Informatics and Computer Engineering Journal

Volume 6 No. 2 Juli 2026

Evaluasi Tata Kelola Layanan TI Berbasis COBIT 5 untuk Resiliensi Operasional: Pembelajaran Sektor Publik Menuju Pengembangan Infrastruktur Digital (Studi Kasus: BPBD DKI Jakarta)

Yustina Meisella Kristania[1*], Supriatiningsih[2], Saghifa Fitriana[3]

[1,2,3]Universitas Bina Sarana Informatika
Jl. Kramat Raya No.98 Jakarta, Indonesia
e-mail: [1*]yustina.yms@bsi.ac.id, [2]supriatiningsih.stq@bsi.ac.id, [3]saghifa.sff@bsi.ac.id

Abstrak - Efektivitas penanggulangan bencana di wilayah megapolitan seperti DKI Jakarta sangat bergantung pada keandalan operasional dan dukungan layanan teknologi informasi. Namun, ketidakselarasan antara Standar Operasional Prosedur (SOP) dengan kerangka kerja tata kelola TI global seringkali menghambat respons insiden yang cepat. Penelitian ini bertujuan untuk mengevaluasi tingkat kapabilitas tata kelola TI pada Badan Penanggulangan Bencana Daerah (BPBD) DKI Jakarta, dengan fokus pada domain Deliver, Service, and Support (DSS) dalam kerangka kerja COBIT 5. Menggunakan pendekatan metode campuran (mixed-method), data dikumpulkan melalui observasi lapangan, dokumentasi SOP, dan kuesioner kepada 12 responden kunci. Hasil analisis menunjukkan tingkat kematangan rata-rata berada pada level 4 (Predictable Process), namun ditemukan kesenjangan signifikan pada sub-domain DSS02.02 terkait klasifikasi insiden yang hanya mencapai level 2.6. Temuan ini mengindikasikan bahwa meskipun infrastruktur fisik dan fasilitas telah dikelola dengan baik, mekanisme pencatatan dan prioritas insiden layanan masih bersifat ad-hoc. Penelitian ini berkontribusi memberikan peta jalan perbaikan SOP berbasis risiko untuk meningkatkan resiliensi organisasi publik dalam situasi darurat. Penelitian ini berkontribusi memberikan peta jalan perbaikan SOP berbasis risiko untuk meningkatkan resiliensi organisasi publik dalam situasi darurat. Lebih jauh, temuan mengenai urgensi sistem manajemen insiden terintegrasi dalam riset ini menjadi fondasi (*best practice*) bagi tim peneliti dalam merancang tata kelola operasional layanan TI pada pengembangan perangkat lunak terapan di sektor strategis lainnya pada penelitian mendatang

Kata Kunci : Audit Sistem Informasi, BPBD DKI Jakarta, COBIT 5, Domain DSS, Tata Kelola Bencana.

Abstracts *- The effectiveness of disaster management in a megapolitan area like DKI Jakarta relies heavily on operational reliability and IT service support. However, misalignment between Standard Operating Procedures (SOP) and global IT governance frameworks often hinders rapid incident response. This study aims to evaluate the IT governance capability level at the Regional Disaster Management Agency (BPBD) of DKI Jakarta, focusing on the Deliver, Service, and Support (DSS) domain within the COBIT 5 framework. Using a mixed-method approach, data was collected through field observation, SOP documentation, and questionnaires distributed to 12 key respondents. The analysis reveals an average maturity level at level 4 (Predictable Process), but a significant gap was found in sub-domain DSS02.02 regarding incident classification, which only reached level 2.6. These findings indicate that while physical infrastructure and facilities are well-managed, the mechanism for recording and prioritizing service incidents remains ad-hoc. This research contributes to providing a risk-based SOP improvement roadmap to enhance public organization resilience in emergency situations.*

Keywords : Information Systems Audit, BPBD DKI Jakarta, COBIT 5, DSS Domain, Disaster Governance.

PENDAHULUAN

Transformasi digital dalam sektor publik menuntut integrasi teknologi informasi yang tidak hanya bersifat pendukung, tetapi sebagai enabler strategis, terutama dalam manajemen krisis dan kebencanaan. Provinsi DKI Jakarta, dengan karakteristik geografis dataran rendah dan kompleksitas demografi, menghadapi risiko kebencanaan multidimensi yang memerlukan respons cepat (Pemerintah Provinsi DKI Jakarta, 2023) . Dalam konteks ini, Badan Penanggulangan Bencana Daerah (BPBD) DKI Jakarta memegang peran vital sebagai koordinator komando yang mengandalkan integritas data dan kesiapan infrastruktur teknologi untuk pengambilan keputusan real-time. Lebih jauh, konsep resiliensi operasional dalam sektor publik tidak dapat dilepaskan dari aspek keamanan basis data (database security) dan integritas arsitektur informasi. Pada saat situasi krisis

kebencanaan, volume lalu lintas data—mulai dari laporan warga, pemetaan titik api atau banjir, hingga pergerakan armada—akan mengalami lonjakan eksponensial. Jika tata kelola layanan tidak memiliki protokol manajemen kapasitas dan mitigasi insiden yang mapan, infrastruktur TI rentan mengalami bottleneck atau bahkan kelumpuhan sistem (system failure). Audit sistem informasi dalam konteks ini berfungsi sebagai instrumen preventif untuk mengidentifikasi celah kerentanan (vulnerabilities) pada lapisan operasional sebelum eksploitasi atau kegagalan sistem benar-benar terjadi. Framework COBIT 5, khususnya pada domain DSS, menyajikan panduan komprehensif untuk memastikan bahwa setiap layanan TI yang berjalan tidak hanya sekadar 'aktif', melainkan juga andal, aman dari gangguan teknis, dan terlindungi ketersediaannya (availability) secara persisten. Meskipun BPBD DKI Jakarta telah memiliki Standar Operasional Prosedur (SOP) sebagai panduan pelaksanaan tugas, observasi awal menunjukkan adanya potensi kesenjangan antara prosedur formal dengan praktik tata kelola teknologi informasi global. Masalah ini krusial karena audit sistem informasi pada layanan publik digital sangat diperlukan untuk menjamin akuntabilitas respons terhadap masyarakat (Hadi & Nasution, 2025). Ketidakefisienan dalam pengelolaan layanan TI, khususnya pada aspek operasional dan dukungan (support), dapat berimplikasi fatal terhadap kecepatan distribusi logistik dan koordinasi Tim Reaksi Cepat (TRC) saat bencana terjadi. Penelitian terdahulu banyak menyoroti penggunaan COBIT 5 untuk audit sistem informasi pada sektor perbankan dan e-commerce (Atqiyak & Santoso, 2022);(Zuraidah, 2020) . Beberapa studi juga menerapkan framework ini pada lembaga asuransi untuk memastikan keselarasan strategi bisnis (Budyanto, 2024).Namun literatur yang secara spesifik mengevaluasi kapabilitas operasional (DSS domain) pada lembaga penanggulangan bencana di negara berkembang masih terbatas. Memahami dinamika operasional teknologi di lingkungan berisiko tinggi (*high-stakes environment*) seperti kelembagaan bencana memberikan *lesson learned* yang esensial. Tata kelola operasional, khususnya pada domain DSS (*Deliver, Service, and Support*), tidak hanya krusial untuk instansi seperti BPBD, tetapi juga menjadi model dasar tata kelola yang wajib disiapkan sebelum peluncuran (*deployment*) sistem informasi ke masyarakat di sektor krusial lainnya, seperti digitalisasi UMKM atau agrikultur terapan. Penelitian ini merupakan bagian integral dari peta jalan riset tim pengusul dalam merancang resiliensi infrastruktur digital. Melalui evaluasi kapabilitas layanan pada BPBD DKI Jakarta, diharapkan terbangun kerangka manajemen operasional dan mitigasi insiden TI yang adaptif untuk menjamin *zero-downtime* pada adopsi produk teknologi di masa depan. COBIT 5 dipilih sebagai kerangka kerja karena pendekatan holistiknya dalam menyelaraskan tujuan TI dengan tujuan strategis organisasi, khususnya melalui domain Deliver, Service, and Support (DSS) yang berfokus pada kesinambungan layanan kritis. Penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan melakukan audit mendalam terhadap SOP BPBD DKI Jakarta. Penelitian ini menggunakan kerangka kerja COBIT 5 karena pendekatan holistiknya dalam menyelaraskan tujuan TI dengan tujuan strategis organisasi (ISACA, 2012)**.** Novelty atau kebaruan dari studi ini terletak pada evaluasi granular terhadap sub-domain DSS01 (Manage Operations) dan DSS02 (Manage Service Requests and Incidents) dalam lingkungan high-stakes (berisiko tinggi). Hasil penelitian ini diharapkan tidak hanya memberikan gambaran level kapabilitas saat ini (as-is), tetapi juga rekomendasi strategis untuk mencapai level yang diharapkan (to-be), guna memastikan infrastruktur TI BPBD mampu mendukung mandat "Zero Victim" dalam penanggulangan bencana. Dalam ekosistem penanggulangan bencana, ketersediaan layanan (availability) dan keamanan basis data (database security) tidak dapat dikompromikan. Ketika insiden terjadi, integritas informasi mengenai titik evakuasi, logistik, dan status korban menjadi krusial. Oleh karena itu, audit tata kelola TI tidak hanya ditujukan untuk menilai efisiensi administratif, tetapi juga untuk memitigasi kerentanan sistem terhadap kegagalan operasional (system failure). Model tata kelola yang tangguh harus mampu memastikan bahwa ketika infrastruktur mengalami tekanan maksimal akibat bencana (seperti banjir besar atau gempa bumi), arsitektur sistem informasi tetap mampu memberikan dukungan keputusan tanpa interupsi. COBIT 5 memberikan panduan komprehensif melalui Process Assessment Model (PAM) yang memungkinkan auditor untuk tidak sekadar melihat hasil akhir, melainkan membedah proses di balik layar—mulai dari manajemen fasilitas fisik hingga prosedur pencatatan insiden di lapangan. Penjabaran domain Deliver, Service, and Support (DSS) dalam penelitian ini diharapkan mampu memberikan cetak biru (blueprint) evaluasi yang terukur, sehingga instansi publik dapat beralih dari budaya reaktif menjadi proaktif dalam manajemen layanan TI.

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan kuantitatif deskriptif dengan kerangka kerja COBIT 5 sebagai instrumen audit utama. Fokus audit dibatasi pada domain DSS (*Deliver, Service, and Support*).

1. Penentuan Domain Audit

Fokus audit dibatasi pada domain *Deliver, Service, and Support* (DSS). Pemilihan domain ini didasarkan pada argumen bahwa DSS merupakan indikator utama untuk mengukur keberhasilan operasional harian dan kesinambungan layanan dalam sebuah organisasi publik (Daffa & lainnya, 2022). Selain itu, domain DSS terbukti efektif dalam memetakan kendala teknis pada instansi pemerintahan yang memiliki birokrasi kompleks (Pasha et al., 2022).

2. Prosedur Pengumpulan dan Analisis Data
Pengumpulan data dilakukan melalui observasi lapangan di kantor BPBD DKI Jakarta, studi dokumentasi SOP, dan penyebaran kuesioner kepada 12 responden kunci (Kusuma et al., 2024). Instrumen kuesioner dirancang berdasarkan *Process Assessment Model* (PAM) yang dikembangkan oleh (ISACA, 2012). Analisis data dilakukan dengan mengonversi skala Likert menjadi indeks kematangan (*maturity level*) untuk mengidentifikasi kesenjangan (*gap*) antara kondisi saat ini (*as-is*) dengan kondisi yang diharapkan (*to-be*).

3. Pemetaan Tujuan (Goals Cascade)
Pemilihan domain DSS didasarkan pada pemetaan strategis (mapping) antara Tujuan Bisnis Organisasi (Enterprise Goals) BPBD DKI Jakarta dengan Tujuan TI (IT-Related Goals), yang kemudian diturunkan menjadi Proses TI yang relevan. Mengingat peran BPBD sebagai lembaga pelayanan publik darurat, prioritas utama adalah kesinambungan layanan.

4. Uji Validitas Pendekatan Assessment
Dalam mengevaluasi tingkat kematangan, penelitian ini bersandar pada Process Assessment Model (PAM) yang merupakan standar baku dari ISACA. Penggunaan kuesioner yang didistribusikan kepada 12 responden kunci (Key Informant) telah melalui proses penyelarasan dengan struktur organisasi BPBD. Responden dipilih menggunakan teknik purposive sampling, difokuskan secara eksklusif pada personel yang memiliki otorisasi, akses langsung terhadap basis data operasional, dan pemahaman teknis mendalam terkait Standar Operasional Prosedur (SOP) layanan TI harian. Keterbatasan jumlah responden diimbangi dengan kedalaman (depth) dari otorisasi yang mereka miliki, sehingga data yang ditarik merepresentasikan kondisi empiris tata kelola yang sebenarnya. Metode skoring dilakukan dengan mengacu pada capability level yang ketat, di mana sebuah proses hanya dapat naik ke level berikutnya apabila indikator kinerja pada level di bawahnya telah terpenuhi secara utuh (fully achieved). Pendekatan ini memastikan bahwa skor kematangan yang dihasilkan terkalibrasi dengan baik dan meminimalisir bias subjektivitas dari responden.

Tabel 1. Pemetaan COBIT 5 Goals Cascade pada BPBD DKI Jakarta

Enterprise Goals (EG)	IT-Related Goals (ITG)	IT Processes (Domain)
EG 10: Optimization of service delivery capabilities (Optimalisasi kapabilitas layanan).	**ITG 07:** Delivery of IT services in line with business requirements (Penyampaian layanan TI sesuai kebutuhan bisnis).	**DSS01** - Manage Operations
EG 16: Product and business service continuity (Kesinambungan layanan bisnis).	**ITG 14:** Availability of reliable and useful information for decision making (Ketersediaan informasi yang andal untuk pengambilan keputusan).	**DSS02** - Manage Service Requests and Incidents
EG 11: Customer-oriented service culture (Budaya layanan berorientasi pelanggan/masyarakat).	**ITG 04:** Managed IT-related business risk (Pengelolaan risiko bisnis terkait TI).	**DSS01 & DSS02**

Melalui pemetaan pada Tabel 1, domain DSS01 dan DSS02 teridentifikasi sebagai proses paling kritis untuk memastikan SOP BPBD berjalan selaras dengan kebutuhan penanggulangan bencana yang *zero-downtime*.

Prosedur Pengumpulan Data
Pengumpulan data dilakukan melalui triangulasi sumber untuk memastikan validitas temuan:

1. **Observasi Lapangan:** Pengamatan langsung dilakukan di kantor BPBD DKI Jakarta (Jl. Kyai Haji Zainul Arifin No.71) untuk memverifikasi kesesuaian antara dokumen SOP dengan eksekusi di lapangan, termasuk kondisi infrastruktur fisik dan fasilitas pusat data.
2. **Studi Dokumentasi:** Analisis terhadap dokumen kebijakan internal, laporan kinerja, dan manual prosedur operasional yang berjalan.
3. **Kuesioner:** Instrumen kuesioner dirancang berdasarkan *process assessment model* (PAM) COBIT 5. Kuesioner didistribusikan kepada 12 responden kunci yang memiliki otoritas dan pengetahuan mendalam terkait operasional TI, termasuk Kepala Satuan Tugas (Kasatgas) BPBD.

Teknik Analisis Data
Analisis data dilakukan melalui konversi data kualitatif dari kuesioner menjadi indeks numerik untuk menentukan tingkat kematangan (Maturity Level). Penilaian menggunakan skala Likert yang dikonversi ke dalam level kapabilitas COBIT 5 (Level 0-5). Perhitungan indeks kematangan menggunakan formula standar audit sistem informasi:

$$MaturityIndex = \frac{\sum(Bobot \times JumlahResponden)}{TotalResponden}$$

Untuk memberikan interpretasi yang presisi terhadap Maturity Index yang dihasilkan dari perhitungan, penelitian ini mengadopsi skala kapabilitas proses COBIT 5 yang terbagi ke dalam enam tingkatan fundamental. Penjabaran level tersebut adalah sebagai berikut:

Level 0 (Incomplete Process): Proses tidak diimplementasikan atau gagal mencapai tujuan prosesnya. Pada tahap ini, tidak ada bukti sistematis pencapaian tujuan TI.

Level 1 (Performed Process): Proses telah diimplementasikan dan berhasil mencapai tujuan prosesnya secara reaktif, namun belum terstandarisasi.

Level 2 (Managed Process): Proses yang telah diimplementasikan, dikelola secara terencana, dimonitor, dan disesuaikan. Hasil dari proses telah ditetapkan, dikendalikan, dan dipelihara dengan baik.

Level 3 (Established Process): Proses telah dikelola dan diimplementasikan menggunakan proses standar yang terdefinisi dengan baik dan terintegrasi dalam SOP organisasi secara menyeluruh.

Level 4 (Predictable Process): Proses telah berjalan sesuai standar dan beroperasi dalam batasan yang terdefinisi untuk mencapai hasil akhir yang dapat diprediksi secara kuantitatif.

Level 5 (Optimizing Process): Proses yang dapat diprediksi tersebut secara berkelanjutan ditingkatkan untuk memenuhi tujuan bisnis saat ini dan masa depan melalui inovasi teknologi.

Penentuan target Expected Maturity pada level 5 (Optimizing) didasarkan pada standar best practice untuk organisasi berisiko tinggi (seperti BPBD), di mana toleransi terhadap kegagalan layanan TI (zero-downtime) adalah mutlak guna mendukung keselamatan publik.

Hasil perhitungan kemudian dipetakan untuk mengidentifikasi *Gap Analysis* antara kondisi saat ini (*Current Maturity*) dengan kondisi yang diharapkan (*Expected Maturity*), yang ditargetkan pada Level 5 (*Optimizing*) mengingat urgensi peran BPBD.

HASIL DAN PEMBAHASAN

Berdasarkan audit yang dilakukan pada domain DSS01 dan DSS02, ditemukan variabilitas tingkat kematangan proses yang mengindikasikan adanya kekuatan infrastruktur namun kelemahan dalam prosedur administratif insiden.

Analisis Domain DSS01: Manage Operations
Domain ini mengevaluasi koordinasi dan eksekusi aktivitas dan prosedur operasional.

1. **DSS01.01 (Perform Operational Procedures):** Mencapai skor **3.8**. Hal ini menunjukkan bahwa prosedur operasional sebagian besar telah terstandarisasi dan terdokumentasi. BPBD telah memiliki SOP yang jelas untuk situasi tanggap darurat, namun konsistensi pelaksanaannya masih perlu peningkatan untuk mencapai level *optimized*.

2. **DSS01.02 (Manage Outsourced IT Services):** Mencapai skor **4.1**.
   Sub-domain ini mencapai skor tertinggi menunjukkan bahwa pengelolaan layanan pihak ketiga dinilai sangat baik. Kontrak dan kinerja vendor TI dipantau secara ketat yang krusial mengingat ketergantungan pada vendor untuk penyediaan infrastruktur komunikasi darurat. Hal ini sejalan dengan prinsip manajemen risiko operasional yang mensyaratkan adanya kendali ketat terhadap layanan *outsourcing* (Budyanto, 2024).
   Pengelolaan layanan pihak ketiga dinilai sangat baik. Kontrak dan kinerja vendor TI dipantau secara ketat, yang krusial mengingat ketergantungan pada vendor untuk penyediaan infrastruktur komunikasi darurat.
3. **DSS01.03 (Monitor IT Infrastructure):** Mencapai skor **4.04**. Sistem pemantauan infrastruktur TI telah berjalan efektif dengan *uptime* yang tinggi, mendukung ketersediaan layanan 24/7.

4. **DSS01.04 (Manage The Environment):** Mencapai skor **4.1**. Aspek fisik lingkungan data center dan perangkat keras pendukung telah dilindungi dengan kontrol akses dan mitigasi risiko fisik (suhu, daya) yang memadai.
5. **DSS01.05 (Manage Facilities):** Mencapai skor **4.06**. Fasilitas pendukung operasi bencana dikelola dengan baik, memastikan kesiapan logistik dan transportasi tim reaksi cepat.

Elaborasi Kinerja Operasional (DSS01)
Pencapaian skor di atas 4.0 pada hampir seluruh sub-domain DSS01 mengindikasikan bahwa BPBD DKI Jakarta telah memiliki fondasi operasional TI yang sangat matang. Pada aspek Manage The Environment (DSS01.04) dan Manage Facilities (DSS01.05), keberhasilan ini sangat ditunjang oleh pemahaman organisasi terhadap krusialnya keamanan fasilitas fisik data center. Kontrol akses ruangan, sistem pendingin presisi, dan ketersediaan catu daya cadangan (UPS dan generator) terpelihara dengan jadwal inspeksi yang ketat. Kematangan pada operasional fisik ini membuktikan bahwa investasi pada perangkat keras dan infrastruktur pendukung telah selaras dengan tujuan Enterprise Goals (EG 16) yakni kesinambungan layanan bisnis. Walaupun demikian, catatan perbaikan tetap diperlukan pada Perform Operational Procedures (DSS01.01) yang mendapat skor terendah di klaster ini (3.8). Hal ini umumnya dipicu oleh pergantian personel atau mutasi pegawai yang tidak diiringi dengan proses knowledge transfer yang memadai, sehingga pelaksanaan SOP operasional harian terkadang masih bergantung pada kompetensi individu (person-dependent) alih-alih mengandalkan sistem yang sudah terotomatisasi.

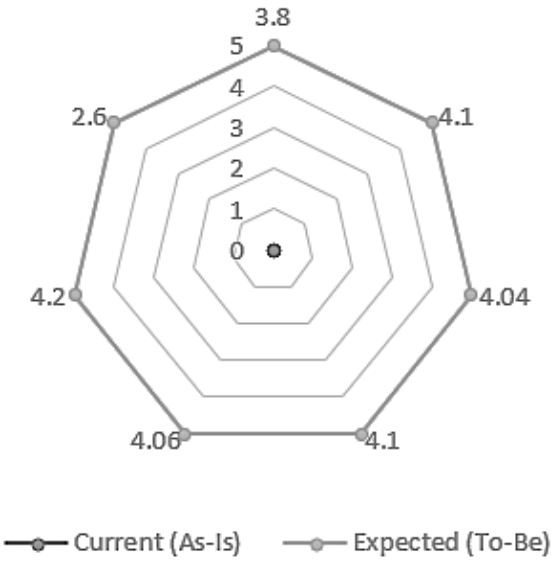
Secara keseluruhan, DSS01 berada pada kategori *Predictable Process* (Level 4), yang berarti proses operasional telah terukur dan terkendali.

Analisis Domain DSS02: Manage Service Requests and Incidents
Domain ini menjadi temuan kritis dalam penelitian ini, khususnya pada aspek klasifikasi insiden.

1. **DSS02.01 (Define Classification Schemes):** Mencapai skor **4.2**. BPBD memiliki skema definisi insiden yang sangat jelas secara teori/dokumen.
2. **DSS02.02 (Record, Classify and Prioritise Requests):** Mencapai skor **2.6**. Ini adalah titik terlemah yang ditemukan. Temuan rendahnya skor pada DSS02.02 mengindikasikan bahwa praktik pencatatan insiden di lapangan masih bersifat *ad-hoc*. Kondisi ini konsisten dengan penelitian (Santoso & Saleh, 2019), yang menemukan bahwa kegagalan pada domain DSS02 sering kali bukan disebabkan oleh ketidakmampuan teknis, melainkan karena absennya sistem *ticketing* yang terintegrasi sehingga petugas enggan melakukan pencatatan manual saat situasi kritis. Skor ini jauh di bawah rata-rata domain lain (Level 2: *Managed Process*). Meskipun definisi insiden jelas (seperti pada DSS02.01), praktik pencatatan, klasifikasi, dan prioritas insiden di lapangan seringkali tidak dilakukan secara sistematis. Dalam situasi bencana yang kacau (*chaotic*), petugas cenderung melakukan tindakan langsung (*adhocracy*) tanpa pencatatan prosedural yang rapi, yang berisiko menghilangkan jejak audit dan data historis untuk evaluasi pasca-bencana.

   Dampak Kesenjangan Manajemen Insiden (DSS02)
   Paradoks yang ditemukan antara tingginya kapabilitas definisi skema insiden (DSS02.01 dengan skor 4.2) dan rendahnya eksekusi pencatatan (DSS02.02 dengan skor 2.6) merupakan potret klasik dari fenomena "silo fungsional" dalam birokrasi pemerintahan. Secara teoretis, dokumen perancangan mengklasifikasikan insiden dari tingkat *Low*, *Medium*, hingga *High Criticality*. Namun, pada implementasinya, ketiadaan antarmuka sistem pelaporan yang ramah pengguna (*user-friendly*) menyebabkan petugas di lapangan mengabaikan prosedur tersebut. Dalam kerangka COBIT 5, kelemahan dalam mencatat dan mengklasifikasikan *request* tidak hanya berdampak pada teknis TI, tetapi menciptakan efek domino terhadap IT-Related Goals (ITG 14), yaitu ketersediaan informasi yang andal. Tanpa basis data insiden yang terpusat, manajemen level atas tidak dapat melakukan analisis akar masalah (*Root Cause Analysis*), sehingga investasi mitigasi di tahun anggaran berikutnya seringkali didasarkan pada asumsi, bukan pada data historis berbasis bukti (*evidence-based data*).

Analisis Kesenjangan (Gap Analysis)



Gambar 1. Diagram Radar Analisis Kesenjangan Domain DSS

Pada diagram memperlihatkan ketimpangan kapabilitas yang signifikan. Salah satu area (Current Maturity) menunjukkan pola yang meluas mendekati level optimal pada aspek operasional fisik (DSS01), namun mengalami kontraksi tajam pada sub-domain DSS02.02. Hal ini mengonfirmasi bahwa hambatan utama tata kelola bukan terletak pada ketersediaan teknologi, melainkan pada prosedur pelaporan insiden.

Tabel 2. Rekapitulasi Tingkat Kematangan dan Gap

Proses Domain	**Sub-Domain**	**Current Maturity (As-Is)**	**Expected Maturity (To-Be)**	**Gap**
DSS01	DSS01.01	3.80	5.00	1.20
	DSS01.02	4.10	5.00	0.90
	DSS01.03	4.04	5.00	0.96
	DSS01.04	4.10	5.00	0.90
	DSS01.05	4.06	5.00	0.94
DSS02	DSS02.01	4.20	5.00	0.80
	DSS02.02	**2.60**	**5.00**	**2.40**

Seperti terlihat pada **Gambar 1**, terdapat kesenjangan tertajam sebesar **2.4 poin** pada sub-domain DSS02.02. Pola grafik menunjukkan bentuk yang hampir sempurna pada sisi luar (mendekati level 5) untuk aspek infrastruktur fisik, namun "penyok" atau menyusut drastis ke dalam pada titik DSS02.02. Terdapat kesenjangan sebesar 2.4 poin pada sub-domain DSS02.02 jika dibandingkan dengan target kematangan Level 5. Ketimpangan ini menunjukkan anomali: organisasi memiliki infrastruktur fisik yang kuat (DSS01 skor >4), namun lemah dalam manajemen data insiden (DSS02.02 skor <3). Implikasi manajerial dari temuan ini adalah risiko *bottleneck* informasi. Ketika insiden layanan TI tidak diklasifikasikan berdasarkan prioritas dampak, sumber daya teknis mungkin dialokasikan untuk masalah trivial sementara isu kritis (misalnya, kegagalan server peringatan dini) terlambat ditangani.

Rekomendasi Perbaikan

Berdasarkan temuan di atas, rekomendasi utama adalah implementasi sistem *helpdesk* otomatis dan integrasi simulasi pencatatan insiden dalam *drill* bencana. Perbaikan pada aspek dokumentasi ini krusial untuk memenuhi standar audit sistem informasi pemerintah (Hadi & Nasution, 2025).

Untuk meningkatkan kapabilitas domain DSS02.02 dari Level 2 ke Level 3, penelitian ini merumuskan strategi perbaikan berbasis *People, Process, dan Technology* (PPT) sebagai berikut:

Tabel 3. Rekomendasi Perbaikan Strategis

Aspek	Masalah Utama	Rencana Tindakan (Action Plan)
Process	SOP sulit dijalankan secara *real-time* saat kondisi darurat (*chaos*).	**Penyederhanaan SOP:** Mengizinkan pencatatan insiden susulan (*log backdate*) maksimal 1x24 jam pasca-bencana dan menstandarisasi kategori insiden.
Technology	Pelaporan manual via WhatsApp menyulitkan rekap data.	**Digitalisasi Pelaporan:** Implementasi sistem *ticketing* berbasis *mobile* (cth: osTicket) agar petugas lapangan dapat melapor dengan sekali klik.
People	Rendahnya kesadaran petugas terhadap dokumentasi teknis.	**Simulasi Terintegrasi:** Menyelipkan skenario "Sistem Down" ke dalam latihan rutin penanggulangan bencana (*Drill*).

Rencana Aksi Implementasi Tata Kelola
Berdasarkan matriks perbaikan pada Tabel 3, implementasi strategi People, Process, and Technology (PPT) harus dijalankan secara paralel.

Pertama, dari aspek Teknologi, pergeseran dari pelaporan berbasis aplikasi pesan instan (seperti WhatsApp) menuju sistem ticketing khusus (seperti osTicket atau sistem helpdesk kustom) adalah urgensi utama. Sistem ticketing ini harus dirancang berbasis aplikasi mobile yang memungkinkan petugas lapangan melaporkan insiden kegagalan layanan TI (seperti radio komunikasi down atau server CCTV terputus) hanya dengan beberapa ketukan. Sistem ini juga harus terintegrasi dengan basis data relasional yang secara otomatis mengklasifikasikan tingkat keparahan berdasarkan kategori aset yang dilaporkan.

Kedua, dari aspek Proses, penyederhanaan SOP di masa darurat (chaos) mutlak diperlukan. Organisasi tidak bisa memaksakan proses administratif yang kaku saat petugas sedang berjibaku dengan penyelamatan. Oleh karena itu, diperkenalkan kebijakan log backdate, di mana petugas diizinkan melakukan pencatatan insiden ke dalam sistem maksimal 1x24 jam pasca-penanganan krisis, selama timeline penanganan dicatat secara kronologis. Hal ini menjaga integritas data tanpa mengorbankan kecepatan layanan.

Ketiga, dari aspek Sumber Daya Manusia (People), resistensi terhadap perubahan prosedur administrasi seringkali menjadi kendala utama. Untuk mengatasi budaya adhocracy, simulasi penanganan insiden TI ("Sistem Down") wajib dimasukkan ke dalam porsi latihan rutin penanggulangan bencana (drill). Petugas tidak hanya dilatih untuk mengevakuasi korban secara fisik, tetapi juga disimulasikan menghadapi blank-spot komunikasi atau kegagalan server data, sehingga mereka terbiasa menggunakan sistem helpdesk pelaporan insiden di bawah tekanan tinggi.

KESIMPULAN

Evaluasi tata kelola teknologi informasi pada BPBD DKI Jakarta menggunakan COBIT 5 menunjukkan bahwa secara umum kematangan organisasi berada pada level yang baik (Level 4), terutama dalam aspek pengelolaan infrastruktur fisik dan hubungan dengan pihak ketiga. Namun, penelitian ini mengungkap kelemahan kritis pada proses *Record, Classify and Prioritise Requests and Incidents* (DSS02.02) yang masih berada pada Level 2.6. Kontribusi utama penelitian ini adalah identifikasi risiko operasional di mana kecanggihan teknologi tidak diimbangi dengan disiplin administrasi insiden. Rekomendasi strategis bagi BPBD DKI Jakarta adalah: (1)

Mengintegrasikan sistem *ticketing* otomatis untuk pencatatan insiden guna mengurangi beban administrasi manual saat krisis, dan (2) Melakukan simulasi berkala yang mewajibkan prosedur klasifikasi insiden sebagai bagian dari *drill* penanggulangan bencana. Perbaikan SOP pada aspek ini krusial untuk memastikan tata kelola TI yang tangguh dan responsif. Perbaikan SOP pada aspek ini krusial untuk memastikan tata kelola TI yang tangguh dan responsif. Selain memberikan rekomendasi strategis bagi mitra studi kasus, pemetaan kerentanan pada mekanisme pelaporan insiden (DSS02.02) ini krusial sebagai pedoman tim peneliti untuk merancang arsitektur *helpdesk* dan mitigasi operasional pada pengembangan aplikasi *mobile* berbasis masyarakat yang tengah dirintis pada riset lanjutan.

REFERENSI

Atqiyak, N. I., & Santoso, D. B. (2022). Audit Sistem Informasi Aplikasi Gramedia Digital Menggunakan Framework COBIT 5. *Jurnal Indonesia Sosial Teknologi*, *3*(6), 740–751. https://doi.org/10.36418/jist.v3i6.440

Budyanto, E. Z. A. (2024). Audit Sistem Informasi Aplikasi DPLK Capital Life Indonesia Menggunakan Framework Cobit 5. *Resolusi: Rekayasa Teknik Informatika Dan Informasi*, *4*(4), 334–347.

Daffa, T. S., & lainnya. (2022). Audit Teknologi Informasi Menggunakan COBIT 5 Domain DSS Pada Universitas Stikubank Semarang. *Jurnal Teknik Informatika Dan Sistem Informasi*, *4*(3), 2804–2814.

Hadi, M. Z., & Nasution, H. (2025). Audit Sistem Informasi Layanan Publik Berbasis COBIT 5 Domain DSS untuk Meningkatkan Kualitas Pelayanan Digital. *Jurnal Sistem Informasi Dan Teknologi Era*, *1*(1), 28–38. https://doi.org/10.71094/sitera.v1i1.54

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. ISACA.

Kusuma, A., Eprianza, D. P., Vinaro, L., Agustian, S. B., Pasyah, A. D. T., & Alfikri, M. F. (2024). *Audit Sistem Informasi Standar Operasional Prosedur Pada Badan Penanggulangan Bencana Daerah Menggunakan Framework COBIT 5*.

Pasha et al. (2022). Analisis Tata Kelola IT Menggunakan Domain DSS Pada Instansi Pemerintahan. *Jurnal Teknoinfo*, *16*(1).

Pemerintah Provinsi DKI Jakarta. (2023). *Profil Kebencanaan Provinsi DKI Jakarta*.

Santoso, C. B., & Saleh, A. A. (2019). Penerapan Metode COBIT 5.0 Domain DSS02 Dan DSS03 Untuk Mengukur Tingkat Kapabilitas Tata Kelola Sistem. *Teknois: Jurnal Ilmiah Teknologi Informasi Dan Sains*, *7*(2), 13–26. https://doi.org/10.36350/jbs.v7i2.24

Zuraidah, E. (2020). Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 4.1. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 84–95. https://doi.org/10.30656/prosisko.v7i2.2289