistem informasi di Tsirwah Indonesia berada pada level 3 (Established) dan level 4 (Predictable).

Tabel 1 Ringkasan Tingkat Kematangan

Domain	Subdom	Keterangan	Maturity Score	Ket
DSS05	DSS 05.01	Protect against malware	3,75	3 - Established
	DSS 05.02	Manage network and connectivity security	3,85	3 – Established
	DSS 05.03	Manage endpoint security	3,96	3 – Established
	DSS 05.04	Manage user identity and logical access	4,20	4 – Predictable
	DSS 05.05	Manage physical access to IT assets	4,42	4 – Predictable
	DSS 05.06	Manage sensitive documents and output devices	4,19	4 – Predictable
	DSS 05.07	Monitor the infrastructure for security-related events	3,88	3 – Established

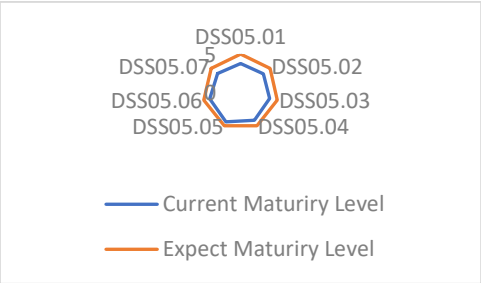
Analisis Kesenjangan (*Gap Analysis*)

Analisis kesenjangan dilakukan dengan membandingkan tingkat kematangan saat ini dengan tingkat kematangan yang diharapkan, yaitu level 5 (Optimized). Hasil analisis menunjukkan adanya kesenjangan pada seluruh subdomain DSS05, terutama pada aspek otomasi pengendalian keamanan, dokumentasi kebijakan yang terintegrasi, serta pemanfaatan indikator kinerja keamanan secara berkelanjutan. Kesenjangan ini menunjukkan bahwa Tsirwah Indonesia masih memerlukan peningkatan pada aspek proses dan teknologi untuk mencapai tata kelola keamanan yang optimal.

Berdasarkan seluruh tahapan penelitian yang telah dilakukan, dapat disimpulkan bahwa Tsirwah Indonesia telah memiliki dasar tata kelola keamanan sistem informasi yang cukup baik, ditunjukkan dengan capaian level 3 dan 4 pada domain DSS05. Namun, insiden keamanan yang pernah terjadi serta hasil gap analysis mengindikasikan perlunya peningkatan berkelanjutan. Peningkatan tersebut dapat dilakukan melalui penyempurnaan kebijakan dan prosedur keamanan, peningkatan kompetensi sumber daya manusia, serta penerapan teknologi keamanan yang lebih terintegrasi dan proaktif. Hasil penelitian ini selaras dengan tujuan penelitian, yaitu memberikan gambaran tingkat kematangan tata kelola keamanan sistem informasi serta rekomendasi perbaikan yang dapat diterapkan oleh Tsirwah Indonesia

Tabel 2 Analisis Kesenjangan (*GAP Analysis)*

Domain	Subdomain	Current Maturity	Expect Maturity	Gap
DSS05	DSS05.01	3,75	5	1,25
	DSS05.02	3,85	5	1,15
	DSS05.03	3,96	5	1,04
	DSS05.04	4,2	5	0,8
	DSS05.05	4,42	5	0,58
	DSS05.06	4,19	5	0,81
	DSS05.07	3,88	5	1,12



Gambar 1 Grafik Analisis Kesenjangan

Dari gambar grafik 2 terlihat jelas bahwa terdapat kesenjangan (gap) antara nilai kematangan saat ini dengan nilai kematangan yang diharapkan. Dengan adanya kesenjangan (gap) tersebut di butuhkan rekomendasi agar nilai maturity level dapat meningkat sesuai dengan tingkat kematangan yang diharapkan

Rekomendasi

Setelah tingkat kematangan (maturity level) ditetapkan, dilakukan penyusunan rekomendasi untuk meningkatkan tata kelola keamanan sistem informasi di Tsirwah Indonesia, sebagai berikut:

a. Perlindungan Malware (DSS05.01)
   Melakukan pemindaian virus dan pembaruan antivirus secara rutin pada seluruh perangkat. Selain itu, diperlukan pelatihan berkala bagi tim IT minimal satu kali per tahun untuk meningkatkan kompetensi keamanan informasi.
b. Keamanan Jaringan dan Konektivitas (DSS05.02)
   Menerapkan prosedur dan kontrol keamanan jaringan guna memastikan data yang dikirim dan diterima melalui jaringan berada pada jalur koneksi yang aman.
c. Keamanan *Endpoint* (DSS05.03)
   Mengamankan seluruh endpoint, seperti laptop, server, dan perangkat jaringan, sesuai kebijakan keamanan dan privasi informasi yang berlaku.
d. Manajemen Identitas dan Akses (DSS05.04)
   Mengatur hak akses pengguna sesuai kebutuhan bisnis, menerapkan prosedur identifikasi, autentikasi, dan otorisasi, serta melakukan peninjauan akses secara berkala.
e. Pengamanan Akses Fisik Aset TI (DSS05.05)
   Menggunakan layanan server yang aman dan membatasi akses fisik hanya kepada pihak berwenang, disertai pencatatan akses secara terkontrol.
f. Pengelolaan Dokumen Sensitif dan Perangkat Keluaran (DSS05.06)
   Membatasi akses terhadap dokumen sensitif, seperti formulir pendaftaran santri dan peserta pelatihan, hanya kepada pihak yang berwenang sesuai kebijakan keamanan informasi.
g. Pemantauan Infrastruktur Keamanan (DSS05.07)
   Menerapkan alat pemantauan keamanan, seperti sistem deteksi intrusi, untuk mengawasi aktivitas tidak sah serta mengintegrasikannya dengan sistem pemantauan dan manajemen insiden.

5. KESIMPULAN

Berdasarkan hasil pembahasan mengenai evaluasi tata kelola keamanan sistem informasi di Tsirwah Indonesia menggunakan framework COBIT 5 pada domain DSS05 (*Manage Security Services*), dapat disimpulkan bahwa penerapan tata kelola keamanan sistem informasi telah berjalan dengan cukup baik. Hal ini ditunjukkan dari hasil pengukuran tingkat kematangan yang berada pada level 3 (*Established)* dan level 4 (*Predictable*), yang menandakan bahwa proses keamanan telah terdokumentasi dan dilaksanakan secara konsisten.

Meskipun demikian, hasil analisis kesenjangan menunjukkan masih adanya perbedaan antara kondisi saat ini dengan

tingkat kematangan yang diharapkan, yaitu level 5 (*Optimized*). Kesenjangan tersebut terutama terdapat pada aspek dokumentasi kebijakan keamanan yang terintegrasi, pemantauan keamanan secara berkelanjutan, serta optimalisasi pengelolaan insiden dan pengamanan infrastruktur.

Berdasarkan hasil tersebut, disusun rekomendasi perbaikan pada setiap subdomain DSS05 yang mencakup perlindungan terhadap malware, pengelolaan keamanan jaringan, pengamanan *endpoint*, manajemen identitas dan akses, pengamanan akses fisik, pengelolaan dokumen sensitif, serta pemantauan infrastruktur keamanan. Implementasi rekomendasi ini diharapkan dapat meningkatkan efektivitas tata kelola keamanan sistem informasi dan meminimalkan risiko keamanan di Tsirwah Indonesia.

REFERENSI

Akmal, F. P. (2024). Kajian Literatur (Systematic Literature Review): IT Risk Management pada Perusahaan. . *Scientica: Jurnal Ilmiah Sains dan Teknologi, 2(1), 233–247. https://jurnal.kolibi.org/index.ph*.

Ayu, D. F. (2025). Evaluation of Information Security Management Capability Level with COBIT 5. *Journal bit-Tech, 8(1), 726–737. https://doi.org/10.32877/bt.v8i1.2682*.

Chai, K. Y. (2021). Review on Confidentiality, Integrity and Availability in Information Security. . *Journal of ICT in Education, 8(2).*

De Haes, S. V. (2020). *Enterprise governance of information technology: Achieving alignment and value (2nd ed.).* . Springer. https://doi.org/10.1007/978-3-030-25918-1.

Fatimah, N. O. (2023). Analisis tata kelola keamanan informasi menggunakan framework COBIT 5 di Perpustakaan Daerah Kota Banjarmasin. . *Jurnal Pendidikan Tambusai, 7(3), 29526–29529. https://doi.org/10.*

Hadi, M. Z. (2024). Audit sistem informasi layanan publik berbasis COBIT 5 domain DSS untuk meningkatkan kualitas pelayanan digital. . *Jurnal Sistem Informasi dan Teknologi Era. https://doi.org/10.71094/sitera.v1i1.54*.

Jannah, R. M. (2025). Evaluasi tingkat kapabilitas tata kelola keamanan teknologi informasi di SDIT Al-Fatih Peusangan dengan menggunakan framework COBIT 2019. *Jurnal Teknologi Terapan & Sains, 6(2). https://doi.org/10.29103/tt*.

Jones, N. W. (2025). A CIA Triad-Based Taxonomy of Prompt Attacks on Large Language Models. . *Future Internet, 17(3), 113*.

Putra, A. P. (2024). Audit sistem informasi jurnal menggunakan framework COBIT 5 pada domain DSS01 dan DSS05. . *Jurnal*

Komputer Teknologi Informasi Sistem Informasi (JUKTISI), 3(1), 649–658. https://doi.org/10.6271.

Rahayu, R. M. (2025). Audit tata kelola TI pada Bappeda dengan COBIT 5 domain DSS. . *Sisfo: Jurnal Ilmiah Sistem Informasi. https://doi.org/10.29103/sisfo.v4i2.6295*.

Rahman, M. M. (2024). AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and cybersecurity risk assessment. *Journal of Information Security, 15, 1–24. https://www.scirp.org/pdf/jis2024154_107801045.pdf*.

Rosmalina & Alhabib, I. S. (2023). Audit sistem informasi perpustakaan berbasis web SLiMS di MAN 1 Bandung menggunakan framework COBIT 5. . *J-SIKA: Jurnal Sistem Informasi Karya Anak Bangsa, 5(2), 97–109. https://ejournal.unibba.ac.id/index.php/j-sika/artic*.

Rosmalina., &. S. (2019). Audit teknologi informasi menggunakan framework COBIT 5: Studi kasus pada MA Persis 20 Ciparay. *J-SIKA: Jurnal Sistem Informasi Karya Anak Bangsa, 1(1), 1–15. https://ejournal.unibba.ac.id/index.php/j-sika/artic*.

Susanto, H. A. (2021). Toward a cybersecurity maturity model for organizations. . *Journal of Information Security and Applications, 58, 102712. https://doi.org/10.1016/j.jisa.2021.102712*.

Whitman, M. E. (2021). *Principles of information security (7th ed.).* Cengage Learning.