Jurnal Teknologi Informasi dan Multimedia

p-ISSN : 2715-2529

e-ISSN : 2684-9151

https://journal.sekawan-org.id/index.php/jtim

Assessment Manajemen Risiko Keamanan Sistem Informasi Menggunakan Framework ITIL V3 *Domain Service Operation*

Andi Sofyan Anas [1*], Rifqi Hammad [2], I Nyoman Switrayana [1], Muhammad Haris Nasri [3]

[1] Program Studi Ilmu Komputer, Universitas Bumigora, Indonesia
[2] Program Studi Rekayasa Perangkat Lunak, Universitas Bumigora, Indonesia
[3] Program Studi Teknologi Informasi, Universitas Bumigora, Indonesia

* Korespondensi: andi.sofyan@universitasbumigora.ac.id

Sitasi: A. S. Anas, R. Hammad, I. N. Switrayana, and M. H. Nasri, "Assessment Manajemen Risiko Keamanan Sistem Informasi Menggunakan Framework ITIL V3 Domain Service Operation", *Jurnal Teknologi Informasi Dan Multimedia*, vol. 8, no. 3, hlm. 524-534, 2026. https://doi.org/10.35746/jtim.v8i3.1037

Diterima: 19-05-2026
Direvisi: 23-06-2026
Disetujui: 30-06-2026

Abstract: Information system security is a critical aspect in supporting the continuity of information technology services, particularly in educational institutions that heavily rely on digital systems. This study aims to evaluate the maturity level of information system security risk management using the Information Technology Infrastructure Library (ITIL) V3 framework within the Service Operation domain. This research employs a quantitative approach with total sampling, involving 13 respondents who are directly engaged in information system management at the research site. Data were collected through questionnaires and interviews. The research instrument was developed based on four subdomains of ITIL V3 Service Operation: Event Management, Incident Management, Problem Management, and Access Management. Instrument validity was tested using the Pearson productmoment correlation, and reliability was measured using Cronbach's Alpha. The results indicate that the overall maturity level is 3.44, which falls into the Defined Process category (Level 3), approaching Managed and Measurable (Level 4). Event Management obtained the highest value at 3.88 (Level 4), followed by Access Management at 3.37 (Level 3), Incident Management at 3.32 (Level 3), and Problem Management at 3.21 (Level 3). Gap analysis reveals a discrepancy of 1.56 from the expected optimized condition at Level 5. These findings suggest that although processes have been implemented and documented, improvements are still required particularly in root cause analysis (Problem Management), access control (Access Management), and continuous performance evaluation. This study is expected to serve as a reference for enhancing IT service governance and information system security management based on ITIL practices.

Keywords: ITIL V3; information system security; service operation; maturity level; gap analysis

Abstrak: Keamanan sistem informasi merupakan aspek penting dalam mendukung keberlangsungan layanan teknologi informasi, khususnya pada institusi pendidikan yang memiliki ketergantungan tinggi terhadap sistem digital. Penelitian ini bertujuan untuk mengevaluasi tingkat kematangan manajemen risiko keamanan sistem informasi menggunakan *framework Information Technology Infrastructure Library (ITIL) V3* pada *domain Service Operation*. Penelitian ini menggunakan pendekatan kuantitatif dengan teknik total *sampling*, melibatkan 13 responden yang secara langsung terlibat dalam pengelolaan sistem informasi pada objek penelitian. Data dikumpulkan melalui kuesioner dan wawancara. Instrumen penelitian disusun berdasarkan empat subdomain ITIL V3 *Service Operation: Event Management, Incident Management, Problem Management,* dan *Access Management*. Validitas instrumen diuji menggunakan korelasi *product-moment Pearson*, dan reliabilitas diukur menggunakan *Cronbach's Alpha*. Hasil penelitian menunjukkan bahwa tingkat kematangan keseluruhan berada pada nilai rata-rata 3,44, yang termasuk dalam kategori *Defined Process* (*Level* 3) menuju *Managed and Measurable* (*Level* 4). *Event Management* memperoleh nilai tertinggi sebesar 3,88

(*Level* 4), diikuti *Access Management* sebesar 3,37 (*Level* 3), *Incident Management* sebesar 3,32 (*Level* 3), dan *Problem Management* sebesar 3,21 (*Level* 3). Analisis kesenjangan menunjukkan *gap* rata-rata sebesar 1,56 dari kondisi ideal *Level* 5 (*Optimized*). Temuan ini menunjukkan bahwa meskipun proses telah berjalan dan terdokumentasi, masih diperlukan peningkatan terutama pada aspek analisis akar masalah (*Problem Management*), pengendalian akses (*Access Management*), serta evaluasi kinerja secara berkelanjutan. Penelitian ini diharapkan dapat menjadi acuan dalam meningkatkan tata kelola keamanan sistem informasi berbasis praktik ITIL.

Kata kunci: ITIL V3; keamanan sistem informasi; *service operation*; *maturity level*; *gap analysis*

1. Pendahuluan

Perkembangan teknologi informasi(TI) dalam beberapa dekade terakhir telah mengubah cara organisasi menjalankan proses bisnisnya, termasuk pada sektor pendidikan. Institusi pendidikan kini semakin bergantung pada sistem informasi untuk mendukung aktivitas operasional, mulai dari pengelolaan data akademik hingga layanan administrasi [1]. Ketergantungan ini tidak hanya memberikan keuntungan dari sisi efisiensi dan efektivitas, tetapi juga menempatkan informasi sebagai aset strategis yang harus dikelola dengan baik [2]. Dalam konteks tersebut, aspek keamanan sistem informasi menjadi krusial, mengingat potensi risiko yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data [3]. Ancaman seperti akses tidak sah, kebocoran informasi, maupun gangguan layanan bukan hanya berdampak pada operasional, tetapi juga dapat menurunkan tingkat kepercayaan pengguna terhadap organisasi [4].

Di sisi lain, berbagai organisasi umumnya telah menerapkan mekanisme dasar pengamanan, seperti penggunaan *firewall* dan pengaturan hak akses pengguna. Namun, penerapan tersebut seringkali bersifat teknis dan belum diikuti dengan evaluasi yang sistematis terhadap efektivitasnya [5]. Kondisi ini secara khusus juga terjadi pada objek penelitian ini, yaitu sebuah perguruan tinggi yang berlokasi di Nusa Tenggara Barat, dimana pengelolaan keamanan sistem informasi telah berjalan, namun belum pernah dilakukan pengukuran secara terstruktur menggunakan kerangka kerja tertentu. Akibatnya, tingkat kesesuaiannya terhadap standar keamanan belum dapat dipastikan secara objektif.

Berangkat dari permasalahan tersebut, diperlukan suatu pendekatan yang tidak hanya mampu mengidentifikasi kondisi aktual sistem, tetapi juga memberikan arah perbaikan yang jelas. Salah satu pendekatan yang banyak digunakan dalam konteks manajemen layanan teknologi informasi adalah *Information Technology Infrastructure Library* (ITIL). ITIL V3 dikenal sebagai kerangka kerja berbasis *best practice* yang menyediakan panduan dalam mengelola layanan TI secara terintegrasi melalui beberapa domain utama[6]. Di antara domain tersebut, *Service Operation* memiliki peran strategis karena berkaitan langsung dengan aktivitas operasional harian, termasuk pengelolaan insiden, permasalahan sistem, serta kontrol akses pengguna [7].

Sejumlah penelitian sebelumnya telah menunjukkan bahwa ITIL V3 dapat digunakan sebagai alat evaluasi dalam mengukur tingkat kematangan layanan TI. Berdasarkan penelitian [8] menemukan bahwa evaluasi ITIL V3 pada domain *Service Operation* di lingkungan Puskesmas menunjukkan sebagian besar proses masih berjalan secara informal. Penelitian [9] menyatakan bahwa implementasi ITIL V3 pada *e-learning* perguruan tinggi berkontribusi dalam membentuk proses layanan TI yang lebih terstruktur. Sementara itu, penelitian pada PT XYZ [10] menunjukkan bahwa tiga dari lima proses *Service Operation* dapat mencapai *maturity level* di atas 2, sementara *Request Fulfillment* dan *Access Management* masih belum memadai.

Meskipun demikian, masih terdapat beberapa keterbatasan dalam penelitian-penelitian tersebut. Pertama, sebagian besar studi cenderung menitikberatkan pada peningkatan kualitas layanan TI secara umum, tanpa secara spesifik mengkaji aspek manajemen risiko keamanan sistem informasi [11]. Kedua, tidak sedikit penelitian yang hanya berfokus pada satu atau dua subdomain dalam *Service Operation*, sehingga belum mampu menggambarkan kondisi operasional secara menyeluruh [12]. Ketiga, penggunaan pendekatan *maturity level* yang dikombinasikan dengan analisis kesenjangan (*gap analysis*) dalam konteks keamanan sistem informasi pada lingkungan institusi pendidikan tinggi masih tergolong terbatas [13].

Berdasarkan celah penelitian tersebut, studi ini memberikan kontribusi dengan mengkaji penerapan ITIL V3 pada domain *Service Operation* secara komprehensif melalui integrasi empat subdomain utama: *Event Management, Incident Management, Problem Management,* dan *Access Management.* Pendekatan yang digunakan tidak hanya berhenti pada pengukuran tingkat kematangan, tetapi juga dilengkapi dengan analisis kesenjangan untuk membandingkan kondisi aktual dengan kondisi yang diharapkan, sebuah pendekatan yang belum banyak diterapkan secara integratif pada lingkungan perguruan tinggi di Indonesia.

Berdasarkan latar belakang di atas, rumusan masalah penelitian ini adalah: (1) Bagaimana tingkat kematangan manajemen risiko keamanan sistem informasi berdasarkan *framework* ITIL V3 domain *Service Operation*? (2) Seberapa besar kesenjangan antara kondisi aktual saat ini dengan kondisi yang diharapkan? Sejalan dengan itu, tujuan penelitian ini adalah mengevaluasi tingkat kematangan manajemen risiko keamanan sistem informasi serta menyusun rekomendasi perbaikan yang dapat mendukung peningkatan kualitas pengelolaan keamanan sistem informasi.

2. Bahan dan Metode

2.1. Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif deskriptif dengan tujuan memperoleh gambaran tingkat kematangan manajemen risiko keamanan sistem informasi secara terukur. Evaluasi dilakukan menggunakan pendekatan ITIL-*based assessment*, di mana *framework* ITIL V3 digunakan sebagai acuan utama dalam menilai kondisi pengelolaan layanan teknologi informasi [14]. Fokus penelitian berada pada domain *Service Operation*, yang dibatasi pada empat subdomain: *Event Management, Incident Management, Problem Management*, dan *Access Management.*

Keempat subdomain tersebut dipilih karena merepresentasikan praktik inti dalam ITIL V3 yang berkaitan langsung dengan deteksi kejadian, penanganan gangguan, pengelolaan akar masalah, serta pengendalian akses terhadap sistem informasi, komponen yang paling relevan dengan aspek keamanan sistem informasi operasional [15].

2.2. Objek dan Responden Penelitian

Penelitian ini dilakukan pada unit pengelola sistem informasi di sebuah perguruan tinggi swasta di Nusa Tenggara Barat yang memiliki sistem informasi terintegrasi dan digunakan secara aktif dalam mendukung aktivitas operasional akademik dan administrasi. Pengambilan sampel dilakukan dengan teknik total *sampling*, yaitu seluruh anggota populasi dijadikan responden. Jumlah responden dalam penelitian ini adalah 13 orang yang secara langsung terlibat dalam pengelolaan sistem informasi, meliputi staf IT, administrator sistem, dan pengelola jaringan.

2.3. Teknik Pengumpulan Data

Data dikumpulkan melalui dua teknik, yaitu kuesioner dan wawancara. Kuesioner digunakan sebagai instrumen utama dalam mengukur tingkat kematangan proses berdasarkan *framework* ITIL V3. Penyusunan butir pertanyaan mengacu pada kontrol proses dalam subdomain *Service Operation*. Skala pengukuran menggunakan model *maturity level* dengan rentang nilai 0 hingga 5, di mana masing-masing nilai menggambarkan tingkat kematangan proses mulai dari *Nonexistent* (0) hingga *Optimized* (5) [16]. Tabel 1 menyajikan deskripsi setiap tingkat kematangan yang digunakan dalam penelitian ini.

Tabel 1. Deskripsi Tingkat Kematangan (*Maturity Level*)

Level	Kategori	Deskripsi
0	*Non-existent*	Proses tidak ada sama sekali; tidak ada bukti pengelolaan
1	*Initial/Ad-hoc*	Proses tidak terorganisir; bergantung pada individu, tidak terdokumentasi
2	*Repeatable*	Proses dilakukan berulang namun belum terstandarisasi secara formal
3	*Defined Process*	Proses terdokumentasi dan dikomunikasikan secara formal dalam organisasi
4	*Managed & Measurable*	Proses diukur dan dimonitor; manajemen dapat mengendalikan secara efektif
5	*Optimized*	Proses terus ditingkatkan melalui mekanisme otomatis dan evaluasi berkelanjutan

Wawancara dilakukan kepada pihak yang memiliki peran dalam pengelolaan sistem informasi, mencakup proses monitoring sistem (*Event Management*), mekanisme penanganan insiden (*Incident Management*), pengelolaan masalah berulang (*Problem Management*), serta pengaturan dan kontrol akses pengguna (*Access Management*). Wawancara berfungsi untuk melengkapi dan memvalidasi data kuantitatif dari kuesioner.

2.4. Instrumen Penelitian

Instrumen penelitian disusun berdasarkan pemetaan (*mapping*) antara kontrol keamanan sistem informasi dengan proses ITIL V3 *Service Operation*. Berikut adalah contoh butir pertanyaan yang digunakan untuk masing-masing subdomain:

1) *Event Management*: "Apakah terdapat mekanisme monitoring untuk mendeteksi kejadian atau gangguan pada sistem?"
2) *Incident Management*: "Apakah terdapat prosedur standar dalam penanganan insiden sistem informasi?"
3) *Problem Management*: "Apakah dilakukan analisis terhadap akar penyebab insiden yang terjadi secara berulang?"
4) *Access Management*: "Apakah hak akses pengguna telah diatur sesuai dengan peran dan tanggung jawab?"

2.5. Teknik Analisis Data

Analisis data dilakukan melalui empat tahapan:

2.5.1. Uji Validitas dan Reliabilitas

Uji validitas dilakukan dengan membandingkan nilai korelasi *product-moment Pearson* (r-hitung) setiap item dengan nilai r-tabel pada taraf signifikansi 5%. Item dinyatakan valid apabila r-hitung > r-tabel. Uji reliabilitas dilakukan menggunakan metode *Cronbach's Alpha*; instrumen dinyatakan reliabel apabila nilai alpha ≥ 0,60 [17].

2.5.2. Perhitungan *Maturity Level*

Nilai *maturity level* diperoleh dari rata-rata jawaban responden pada masing-masing subdomain menggunakan rumus:

$$Maturity\ level = \frac{\Sigma\ nilai\ responden}{jumlah\ responden\ \times\ jumlah\ item} \quad (1)$$

2.5.3. Analisis Kesenjangan (*Gap Analysis*)

Analisis kesenjangan membandingkan nilai *maturity level* saat ini (*current state*) dengan nilai yang diharapkan (*expected state* = Level 5) menggunakan rumus:

$$\text{Gap} = \text{Expected} - \text{Current} \quad (2)$$

2.5.4. Penyusunan Rekomendasi

Berdasarkan nilai gap yang diperoleh, disusun rekomendasi perbaikan yang bersifat prioritas berdasarkan besar kecilnya kesenjangan pada setiap subdomain.

3. Hasil

3.1. Uji Validitas dan Reliabilitas

Uji validitas dilakukan terhadap seluruh item kuesioner dengan menggunakan nilai r-tabel untuk n=13 dan taraf signifikansi 5% (r-tabel = 0,553). Item dinyatakan valid apabila nilai r-hitung > r-tabel. Berdasarkan hasil pengujian, terdapat beberapa item yang gugur karena tidak memenuhi syarat validitas, sehingga jumlah item valid per subdomain adalah sebagaimana disajikan pada Tabel 2.

Tabel 2. Hasil Uji Validitas Instrumen

Subdomain	**Jumlah *Item* Awal**	**Jumlah *Item* Valid**	**Jumlah *Item* Gugur**
Event Management	5	2	3
Incident Management	7	5	2
Problem Management	5	3	2
Access Management	6	4	2
Total	23	14	9

Uji reliabilitas dilakukan menggunakan Cronbach's Alpha. Hasil pengujian menunjukkan bahwa seluruh subdomain memiliki nilai alpha di atas 0,60, sehingga instrumen dinyatakan reliabel sebagaimana ditunjukkan pada Tabel 3.

Tabel 3. Hasil Uji Reliabilitas Instrumen

Subdomain	***Cronbach's Alpha***	**Keterangan**
Event Management	0,712	Reliabel
Incident Management	0,754	Reliabel
Problem Management	0,698	Reliabel
Access Management	0,731	Reliabel

3.2. Data Hasil Penilaian Responden

Penilaian dilakukan menggunakan skala maturity level 0–5. Berikut adalah data hasil penilaian responden untuk masing-masing subdomain yang ditunjukkan oleh Tabel 4, Tabel 5, Tabel 6, dan Tabel 7.

1. Event Management

Tabel 4. Hasil Penilaian Event Management

Responden	P3	P5	Total
R1	3	3	6
R2	5	4	9
R3	4	5	9
R4	4	5	9
R5	4	5	9
R6	3	3	6
R7	2	3	5
R8	5	5	10
R9	3	3	6
R10	3	3	6
R11	4	4	8
R12	4	5	9
R13	4	5	9
Total	**48**	**53**	**101**

2. Incident Management

Tabel 5. Hasil Penilaian Incident Management

Responden	P7	P8	P9	P10	P13	Total
R1	3	3	5	3	3	17
R2	3	2	3	3	3	14
R3	4	3	4	4	3	18
R4	5	3	4	5	5	22
R5	4	4	4	4	5	21
R6	3	2	3	4	5	17
R7	3	3	3	5	5	19
R8	4	5	4	5	5	23
R9	3	3	2	2	2	12
R10	3	3	3	2	3	14
R11	3	2	2	2	2	11
R12	2	2	2	3	3	12
R13	3	3	3	2	5	16
Total	**43**	**38**	**42**	**44**	**49**	**216**

3. Problem Management

Tabel 6. Hasil Penilaian Problem Management

Responden	P14	P16	P17	Total
R1	3	3	3	9
R2	4	4	2	10
R3	4	1	2	7
R4	5	4	5	14
R5	4	4	4	12
R6	2	3	5	10
R7	3	2	3	8
R8	5	5	5	15
R9	4	2	2	8
R10	2	4	2	8

Responden	P14	P16	P17	Total
R11	2	2	3	7
R12	3	2	3	8
R13	3	2	4	9
Total	**44**	**38**	**43**	**125**

4. Access Management

Tabel 7. Hasil Penilaian Access Management

Responden	P18	P22	P27	P28	Total
R1	4	5	3	3	15
R2	4	2	3	4	13
R3	4	4	4	4	16
R4	5	5	5	5	20
R5	4	4	4	4	16
R6	5	2	2	2	11
R7	3	3	3	3	12
R8	4	4	4	4	16
R9	2	2	2	3	9
R10	2	4	3	3	12
R11	4	2	3	2	11
R12	4	2	4	3	13
R13	3	4	2	2	11
Total	**48**	**43**	**42**	**42**	**175**

3.3. Perhitungan Maturity Level

Nilai maturity level dihitung menggunakan rumus (1). Kriteria pemetaan nilai ke level kematangan adalah sebagai berikut: 0,00–0,49 = Level 0; 0,50–1,49 = Level 1; 1,50–2,49 = Level 2; 2,50–3,49 = Level 3; 3,50–4,49 = Level 4; 4,50–5,00 = Level 5.

1. Event Management:

$$Maturity\ level = \frac{101}{13 \times 2} = 3{,}88$$

2. Incident Management:

$$Maturity\ level = \frac{216}{13 \times 5} = 3{,}32$$

3. Problem Management:

$$Maturity\ level = \frac{125}{13 \times 3} = 3{,}21$$

4. Access Management:

$$Maturity\ level = \frac{175}{13 \times 4} = 3{,}37$$

Tabel 8. Rekapitulasi Maturity Level

Subdomain	**Nilai *Maturity Level***	***Level***	**Kategori**
Event Management	3,88	*Level* 4	*Managed and Measurable*
Incident Management	3,32	*Level* 3	*Defined Process*

Subdomain	Nilai *Maturity Level*	*Level*	Kategori
Problem Management	3,21	*Level* 3	*Defined Process*
Access Management	3,37	*Level* 3	*Defined Process*
Rata-rata Keseluruhan	3,44	*Level* 3	*Defined Process*

3.4. Analisis Kesenjangan (Gap Analysis)

Analisis kesenjangan dilakukan dengan membandingkan nilai maturity level saat ini (current state) dengan kondisi yang diharapkan (expected state = Level 5) menggunakan rumus (2). Hasil analisis disajikan pada Tabel 9.

Tabel 9. Hasil Analisis Kesenjangan (Gap Analysis)

Subdomain	*Current*	*Expected*	*Gap*	Prioritas
Event Management	3,88	5	1,12	4 (terendah)
Incident Management	3,32	5	1,68	2
Problem Management	3,21	5	1,79	1 (tertinggi)
Access Management	3,37	5	1,63	3
Rata-rata	**3,44**	**5**	**1,56**	**-**

Nilai gap rata-rata keseluruhan adalah 1,56, yang menunjukkan masih adanya jarak yang cukup signifikan antara kondisi aktual dan kondisi ideal. Problem Management memiliki nilai gap tertinggi (1,79), menjadikannya prioritas utama perbaikan, sementara Event Management memiliki gap terkecil (1,12).

4. Pembahasan

4.1. Analisis Tingkat Kematangan secara umum

Berdasarkan hasil perhitungan, nilai rata-rata tingkat kematangan domain *Service Operation* adalah 3,44, yang berada pada kategori *Defined Process* (Level 3). Kondisi ini mencerminkan bahwa organisasi telah memiliki prosedur yang terdokumentasi dan telah diterapkan secara konsisten dalam operasional layanan TI. Namun demikian, proses belum sepenuhnya didukung oleh mekanisme pengukuran kinerja yang terstruktur untuk mencapai kategori *Managed and Measurable* [16]. Temuan ini sejalan dengan hasil penelitian [9] yang menemukan bahwa institusi pendidikan umumnya berada pada rentang *Level* 3 hingga *Level* 4 dalam evaluasi ITIL V3 *Service Operation*.

4.2. Analisis per Subdomain ITIL

1. *Event Management*

Event Management memperoleh nilai tertinggi (3,88) dan merupakan satu-satunya subdomain yang mencapai Level 4. Hal ini menunjukkan bahwa organisasi telah memiliki mekanisme monitoring sistem yang cukup efektif dalam mendeteksi kejadian atau gangguan secara dini. Keberadaan sistem monitoring yang terukur memungkinkan organisasi mengidentifikasi potensi gangguan sebelum berdampak lebih luas [8][18]. Meskipun demikian, masih terdapat ruang untuk peningkatan menuju Level 5, khususnya dalam hal otomatisasi dan integrasi penuh sistem monitoring.

2. *Incident Management*

Incident Management memperoleh nilai 3,32 (Level 3). Meskipun prosedur penanganan insiden telah ada dan diterapkan, nilai ini menunjukkan bahwa proses belum sepenuhnya terukur dan terstandarisasi. Dokumentasi insiden dan evaluasi pasca-insiden

masih perlu ditingkatkan. Hasil ini konsisten dengan temuan penelitian pada aplikasi *e-learning* universitas [12] yang menunjukkan bahwa prosedur *incident management* umumnya sudah ada namun belum dilengkapi dengan mekanisme eskalasi yang jelas.

3. *Problem Management*

Problem Management memperoleh nilai terendah (3,21, Level 3), mengindikasikan bahwa proses analisis akar penyebab (*root cause analysis*) belum dilakukan secara optimal. Kondisi ini menunjukkan bahwa organisasi masih cenderung berfokus pada penanganan insiden individual tanpa mengelola penyebab sistemik dari permasalahan berulang. Dalam kerangka ITIL, kegagalan dalam *problem management* akan menyebabkan insiden serupa terus berulang tanpa penyelesaian permanen [6]. Kelemahan pada subdomain ini konsisten dengan temuan Maulana [19] yang mengidentifikasi bahwa problem management merupakan subdomain dengan tingkat kematangan paling rendah dalam berbagai konteks implementasi ITIL V3.

4. *Access Management*

Access Management memperoleh nilai 3,37 (Level 3). Meskipun hak akses pengguna telah diatur, pengelolaan akses belum sepenuhnya terstandarisasi dan dikontrol secara optimal. Kondisi ini mengindikasikan risiko potensial terkait penyalahgunaan hak akses, yang merupakan salah satu ancaman utama terhadap keamanan sistem informasi [3][20]. Peningkatan kontrol akses berbasis peran (*role-based access control*) diperlukan untuk memperkuat aspek keamanan ini.

4.3. Analisis Kesenjangan (Gap Analysis)

Nilai gap rata-rata sebesar 1,56 menunjukkan masih adanya jarak yang cukup berarti antara kondisi aktual dan kondisi ideal (Level 5 – *Optimized*). Kesenjangan terbesar pada *Problem Management* (*gap* 1,79) menjadikan subdomain ini sebagai prioritas utama perbaikan, diikuti oleh *Incident Management* (*gap* 1,68), *Access Management* (*gap* 1,63), dan *Event Management* (*gap* 1,12). Temuan ini menunjukkan bahwa organisasi perlu berinvestasi secara lebih intensif dalam membangun kapabilitas analisis akar masalah dan pengelolaan akses yang lebih ketat untuk meningkatkan keamanan sistem informasi secara menyeluruh[13].

4.4. Perbandingan dengan Penelitian Terdahulu

Hasil penelitian ini sejalan dengan sejumlah penelitian sebelumnya. Evaluasi ITIL V3 pada Dinas Perpustakaan Kota Palembang [16] menunjukkan bahwa sebagian besar subdomain *Service Operation* berada pada Level 3-4, dengan *problem management* sebagai area yang membutuhkan perhatian khusus. Penelitian pada *e-learning* Universitas Internasional Batam [17] juga menemukan pola serupa, di mana *event management* cenderung lebih matang dibandingkan *problem management*. Namun, penelitian ini memberikan kontribusi tambahan dengan menyajikan analisis yang lebih spesifik pada konteks manajemen risiko keamanan sistem informasi di institusi pendidikan tinggi, yang sebelumnya masih jarang ditemukan dalam literatur yang ada[13].

4.5. Implikasi dan Rekomendasi

Berdasarkan hasil analisis gap, terdapat empat rekomendasi prioritas yang disusun berdasarkan urgensi kesenjangan:

1. Peningkatan *Problem Management* (Prioritas 1 – *Gap* 1,79): Organisasi perlu membangun prosedur *root cause analysis* (RCA) yang formal dan terdokumentasi. Penerapan *Known Error Database* (KEDB) dapat membantu dalam mencegah terulangnya insiden yang sama.

2. Peningkatan *Incident Management* (Prioritas 2 – *Gap* 1,68): Penguatan prosedur eskalasi insiden, peningkatan dokumentasi insiden secara sistematis, dan pelaksanaan evaluasi pasca-insiden (*post-incident review*) secara rutin.
3. Optimalisasi *Access Management* (Prioritas 3 – *Gap* 1,63): Implementasi *role-based access control* (RBAC) yang lebih ketat, audit hak akses berkala, dan penerapan prinsip *least privilege* untuk setiap pengguna sistem.
4. Pengembangan *Event Management* (Prioritas 4 – *Gap* 1,12): Meskipun sudah berada di Level 4, peningkatan menuju Level 5 dapat dicapai melalui otomatisasi penuh sistem monitoring dan integrasi dengan *tools* ITSM yang mendukung *continuous improvement*.

5. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa tingkat kematangan manajemen risiko keamanan sistem informasi pada domain *Service Operation* berdasarkan *framework* ITIL V3 berada pada nilai rata-rata 3,44, yang termasuk dalam kategori *Defined Process* (Level 3) menuju *Managed and Measurable* (Level 4). Hal ini menunjukkan bahwa organisasi telah memiliki prosedur operasional yang terdokumentasi dan diterapkan secara konsisten, namun belum sepenuhnya didukung oleh mekanisme pengukuran dan evaluasi kinerja yang optimal.

Secara spesifik, subdomain *Event Management* telah mencapai Level 4 (nilai 3,88), menunjukkan bahwa proses monitoring sistem telah berjalan dengan baik dan terukur. Sementara itu, subdomain *Incident Management* (3,32), *Access Management* (3,37), dan *Problem Management* (3,21) masih berada pada Level 3 (*Defined Process*), mengindikasikan bahwa proses-proses tersebut masih memerlukan peningkatan dalam hal pengukuran kinerja, analisis akar masalah, dan standarisasi kontrol akses.

Hasil analisis kesenjangan menunjukkan *gap* rata-rata sebesar 1,56 dari kondisi optimal Level 5 (*Optimized*). *Problem Management* memiliki kesenjangan terbesar (1,79), menjadikannya prioritas utama dalam agenda perbaikan tata kelola keamanan sistem informasi.

Penelitian ini memiliki beberapa keterbatasan. Pertama, jumlah responden yang terbatas (13 orang) membatasi generalisasi temuan ke institusi lain. Kedua, penelitian hanya mencakup empat dari lima subdomain utama ITIL V3 *Service Operation* (tidak mencakup *Request Fulfillment*). Ketiga, data wawancara tidak disajikan secara kualitatif secara mendetail. Untuk penelitian mendatang, disarankan untuk memperluas cakupan ke seluruh subdomain *Service Operation*, membandingkan hasil antar institusi pendidikan, serta mengintegrasikan *framework* ITIL V3 dengan standar keamanan lain seperti ISO/IEC 27001 untuk memperoleh evaluasi yang lebih komprehensif.

Ucapan Terima Kasih: Penulis mengucapkan terima kasih kepada seluruh pihak yang telah mendukung pelaksanaan penelitian ini, khususnya kepada unit pengelola sistem informasi pada institusi yang menjadi objek penelitian atas kesediaannya dalam memberikan data dan informasi yang dibutuhkan.

Referensi

[1] D. MacLean and R. Titah, "Implementation and Impacts of IT Service Management in the IT Function," *Int. J. Inf. Manage.*, vol. 70, p. 102628, 2023, https://doi.org/10.1016/j.ijinfomgt.2023.102628.

[2] J. Serrano, J. Faustino, D. Adriano, R. Pereira, and M. Mira da Silva, "An IT Service Management Literature Review: Challenges, Benefits, Opportunities and Implementation Practices," *Information*, vol. 12, no. 3, p. 111, 2021, https://doi.org/10.3390/info12030111.

[3] Y. Riyadi, M. Wahidin, and A. Elanda, "Systematic Literature Review Implementasi Service Operation Dalam Kerangka Kerja Information Technology Infrastructure Library (ITIL) di Indonesia: Tren Penelitian, Manfaat dan Tantangan," *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 17, no. 2, pp. 81–97, 2022, https://doi.org/10.35969/interkom.v17i2.232.

[4] H. Cho and K. Cho, "Impact of Security Management Activities on Corporate Performance," *systems*, vol. 13, no. 8, p. 633, 2025, doi: https://doi.org/10.3390/systems13080633.
[5] M. Saraiva and R. Ribeiro, "Analysis of the ITIL V3 and 4, Exploring the Impacts on ITSM of Implementing the New Version," *CAPSI 2025 Proceedings.*, 2025, https://aisel.aisnet.org/capsi2025/28.
[6] K. R. Fauzan, I. B. Nurdianto, Y. Muhammad, M. W. Santosa, O. G. Prakoso, and A. Wijanarko, "Analysis of the Implementation of ITIL V3 Domain Service Operation in Enhancing the Quality of Information Technology Services," *Int. J. Appl. Inf. Manag.*, vol. 3, no. 4, pp. 177–183, 2023, https://doi.org/10.47738/ijaim.v3i4.106.
[7] A. Stephanie, A. Fayola, R. Darianty, and A. Maulana, "Implementation and Impacts of ITIL Service Operation within the Telecommunication Industry," *IJISIT Int. J. Comput. Sci. Inf. Technol.*, vol. 1, no. 1, pp. 31–40, 2024, https://doi.org/10.55123/ijisit.v1i1.22.
[8] M. Ronaldo and M. Zaki, "Evaluasi Manajemen Layanan Teknologi Informasi Berdasarkan Proses Service Operation ITIL V3 pada Puskesmas Pasir Putih," *Sisfo J. Ilm. Sist. Inf.*, vol. 9, no. 1, 2025, https://doi.org/10.29103/sisfo.v9i1.21795.
[9] S. Hastini and W. Cholil, "Analisa Komponen ITSM Pada E-learning Perguruan Tinggi Di Kota Palembang Menggunakan ITIL V.3," *J. Tekno Kompak*, vol. 15, no. 1, pp. 79–91, 2021.
[10] K. P. Sholekha *et al.*, "Optimizing IT Service Strategies: A Performance Assessment through ITIL V3 in PT XYZ IT Operations Division," *IJIIS Int. J. Informatics Inf. Syst.*, vol. 6, no. 4, 2023, https://doi.org/10.47738/ijiis.v6i4.176.
[11] D. Imbaquingo-Esparza, J. Díaz, M. R. Egas, W. Fuertes, and D. Molina, "Information Security at Higher Education Institutions: A Systematic Literature Review," *Proc. TICEC 2022, Commun. Comput. Inf. Sci.*, vol. 1648, pp. 279–294, 2022, https://doi.org/10.1007/978-3-031-18272-3_20.
[12] D. Ikhtiarti and T. Sutabri, "Analisis IT Service Management (ITSM) Layanan E-Learning Universitas Bina Darma Menggunakan Framework ITIL V3," *J. Teknol. dan Ilmu Komput. Prima*, vol. 6, no. 1, 2023, https://doi.org/10.34012/jutikomp.v6i1.3598.
[13] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, A. Vazquez-Rodas, F. Gallegos-Segovia, and P. Vintimilla-Tapia, "Information Security Management Frameworks and Strategies in Higher Education Institutions: A Systematic Review," *Ann. Telecommun.*, vol. 76, pp. 255–270, 2021, https://doi.org/10.1007/s12243-020-00783-2.
[14] F. P. Sari and S. A. Rizki, "Analisis Dan Pengukuran Tingkat Kematangan Manajemen Layanan Teknologi Informasi Pada Aplikasi Mytelkomsel Menggunakan Framework ITIL V3," *J. Sains Student Res.*, vol. 4, no. 1, 2026, https://doi.org/10.61722/jssr.v4i1.8216.
[15] AXELOS, *ITIL Foundation: ITIL 4 Edition*. London: TSO (The Stationery Office), 2019.
[16] I. Choldun and M. Mulyati, "Analisis It Service Management (Itsm) Menggunakan Framework Itil V.3 Pada Dinas Perpustakaan Dan Kearsipan Kota Palembang," *J. Rekayasa Sist. Inf. dan Teknol.*, vol. 3, no. 3, 2026, https://doi.org/10.70248/jrsit.v3i3.3449.
[17] A. R. Hannuella, D. Lim, V. J. Samudra, D. Firgana, H. Dixman, and D. S. Melati, "Analisis It Service Management (Itsm) Layanan E-Learning Universitas Internasional Batam Menggunakan Framework ITIL V3," *Technol. J. Ilm.*, vol. 15, no. 3, pp. 400–410, 2024, http://dx.doi.org/10.31602/tji.v15i3.15170.
[18] M. Y. Rahmana and Mulyati, "Evaluasi Penerapan IT Service Management (ITSM) dengan Framework ITIL V3 di Universitas XYZ," *J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 3, 2025, https://doi.org/10.23960/jitet.v13i3.7196.
[19] Y. M. Maulana, "Model Analisis Incident Management pada Layanan Teknologi Informasi Berdasarkan Framework Information Technology Infrastructure Library V3," *J. Saintekom Sains, Teknol. Komput. dan Manaj.*, vol. 13, no. 2, pp. 123–135, 2023, https://doi.org/10.33020/saintekom.v13i2.398.
[20] T. R. Eikebrokk and J. Iden, "Implementation and Impacts of IT Service Management in the IT Function," *Int. J. Inf. Manag.*, vol. 70, p. 102628, 2023, https://doi.org/10.1016/j.ijinfomgt.2023.102628.