

Analisis *Business Continuity Management* Media Informasi Kabupaten Tuban Menggunakan Standar ISO 22301

Maulidina Rahmawati Surya^{1*}, Pratiwi Susanti², dan Muhammad Bachtyar Rosyadi³

^{1,3}Institut Teknologi dan Bisnis Tuban

²Universitas PGRI Madiun

*Penulis Korespondensi : maulidinarahmawati14@gmail.com

ABSTRACT

Information media platforms play a crucial role in the delivery of information services. Disruptions to the underlying infrastructure can halt public services and trigger the spread of disinformation. This study aims to analyze and design a Business Continuity Management (BCM) system for the Tuban Regency information media service, based on the ISO 22301 standard. A qualitative research approach was employed, utilizing observation, interviews, and risk analysis via Business Impact Analysis (BIA). The analysis identified several critical threats, such as cyberattacks, hardware failures, and power outages. Risk assessment results indicate that the dominant risks stem from IT aspects (server downtime, cyberattacks, network disruptions), operational support factors (power outages, equipment failure), and human factors (operational errors). The BIA identified news distribution via social media and digital news portals as the most critical services, requiring a relatively rapid recovery time objective (RTO) of 2–4 hours. Recommended mitigation strategies include implementing redundancy systems, strengthening cybersecurity, enforcing backup policies with routine restoration testing, and establishing a Business Continuity/Disaster Recovery (BC/DR) team with clear crisis communication protocols. The designed BCP provides guidelines for recovery steps across various disruption scenarios. Ultimately, this study yields recommendations for a Disaster Recovery Plan and standard operating procedures to ensure the continued availability of Tuban Regency's information media services during a crisis.

Article History

Received : 29-06-2026
Revised : 17-07-2026
Accepted : 30-06-2026

Keywords

BCM,
BIA,
ISO 22301,
Media Informasi Kabupaten
Tuban

ABSTRAK

Media informasi merupakan salah satu bagian penting atau krusial pada pelayanan informasi. Gangguan pada infrastruktur media informasi dapat menghentikan pelayanan publik dan memicu disinformasi. Penelitian ini bertujuan untuk menganalisis dan merancang sistem manajemen kelangsungan bisnis (*Business Continuity Management*) pada media informasi Kabupaten Tuban berbasis standar ISO 22301. Metode penelitian menggunakan pendekatan kualitatif melalui observasi, wawancara, dan analisis risiko menggunakan *Business Impact Analysis* (BIA). Hasil analisis menunjukkan beberapa ancaman kritis, seperti serangan siber, kerusakan perangkat keras, dan pemadaman listrik. Hasil *risk assessment* menunjukkan risiko dominan berasal dari aspek TI (server down, serangan siber, gangguan jaringan), faktor pendukung operasional (pemadaman listrik, kerusakan perangkat), serta faktor manusia (kesalahan operasional). *Business Impact Analysis* (BIA), layanan yang paling kritis adalah distribusi berita via media sosial dan portal berita digital dengan target pemulihan yang relatif cepat (RTO 2–4 jam). Strategi mitigasi yang disarankan meliputi redundansi sistem, penguatan keamanan siber, penerapan kebijakan backup dan uji restore rutin, serta pembentukan tim BC/DR dengan alur komunikasi krisis yang jelas. BCP yang dirancang memberikan pedoman langkah-langkah pemulihan selama berbagai skenario gangguan. Penelitian ini menghasilkan rekomendasi strategi pemulihan bencana (*Disaster Recovery Plan*) dan prosedur operasional standar untuk menjaga ketersediaan layanan media informasi Kabupaten Tuban saat terjadi krisis.

PENDAHULUAN

Media informasi merupakan salah satu bagian penting atau krusial pada pelayanan informan publik tingkat daerah. teknologi informasi telah mengubah cara masyarakat mengonsumsi berita. Jika sebelumnya media cetak mendominasi, kini masyarakat cenderung mengakses berita melalui portal digital, media sosial, dan aplikasi pesan instan. Infrastruktur digital pemerintah daerah kerap

menghadapi berbagai ancaman yang dapat menghentikan operasional layanan. Ancaman tersebut meliputi serangan siber (*hacking/ransomware*), gangguan jaringan komunikasi, kerusakan perangkat keras, hingga bencana alam. Berdasarkan pengamatan awal, media informasi Kabupaten Tuban belum memiliki sistem mitigasi yang terintegrasi untuk menghadapi gangguan skala besar secara cepat [1]. Media informasi resmi Kabupaten Tuban, seperti situs web dan media sosial instansi, menjadi saluran utama diseminasi kebijakan, program kerja, dan layanan publik. Ketersediaan informasi yang akurat dan cepat sangat bergantung pada keandalan infrastruktur teknologi yang digunakan. Kondisi ini mendorong perusahaan media informasi atau instansi komunikasi pemerintah untuk mengoptimalkan sistem digital guna menjaga kecepatan distribusi informasi dan meningkatkan daya saing [2].

Digitalisasi menyebabkan ketergantungan tinggi pada infrastruktur TI: server hosting, database berita, jaringan internet, perangkat *workstation* redaksi, sistem manajemen konten (CMS), serta keamanan siber. Ketergantungan tersebut membuat perusahaan media lebih rentan terhadap gangguan operasional. Gangguan dapat berupa pemadaman listrik, kerusakan perangkat, gangguan jaringan, kegagalan *server*, hingga serangan *siber* yang berpotensi melumpuhkan publikasi berita [3]. Risiko tersebut dapat berasal dari faktor internal, seperti kegagalan sistem informasi, kesalahan manusia dalam pengambilan keputusan, keterbatasan sumber daya manusia maupun material, serta kekurangan dalam perencanaan operasional[4]. Selain itu, risiko juga muncul dari faktor eksternal, termasuk bencana alam, gangguan pada rantai pasok, perubahan regulasi, fluktuasi kondisi ekonomi, hingga dinamika politik yang tidak menentu. Ketidakefektifan pengelolaan risiko dapat menyebabkan gangguan operasional, peningkatan biaya, serta penurunan produktivitas dan kinerja karyawan[5]. Kondisi tersebut berpotensi menghambat pencapaian tujuan organisasi apabila tidak diimbangi dengan strategi mitigasi risiko yang tepat, khususnya dalam pengelolaan sumber daya manusia [6]. Penelitian terdahulu memberikan landasan penting untuk memahami penerapan ISO 22301 dalam manajemen risiko serta *Business Continuity Management* (BCM). Penerapan ISO 22301 memungkinkan organisasi membangun sistem manajemen kontinuitas bisnis yang terstruktur dan sistematis, sehingga mampu mengidentifikasi risiko, merencanakan strategi mitigasi, serta memastikan pemulihan operasional secara cepat saat terjadi gangguan[7]. Penelitian Hendaryatna bahwa kompleksitas proyek, ketergantungan pada rantai pasok, serta risiko keselamatan kerja menjadi faktor krusial yang memengaruhi keberhasilan BCM. Penelitian tersebut menunjukkan bahwa integrasi manajemen risiko dengan perencanaan kelangsungan bisnis mampu meningkatkan ketahanan operasional perusahaan. Selain itu, penerapan standar ini di perusahaan konstruksi membantu organisasi mengenali risiko utama, menyusun rencana darurat yang tepat, dan meminimalkan kerugian akibat gangguan internal maupun eksternal. Hal ini memperkuat relevansi standar internasional tersebut dalam menjaga kontinuitas dan stabilitas bisnis [8].

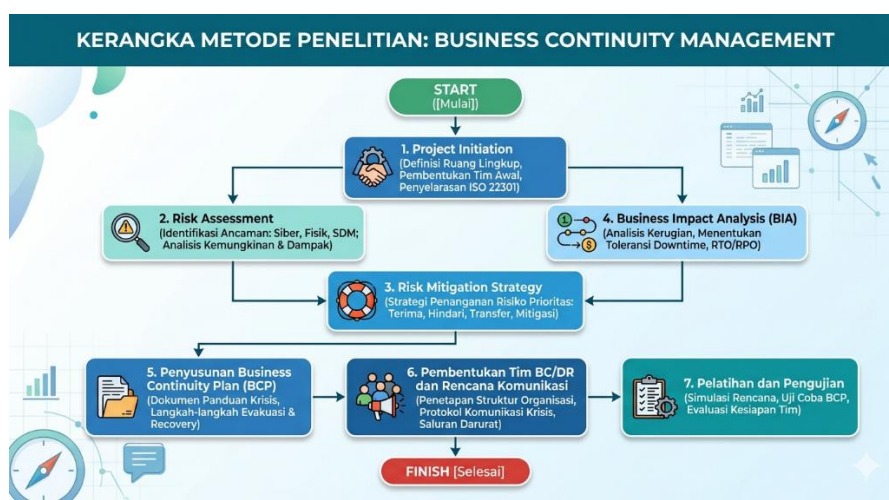
Business Continuity Management (BCM) sebagai pendekatan sistematis untuk memastikan organisasi mampu mempertahankan layanan penting selama gangguan dan memulihkan proses bisnis secara terencana. Standar ISO 22301 memberikan kerangka kerja bagi organisasi untuk membangun *Business Continuity Management System* (BCMS) yang terdokumentasi, terukur, dan terus ditingkatkan [9]. Penerapan ISO 22301, Standar ini menyediakan kerangka kerja formal untuk mengidentifikasi potensi ancaman, melakukan *Business Impact Analysis* (BIA), serta merumuskan strategi pemulihan yang tepat dapat menyusun perencanaan pemulihan yang realistis, menetapkan peran dan tanggung jawab, serta mengurangi risiko kerugian operasional maupun reputasi [10].

Penelitian ini berfokus pada analisis kondisi kesiapan sistem informasi saat ini di Kabupaten Tuban menggunakan klausul-klausul dalam ISO 22301. Hasil akhir dari penelitian ini diharapkan dapat memberikan rekomendasi strategis dan panduan praktis bagi Perusahaan Media Informasi dan

Pemerintah Kabupaten Tuban. Rekomendasi ini bertujuan untuk meminimalkan dampak gangguan operasional pada media informasi publik daerah.

METODE

Penelitian mengenai Business Continuity Management (BCM) menunjukkan bahwa keberhasilan penerapan BCM sangat bergantung pada kesesuaian strategi dengan karakteristik industri [11]. Pada organisasi berbasis TI, BCP menjadi instrumen penting untuk meminimalkan downtime dan menjaga ketersediaan layanan. Studi lain menekankan bahwa BIA merupakan elemen kunci karena membantu organisasi memahami layanan mana yang paling kritikal dan bagaimana menentukan target pemulihan yang realistis. Metode penyusunan BCP dalam penelitian ini dengan menggunakan ISO 22301 [12]. Adapun gambar metode penelitian ini sebagai Gambar 1.



Gambar 1. Alur Penelitian BCP dengan menggunakan ISO 22301.

Gambar 1. menjelaskan tentang alur BCP dengan menggunakan ISO 22301 adapun penjelasan secara rinci sebagai berikut :

a. *Project Initiation* (Inisiasi Proyek)

Tahap awal ini berfokus pada penentuan ruang lingkup (*scope*) sistem informasi yang akan dilindungi di Kabupaten Tuban. Ruang lingkupnya mencakup seluruh media komunikasi publik resmi, seperti website pemerintah daerah (tubankab.go.id), portal berita dinas, aplikasi layanan publik daerah, hingga akun media sosial resmi yang dikelola oleh Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Tuban, jika perusahaan yakni ada Radar Tuban . Tahap inisiasi proyek bertujuan menentukan ruang lingkup dan komitmen organisasi. Pengumpulan data untuk penyusunan BCM pada Media Komunikasi Kabupaten Tuban dilakukan melalui beberapa teknik, yaitu studi dokumen, kuesioner, dan layanan TIK. Studi dokumen meliputi penelaahan kebijakan keamanan informasi. Media komunikasi Kabupaten Tuban, ruang lingkup difokuskan pada layanan publikasi berita digital dan pendukungnya, termasuk sistem redaksi, server/hosting, jaringan, perangkat kerja, serta jalur distribusi informasi. Pada tahap ini juga ditetapkan pemangku kepentingan utama, peran BCM Leader, dan tujuan umum BCMS.

b. *Risk Assessment* (Penilaian Risiko)

Tahap ini mengidentifikasi dan menganalisis segala bentuk ancaman potensial yang dapat menghentikan fungsi media informasi Kabupaten Tuban. Ancaman diklasifikasikan ke dalam beberapa aspek: Siber: Serangan ransomware, defasemen halaman muka website Pemkab, atau serangan DDoS pada server lokal. Secara fisik/infrastruktur bisa terjadi kebakaran pusat data (*Data Center*), kerusakan perangkat keras, gangguan pemadaman

listrik berkepanjangan, Sedangkan secara Sumber Daya Manusia (SDM): Kelalaian operator (*human error*), dll

c. *Business Impact Analysis* (BIA - Analisis Dampak Bisnis)

Tahap ini melakukan analisis kuantitatif dan kualitatif untuk mengukur kerugian yang terjadi jika media informasi Kabupaten Tuban mengalami *downtime* (mati total). Fokus utama dari BIA di sini adalah menentukan parameter kritis: *Recovery Time Objective* (RTO): Target waktu maksimal layanan media informasi harus bisa menyala kembali setelah terjadi gangguan (misalnya: website berita daerah harus kembali aktif dalam waktu maksimal 2 jam saat terjadi krisis). *Recovery Point Objective* (RPO): Batas maksimal toleransi kehilangan data (misalnya: data berita atau dokumen publik yang hilang maksimal adalah data 4 jam terakhir sebelum sistem tumbang).

d. *Risk Mitigation Strategy* (Strategi Mitigasi Risiko)

Tahap ini hasil dari *Risk Assessment* dan BIA yang telah dilakukan, dirumuskan strategi penanganan yang tepat untuk meminimalkan paparan risiko pada infrastruktur informasi Tuban

e. Penyusunan *Business Continuity Plan* (BCP)

Tahap BCP dirancang dalam bentuk prosedur operasional yang dapat dijalankan saat insiden terjadi. BCP mencakup definisi trigger aktivasi, langkah respons awal, prosedur pemulihan layanan, komunikasi internal dan eksternal, serta mekanisme pemantauan kondisi hingga layanan kembali normal.

f. Pembentukan Tim BC/DR dan Rencana

Tim BC/DR dibentuk agar proses pemulihan memiliki struktur komando yang jelas. Selain itu, *communication plan* diperlukan untuk memastikan informasi insiden tersampaikan kepada pihak internal, mitra, dan publik secara konsisten dan terkoordinasi. Dalam sektor media, komunikasi juga mencakup transparansi publik agar reputasi media tetap terjaga.

g. *Training and Testing*

Pelatihan dan pengujian dilakukan agar BCP tidak hanya menjadi dokumen, tetapi benar-benar dapat dijalankan. Pengujian dapat berupa *tabletop exercise* (simulasi diskusi), drill pemulihan, hingga uji restore backup. Evaluasi hasil pengujian digunakan untuk memperbaiki prosedur dan menutup gap yang ditemukan.

Business Continuity Planning (BCP)

Business Continuity Planning adalah serangkaian proses terintegrasi yang memungkinkan organisasi mempertahankan operasi penting ketika terjadi gangguan besar, dan meminimalkan dampak negatif terhadap layanan, keuangan, dan reputasi [13].

Sedangkan menurut ahli lainnya BCP perencanaan preventif dan responsif yang memungkinkan organisasi tetap berfungsi dalam keadaan darurat melalui prosedur, peran, dan sumber daya yang jelas [14].

Berdasarkan beberapa ahli diatas dapat disimpulkan bahwa suatu rangkaian atau proses responsif organisasi pada saat terjadi gangguan besar tetapi bagaimana perusahaan atau instansi tersebut cepat tanggap dalam menanggulangnya.

Disaster Recovery Planning (DRP)

Disaster Recovery Plan (DRP) adalah rencana pemulihan yang fokus pada aspek TI setelah terjadi bencana atau gangguan besar [15]. DRP berisi langkah pemulihan infrastruktur, data, aplikasi, dan konfigurasi sistem agar dapat kembali beroperasi. DRP biasanya mencakup strategi backup, replikasi data, *failover*, serta *prosedur restore* [16].

BCP dan DRP saling melengkapi. BCP berorientasi pada kontinuitas proses bisnis secara end-to-end, sedangkan DRP merupakan bagian yang lebih teknis untuk memulihkan sistem TI. Dalam praktiknya, keberhasilan BCP sangat ditentukan oleh kesiapan DRP karena layanan digital bergantung pada pemulihan data dan aplikasi.

HASIL DAN PEMBAHASAN

a. *Risk Assessment*

Risk assessment pada Media Informasi Kabupaten Tuban menitik beratkan pada risiko yang dapat menghambat produksi dan distribusi informasi. Penilaian dilakukan dengan menggabungkan probabilitas dan dampak untuk menentukan tingkat prioritas penanganan. Risiko dengan skor tertinggi memerlukan tindakan mitigasi segera karena dapat menyebabkan downtime signifikan dan kerugian reputasi.

Tabel 1. *Risk Assessment* (Penilaian Risiko)

<i>Threat Name</i>	<i>Threat Source</i>	<i>Likelihood</i>	<i>Impact</i>	<i>Overall Risk</i>	<i>Risk Response</i>
Layanan TI terhambat (server down/jaringan putus)	Internal (infrastruktur TI)	Very High	High	Very High	Reduce: monitoring & perawatan berkala, redundansi
Serangan siber (deface/malware/phishing)	Eksternal (hacker/aktor ancaman)	High	High	Very High	Reduce: firewall, patching, MFA, IDS/IPS
Pemadaman listrik	Eksternal (PLN)	High	Medium	High	Reduce/Transfer : UPS, genset, SOP shutdown
Kesalahan manusia (human error)	Internal (operator/admin)	Medium	High	High	Reduce: SOP, pelatihan, kontrol akses
Bencana alam (banjir/gempa)	Eksternal (lingkungan)	Low	Very High	High	Avoid/Reduce: lokasi backup, cloud, DR site
Kerusakan perangkat (hardware failure)	Internal (perangkat)	Medium	Medium	Medium	Reduce: preventive maintenance, sparepart, garansi
Gangguan komunikasi internal	Internal/Eksternal	Medium	Medium	Medium	Reduce: kanal alternatif (WA, telepon, radio)

Tabel 1 menjelaskan tentang penilaian resiko terdapat beberapa alasan munculnya risiko dua kategori sumber utama yaitu sumber internal dalam infrastruktur dan kerusakan perangkat IT ketergantungan penuh organisasi pada sistem digital akan memicu risiko layanan TI terhambat (server down atau jaringan putus), human error atau faktor manusia dalam aktivitas operasional harian dijalankan oleh operator atau admin, serta komunikasi internal sistem koordinasi yang buruk atau tidak memadai antar divisi dalam organisasi. Sedangkan alasan sumber eksternal seperti penyedia utilitas ketergantungan pasokan daya utama pada pihak ketiga memicu risiko jika terjadi pemadaman listrik secara mendadak. Dampak Tinggi “*high*” maka terhentinya seluruh aktivitas operasional utama secara total misal server down, listrik padam, terkena

serangan siber, dampak “*medium*” penurunan produktivitas kerja karyawan untuk sementara waktu, miskomunikasi, biaya tambahan penggantian komponen pada kerusakan perangkat. Tingkat prioritas ditentukan menggunakan Matriks Risiko yang mengalikan tingkat kemungkinan terjadinya (*Likelihood*) dengan tingkat keparahan dampaknya (*Impact*) Prioritas Tinggi “*high*” diberikan kejadian yang dampaknya sangat parah meskipun peluang terjadinya kecil seperti bencana alam, pemadaman listrik. Prioritas “*medium*” peluang keterjadian sedang dan dampak operasional yang bersifat lokal atau tidak melumpuhkan bisnis secara keseluruhan contoh kerusakan perangkat IT dan gangguan komunikasi internal.

b. Business Impact Analysis (BIA) sesuai ISO 22301

BIA dilakukan untuk mengidentifikasi proses bisnis yang paling kritikal dan menetapkan target pemulihan. Pada Media Informasi Tuban, layanan kritikal utama adalah distribusi berita cepat (media sosial) dan portal berita digital, karena kedua layanan tersebut paling sering diakses publik dan berpengaruh langsung terhadap persepsi kredibilitas.

Tabel 2. *Business Impact Analysis* (BIA)

Proses Bisnis Kritikal	Dampak Bila Terganggu	RTO	RPO	Prioritas
Distribusi berita via media sosial	Penurunan engagement, keterlambatan informasi publik	2 jam	1 jam	1
Portal berita digital (website)	Downtime, kehilangan pembaca, reputasi menurun	4 jam	1 jam	2
Produksi berita redaksi	Keterlambatan publikasi berita, backlog konten	8 jam	4 jam	3
Sistem arsip berita/dokumen	Kehilangan data dan histori pemberitaan	12 jam	6 jam	4
Sistem email/komunikasi resmi	Gangguan koordinasi internal & eksternal	12 jam	6 jam	5

Tabel 2. *Business Impact Analysis* (BIA) pada media komunikasi Kabupaten Tuban ini menunjukkan bahwa lini distribusi berita via media sosial dan portal berita (*website*) memiliki prioritas pemulihan tertinggi (Prioritas 1 dan 2) karena berdampak langsung pada penurunan engagement, hilangnya pembaca, serta rusaknya reputasi secara instan, sehingga menuntut target pemulihan sistem yang sangat ketat (RTO 2–4 jam) dan toleransi kehilangan data yang sangat minim (RPO 1 jam). Sebaliknya, proses internal seperti produksi redaksi, sistem arsip, dan email komunikasi resmi ditempatkan pada prioritas yang lebih rendah (Prioritas 3 hingga 5) dengan kelonggaran waktu pemulihan hingga 8–12 jam serta toleransi kehilangan data sampai 4–6 jam, karena gangguan pada area ini dinilai tidak langsung melumpuhkan bisnis di mata publik melainkan hanya menghambat operasional dan koordinasi internal untuk sementara waktu.

c. Risk Mitigation Strategy

Strategi mitigasi disusun berdasarkan hasil risk assessment dan BIA. Fokus mitigasi diarahkan pada risiko berlevel tinggi dan sangat tinggi, terutama yang berdampak pada publikasi digital. Kontrol mitigasi mencakup pencegahan (*preventive*), deteksi (*detective*), dan pemulihan (*recovery*).

Table 3. *Risk Mitigation Strategy* (Strategi Mitigasi Risiko)

<i>Risk</i>	<i>Type of Mitigation</i>	<i>Mitigation Action</i>	<i>PIC</i>	<i>Target Waktu</i>
Server/website down	Risk Reduction	Redundansi server, CDN, cloud failover, monitoring 24/7	Tim IT	1–3 bulan
Serangan siber	Risk Reduction	Firewall, MFA, patching rutin, backup immutable, awareness phishing	Tim IT + Manajemen	1–2 bulan
Pemadaman listrik	Risk Reduction/Transfer	UPS untuk server & perangkat redaksi, genset, SOP listrik	Logistik + IT	1 bulan
Kesalahan manusia	Risk Reduction	SOP operasional, role-based access, pelatihan admin	Manajemen + HR	1–2 bulan
Bencana alam	Risk Avoidance/Reduction	Offsite backup, cloud storage, DR site, prosedur evakuasi	Manajemen	3–6 bulan

d. ***Business Continuity Plan (BCP)***

BCP dirancang untuk memastikan layanan tetap berjalan dengan memanfaatkan prosedur alternatif ketika sistem utama terganggu. Pada sektor media, strategi alternatif publikasi menjadi kunci untuk menjaga kontinuitas informasi. BCP berikut memuat trigger, rencana tindakan, dan output yang diharapkan.

Tabel 4. *Business Continuity Plan (BCP)*

<i>Trigger/Insiden</i>	<i>Business Continuity Plan</i>	<i>Tata Cara Pelaksanaan (Ringkas)</i>	<i>Output</i>
Kegagalan infrastruktur TI	Aktivasi SOP layanan TI terhambat	Identifikasi <i>root cause</i> , alihkan ke backup server/cloud, umumkan status internal	Layanan minimal tetap berjalan
Website tidak bisa diakses	Alihkan publikasi ke kanal alternatif	Publikasi berita via media sosial, siapkan mirror site, eskalasi ke IT	Informasi tetap tersalurkan
Serangan siber terdeteksi	Isolasi sistem dan restore backup bersih	Putus akses, scanning, restore, reset kredensial, klarifikasi publik bila perlu	Sistem pulih & aman
Pemadaman listrik total	Aktifkan UPS/Genset	Server kritikal berjalan di UPS, nyalakan genset, prioritaskan perangkat redaksi	Operasional berlanjut

Bencana alam	Aktivasi mode darurat & remote working	Evakuasi, pindah operasi ke lokasi alternatif/remote, akses data via cloud	Operasi dengan aman	berlanjut
--------------	--	--	---------------------	-----------

e. BC/DR Team dan Communication Plan

Tim BC/DR dibentuk untuk memastikan pembagian tugas yang jelas selama insiden. Komunikasi menjadi aspek penting agar koordinasi berjalan cepat dan keputusan dapat dieksekusi tanpa kebingungan.

Tabel 5. Struktur Tim BC/DR

Peran	Tanggung Jawab	Kontak/Media Komunikasi
BCM Leader / Manajer Operasional	Mengambil keputusan aktivasi BCP, koordinasi lintas tim	Telepon/WA/Email
Tim IT Support	Pemulihan sistem, data, jaringan, keamanan siber	WA Group IT + Ticketing
Tim Redaksi	Menyesuaikan alur kerja berita, prioritas konten krisis	WA Group Redaksi
Tim Publikasi & Sosial Media	Distribusi informasi alternatif, update publik	IG/FB/Twitter + WA
Tim Keamanan & Logistik	Pengamanan aset, listrik cadangan, kebutuhan operasional	Telepon/WA

Communication plan meliputi: (1) kanal komunikasi internal (WhatsApp Group resmi, telepon, email) untuk koordinasi cepat; (2) kanal komunikasi eksternal (mitra hosting, vendor, kontributor) untuk dukungan pemulihan; dan (3) komunikasi publik melalui media sosial atau pernyataan resmi agar publik mengetahui status layanan.

f. Training and Testing Method

Pengujian dan pelatihan dilakukan agar tim memahami prosedur dan BCP dapat dievaluasi efektivitasnya. Pengujian yang konsisten juga membantu meningkatkan kepatuhan terhadap RTO/RPO yang telah ditetapkan.

Tabel 6. Training & Testing Methods

Jenis Uji	Frekuensi	Skenario	Kriteria Sukses	Dokumentasi
Tabletop Exercise	6 bulan	Website down, pemadaman listrik	Tim memahami peran & alur eskalasi	Notulen & evaluasi
Uji Restore Backup	3 bulan	Pemulihan database/arsip	Restore sesuai RTO/RPO	Log pemulihan
Simulasi Serangan Siber	6 bulan	Phishing/deface	Respon cepat, isolasi, pemulihan	Laporan insiden
Audit SOP BCP	12 bulan	Review dokumen & perubahan proses	BCP up to date	Versi dokumen

g. Komponen Matrix BCP

Berikut BCP Matrix standar ISO 22301 yang berisi: proses bisnis kritis, ancaman, dampak, RTO, strategi mitigasi, dan prosedur pemulihan.

Table 7. Matrix BCP

Proses Bisnis	Ancaman	Dampak Gangguan	RTO	RPO	Strategi Mitigasi	Prosedur Pemulihan (BCP)
Distribusi berita via media sosial	Server down, jaringan putus	Publik tidak menerima informasi, engagement turun	2 jam	1 jam	Backup server, koneksi internet cadangan, SOP posting darurat	Publikasi dialihkan ke media sosial manual, gunakan device cadangan, update informasi darurat
Portal berita (website Media Informasi Tuban)	Serangan siber, malware, DDoS	Website tidak dapat diakses, reputasi menurun	4 jam	1 jam	Firewall, IDS/IPS, patching, backup harian	Isolasi server, restore backup, aktifkan mirror site
Produksi konten redaksi	Kerusakan PC/Software	Terhambatnya penyusunan berita	8 jam	4 jam	Penyediaan laptop cadangan, cloud document	Pindah ke perangkat cadangan, akses file via cloud
Sistem arsip berita	Kegagalan storage	Kehilangan data arsip	12 jam	6 jam	Backup offsite & cloud	Restore data dari backup, verifikasi integritas file
Sistem komunikasi internal	Gangguan email/jaringan	Koordinasi redaksi terhambat	12 jam	6 jam	Alternatif WA/telepon	Pindah ke jalur komunikasi alternatif

h. Tabel Racichart

Tabel RACI-CHART merupakan pengembangan dari model RACI (*Responsible, Accountable, Consulted, Informed*) yang digunakan untuk menjelaskan pembagian peran dan tanggung jawab dalam proses Business Continuity Management (BCM). Model ini membantu organisasi memastikan bahwa setiap aktivitas dalam BCP memiliki penanggung jawab yang jelas sehingga proses pemulihan dapat berjalan lebih efektif, cepat, dan terkoordinasi.

Tabel 8. Raci Chart

Aktivitas BCP	Manajemen Media Informasi Tuban	Tim IT	Tim Sosial Media	Tim Redaksi	Admin Proyek	Mitra Eksternal	Publik Pembaca
Risk Assessment	A	C	C	C	R	I	-
Business Impact Analysis	A	C	C	C	R	I	-

Aktivitas BCP	Manajemen Media Informasi Tuban	Tim IT	Tim Sosial Media	Tim Redaksi	Admin Proyek	Mitra Eksternal	Publik Pembaca
Penyusunan BCP	A	R	R	R	R	C	-
Aktivasi BCP saat	A	R	R	R	R	I	I
Gangguan Pemulihan Sistem IT	C	A/R	I	I	I	I	-
Pengumuman publik	C	I	I	A/R	R	I	I
Informasi gangguan & pemulihan	C	I	A/R	I	R	I	I
Komunikasi Krisis	A	C	C	C	R	I	I
Evaluasi dan Pelaporan	A	C	C	C	R	I	I
Testing dan Training BCP	A	R	R	R	R	C	-

KESIMPULAN

Penerapan Business Continuity Management (BCM) pada Media Informasi Kabupaten Tuban berdasarkan ISO 22301 sangat penting untuk menjaga keberlangsungan layanan informasi publik. Hasil *risk assessment* menunjukkan risiko dominan berasal dari aspek TI (server down, serangan siber, gangguan jaringan), faktor pendukung operasional (pemadaman listrik, kerusakan perangkat), serta faktor manusia (kesalahan operasional). *Business Impact Analysis* (BIA), layanan yang paling kritis adalah distribusi berita via media sosial dan portal berita digital dengan target pemulihan yang relatif cepat (RTO 2–4 jam). Strategi mitigasi yang disarankan meliputi redundansi sistem, penguatan keamanan siber, penerapan kebijakan backup dan uji *restore* rutin, serta pembentukan tim BC/DR dengan alur komunikasi krisis yang jelas. *Business Continuity Plan* (BCP) yang dirancang memberikan pedoman langkah-langkah pemulihan selama berbagai skenario gangguan. Dengan pelaksanaan pelatihan dan pengujian berkala, sektor media Kabupaten Tuban dapat meningkatkan kesiapan menghadapi insiden sehingga meminimalkan *downtime* dan menjaga reputasi media komunikasi Kabupaten Tuban. Penelitian ini memberikan manfaat praktis bagi Pemerintah Kabupaten Tuban sebagai panduan taktis dalam memetakan proses bisnis kritis daerah dan menetapkan target pemulihan (RTO/RPO) sesuai standar internasional ISO 22301, guna menjamin keberlangsungan penyebaran informasi publik secara akurat dan meminimalkan hoaks di tengah situasi krisis atau bencana. Bagi masyarakat, penelitian ini memastikan adanya akses informasi darurat, cepat, dan terpercaya langsung dari saluran resmi pemerintah daerah. Sementara dari aspek akademis, studi ini berkontribusi sebagai referensi empiris dan rujukan ilmiah mengenai implementasi Business Continuity Management System (BCMS) yang berfokus pada sektor tata kelola pemerintahan dan industri media informasi di tingkat daerah.

DAFTAR PUSTAKA

- [1] Dinas Komunikasi dan Informatika Kabupaten Tuban, *Laporan Akuntabilitas Kinerja Instansi Pemerintah (LAKIP) Dinas Komunikasi dan Informatika Kabupaten Tuban Tahun 2024*, Diskominfo Kabupaten Tuban, Tuban, Indonesia, 2025.
- [2] International Organization for Standardization. (n.d.). ISO 22301: Business continuity management systems — Brochure. Geneva: ISO.

- [3] R. S. Tarigan and A. P. Widodo, "Analisis Risiko dan Dampak Bisnis Layanan Publik Digital Terintegrasi Menggunakan Metode BIA dan ISO 22301," *Jurnal Sistem Informasi Bisnis*, vol. 13, no. 2, pp. 142–151, Jul. 2023.
- [4] Pamungkas, E. D. ... Akbar, H. (2023). *Disaster Recovery Plan Analysis Based on the NIST SP 800-34 Framework (Case Study : PT Wijaya Karya (Persero) Tbk .)*. 4(09), 936–947.
- [5] Păunescu, C. ... Blid, L. (2018). *Business impact analysis for business continuity : Evidence from Romanian enterprises on critical functions*. 13(3), 1035–1050. <https://doi.org/10.2478/mmcks-2018-0021>. Vol.
- [6] Attariqh, A. R., Nelvina, B. U., Purnomo, C. N., Lucky, F. R., Pratama, I. S., Mawla, M. F., Pembangunan, U., & Veteran, N. (2025). *Rancangan Keamanan Informasi Dan Perancangan Disaster Recovery Satker Zyx*. 19, 378–402.
- [7] Wibowo, B. S. A., & Hermawan, A. (2023). *Faktor Dan Rencana Aksi Implementasi Bcms Pada Sektor Publik: Studi Kasus Pada Sekretariat Utama BPKP*. 6(3), 323–344. <https://doi.org/10.22219/jaa.v6i3.27089>
- [8] Hendaryatna ... Widodo, A. M. (2023). *Performance Evaluation of Business Continuity Plan in Dealing with Threats and Risks in Cilegon Companies Use ISO 22301 : 2019 & NIST Sp 800-30 R1 Frameworks Case Study : PT. X*. 1(12), 1159–1174
- [9] National Institute of Standards and Technology. (2010). *Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34 Revision 1)*. Gaithersburg, MD: U.S. Department of Commerce.
- [10] A. H. S. Barahama, S. Suroto, and Y. T. Mursityo, "Perancangan Business Continuity Plan (BCP) Layanan E-Government Berdasarkan Standar ISO 22301:2019 (Studi Kasus: Dinas Komunikasi dan Informatika Provinsi Jawa Timur)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 12, pp. 5420–5429, Dec. 2021.
- [11] Federal Emergency Management Agency. (n.d.). *Continuity Plan Template*. Washington, DC: FEMA.
- [12] Federal Emergency Management Agency. (2020). *Continuity of Operations (COOP) Planning Template for Federal Departments and Agencies*. Washington, DC: FEMA.
- [13] Cabinet Office. (2011). *Business Continuity Management Toolkit*. London: UK Government.
- [14] NHS England. (2023). *NHS England Business Continuity Management Toolkit (Version 2)*. London: NHS England.
- [15] NHS England. (2023). *Part 1A: Business Continuity Management Strategy*. London: NHS England.
- [16] St Helens Council. (n.d.). *Business Continuity Management Toolkit: Business Continuity and Resilience for Businesses and Voluntary Organisations*. St Helens: St Helens Council.