Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

AUDIT TEKNOLOGI INFORMASI MENGGUNAKAN ITIL VERSI 4

Wahyu Hudaya[1*], Cahyani Budihartanti[2]

Program Studi Sistem Informasi
Fakultas Teknologi Informasi
Universitas Nusa Mandiri

Correspondent Email: wahyuhudaya36@gmail.com

Author Email: wahyuhudaya36@gmail.com[1],
cahyani.cbh@nusamandiri.ac.id[2]

Received: September 12, 2025**. Revised:** October 10, 2025**. Accepted:** October 13,20025**. Issue Period:** Vol.9 No.4 (2025), Pp.1370-1380

Abstrak: Perkembangan teknologi informasi menuntut jaringan internet dan intranet yang aman, stabil, dan andal untuk mendukung operasional PT XYZ. Penelitian studi kasus ini menganalisis efektivitas FortiGate Firewall serta keselarasan pengelolaannya dengan ITIL V4. Audit difokuskan pada domain Service Management Practices dengan delapan subdomain: Information Security Management, Incident Management, Problem Management, Monitoring & Event Management, Change Control, Service Continuity Management, Service Request Management, dan Service Desk. Metode penelitian menggunakan observasi, wawancara, dokumentasi, dan kuesioner Likert kepada enam responden. Tingkat kematangan diukur dengan ITIL V4 Maturity Model. Hasil menunjukkan kekuatan pada aspek teknis, yaitu Information Security Management dan Monitoring & Event Management berada pada Level 4, sedangkan Service Desk pada Level 3. Kesenjangan terbesar terdapat pada lima praktik yang masih di Level 2, menunjukkan kelemahan pada aspek pengelolaan dan kurangnya SOP. Rekomendasi mencakup implementasi sistem ticketing terpusat, penguatan Change Control, peningkatan Service Continuity melalui pencadangan konfigurasi dan uji pemulihan bencana, serta penerapan SOP Problem Management dan standarisasi Service Request Management. Penelitian ini berkontribusi dalam penguatan keamanan jaringan berbasis FortiGate yang terintegrasi dengan tata kelola TI ITIL V4, serta menawarkan strategi perbaikan bertahap menuju tingkat kematangan yang lebih tinggi.

Kata kunci: Fortigate Firewall, keamanan jaringan, ITIL V4, sistem informasi, PT XYZ.

Abstract: *The rapid development of information technology requires secure, stable, and reliable internet and intranet networks to support the operations of PT XYZ. This case study analyzes the effectiveness of the FortiGate Firewall and its alignment with ITIL V4 governance. The audit focuses on the Service Management Practices domain with eight relevant subdomains: Information Security Management, Incident Management, Problem Management, Monitoring & Event Management, Change Control, Service Continuity Management, Service Request Management, and Service Desk. The research method applies a mixed approach through observation,*

DOI: 10.52362/jisamar.v9i4.2063

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

interviews, documentation, and a Likert-scale questionnaire administered to six respondents. The maturity level was assessed using the ITIL V4 Maturity Model. The findings indicate strengths in the technical aspects, with Information Security Management and Monitoring & Event Management achieving Level 4, and Service Desk at Level 3. However, five practices remain at Level 2, highlighting weaknesses in management processes and the absence of formal SOPs. Recommendations include implementing a centralized ticketing system, strengthening Change Control, enhancing Service Continuity with scheduled configuration backups and disaster recovery tests, applying SOPs for Problem Management, and standardizing Service Request Management. This study contributes to strengthening network security based on the FortiGate Firewall integrated with ITIL V4 service governance, offering step-by-step improvements toward higher maturity level.

Keywords: *Fortigate Firewall, network security, ITIL V4, information systems, PT XYZ*

I. PENDAHULUAN

PT XYZ adalah BUMN terbesar di Indonesia yang memiliki peran strategis dalam memberikan pelayanan kepada konsumen mulai dari masyarakat umum hingga sektor industri dan perkantoran. Perkembangan teknologi informasi yang begitu cepat saat ini telah memberikan dampak signifikan terhadap sektor energi, termasuk pada sistem distribusi listrik yang dikelola PT XYZ. Dalam era digitalisasi, kebutuhan akan jaringan internet dan intranet yang aman, stabil, dan andal menjadi semakin krusial untuk mendukung kelancaran operasional perusahaan.

Namun, seiring dengan meningkatnya ketergantungan pada layanan berbasis TI, ancaman siber terhadap sistem jaringan PT XYZ juga semakin kompleks dan beragam. Serangan tidak hanya menyasar infrastruktur fisik, tetapi juga menargetkan pencurian data, perusakan sistem informasi internal, hingga mengganggu keberlangsungan layanan digital. Gangguan semacam ini dapat berdampak serius pada proses bisnis PT XYZ, termasuk terhambatnya layanan administratif, komunikasi antarunit, dan bahkan koordinasi pelayanan publik. Kondisi ini menunjukkan bahwa keamanan jaringan bukan hanya sekadar persoalan teknis, tetapi juga menyangkut keandalan layanan organisasi di mata publik dan stakeholder[1],[2].

Sejumlah penelitian sebelumnya telah mengkaji efektivitas firewall maupun tata kelola TI berbasis ITIL V4, namun sebagian besar masih berfokus pada satu aspek tertentu. Fitrian et al. (2025) misalnya, menekankan bahwa Next-Generation Firewall (NGFW) memiliki keunggulan dibanding firewall tradisional dalam mendeteksi dan mencegah serangan siber yang lebih kompleks seperti DDoS, malware, dan ransomware[3]. Sementara itu, Fayola et al. (2024) menegaskan bahwa penerapan ITIL Service Operation dapat meningkatkan kualitas layanan melalui praktik incident management, problem management, dan service desk yang terbukti membantu organisasi lebih responsif dalam menangani gangguan layanan[4]. Lebih lanjut, penelitian Arbie & Raharjo (2024) menunjukkan bahwa penggunaan Fortigate dengan metode security profiles seperti web filtering, application control, dan network scheduling mampu menjaga stabilitas jaringan, membatasi akses yang tidak relevan, serta meningkatkan produktivitas pegawai[5].

Meskipun sudah ada banyak kajian terkait penggunaan firewall maupun penerapan ITIL V4, penelitian yang secara khusus menggabungkan perlindungan teknis Fortigate dengan kerangka tata kelola layanan TI masih jarang dilakukan, terutama di sektor energi. Padahal, kolaborasi antara aspek teknis dan manajerial menjadi hal yang penting, karena keamanan jaringan tidak cukup hanya berfokus pada pencegahan serangan, tetapi juga harus menjamin keberlangsungan layanan yang berkesinambungan serta mendukung perbaikan berkelanjutan. Berdasarkan hal tersebut, penelitian ini diarahkan untuk menelaah sejauh mana *Fortigate Firewall* efektif dalam menjaga keamanan jaringan internet dan intranet di PT XYZ, sekaligus menilai kesesuaian pengelolaannya dengan praktik ITIL V4. Hasil yang diperoleh diharapkan dapat memberikan manfaat praktis berupa rekomendasi penguatan keamanan jaringan internal PT XYZ, serta kontribusi akademis dengan menambah kajian literatur mengenai integrasi keamanan jaringan dan tata kelola layanan TI.

DOI: 10.52362/jisamar.v9i4.2063

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

II. METODE DAN MATERI

2.1 MATERI PENELITIAN

Audit Sistem Informasi

Audit sistem informasi merupakan proses pengumpulan dan evaluasi bukti untuk menilai sejauh mana sistem komputer mampu melindungi aset, menjaga integritas data, mendukung pencapaian tujuan organisasi, dan memastikan penggunaan sumber daya yang efisien[6]. Dalam penelitian ini audit difokuskan pada keamanan jaringan internet dan intranet PT XYZ, dengan dasar: meningkatnya ancaman siber *(malware, phishing, brute-force, DDoS)*, kebutuhan proteksi berlapis, kepatuhan terhadap tata kelola TI berbasis ITIL V4, evaluasi efektivitas infrastruktur keamanan, serta peningkatan kepercayaan stakeholder [7],[8].

Keamanan Jaringan

Keamanan jaringan bertujuan menjaga integritas, kerahasiaan, dan ketersediaan data dari akses ilegal maupun gangguan. Fortinet mendefinisikan keamanan jaringan sebagai kombinasi teknologi, kebijakan, prosedur, dan manusia untuk melindungi infrastruktur komunikasi dari serangan siber[9]. Keamanan jaringan sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data yang sensitif. Sistem keamanan jaringan yang efektif dapat mencegah akses tidak sah dan serangan terhadap sistem informasi yang bersifat vital bagi organisasi[10].

Firewall

Firewall berfungsi memantau dan mengatur lalu lintas data berdasarkan kebijakan tertentu. Fungsinya antara lain menyaring paket data, mencegah serangan dari luar, mengatur akses internal-eksternal, dan melindungi data dari akses ilegal. Dalam organisasi besar, firewall juga digunakan untuk segmentasi jaringan dan mencegah kebocoran informasi[10].

Fungsi utama dari firewall itu sendiri antara lain:

1. Firewall dapat menentukan apakah paket data boleh melewati jaringan atau tidak berdasarkan kebijakan yan sudah di tetepakan.
2. Firewall dapat mencegah serangan dari luar dengan mengidentifikasi lalu lintas yang mencurigakan
3. Menjaga data agar tetap aman dari akses ilegal
4. Mengatur akses pengguna terhadap jaringan internal maupun eksternal

Fortigate

FortiGate merupakan perangkat jaringan yang dilengkapi dengan fitur keamanan canggih dan dikembangkan oleh perusahaan *Fortinet*. *Fortinet* sendiri adalah penyedia solusi keamanan jaringan berskala global, yang telah digunakan oleh banyak perusahaan besar, termasuk sebagian besar anggota Fortune Global 100 pada tahun 2009. *Fortinet* dikenal sebagai pemimpin dalam kategori unified threat management (UTM). Sebagai komponen utama dalam infrastruktur jaringan, FortiGate tidak hanya menyediakan perlindungan menyeluruh terhadap ancaman siber, tetapi juga berfungsi sebagai gateway serta router untuk jaringan lokal (LAN). Dengan demikian, penggunaan FortiGate dapat menghilangkan kebutuhan akan perangkat router tambahan atau load balancer, terutama saat menangani lebih dari satu koneksi WAN[11].

ITIL V4

ITIL merupakan kerangka praktik terbaik dalam manajemen layanan TI[12]. ITIL V4 menghadirkan konsep Service Value System (SVS) yang menekankan integrasi antar komponen organisasi, continual improvement, dan co-creation of value[13]. Dari 34 praktik ITIL V4, penelitian ini menekankan pada 8 subdomain relevan, yaitu:

1. Information Security Management
2. Incident Management
3. Problem Management
4. Monitoring & Event Management
5. Change Control
6. Service Continuity Management
7. Service Request Management

DOI: 10.52362/jisamar.v9i4.2063

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

8. Service Desk[14].

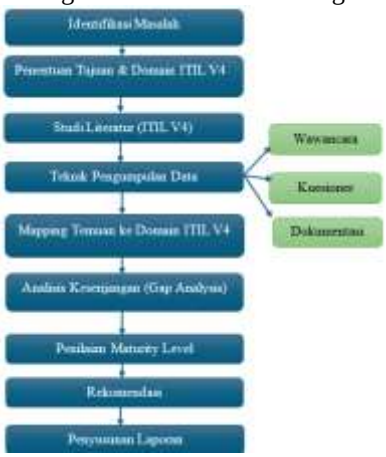
2.2 METODE PENELITIAN

Pendekatan

Penelitian ini menggunakan kombinasi pendekatan kualitatif deskriptif dan kuantitatif dengan metode studi kasus yang dilaksanakan di PT XYZ. Pemilihan pendekatan ini bertujuan untuk memperoleh gambaran mendalam mengenai kondisi nyata di lapangan terkait penerapan sistem keamanan jaringan *FortiGate Firewall*, sekaligus menilai tingkat kesesuaian penerapannya dengan kerangka kerja tata kelola layanan TI berbasis ITIL V4.

Tahap Penelitian

Tahap pelaksanaan penelitian dirancang secara sistematis dan digambarkan dalam gambar III.1 berikut ini:



Gambar 1 Tahap Penelitian

Teknik Pengumpulan Data

Tujuan dari tahap ini adalah untuk mengumpulkan data observasi yang mendalam dan relevan untuk mendukung proses analisis pada penelitian ini, berikut:

1. Wawancara, dilakukan secara semi terstruktur dengan staf TI untuk menggali konfigurasi *FortiGate*, kebijakan keamanan, dan praktik operasional dalam menghadapi serangan siber.
2. Kuesioner, dibagikan kepada responden terpilih dengan metode *purposive sampling* (staf TI dan manajemen) yang terlibat langsung dalam pengelolaan keamanan jaringan.
3. Dokumentasi, meninjau bukti objektif seperti konfigurasi *firewall*, *event log*, SOP, laporan insiden, dan kebijakan layanan untuk memvalidasi temuan wawancara dan kuesioner.

Setelah dilakukan pengumpulan data kemudian selanjutnya penilaian *mauturity level*, yaitu menilai tingkat kematangan dari implementasi manajemen keamanan jaringan yang sedang berjalan. Skala yang digunakan mengacu pada standar ITIL V4 *Maturity Model*, sebagai berikut:

Tabel 1 Penilaian *Maturity Level*

Skor Rata-rata	Level	Deskripsi
1.00-1.80	Level 1 (*Initial*)	Proses belum terdokumentasi dan dilakukan secara *ad hoc*.
1.81-2.60	Level 2 (*Repeatable*)	Proses telah dijalankan secara konsisten namun belum terdokumentasi secara formal.
2.61-3.40	Level 3 (*Defined*)	Proses telah terdokumentasi dan dijalankan sesuai prosedur.
3.41-4.20	Level 4 (*Quantitatively Managed*)	Proses dimonitor dan diukur menggunakan metrik tertentu.
4.21-5.00	Level 5 (*Optimizing*)	Proses dievaluasi secara berkelanjutan untuk perbaikan.

Sumber:[14]

DOI: 10.52362/jisamar.v9i4.2063

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

Penilaian ini dilakukan pada masing-masing subdomain ITIL V4 untuk mengetahui area yang sudah matang dan area yang masih perlu ditingkatkan.

Kerangka Audit

Dalam audit sistem informasi ini, evaluasi dilakukan dengan mengacu pada kerangka *Service Value System (SVS)* dari ITIL V4. SVS menggambarkan integrasi antara prinsip, tata kelola, praktik layanan, dan perbaikan berkelanjutan dalam menciptakan nilai layanan TI.

Gambar 2 Service Value System ITIL V4

Sumber:[15]

Seperti ditunjukkan pada Gambar II.2, kerangka kerja ITIL v4 berpusat pada *Service Value System (SVS).* Dalam penelitian ini, evaluasi difokuskan pada delapan subdomain praktik yang telah ditetapkan sebelumnya, yang merupakan komponen kunci dalam SVS. Pemetaan temuan terhadap kedelapan praktik ini bertujuan untuk menilai sejauh mana penerapan keamanan jaringan PT XYZ telah sejalan dengan prinsip tata kelola layanan TI yang tersutruktur dan berbasis nilai.

III. PEMBAHASA DAN HASIL

3.1. Analisa dan Rancangan Audit Sistem Informasi

Analisis dan rancangan audit sistem informasi dalam penelitian ini disusun berdasarkan kerangka kerja ITIL versi 4 *(Information Technology Infrastructure Library V4), y*ang merupakan *framework* praktik terbaik dalam manajemen layanan teknologi informasi *(IT Service Management)*. Kerangka kerja ini dipilih karena menyediakan pendekatan yang tidak hanya fokus pada aspek teknis, tetapi juga mencakup nilai layanan, proses bisnis, serta siklus perbaikan berkelanjutan *(continual improvement).* Evaluasi diarahkan pada delapan subdomain utama: *Information Security Management, Incident Management, Problem Management, Monitoring & Event Management, Change Control, Service Request Management, Service Continuity Management,* dan *Service Desk*.

3.2. Profil Responden

Responden penelitian terdiri dari enam pegawai bagian TI PT XYZ yang dipilih dengan metode *purposive sampling:*

Tabel 2 Responden Penelitian

Kode Responden	Jabatan	Bagian
MAN	Manager TI	Manajemen TI
AMN	Asisten Manager TI	Manajemen TI
Infra 1	Administator Infrastruktur	Sub Bidang Infrastruktur
Infra 2	Administator Infrastruktur	Sub Bidang Infrastruktur
Te 1	Staf Teknis TI	Sub Bidang Infrastruktur

DOI: 10.52362/jisamar.v9i4.2063

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

Te 2	Staf Teknis TI	Sub Bidang Infrastruktur

Sumber: Sub Bidang TI PT XYZ

3.3. Domain Praktik ITIL V4

Dalam konteks penelitian ini, kerangka audit mengacu pada domain praktik *(practice domains)* ITIL V4 yang paling berkaitan dengan keamanan jaringan dan efektivitas pengelolaan insiden. Delapan subdomain yang dijadikan kerangka audit meliputi:

Tabel 3 Subdomain Praktik ITIL V4

***Subdomain* ITIL V4**	**Tujuan Evaluasi**
Information Security Management	Mengelola risiko keamanan informasi secara menyeluruh agar kerahasiaan, integritas, dan ketersediaan data tetap terjaga.
Incident Management	Menangani insiden layanan TI secara cepat untuk meminimalkan dampak terhadap bisnis.
Problem Management	Mengidentifikasi akar penyebab insiden itu terjadi secara berulang serta pencegahannya.
Monitoring and Event Management	Mengidentifikasi dan merespons peristiwa yang berdampak pada layanan TI secara proaktif.
Change Control	Menjamin bahwa seluruh perubahan pada infrastruktur TI dilakukan secara terkendali dan terdokumentasi.
Service Request Management	Mengelola permintaan standar user, seperti aktivasi akses layanan.
Service Continuity Management	Menyusun strategi pemulihan dan ketersediaan layanan TI ketika terjadi gangguan besar atau bencana.
Servic Desk	Memberikan titik kontak pusat bagi user dalam pelaporan gangguan maupun permintaan layanan.

Sumber: Pengolahan Data

3.4. Hasil Tingkat Kematangan

Langkah awal analisis adalah mengolah data kuesioner menjadi informasi terstruktur untuk dibandingkan antar subdomain. Instrumen **Checklist ITIL V4** digunakan untuk memetakan kondisi lapangan berdasarkan indikator. Enam responden dari tim IT mengisi kuesioner dengan skala Likert 5 poin:

1 = Tidak Pernah
2 = Jarang Dilakukan
3 = Kadang-Kadang
4 = Sering Dilakukan
5 = Selalu Dilakukan

Berikut Tabel 4 adalah hasil pemetaan untuk menjadi dasar perhitungan:

Tabel 4 Hasil Pengisian Instrumen Audit *Checklist*

No	**Subdomain ITIL V4**	**Pertanyaan**	**Responden**					
			MAN	**AMN**	**Infra 1**	**Infra 2**	**Te 1**	**Te 2**
1	Information Security Management	Apakah kebijakan keamanan telah disosialisasikan?	4	4	4	4	4	4
2	Information Security Management	Apakah Fortigate dikonfigurasi berdasarkan	5	5	5	5	4	4

DOI: 10.52362/jisamar.v9i4.2063

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

		klasifikasi risiko?						
3	Incident Management	Apakah pencatatan insiden terdokumentasi?	4	4	3	3	2	2
4	Incident Management	Apakah tersedia alur eskalasi formal dalam penanganan insiden?	2	2	1	1	2	1
5	Monitoring and Event Management	Apakah telah terintegrasi log terpusat?	5	5	5	5	4	4
6	Monitoring and Event Management	Apakah terdapat rotasi log otomatis?	4	4	4	4	4	4
7	Change Control	Apakah perubahan konfigurasi terdokumentasi secara formal?	3	2	2	2	2	2
8	Change Control	Apakah tersedia SOP dan alur persetujuan?	2	2	2	2	2	2
9	Service Continuity Management	Apakah pengujian pemulihan berkala?	3	3	3	3	2	2
10	Service Continuity Management	Apakah backup konfigurasi otomatis?	1	1	1	2	2	2
11	Problem Management	Apakah ada prosedur identifikasi akar masalah secara formal?	2	2	2	2	2	2
12	Problem Management	Apakah dokumentasi problem record dilakukan dan digunakan sebagai pembelajaran?	4	4	3	3	3	3
13	Service Request Management	Apakah permintaan layanan tercatat dan diproses terpusat?	2	2	1	1	1	2
14	Service Request Management	Apakah ada kategori standar untuk jenis permintaan layanan?	4	4	3	4	3	3
15	Service Desk	Apakah sudah tersedia sistem helpdesk?	4	4	4	4	4	4
16	Service Desk	Apakah ada SLA atau waktu tanggap standar permintaan?	4	4	2	3	2	2

Sumber: Pengolahan Data

Setelah hasil kuesioner dipetakan pada masing-masing indikator, langkah berikutnya adalah menghitung tingkat kematangan dari setiap subdomain ITIL V4. Setiap subdomain terdiri atas dua indikator penilaian. Jawaban responden kemudian dikonversi menjadi skor numerik, dirata-rata untuk memperoleh nilai per indikator, dan selanjutnya dihitung kembali menjadi nilai rata-rata per subdomain. Nilai ini kemudian dikonversi ke dalam level kematangan sesuai rentang yang telah ditentukan.

Perhitungan dilakukan dengan tahapan sebagai berikut:

1. Setiap indikator dinilai dengan skala Likert 1–5 (1 = terendah, 5 = tertinggi).
2. Skor rata-rata indikator dihitung dengan rumus:

$$\textbf{Skor Rata} - \textbf{rata Indikator} = \frac{\sum \textbf{Skor Responden}}{n}$$

3. Dua skor indikator dijumlahkan lalu dirata-rata untuk memperoleh skor subdomain:

Skor rata-rata subdomain = (Skor Indikator 1 + Skor Indikator 2) / 2

4. Skor subdomain dikonversi ke Level Kematangan berdasarkan tabel acuan.

DOI: 10.52362/jisamar.v9i4.2063

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

5. Gap dihitung dengan formula:

Gap = Target Level (4) – Level saat ini

.

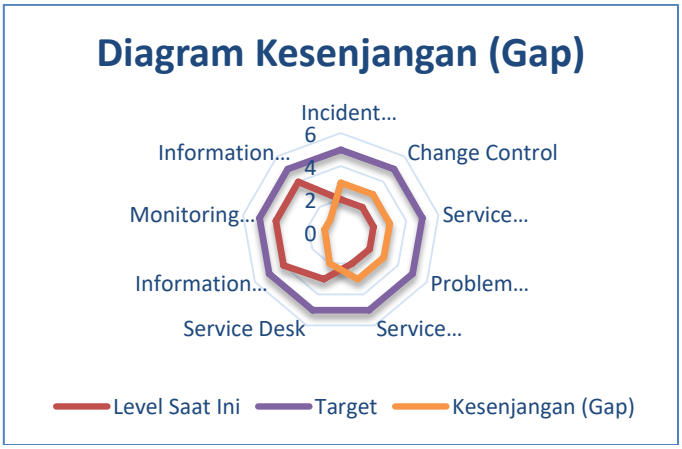
Seluruh hasil perhitungan kemudian dirangkum dalam tabel III.4 hasil evaluasi sebagai dasar analisis kesiapan manajemen layanan TI di PT XYZ.

Tabel 5 Hasil Perhitungan Kematangan dan Analisis Kesenjangan

***Sub Domain* ITIL V4**	**Jumlah Indikator**	**Skor rata - rata Indikator 1**	**Skor rata-rata Indikator 2**	**Skor Rata – rata subdomain**	**Kematangan Saat ini**	**Target**	**Kesenjangan (Gap)**
Information Security Management	2	4	5	4.5	Level 4	Level 5	1
Incident Management	2	3.5	1.5	2.5	Level 2	Level 5	3
Monitoring and Event Management	2	4.83	4	4.42	Level 4	Level 5	1
Change Control	2	2.17	2	2.08	Level 2	Level 5	3
Service Continuity Management	2	2.67	1.5	2.08	Level 2	Level 5	3
Problem Management	2	2	3.33	2.67	Level 2	Level 5	3
Service Request Management	2	1.67	3.33	2.5	Level 2	Level 5	3
Service Desk	2	4	2.83	3.42	Level 3	Level 5	2

Sumber: Pengolahan Data

Berikut adalah gambaran visual yang lebih jelas mengenai hasil analisis kesenjangan data pada tabel di atas disajikan dalam bentuk diagram pada gambar III.1:



Gambar 3 Diagram Analisis Kesenjangan

3.5. Pembahasan Temuan dan rekomendasi

DOI: 10.52362/jisamar.v9i4.2063

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.4 (November 2025)

Analisis hasil audit menunjukkan bahwa akar permasalahan keamanan jaringan di PT XYZ bukan pada keterbatasan teknologi, melainkan pada aspek pengelolaan dan proses. Meskipun FortiGate Firewall telah tersedia, pemanfaatannya belum optimal karena kurangnya SOP, dokumentasi, dan kontrol yang konsisten. Oleh karena itu, rekomendasi difokuskan tidak hanya pada aspek teknis, tetapi juga pada penguatan tata kelola layanan TI, dengan prioritas ditentukan berdasarkan besar kesenjangan di tiap subdomain.

Tabel 6 Ringkasan Rekomendasi Berdasarkan Prioritas

Prioritas	Subdomain (Gap)	Rekomendasi Strategis
Tinggi	*Incident Management* (3)	1. Mengimplementasikan sistem *ticketing* untuk pencatatan insiden terpusat. 2. Penyusunan SOP penanganan insiden yang mencakup eskaliasi formal. 3. Mengintegrasikan *alert* dari *FortiAnalyzer* ke sistem *ticketing* untuk respon otomatis.
Tinggi	*Change Control* (3)	1. Mewajibkan penggunaan formulir permintaan perubahan untuk ketika ada konfigurasi yang akan dirubah 2. Menetapkan alur persetujuan yang jelas dan terdokumentasi 3. Mengaktifkan fitur audit Trail di *Fortigate* untuk akuntabilitas
Tinggi	*Service Continuity Management* (3)	1. Mengaktifkan fitur *Backup Scheduler* pada *Fortigate* untuk otomatis *backup* konfigurasi. 2. Merencanakan dan melaksanakan simulasi backup secara rutin.
Tinggi	*Problem Management* (3)	1. Buat SOP identifikasi akar masalah 2. Penerapan dokumentasi problem record sebagai sarana pembelejaran.
Tinggi	*Service Request Management* (3)	1. Penerapan sistem manajemen permohonan layanan 2. Kategorisasi standar untuk jenis permintaan
Menengah	*Service Desk* (2)	1. Tambahkan SLA respon dan eskalasi waktu penanganan. 2. Sosialisasi penggunaan *Helpdesk* sebagai pintu utama permintaan pelayanan.
Rendah	*Information Security Management* (1)	1. Menyelenggarakan sesi sosialisasi dan pelatihan kebijakan keamanan secara berkala. 2. Melakukan audit konfigurasi secara berkala.
Rendah	*Monitoring and Event Management* (1)	1. Melakukan optimalisasi *(fine-tuning)* pada *threshold alert* di *FortiAnalyzer* untuk akurasi deteksi. 2. Mengembangkan *Dashboard* khusus untuk laporan manajemen yang menampilkan metrik keamanan.

Sumber: Pengolahan Data

Berdasarkan analisis gap dan tingkat kematangan, rekomendasi strategis disusun untuk tiap subdomain dengan prioritas sesuai besarnya kesenjangan. Subdomain dengan gap 3 poin mendapat prioritas tinggi, sedangkan *Service Desk*, *Information Security Management*, dan *Monitoring & Event Management* menjadi prioritas menengah. Implementasi rekomendasi secara bertahap diharapkan meningkatkan pengelolaan keamanan jaringan dan layanan TI, sekaligus memperkuat penerapan tata kelola berbasis ITIL V4 guna mencapai level kematangan optimal serta ketahanan terhadap ancaman siber di masa depan.

IV. KESIMPULAN

DOI: 10.52362/jisamar.v9i4.2063

Audit sistem informasi keamanan jaringan di PT XYZ menggunakan kerangka ITIL V4 menunjukkan bahwa perangkat *FortiGate Firewall* telah memberikan perlindungan teknis yang memadai. Hal ini tercermin pada praktik *Information Security Management* dan *Monitoring & Event Management* yang mencapai Level 4 (*Managed*), serta *Service Desk* pada Level 3 (*Defined*).

Namun, terdapat lima praktik utama *Incident Management, Change Control, Service Continuity Management, Problem Management,* dan *Service Request Management* yang masih berada pada Level 2 (*Repeatable*). Kondisi ini menandakan bahwa kelemahan utama bukan terletak pada teknologi, melainkan pada aspek manajerial, yaitu ketiadaan SOP, dokumentasi formal, serta mekanisme kontrol yang konsisten. Dengan demikian, integrasi antara teknologi *FortiGate* dan tata kelola ITIL V4 masih dalam tahap awal dan memerlukan perbaikan sistematis.

REFERENSI

[1] A. Riduan and N. Sadikin, "Perancangan firewall menggunakan Fortigate di PT Swadharma Duta Data," *Jurnal Teknologi Informasi*, vol. 5, no. 2, pp. 45–52, 2023.

[2] "Analisis Potensi Ancaman Siber pada Bidang Ekonomi di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional*, vol. 7, no. 1, Jun. 2024, doi: 10.7454/jkskn.v7i1.10089.

[3] H. P. Fitrian, B. Fajri Noorjamil, F. Rahmawati, and S. A. Rachman, "Analisis Efektivitas Firewall dalam Memfilter dan Melindungi Lalu Lintas Jaringan," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 8, no. 1, pp.95-102,Feb. 2025.

[4] A. Fayola, R. Darianty, and A. Maulana, "Implementation and Impacts of ITIL Service Operation Within The Telecommunication Industry," *International Journal of Computer Science and Information Technology (IJISIT)*, vol. 1, no. 1, pp. 31–40, 2024, doi: 10.55123/ijisit.

[5] F. R. Arbie and M. Raharjo, "Implementasi keamanan jaringan dengan metode security profiles menggunakan Fortigate pada Komisi Aparatur Sipil Negara," *Jurnal Informatika Terpadu*, vol. 10, no. 1, pp. 27–34, 2024, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[6] S. Ratna, *Audit Sistem Informasi*. Banjarmasin: Yayasan Kita Menulis, Jun. 2023. ISBN 978-623-342-860-6.

[7] FIKTI UMSU, "Audit Sistem Informasi: Pengertian, Tujuan, Jenis dan Tahapan." [Online]. Available: https://fikti.umsu.ac.id/audit-sistem-informasi-pengertian-tujuan-jenis-dan-tahapan/. [Accessed: May 03, 2025].

[8] D. Herlinudinkhaji and L. Kurnia Ramadhani, "Tata Kelola Layanan Teknologi Informasi dengan ITIL V4 untuk Estimasi Layanan," *Remik*, vol. 7, no. 1, pp. 452–457, Jan. 2023, doi: 10.33395/remik.v7i1.12058.

[9] R. Aryandi, "Implementasi manajemen bandwidth dan firewall pada router Mikrotik untuk optimalisasi hotspot publik dan kontrol akses internet di lingkungan SMKN 1 Mesjid Raya," Skripsi, Fakultas Tarbiyah dan Keguruan, Program Studi Pendidikan Teknologi Informasi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, Indonesia, May 2024.

[10] S. L. Ajimoko, "The Importance of Network Security in Protecting Sensitive Data and Information," *ResearchGate*, 2024. [Online]. Available:

DOI: 10.52362/jisamar.v9i4.2063

https://www.researchgate.net/publication/382057178_The_Importance_of_Network_Security_in_Protecting_Sensitive_Data_and_Information

[11] E. D. Setiawan and M. Raharjo, "Implementasi Sistem Keamanan Jaringan Berbasis Fortigate," *Jurnal Informatika Terpadu*, vol. 9, no. 1, pp. 34–39, 2023, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[12] E. S. Negara and W. Nugraha, "Analisis layanan TI pada domain service operation dengan menggunakan framework ITIL V3," *JUSIM (Jurnal Sistem Informasi Musirawas)*, vol. 6, no. 2, pp. 123-136, Dec. 2021.

[13] A. H. Nuradira, N. Azizah, and J. Minardi, "Audit of Governance and Service Management of Unisnu Jepara's Library Information System (SIPERPUS) Using ITIL V4 Based on Website," *Scientific Journal of Informatics*, vol. 12, no. 1, pp. 31–42, May 2025, doi: 10.15294/sji.v12i1.19168.

[14] Axelos, *ITIL® Foundation: ITIL 4 Edition.* London, U.K.: TSO (The Stationery Office), 2019.

[15] Axelos Limited, "ITIL ® Foundation ITIL 4 Edition 2," 2019. [Online]. Available: https://www.axelos.com

DOI: 10.52362/jisamar.v9i4.2063