OPERATIONAL CYBER RESILIENCE SEBAGAI VARIABEL MEDIASI ANTARA DIGITAL TRANSFORMATION DAN BUSINESS CONTINUITY PADA PT XYZ

Mochamad Ardi Setyawan
Universitas Tulungagung, Indonesia
email: mochamadardisetyawan@unita.ac.id

Article Info

Article history:

Received : 28 - 04, 2026
Revised : 07 - 05, 2026
Accepted : 28 - 05, 2026

Keywords:

business continuity, digital transformation, operational cyber resilience, keamanan siber, studi kasus

ABSTRACT

Transformasi digital meningkatkan kecepatan, integrasi, dan fleksibilitas proses bisnis, tetapi pada saat yang sama memperluas ketergantungan organisasi terhadap sistem informasi, layanan komputasi awan, konektivitas, data, dan pihak ketiga digital. Penelitian ini bertujuan menganalisis peran operational cyber resilience sebagai variabel mediasi antara digital transformation dan business continuity pada PT XYZ. Operational cyber resilience didefinisikan sebagai kemampuan sosio-teknis organisasi untuk mengantisipasi, menahan, mendeteksi, merespons, memulihkan, dan beradaptasi terhadap gangguan yang menggunakan atau memengaruhi sumber daya siber, sambil mempertahankan layanan bisnis kritis pada tingkat yang dapat diterima. Penelitian menggunakan pendekatan kualitatif studi kasus dengan sintesis tematik dan pattern matching terhadap dimensi transformasi digital, ketahanan siber operasional, dan keberlangsungan bisnis. Hasil analisis konseptual menunjukkan bahwa transformasi digital menyediakan visibilitas data, otomatisasi, fleksibilitas kerja, dan skalabilitas infrastruktur yang berpotensi memperkuat keberlangsungan bisnis. Namun, manfaat tersebut tidak otomatis terbentuk karena peningkatan konektivitas juga menciptakan risiko konsentrasi teknologi, serangan siber, kegagalan integrasi, serta ketergantungan vendor. Operational cyber resilience memediasi hubungan tersebut melalui tata kelola risiko siber yang terintegrasi, arsitektur yang tahan gangguan, kemampuan deteksi dan respons, pemulihan berbasis prioritas bisnis, serta pembelajaran pascainsiden. Dengan demikian, mediasi yang terbentuk bersifat parsial: transformasi digital memiliki pengaruh langsung terhadap kontinuitas, tetapi dampaknya menjadi lebih stabil dan dapat dipertanggungjawabkan ketika diterjemahkan menjadi kapabilitas ketahanan siber operasional. Implikasi penelitian menekankan perlunya penyelarasan strategi digital, keamanan siber, manajemen risiko, dan business continuity management dalam satu kerangka operasional yang diuji secara berkala.

Corresponding Author:

Author Name
Affiliation
Email: abcd@gmail.com

1. PENDAHULUAN

Perubahan lingkungan bisnis yang ditandai oleh percepatan teknologi, volatilitas permintaan, ketergantungan pada ekosistem digital, serta meningkatnya ancaman siber telah menjadikan transformasi digital dan keberlangsungan bisnis sebagai dua agenda strategis yang tidak dapat dipisahkan. Organisasi

menggunakan komputasi awan, enterprise resource planning, analitik data, otomatisasi proses, aplikasi bergerak, kecerdasan buatan, dan integrasi application programming interface untuk meningkatkan efisiensi dan menciptakan pengalaman pelanggan yang lebih baik. Transformasi digital bukan sekadar penggantian teknologi lama dengan teknologi baru, melainkan perubahan menyeluruh pada strategi, struktur, proses, kapabilitas, dan pola penciptaan nilai organisasi (Vial, 2019; Verhoef et al., 2021).

Di sisi lain, digitalisasi yang semakin luas meningkatkan ketergantungan operasi terhadap ketersediaan sistem, integritas data, identitas digital, jaringan komunikasi, dan layanan pihak ketiga. Ketika proses bisnis kritis telah terotomasi dan saling terhubung, gangguan pada satu komponen dapat menyebar dengan cepat ke proses lain. Kegagalan layanan komputasi awan, ransomware, kompromi kredensial, kesalahan konfigurasi, kegagalan pembaruan perangkat lunak, atau gangguan penyedia teknologi dapat menghentikan aktivitas operasional meskipun aset fisik perusahaan tidak mengalami kerusakan. Kondisi ini menunjukkan bahwa keberhasilan transformasi digital tidak cukup diukur melalui tingkat adopsi teknologi atau efisiensi proses, tetapi juga melalui kemampuan organisasi mempertahankan layanan penting ketika terjadi gangguan.

Business continuity mengacu pada kemampuan organisasi untuk terus menyediakan produk dan layanan pada tingkat yang dapat diterima setelah terjadinya insiden disruptif. ISO 22301:2019 menempatkan analisis dampak bisnis, penilaian risiko, strategi kontinuitas, prosedur respons, latihan, evaluasi, dan perbaikan berkelanjutan sebagai komponen utama sistem manajemen keberlangsungan bisnis. Dalam konteks operasi digital, business continuity harus terhubung dengan keamanan informasi, respons insiden siber, pemulihan teknologi, manajemen krisis, dan pengelolaan ketergantungan pihak ketiga. Pemisahan fungsi-fungsi tersebut berpotensi menghasilkan rencana yang tampak lengkap secara administratif tetapi gagal ketika diuji pada skenario gangguan yang melintasi batas unit organisasi.

Konsep operational cyber resilience menawarkan jembatan antara agenda transformasi digital dan business continuity. NIST mendefinisikan cyber resiliency sebagai kemampuan untuk mengantisipasi, menahan, memulihkan, dan beradaptasi terhadap kondisi merugikan, tekanan, serangan, atau kompromi yang menggunakan atau dimungkinkan oleh sumber daya siber (Ross et al., 2021). Dalam penelitian ini, istilah operational menegaskan bahwa ketahanan tersebut tidak berhenti pada perlindungan teknis, melainkan harus terlihat pada kemampuan proses bisnis kritis untuk tetap berjalan, beralih ke mode alternatif, dipulihkan sesuai prioritas, dan diperbaiki berdasarkan pembelajaran insiden. Dengan demikian, operational cyber resilience merupakan kapabilitas lintas fungsi yang menggabungkan tata kelola, manusia, proses, teknologi, data, pemasok, dan pengambilan keputusan krisis.

PT XYZ dalam naskah ini digambarkan sebagai perusahaan nasional yang mengandalkan platform digital untuk mendukung transaksi, operasi internal, layanan pelanggan, pelaporan manajemen, dan koordinasi dengan mitra. Perusahaan telah menjalankan berbagai inisiatif transformasi digital, seperti integrasi aplikasi inti, migrasi sebagian beban kerja ke cloud, otomatisasi alur kerja, digitalisasi layanan pelanggan, dan penggunaan dashboard analitik. Meskipun inisiatif tersebut meningkatkan fleksibilitas dan kecepatan kerja, terdapat risiko bahwa peningkatan kompleksitas dan ketergantungan digital tidak diikuti dengan peningkatan kapabilitas ketahanan operasional yang sepadan. Isu yang perlu dianalisis adalah apakah transformasi digital secara langsung memperkuat business continuity atau apakah manfaat tersebut terutama muncul melalui operational cyber resilience.

Penelitian mengenai transformasi digital banyak membahas perubahan model bisnis, kapabilitas digital, dan kinerja organisasi, sedangkan penelitian business continuity dan cyber resilience sering berkembang dalam disiplin yang terpisah. Kesenjangan tersebut membuka ruang untuk menjelaskan mekanisme mediasi: transformasi digital menyediakan sumber daya dan kemampuan digital, tetapi operational cyber resilience menentukan apakah sumber daya tersebut dapat dipertahankan dan dipulihkan dalam kondisi gangguan. Oleh karena itu, tujuan penelitian ini adalah: (1) mengidentifikasi bentuk transformasi digital yang relevan dengan kesinambungan operasi PT XYZ; (2) menganalisis dimensi operational cyber resilience yang menghubungkan transformasi digital dan business continuity; (3) menjelaskan sifat mediasi operational cyber resilience; dan (4) merumuskan rekomendasi manajerial untuk penguatan keberlangsungan bisnis berbasis risiko siber.

2. TINJAUAN PUSTAKA

2.1 Digital Transformation

Digital transformation merupakan proses perubahan organisasi yang dipicu dan dimungkinkan oleh kombinasi teknologi informasi, komputasi, komunikasi, dan konektivitas. Vial (2019) menjelaskan bahwa teknologi digital dapat menciptakan disrupsi yang mendorong respons strategis, perubahan jalur penciptaan nilai, serta penyesuaian struktur organisasi. Verhoef et al. (2021) membedakan digitization, digitalization, dan digital transformation. Digitization berfokus pada konversi informasi analog menjadi digital; digitalization menggunakan teknologi untuk memperbaiki proses; sedangkan digital transformation mencakup perubahan yang lebih luas terhadap model bisnis, struktur, kapabilitas, dan hubungan dengan pemangku kepentingan.

Strategi transformasi digital perlu mencakup penggunaan teknologi, perubahan dalam penciptaan nilai, perubahan struktural, dan aspek finansial (Matt et al., 2015). Dalam perspektif strategi bisnis digital, batas antara strategi teknologi informasi dan strategi bisnis menjadi semakin kabur karena sumber daya digital melekat langsung pada produk, layanan, proses, dan jaringan mitra (Bharadwaj et al., 2013). Oleh karena itu, indikator transformasi digital pada PT XYZ tidak hanya berupa jumlah aplikasi atau tingkat investasi, tetapi juga tingkat integrasi proses, kualitas data, kemampuan otomatisasi, fleksibilitas infrastruktur, kompetensi digital, tata kelola portofolio, dan perubahan cara kerja.

Transformasi digital memiliki karakter ambivalen terhadap continuity. Di satu sisi, cloud, otomatisasi, kolaborasi digital, dan data real-time dapat meningkatkan redundansi, kerja jarak jauh, pengambilan keputusan, dan kemampuan pemulihan. Di sisi lain, konsolidasi pada platform tertentu, integrasi yang kompleks, penggunaan komponen pihak ketiga, serta perluasan permukaan serangan dapat menciptakan titik kegagalan baru. Dengan demikian, digital transformation diposisikan sebagai antecedent yang menyediakan potensi ketahanan, tetapi efeknya bergantung pada bagaimana risiko dan ketergantungan digital dikelola.

2.2 Operational Cyber Resilience

Cyber resilience berbeda dari pendekatan keamanan siber yang hanya berorientasi pada pencegahan. Asumsi dasarnya adalah bahwa tidak semua serangan, kesalahan, atau kegagalan dapat dicegah. Organisasi harus mampu mempertahankan fungsi esensial ketika kontrol preventif ditembus dan harus mampu memulihkan operasi secara aman. NIST SP 800-160 Volume 2 Revision 1 menempatkan empat tujuan utama cyber resiliency, yaitu anticipate, withstand, recover, dan adapt (Ross et al., 2021). Tujuan tersebut dapat diwujudkan melalui teknik seperti segmentasi, redundansi, diversitas, deception, monitoring, pembatasan hak akses, perubahan dinamis, substantiated integrity, dan reconstitution.

Penambahan istilah operational pada penelitian ini menempatkan layanan bisnis kritis sebagai unit analisis. Operational cyber resilience adalah kemampuan terintegrasi untuk: (1) memahami layanan penting dan ketergantungannya; (2) mengantisipasi ancaman serta skenario kegagalan; (3) menahan dampak agar tidak melewati batas toleransi; (4) mendeteksi dan merespons secara cepat; (5) memulihkan data, aplikasi, dan proses sesuai prioritas; serta (6) beradaptasi melalui pembelajaran dan perbaikan. Konsep ini beririsan dengan operational resilience yang menilai kemampuan suatu sistem mempertahankan fungsi kritis sepanjang waktu gangguan (Ganin et al., 2016) dan organizational resilience sebagai meta-capability yang mencakup anticipation, coping, serta adaptation (Duchek, 2020).

Dimensi operational cyber resilience yang digunakan dalam artikel ini terdiri atas enam komponen. Pertama, governance and risk integration, yaitu kejelasan akuntabilitas, risk appetite, kebijakan, dan integrasi risiko siber dengan risiko perusahaan. Kedua, situational awareness, yaitu inventaris aset, pemetaan ketergantungan, monitoring, threat intelligence, dan deteksi anomali. Ketiga, protective and withstand capability, yaitu arsitektur berlapis, segmentasi, manajemen identitas, hardening, redundansi, dan kapasitas untuk tetap beroperasi secara terdegradasi. Keempat, coordinated response, yaitu playbook, command structure, komunikasi krisis, dan keputusan lintas fungsi. Kelima, recoverability, yaitu backup yang terlindungi, failover, disaster recovery, target recovery time objective dan recovery point objective yang selaras dengan business impact analysis. Keenam, learning and adaptation, yaitu post-incident review, pengujian skenario, pengelolaan temuan, dan pembaruan desain.

2.3 Business Continuity

Business continuity merupakan kemampuan organisasi untuk melanjutkan penyediaan produk atau layanan pada kapasitas yang telah ditentukan setelah terjadi gangguan. ISO 22301:2019 mengarahkan organisasi untuk memahami konteks, menetapkan kepemimpinan dan kebijakan, melakukan business impact analysis dan risk assessment, menentukan strategi kontinuitas, mengembangkan prosedur, melakukan latihan, mengevaluasi kinerja, dan meningkatkan sistem secara berkelanjutan. Business continuity tidak identik dengan disaster recovery. Disaster recovery terutama berfokus pada pemulihan teknologi, sedangkan business continuity mencakup keberlanjutan proses, manusia, fasilitas, informasi, pemasok, komunikasi, dan keputusan manajemen.

Dalam operasi digital, ukuran business continuity harus mencerminkan kemampuan layanan penting untuk bertahan dan pulih. Indikator yang relevan mencakup pemenuhan maximum tolerable period of disruption, pencapaian RTO dan RPO, ketersediaan alternatif proses, kemampuan pemindahan beban kerja, keandalan komunikasi krisis, kesiapan personel, pemulihan data yang bersih, serta konsistensi pengujian. NIST SP 800-34 Rev. 1 menekankan hubungan antara business impact analysis, strategi pemulihan, pengembangan rencana, pengujian, pelatihan, dan pemeliharaan rencana (Swanson et al., 2010).

Business continuity yang efektif bersifat adaptif. Herbane (2019) menunjukkan bahwa resilience tidak hanya terkait pemulihan jangka pendek, tetapi juga pembaruan strategis dan pembelajaran organisasi. Karena itu, keberlangsungan bisnis pada PT XYZ perlu dipahami sebagai hasil dari kombinasi kesiapan sebelum insiden, koordinasi selama insiden, kecepatan pemulihan, dan kemampuan memperbaiki sistem setelah insiden.

2.4 Hubungan Antarvariabel dan Kerangka Mediasi

Hubungan digital transformation dengan business continuity dapat berlangsung secara langsung. Digitalisasi dokumen mendukung akses jarak jauh; cloud dapat menyediakan elastisitas dan replikasi; otomatisasi dapat mengurangi ketergantungan pada aktivitas manual; dan dashboard terintegrasi dapat mempercepat pengambilan keputusan. Namun, hubungan langsung tersebut tidak selalu menghasilkan continuity yang andal. Teknologi yang sama dapat menimbulkan risiko baru apabila konfigurasi lemah, dependensi tidak dipetakan, backup tidak dapat dipulihkan, atau respons insiden tidak terkoordinasi.

Operational cyber resilience berperan sebagai mekanisme konversi yang mengubah kapabilitas digital menjadi kemampuan kontinuitas. Transformasi digital meningkatkan data, konektivitas, otomatisasi, dan skalabilitas. Operational cyber resilience memastikan bahwa aset digital tersebut dikelola melalui governance, protected architecture, monitoring, incident response, recovery, dan adaptive learning. Selanjutnya, kemampuan tersebut mengurangi kemungkinan gangguan meluas, memperpendek durasi pemulihan, dan menjaga layanan penting pada batas dampak yang dapat diterima.

Berdasarkan hubungan tersebut, penelitian ini menggunakan empat proposisi analitis. Pertama, digital transformation berkontribusi positif terhadap business continuity. Kedua, digital transformation mendorong pembentukan operational cyber resilience ketika implementasinya memasukkan prinsip security and resilience by design. Ketiga, operational cyber resilience berkontribusi positif terhadap business continuity. Keempat, operational cyber resilience memediasi hubungan antara digital transformation dan business continuity. Mediasi diperkirakan bersifat parsial karena beberapa manfaat digital, seperti kerja jarak jauh dan otomatisasi, dapat langsung mendukung continuity, sedangkan stabilitas manfaat dalam kondisi serangan atau kegagalan sangat bergantung pada ketahanan siber operasional.

Tabel 1. Konstruk dan indikator analitis

Konstruk	Dimensi	Indikator Kualitatif	Peran
Digital Transformation	Teknologi, proses, data, organisasi	Cloud dan integrasi aplikasi; otomatisasi; digitalisasi layanan; kualitas dan akses data; kompetensi digital; tata kelola portofolio.	Variabel awal
Operational Cyber Resilience	Govern, anticipate, withstand, detect/respond, recover, adapt	Pemetaan layanan dan dependensi; risk appetite; segmentasi; IAM; monitoring; playbook; failover; backup terlindungi; latihan; pembelajaran.	Mediator
Business Continuity	Kesiapan, kelangsungan, pemulihan, perbaikan	Pemenuhan RTO/RPO; operasi pada mode alternatif; toleransi dampak; komunikasi krisis; pemulihan layanan; kesiapan pemasok; hasil pengujian.	Variabel hasil

Sumber: Dikembangkan dari Vial (2019), Duchek (2020), Ross et al. (2021), NIST (2024), dan ISO 22301:2019.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus tunggal pada PT XYZ untuk memperoleh pemahaman kontekstual mengenai mekanisme mediasi operational cyber resilience dalam

hubungan digital transformation dan business continuity (Yin, 2018; Creswell & Poth, 2018). Unit analisis adalah layanan bisnis kritis beserta ketergantungan manusia, proses, teknologi, data, fasilitas, dan pihak ketiga. Data idealnya dikumpulkan melalui wawancara semi-terstruktur dengan pimpinan teknologi informasi, keamanan siber, manajemen risiko, operasional, audit internal, pengelola business continuity, dan pemilik proses; observasi terhadap latihan atau simulasi; serta telaah dokumen seperti strategi transformasi digital, arsitektur aplikasi, risk register, business impact analysis, incident response plan, disaster recovery plan, laporan insiden, hasil vulnerability assessment, kontrak penyedia layanan, dan laporan pengujian. Pemilihan informan dilakukan secara purposive berdasarkan peran dan pengetahuan terhadap layanan kritis. Analisis dilakukan melalui pengodean tematik, pemetaan hubungan sebab-akibat, dan pattern matching antara bukti empiris dengan proposisi penelitian; mediasi dinilai dari keberadaan mekanisme yang menunjukkan bahwa inisiatif digital membentuk kapabilitas governance, withstand, response, recovery, dan adaptation yang kemudian meningkatkan continuity. Kredibilitas data dijaga melalui triangulasi sumber, member checking, audit trail, dan pembahasan kasus negatif. Karena data primer PT XYZ belum tersedia pada penyusunan naskah ini, hasil berikut merupakan analisis konseptual berbasis literatur dan skenario organisasi yang harus divalidasi sebelum digunakan sebagai klaim empiris.

4. HASIL DAN PEMBAHASAN

4.1 Transformasi Digital PT XYZ dan Perubahan Profil Ketergantungan

Analisis konseptual menunjukkan bahwa transformasi digital PT XYZ menghasilkan empat manfaat operasional utama. Pertama, integrasi aplikasi dan data mengurangi keterlambatan pertukaran informasi antarunit. Kedua, otomatisasi mempercepat pemrosesan transaksi dan mengurangi kesalahan manual. Ketiga, penggunaan cloud dan akses jarak jauh meningkatkan fleksibilitas lokasi kerja serta kapasitas layanan. Keempat, dashboard analitik memperbaiki visibilitas kondisi operasional dan mendukung keputusan berbasis data. Manfaat tersebut dapat secara langsung mendukung business continuity karena organisasi memiliki alternatif cara bekerja, informasi yang lebih cepat, dan sumber daya komputasi yang lebih adaptif.

Namun, transformasi tersebut juga menggeser profil risiko. Integrasi membuat kegagalan antarmuka atau identitas digital dapat memengaruhi banyak proses sekaligus. Konsolidasi data dan aplikasi pada platform tertentu menciptakan concentration risk. Penggunaan software as a service, managed service, dan komponen open-source memperpanjang rantai ketergantungan yang tidak seluruhnya berada dalam kendali PT XYZ. Otomatisasi dapat mempercepat kesalahan jika aturan atau data input tidak valid. Dengan kata lain, transformasi digital meningkatkan kapasitas organisasi sekaligus meningkatkan blast radius apabila terjadi kompromi atau kegagalan.

Temuan ini konsisten dengan pandangan bahwa digital transformation merupakan perubahan sosio-teknis, bukan proyek teknologi yang berdiri sendiri. Ketika proses menjadi digital, continuity harus dirancang pada level layanan end-to-end. Inventaris server saja tidak cukup; PT XYZ perlu mengetahui layanan apa yang penting, pengguna yang bergantung padanya, aplikasi pendukung, aliran data, identitas, jaringan, pemasok, dan prosedur manual yang tersedia. Pemetaan ini menjadi titik awal operational cyber resilience karena menentukan prioritas proteksi, deteksi, respons, dan pemulihan.

4.2 Dimensi Operational Cyber Resilience sebagai Mekanisme Mediasi

a. Tata Kelola dan Integrasi Risiko

Mekanisme mediasi pertama adalah penyatuan tata kelola transformasi digital dengan manajemen risiko siber dan business continuity. Inisiatif digital yang dievaluasi hanya berdasarkan biaya, jadwal, dan manfaat bisnis cenderung mengabaikan toleransi gangguan, kebutuhan pemulihan, serta ketergantungan pihak ketiga. Operational cyber resilience mengubah proses investasi dengan memasukkan criticality assessment, security architecture review, resilience requirements, RTO/RPO, exit strategy, dan kewajiban pengujian sejak tahap perencanaan.

Pada PT XYZ, tata kelola yang matang mensyaratkan pemilik layanan bisnis bertanggung jawab bersama fungsi TI dan keamanan, bukan menyerahkan seluruh risiko kepada tim teknis. Manajemen perlu menetapkan impact tolerance untuk setiap layanan penting, yaitu batas maksimum dampak yang masih dapat diterima. Batas ini kemudian diterjemahkan menjadi target teknis, kapasitas personel, strategi komunikasi, serta persyaratan vendor. Fungsi Govern dalam NIST CSF 2.0 menguatkan perlunya konteks organisasi, strategi, kebijakan, peran, pengawasan, dan pengelolaan risiko rantai pasok sebagai dasar siklus keamanan siber.

b. **Kemampuan Mengantisipasi dan Memahami Situasi**

Transformasi digital menghasilkan data operasional yang melimpah, tetapi data tersebut baru menjadi sumber resilience apabila digunakan untuk membangun situational awareness. PT XYZ memerlukan inventaris aset yang akurat, klasifikasi data, pemetaan dependensi, baseline perilaku, logging terpusat, monitoring

ketersediaan, dan threat intelligence. Kemampuan ini memungkinkan organisasi mendeteksi gejala gangguan sebelum dampak meluas dan menentukan layanan mana yang harus diprioritaskan.

Kesenjangan yang sering terjadi adalah perbedaan antara daftar aset teknis dan peta layanan bisnis. Tim infrastruktur dapat mengetahui server yang gagal, tetapi manajemen tidak segera mengetahui transaksi, pelanggan, lokasi, atau kewajiban regulasi yang terdampak. Operational cyber resilience memediasi dengan menghubungkan telemetri teknis dan konteks bisnis, sehingga keputusan respons tidak hanya berorientasi pada perangkat, tetapi pada pemulihan fungsi yang paling penting.

c. Kemampuan Menahan Gangguan dan Beroperasi Secara Terdegradasi

Manfaat transformasi digital terhadap continuity akan rapuh jika arsitektur tidak mampu menahan kegagalan. Kapabilitas withstand meliputi segmentasi jaringan, zero-trust-oriented access, least privilege, redundancy, high availability, diversitas komponen, proteksi endpoint, secure configuration, kapasitas jaringan, serta pemisahan domain produksi dan pemulihan. Tujuan utamanya bukan menjamin tidak ada gangguan, melainkan membatasi penyebaran dan mempertahankan fungsi minimum.

Bagi PT XYZ, mode operasi terdegradasi perlu didefinisikan untuk setiap layanan kritis. Contohnya, proses dapat dialihkan ke antrean lokal, transaksi dapat dibatasi pada jenis tertentu, atau persetujuan dapat dilakukan melalui prosedur alternatif dengan kontrol kompensasi. Pengaturan tersebut memperlihatkan bagaimana operational cyber resilience menghubungkan desain digital dan continuity: sistem tidak hanya dibangun untuk kondisi normal, tetapi juga untuk tetap aman ketika sebagian komponen tidak tersedia.

d. Deteksi, Respons, dan Koordinasi Krisis

Transformasi digital dapat mempercepat deteksi melalui monitoring dan otomatisasi, tetapi kecepatan teknis harus diikuti koordinasi organisasi. Respons insiden membutuhkan kriteria eskalasi, incident commander, jalur keputusan, pembagian peran, komunikasi internal-eksternal, keterlibatan legal dan hubungan pelanggan, serta mekanisme pencatatan keputusan. Tanpa struktur tersebut, tim dapat mengisolasi sistem secara teknis tetapi terlambat menentukan dampak bisnis atau menyampaikan informasi kepada pemangku kepentingan.

Pada PT XYZ, playbook sebaiknya disusun berdasarkan skenario, seperti ransomware, kompromi akun istimewa, gangguan cloud, kebocoran data, kegagalan integrasi, dan gangguan penyedia utama. Latihan tabletop perlu melibatkan pimpinan bisnis, bukan hanya tim TI. Hasil latihan menjadi bukti apakah organisasi dapat beralih dari deteksi menuju keputusan operasional dalam waktu yang sesuai dengan impact tolerance.

e. Recoverability dan Pemulihan Berbasis Prioritas Bisnis

Recoverability merupakan mekanisme mediasi yang paling langsung terhadap business continuity. Transformasi digital menyediakan kemampuan replikasi, orchestration, infrastructure as code, dan otomatisasi pemulihan, tetapi efektivitasnya bergantung pada desain backup, pemisahan kredensial, immutability, integritas data, urutan pemulihan, kapasitas lokasi alternatif, serta pengujian end-to-end. Backup yang berhasil dibuat belum tentu dapat dipulihkan secara bersih setelah serangan siber.

PT XYZ perlu menyelaraskan RTO dan RPO dengan hasil business impact analysis, bukan hanya target teknis generik. Pemulihan harus memperhatikan dependensi: aplikasi mungkin telah aktif, tetapi layanan belum dapat digunakan karena identity provider, database, API, jaringan, atau vendor belum pulih. Oleh sebab itu, uji disaster recovery perlu menggunakan skenario kehilangan sistem dan kompromi keamanan, termasuk validasi data, pemeriksaan malware, rekonsiliasi transaksi, dan persetujuan bisnis sebelum layanan dinyatakan normal.

f. Pembelajaran dan Adaptasi

Operational cyber resilience tidak selesai ketika layanan pulih. Organisasi perlu mengubah pengalaman insiden dan latihan menjadi perbaikan kebijakan, arsitektur, proses, kompetensi, dan kontrak pemasok. Duchek (2020) menempatkan adaptation sebagai bagian penting resilience, sedangkan NIST menekankan kemampuan beradaptasi terhadap perubahan ancaman dan kondisi sistem. Mekanisme ini memastikan bahwa investasi transformasi digital tidak menghasilkan akumulasi technical debt dan control debt.

Pada PT XYZ, pembelajaran dapat diformalkan melalui post-incident review tanpa budaya menyalahkan, root cause analysis, pencatatan corrective action, pemilik tindakan, batas waktu, dan verifikasi efektivitas. Indikator yang perlu dipantau bukan hanya jumlah insiden, tetapi juga mean time to detect, mean time to contain, mean time to recover, keberhasilan restore, jumlah temuan berulang, cakupan latihan, dan persentase layanan yang telah memiliki dependency map.

Tabel 2. Matriks analisis mekanisme mediasi pada PT XYZ

Inisiatif Digital	Risiko/Gangguan Potensial	Kapabilitas Mediator	Dampak pada Continuity
Migrasi cloud dan layanan SaaS	Outage, salah konfigurasi, vendor lock-in, kegagalan identitas	Multi-zone design, exit plan, monitoring, backup terpisah, uji failover	Kapasitas dan akses alternatif tersedia; waktu pemulihan lebih terukur
Integrasi API dan otomasi proses	Gangguan berantai, data salah menyebar, kredensial bocor	Segmentasi, API security, circuit breaker, validasi data, mode manual	Blast radius terbatas dan proses kritis tetap dapat berjalan
Kerja digital dan akses jarak jauh	Kompromi akun, endpoint tidak aman, gangguan konektivitas	MFA, conditional access, endpoint detection, redundant connectivity	Tenaga kerja dapat beroperasi dengan risiko terkendali
Analitik dan data terpusat	Korupsi/kehilangan data, single point of failure, privasi	Data classification, immutable backup, replication, integrity checks	Keputusan tetap berbasis data dan pemulihan data lebih terpercaya
Otomasi infrastruktur dan deployment	Perubahan salah berskala luas, supply-chain compromise	Change controls, code signing, rollback, secure pipeline, separation of duties	Pemulihan konfigurasi lebih cepat dan kesalahan dapat dibatalkan

*Sumber: Hasil sintesis konseptual penulis.*Sumber: Hasil sintesis konseptual penulis.

4.3 Sifat Mediasi Operational Cyber Resilience

Hasil pattern matching konseptual mendukung mediasi parsial. Jalur langsung digital transformation menuju business continuity terlihat dari kemampuan akses jarak jauh, digitalisasi dokumen, elastisitas komputasi, dan otomatisasi yang memungkinkan proses tetap berjalan dalam berbagai kondisi. Akan tetapi, jalur langsung tersebut dapat berubah menjadi sumber kerentanan ketika tidak dilengkapi kontrol dan kemampuan pemulihan. Oleh sebab itu, pengaruh yang lebih konsisten berlangsung melalui operational cyber resilience.

Jalur mediasi dapat dijelaskan dalam tiga tahap. Tahap pertama adalah enablement: transformasi digital menyediakan sumber daya berupa data, konektivitas, komputasi, integrasi, otomatisasi, dan tools monitoring. Tahap kedua adalah conversion: governance, architecture, detection-response, recovery, dan learning mengubah sumber daya tersebut menjadi kemampuan menahan serta mengelola gangguan. Tahap ketiga adalah continuity outcome: layanan bisnis dapat dipertahankan, dampak dibatasi, RTO/RPO dicapai, dan pemulihan dilakukan secara aman. Tanpa tahap conversion, digital transformation hanya meningkatkan kapasitas normal operation, bukan kemampuan bertahan pada kondisi abnormal.

Mediasi parsial juga menunjukkan bahwa operational cyber resilience bukan pengganti transformasi digital atau business continuity management. Ketiganya saling melengkapi. Transformasi digital menyediakan kemampuan inovasi dan fleksibilitas; cyber resilience menjaga keandalan kemampuan tersebut dalam kondisi adversarial; sedangkan business continuity menetapkan prioritas layanan, batas dampak, strategi alternatif, dan hasil yang harus dicapai. Integrasi ketiganya menghasilkan digital transformation yang resilient by design dan continuity yang cyber-informed.

4.4 Kesenjangan yang Perlu Diuji pada PT XYZ

Berdasarkan model analisis, terdapat beberapa kesenjangan yang perlu diverifikasi melalui data primer. Pertama, apakah daftar layanan kritis dan dependency map telah disepakati antara unit bisnis dan TI. Kedua, apakah target RTO/RPO konsisten dengan arsitektur nyata, kapasitas pemulihan, dan kontrak vendor. Ketiga, apakah backup terlindungi dari kredensial produksi dan telah diuji untuk skenario ransomware. Keempat, apakah incident response, crisis management, disaster recovery, dan business continuity menggunakan struktur komando dan terminologi yang selaras. Kelima, apakah transformasi digital mewajibkan resilience requirements sebelum go-live. Keenam, apakah hasil latihan dan insiden benar-benar ditutup melalui corrective action yang terukur.

Kesenjangan lain adalah risiko pihak ketiga. PT XYZ dapat memiliki kontrol internal yang baik, tetapi continuity tetap terganggu apabila vendor utama tidak mampu memenuhi target pemulihan, tidak menyediakan transparansi insiden, atau tidak memiliki exit mechanism yang realistis. Karena itu, penilaian vendor perlu meliputi arsitektur layanan, lokasi data, subprocessor, dukungan insiden, hak audit, portabilitas data, strategi penghentian layanan, dan bukti pengujian kontinuitas.

Aspek manusia juga menentukan keberhasilan mediasi. Kapabilitas resilience tidak terbentuk hanya melalui produk keamanan. Personel harus memahami peran pada kondisi darurat, memiliki kompetensi untuk mengambil keputusan dengan informasi terbatas, dan mampu berkomunikasi lintas fungsi. Budaya yang terlalu menghukum kesalahan dapat menunda pelaporan insiden, sedangkan budaya yang tidak disiplin dapat mengabaikan kontrol. PT XYZ perlu membangun budaya pelaporan cepat, akuntabilitas yang jelas, dan pembelajaran yang konstruktif.

4.5 Implikasi Manajerial

Implikasi pertama adalah perlunya model operasi terpadu. Komite transformasi digital, keamanan siber, manajemen risiko, dan business continuity perlu menggunakan daftar layanan kritis dan impact tolerance yang sama. Portofolio proyek digital harus dinilai berdasarkan manfaat, risiko, ketergantungan, dan kemampuan pemulihan. Keputusan arsitektur yang meningkatkan efisiensi tetapi menciptakan single point of failure harus dilengkapi strategi mitigasi dan penerimaan risiko yang eksplisit.

Implikasi kedua adalah pergeseran ukuran keberhasilan. PT XYZ tidak cukup mengukur jumlah sistem yang dimigrasikan, jumlah kontrol yang diterapkan, atau persentase uptime tahunan. Organisasi perlu mengukur kemampuan menghadapi skenario nyata melalui recovery success rate, time to detect, time to contain, time to restore, pencapaian impact tolerance, efektivitas komunikasi krisis, dan penyelesaian temuan latihan. Pengukuran harus dilakukan per layanan bisnis, bukan hanya per komponen teknologi.

Implikasi ketiga adalah pengujian berbasis skenario end-to-end. Latihan perlu mensimulasikan kompromi yang menyebabkan data tidak dapat dipercaya, bukan hanya outage sederhana. Skenario dapat mencakup kehilangan akses identitas, ransomware pada produksi dan backup, kegagalan cloud region, korupsi data, serta tidak tersedianya vendor. Latihan yang baik menghasilkan keputusan, bukti, waktu aktual, hambatan koordinasi, dan daftar perbaikan yang dapat diverifikasi.

5. KESIMPULAN

5.1 Kesimpulan

Transformasi digital pada PT XYZ berpotensi meningkatkan business continuity melalui integrasi informasi, otomatisasi, fleksibilitas kerja, dan skalabilitas teknologi. Akan tetapi, peningkatan ketergantungan pada sistem, data, konektivitas, dan penyedia digital juga memperluas risiko gangguan dan serangan siber. Oleh karena itu, transformasi digital tidak secara otomatis menghasilkan keberlangsungan bisnis.

Operational cyber resilience berperan sebagai variabel mediasi yang menjelaskan bagaimana sumber daya digital dikonversi menjadi kemampuan untuk mempertahankan layanan kritis. Mekanisme mediasi bekerja melalui integrasi tata kelola risiko, pemetaan dependensi, kemampuan mengantisipasi dan mendeteksi, arsitektur yang mampu menahan gangguan, respons lintas fungsi, pemulihan berbasis prioritas bisnis, serta pembelajaran dan adaptasi. Hubungan mediasi diperkirakan bersifat parsial karena digital transformation juga memiliki pengaruh langsung terhadap continuity, tetapi ketahanan dan konsistensi manfaatnya sangat bergantung pada kapabilitas cyber resilience.

Secara teoretis, penelitian ini menghubungkan literatur digital transformation, organizational/operational resilience, cyber resilience, dan business continuity dalam satu model proses. Secara praktis, model menunjukkan bahwa agenda digital, keamanan, risiko, dan continuity harus dikelola sebagai satu sistem sosio-teknis. Kesimpulan ini masih bersifat konseptual dan perlu dikonfirmasi melalui data empiris PT XYZ.

5.2 Saran

1. PT XYZ perlu menetapkan daftar layanan bisnis kritis, pemilik layanan, dependency map, dan impact tolerance sebagai dasar bersama transformasi digital, keamanan siber, dan business continuity.
2. Setiap proyek digital perlu menerapkan security and resilience by design, termasuk persyaratan availability, recoverability, logging, segregasi, exit strategy, dan pengujian sebelum go-live.
3. Perusahaan perlu menyelaraskan business impact analysis, risk register, incident response plan, disaster recovery plan, crisis communication plan, dan rencana continuity agar tidak terjadi tumpang tindih atau celah tanggung jawab.
4. Backup dan pemulihan perlu diuji secara berkala pada skenario siber, termasuk ransomware, kredensial administrator yang dikompromikan, data yang korup, dan kegagalan vendor. Keberhasilan backup harus dinilai dari keberhasilan restore yang aman dan utuh.
5. PT XYZ perlu membangun program latihan berjenjang yang mencakup tabletop exercise untuk pimpinan, technical recovery exercise, dan simulasi end-to-end dengan pemasok penting.

6. Pengukuran maturity sebaiknya menggunakan indikator berbasis layanan seperti pencapaian impact tolerance, mean time to detect, mean time to contain, mean time to recover, persentase layanan dengan dependency map, tingkat keberhasilan restore, dan penyelesaian corrective action.
7. Penelitian lanjutan disarankan mengumpulkan data wawancara, observasi latihan, dan dokumen internal, kemudian membandingkan beberapa layanan kritis atau beberapa perusahaan agar pola mediasi dapat diuji secara lebih kuat. Studi kuantitatif selanjutnya dapat mengembangkan instrumen pengukuran dan menguji pengaruh langsung serta tidak langsung dengan structural equation modeling.

DAFTAR PUSTAKA

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471–482. https://doi.org/10.25300/MISQ/2013/37:2.3

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. Business Research, 13, 215–246. https://doi.org/10.1007/s40685-019-0085-7

Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A., Mangoubi, R., & Linkov, I. (2016). Operational resilience: Concepts, design and analysis. Scientific Reports, 6, 19540. https://doi.org/10.1038/srep19540

Herbane, B. (2019). Rethinking organizational resilience and strategic renewal in SMEs. Entrepreneurship & Regional Development, 31(5–6), 476–495. https://doi.org/10.1080/08985626.2018.1541594

International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements. ISO.

International Organization for Standardization. (2020). ISO 22313:2020 Security and resilience—Business continuity management systems—Guidance on the use of ISO 22301. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO.

Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. Business & Information Systems Engineering, 57(5), 339–343. https://doi.org/10.1007/s12599-015-0401-5

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach (NIST Special Publication 800-160, Vol. 2, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency planning guide for federal information systems (NIST Special Publication 800-34, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-34r1

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research, 122, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.