Available on: https://jefrr.ep-journals.org/ E-ISSN: 3051-3650, P-ISSN: 3051-3642

Journal of Economic Finance Research and Review

Volume: 02 Issue: 08 August 2026

Business Continuity and Organizational Resilience Across the Disaster Management Cycle: A Public-Private Common Operating Picture Framework

SK Monirul Islam Mahadi

Department of Emergency and Threat Response Management, Rowan University, Glassboro, New Jersey, USA

Published Date: August 15, 2026 **Article DOI: 10.65150/EP-jefrr/V2E8/2026-07**

ABSTRACT: Disasters and complex emergencies disrupt not only public safety systems but also the organizations, infrastructure networks, supply chains, utilities, healthcare providers, logistics systems, and service sectors that communities depend on for continuity and recovery. Although business continuity management is often treated as an internal organizational responsibility, major disasters show that continuity cannot be achieved by individual organizations acting alone. This article uses a qualitative document-based conceptual analysis to examine how business continuity and organizational resilience depend on public-private coordination across the disaster management cycle. The analysis synthesizes business continuity and organizational resilience standards, emergency management doctrine, Community Lifelines guidance, situational awareness theory, public-private coordination research, supply chain resilience literature, infrastructure interdependency theory, and emergency information systems research. The findings show that business continuity gaps are often coordination, dependency-visibility, information-sharing, and recovery-tracking problems, not only internal planning failures. The article develops a six-component Public-Private Common Operating Picture framework that integrates risk intelligence and dependency mapping, public-private information sharing, critical service continuity coordination, infrastructure and supply chain visibility, operational recovery tracking, and resilience learning. The article contributes to disaster management and business continuity scholarship by reframing business continuity as a public-private disaster resilience function and by positioning the Common Operating Picture as a human-led decision support mechanism for connecting organizational operations with community lifeline stabilization and operational recovery.

KEYWORDS: business continuity; organizational resilience; Common Operating Picture; qualitative document analysis; public-private coordination; disaster management; critical service continuity; community lifelines; supply chain resilience

INTRODUCTION

Disasters create severe disruption across organizations, communities, infrastructure systems, supply chains, and public services. In these conditions, business continuity becomes more than an internal management function. It becomes part of a wider disaster management challenge involving public agencies, emergency operations centers, infrastructure operators, healthcare systems, logistics providers, suppliers, nonprofit organizations, and affected communities. ISO 22301 identifies business continuity management as a management system for preparing organizations to continue and recover from disruptive incidents, while ISO 22316 frames organizational resilience as the ability to absorb and adapt in changing conditions in order to continue pursuing organizational objectives (International Organization for Standardization [ISO], 2017, 2019).

A business may have a continuity plan, emergency procedures, alternate worksites, backup technology, recovery time objectives, and supplier arrangements, but these internal measures may still fail if external systems are disrupted. Transportation access, electricity, water, communications, public safety, fuel, healthcare access, workforce mobility, and supplier networks directly influence whether an organization can maintain or restore priority services after a disaster (Christopher & Peck, 2004; Rinaldi et al., 2001; Sheffi & Rice, 2005). Organizational resilience during disasters therefore depends not only on internal preparedness but also on the ability to coordinate with emergency management agencies, infrastructure operators, suppliers, and community partners across the disaster management cycle (Comfort, 2007; Kapucu, 2006; Tierney, 2007).

Emergency management doctrine supports this broader view. FEMA's National Incident Management System emphasizes communications and information management, resource coordination, shared situational awareness, and the Common Operating Picture as essential elements of incident management (Federal Emergency Management Agency [FEMA], 2017). NIMS also recognizes that government, nongovernmental organizations, and private sector partners must work together during incidents, which directly supports the argument that business continuity should be connected to public-private emergency coordination (FEMA, 2017).

FEMA's Community Lifelines approach further strengthens the connection between business continuity and disaster management. Community Lifelines organize disaster impacts around essential services such as safety and security, food, hydration, shelter, health and medical services, energy, communications, transportation, hazardous materials, and water systems (FEMA, 2023). These lifelines are not maintained by government alone. Energy restoration depends on utilities, contractors, fuel providers, equipment vendors, and logistics systems. Food access depends on

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

retailers, distributors, warehouses, transportation networks, and suppliers. Healthcare continuity depends on hospitals, pharmacies, medical supply chains, insurers, and emergency medical logistics.

A Common Operating Picture is especially relevant because disasters produce fragmented information across public, private, nonprofit, and community systems. Public agencies may know incident priorities, emergency declarations, evacuation zones, shelter needs, public safety conditions, and resource constraints. Utility companies may know outage locations, repair priorities, and restoration timelines. Transportation agencies may know road closures, bridge damage, public transit interruption, and access limitations. Businesses may know workforce availability, facility damage, customer demand, inventory status, supplier disruption, and operational capacity. When these information streams remain disconnected, public agencies and private organizations may make decisions using incomplete, delayed, or inconsistent information (Comfort, 2007; Kapucu, 2006; Turoff et al., 2004).

This article develops an Integrated Public-Private Common Operating Picture Framework for Business Continuity and Organizational Resilience. It does not propose a new software product and does not claim to test the framework empirically. Instead, it uses qualitative document-based conceptual analysis to synthesize selected standards, doctrine, official guidance, and peer-reviewed scholarship into a practical framework for integrating shared situational awareness, dependency visibility, critical service continuity, infrastructure and supply chain information, operational recovery tracking, and resilience learning.

Research Questions

RQ1: How do business continuity and organizational resilience depend on public-private coordination across the disaster management cycle?

RQ2: What business continuity gaps emerge when organizations lack shared situational awareness, infrastructure dependency visibility, supply chain information, and coordination with emergency management partners?

RQ3: How can an Integrated Public-Private Common Operating Picture Framework strengthen critical service continuity, organizational resilience, and operational recovery before, during, and after disasters?

LITERATURE REVIEW

Business Continuity and Organizational Resilience

Business continuity is a structured organizational capability for preparing for disruption, maintaining priority operations, and restoring services within acceptable timeframes. ISO 22301 provides requirements for establishing, implementing, maintaining, and improving a business continuity management system (ISO, 2019). This makes business continuity more than an emergency plan. It is a management system involving leadership commitment, business impact analysis, risk assessment, continuity strategies, exercises, performance evaluation, and continual improvement.

Organizational resilience expands the discussion by emphasizing the broader ability of organizations to absorb disruption, adapt to changing conditions, and continue pursuing their objectives. ISO 22316 provides guidance for enhancing organizational resilience and describes resilience as a capability that enables organizations to anticipate, respond to, and adapt to threats and opportunities arising from sudden or gradual change (ISO, 2017). Business continuity focuses on maintaining and restoring priority services, while organizational resilience includes leadership, culture, stakeholder relationships, adaptation, and learning (ISO, 2017, 2019; Sheffi & Rice, 2005).

In disaster management, business continuity becomes more complex because organizational disruption is rarely isolated. A business may lose access to employees, suppliers, transportation routes, utilities, telecommunications, facilities, customers, fuel, financial systems, or public services. Christopher and Peck (2004) argue that resilient supply chains require visibility, flexibility, collaboration, and attention to vulnerability across networks. Sheffi and Rice (2005) similarly emphasize enterprise resilience as the capacity to withstand disruption and recover operations. These arguments show that continuity cannot be understood only as an internal organizational process. It must also be examined as a coordination problem involving external dependencies.

Public-Private Coordination in Disaster Management

Public-private coordination is central to disaster management because many essential services are operated, owned, supplied, or restored by private-sector organizations. Energy, telecommunications, transportation, healthcare, food distribution, logistics, construction, banking, fuel, retail supply chains, and information technology are deeply connected to disaster response and recovery (FEMA, 2023; Tierney, 2007). NIMS explicitly recognizes that incident management requires coordination among government, nongovernmental organizations, and the private sector (FEMA, 2017).

The coordination problem becomes visible during large scale disasters. Public agencies need timely information about supply chain disruption, utility restoration, facility closures, fuel availability, private sector resource capacity, employee mobility, and business reopening status. Businesses need timely information about road closures, evacuation orders, curfews, emergency declarations, restoration priorities, public safety conditions, shelter needs, infrastructure status, and community recovery priorities. Kapucu (2006) shows that effective emergency management depends on interorganizational communication and information technologies that support emergency decision-making. Comfort (2007) similarly argues that crisis management performance depends on cognition, communication, coordination, and control across complex systems.

Public-private coordination also faces organizational, technological, legal, and cultural barriers. Public and private organizations may have different missions, vocabularies, authorities, technologies, reporting procedures, risk tolerances, and information-sharing expectations. Private organizations may hesitate to share sensitive operational or commercial information, while public agencies may lack procedures for integrating private-sector data into emergency operations. A Common Operating Picture can help address these barriers when supported by governance, trust, validation procedures, data standards, privacy safeguards, and agreed information-sharing protocols (Steen-Tveit & Munkvold, 2021; Turoff et al., 2004).

Common Operating Picture and Shared Situational Awareness

A Common Operating Picture is a shared representation of operational conditions that helps multiple stakeholders understand what is happening, where impacts are occurring, which resources are available, what priorities exist, and what decisions are required. FEMA's NIMS doctrine

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

identifies communications and information management as a core component of incident management and emphasizes shared situational awareness across command and coordination structures (FEMA, 2017).

Shared situational awareness is more than access to the same data. Endsley (1995) explains that situational awareness in dynamic systems involves perception of relevant information, comprehension of its meaning, and projection of future conditions. This theory is directly relevant to business continuity because operational decisions during disasters require organizations to interpret changing hazards, infrastructure disruption, workforce constraints, supplier conditions, customer needs, community impacts, and public sector priorities.

A Common Operating Picture should therefore be treated as a decision support capability rather than a static dashboard. It is a process of collecting, integrating, validating, visualizing, interpreting, and acting on information across organizations. Steen-Tveit and Munkvold (2021) argue that a Common Operating Picture does not automatically produce common situational understanding because users also need role awareness, trust, shared interpretation, and communication tools. This distinction is important for public-private coordination because businesses and public agencies may interpret the same incident information differently based on mission, authority, risk exposure, and operational responsibility.

Community Lifelines, Supply Chains, and Infrastructure Dependencies

FEMA's Community Lifelines concept is highly relevant to business continuity because it organizes disaster impacts around essential services needed for community stabilization (FEMA, 2023). Many community lifelines depend heavily on private-sector participation. Energy restoration depends on utility companies, contractors, fuel suppliers, logistics providers, and equipment vendors. Food and water access depend on grocery distributors, retailers, transportation companies, warehouses, and suppliers. Health and medical continuity depend on hospitals, pharmacies, medical suppliers, insurance systems, and healthcare logistics.

This means that business continuity and community lifeline stabilization are interconnected. When businesses fail to continue critical services, communities may experience longer disruption. When public agencies cannot provide timely situational information or infrastructure restoration priorities, businesses may struggle to reopen or support recovery (FEMA, 2023; Kapucu, 2006; Tierney, 2007). A public-private COP can help connect these two sides by showing which business operations support which lifelines, where service disruptions are occurring, what dependencies exist, and which restoration actions should be prioritized.

Infrastructure dependency creates a related continuity problem. Rinaldi et al. (2001) explain that critical infrastructure systems are interdependent through physical, cyber, geographic, and logical relationships. A business may be physically undamaged but unable to operate because electricity is unavailable, internet service is down, water systems are compromised, employees cannot reach the facility, emergency restrictions prevent reopening, or suppliers cannot deliver. Continuity planning therefore requires visibility into infrastructure status, restoration timelines, alternate routes, lifeline priorities, and coordination with public agencies and infrastructure operators.

Research Gap

The literature shows that business continuity, organizational resilience, emergency management coordination, community lifelines, supply chain resilience, infrastructure interdependency, and public-private partnerships are closely connected. Business continuity standards emphasize structured planning, recovery capability, continuity management, and continual improvement. Organizational resilience guidance expands the focus to adaptation, learning, leadership, and long-term capacity. Emergency management doctrine emphasizes shared situational awareness, communications, resource coordination, and the Common Operating Picture. Community Lifelines show that disaster stabilization depends on essential services, many of which involve private-sector organizations (FEMA, 2023; ISO, 2017, 2019).

However, these areas are often discussed separately. Business continuity literature tends to focus on internal organizational planning and recovery. Emergency management doctrine tends to focus on public-sector coordination and incident management. Public-private coordination literature emphasizes interorganizational cooperation but often does not provide a detailed COP model for connecting business operations with emergency management decision-making. Community Lifelines guidance identifies essential service areas but does not fully explain how private-sector continuity information should be integrated into a shared operational framework. Supply chain and infrastructure literature explains dependency and disruption but is not always integrated into disaster management COP frameworks.

This creates a conceptual and practical gap. There is a need for a framework that connects business continuity and organizational resilience with public-private coordination, Common Operating Picture development, critical service continuity, infrastructure dependency visibility, supply chain disruption tracking, and operational recovery across the full disaster management cycle. This article addresses that gap by using selected standards, doctrine, guidance, and peer-reviewed literature to develop an Integrated Public-Private Common Operating Picture Framework for Business Continuity and Organizational Resilience. The article does not treat sector examples as empirical cases; they are used illustratively to show how continuity dependencies appear across organizational and community systems.

METHODOLOGY

This study uses a qualitative document based conceptual analysis. It does not claim to be a systematic literature review, statistical study, interview-based study, simulation, or formal case study. The purpose is to synthesize selected business continuity standards, organizational resilience guidance, emergency management doctrine, official guidance, and peer-reviewed literature in order to develop a defensible conceptual framework for strengthening business continuity and organizational resilience through a Public-Private Common Operating Picture. The source base was selected through purposive relevance sampling. The selection was not intended to be exhaustive; rather, it was designed to include high relevance sources that directly informed the conceptual development of the framework. Sources were included when they directly addressed one or more of the article's core concepts: business continuity management, organizational resilience, public-private coordination, Common Operating Picture development, shared situational awareness, Community Lifelines, infrastructure interdependency, supply chain resilience, emergency information systems, or operational recovery. The analytical approach combined document analysis and thematic synthesis. Document analysis is appropriate when published documents, standards, and official guidance are used as qualitative evidence for interpreting policy, organizational, and institutional issues (Bowen, 2009). The thematic process was used to identify recurring patterns across the selected sources and translate those patterns into framework components (Braun & Clarke, 2006). The analytical procedure followed four steps. First, the selected sources were

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

reviewed to identify recurring references to continuity disruption, external dependencies, public-private coordination, shared situational awareness, lifeline stabilization, infrastructure and supply chain disruption, recovery tracking, and resilience learning. Second, these recurring issues were grouped into thematic categories aligned with the research questions. Third, the themes were compared across standards, emergency management doctrine, official guidance, and peer-reviewed scholarship to identify common patterns. Fourth, the themes were translated into framework components that could support practical COP design, public-private coordination, and future empirical testing. Trustworthiness was supported through triangulation across different source types: international standards, emergency management doctrine, official guidance, and peer-reviewed scholarship. The framework was not developed from a single standard, one sector, or one institutional source. Ethical concerns were limited because the study used publicly available standards information, official guidance, and published literature and did not involve human subjects, private records, field interviews, or personally identifiable data.

Table 1. Source Categories and Analytical Roles

Source category	Examples used	Analytical role
Business continuity and resilience standards	ISO 22301; ISO 22316	Defined business continuity management, organizational resilience, recovery capability, adaptation, and continual improvement.
Emergency management doctrine and guidance	FEMA NIMS; FEMA Community Lifelines	Supported the public-private coordination, shared situational awareness, resource coordination, and lifeline stabilization logic.
Public-private coordination and crisis management literature	Comfort; Kapucu; Tierney; Steen-Tveit and Munkvold	Provided grounding for interorganizational communication, public-private coordination, common situational understanding, trust, and role awareness.
Infrastructure and supply chain resilience literature	Rinaldi et al.; Christopher and Peck; Sheffi and Rice	Explained cascading dependencies, network vulnerability, supply chain resilience, visibility, flexibility, and recovery capability.
Emergency information systems and methodology literature	Turoff et al.; Bowen; Braun and Clarke	Supported the role of shared information environments, document analysis, thematic synthesis, and framework development.

RESULTS & ANALYTICAL FINDINGS

Finding 1: Business continuity depends on external systems, not only internal plans.

The analysis shows that business continuity and organizational resilience are weakened when organizations treat disruption only as an internal planning problem. Continuity plans, recovery time objectives, alternate worksites, and supplier arrangements remain important, but they are insufficient when transportation, energy, communications, water, healthcare access, workforce mobility, fuel, public safety, and supplier networks are disrupted.

Finding 2: Public-private information fragmentation weakens shared situational awareness.

Across the source base, public agencies, utilities, transportation agencies, healthcare systems, businesses, suppliers, and community partners hold different pieces of operational information. When these information streams remain disconnected, both public and private decision makers may lack timely awareness of hazards, restrictions, outages, resource constraints, service capacity, supplier disruption, workforce availability, and reopening status.

Finding 3: Community lifeline stabilization and business continuity are interdependent.

FEMA Community Lifelines show that disaster stabilization depends on essential services, many of which are delivered or supported by private sector organizations. Food, fuel, healthcare, communications, transportation, banking, logistics, shelter support, and construction services are not only business activities. During disasters, they become part of the community survival and recovery system.

Finding 4: Infrastructure and supply chain dependencies create cascading continuity failures.

The analysis identifies dependency visibility as a central continuity gap. Businesses may be physically undamaged but unable to operate because power, water, communications, transportation access, fuel, suppliers, or workforce mobility are disrupted. Infrastructure and supply chain failures can cascade across organizations and community lifelines, making isolated continuity planning inadequate.

Finding 5: A Public-Private COP requires governance, trust, data-sharing rules, and exercises.

The analysis shows that a shared information platform alone does not create common situational understanding. A Public-Private COP requires agreed reporting fields, validation procedures, access controls, privacy safeguards, cybersecurity protection, common terminology, pre-disaster relationships, role clarity, and exercises that test whether information can support real decisions.

ANALYSIS AND FRAMEWORK DEVELOPMENT

The findings indicate that business continuity failures can be analyzed as a chain of connected problems. Organizations depend on external lifeline systems; external systems generate disruption information that is spread across public and private actors; fragmented information weakens shared situational awareness; weak situational awareness limits coordinated continuity decisions; limited coordination slows critical service continuity

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

and operational recovery; and weak recovery learning prevents future resilience improvement. This chain explains why a public-private COP must include more than internal business continuity data.

The first analytical step was to translate the identified continuity gaps into functional COP requirements. External dependency gaps require risk intelligence and dependency mapping. Public-private information fragmentation requires agreed information sharing processes. Lifeline disruption requires critical service continuity coordination. Cascading infrastructure and supply chain failures require infrastructure and supply chain visibility. Separate recovery reporting requires operational recovery tracking. Weak after-action learning requires resilience learning and improvement. The second analytical step was to organize these functions across the disaster management cycle. Before disaster, the COP should support hazard and risk intelligence, business impact analysis, dependency mapping, supplier and workforce readiness, continuity planning, public-private coordination, lifeline prioritization, and resilience readiness. During disaster, it should support real time-shared situational awareness, business operating status, infrastructure and supply chain disruption monitoring, operational feedback, critical service continuity, and coordinated response decisions. After disaster, it should support business reopening status, infrastructure restoration, supply chain recovery, community service restoration, operational recovery tracking, coordinated restoration priorities, community lifeline recovery, and resilience learning.

The third analytical step was to identify enabling conditions. The framework requires governance arrangements, data-sharing agreements, common reporting templates, validation procedures, access controls, privacy safeguards, cybersecurity protections, joint exercises, and role clarity. Without these foundations, a public-private COP may reproduce existing information silos or expose sensitive organizational information without improving coordination. The resulting framework is therefore both operational and institutional: it connects continuity information with the governance conditions needed to use that information responsibly. The Integrated Public-Private Common Operating Picture Framework is based on the argument that business continuity failures during disasters are not caused only by weak internal planning. They are also caused by fragmented information, limited public-private coordination, weak infrastructure dependency visibility, supply chain uncertainty, unclear lifeline priorities, and delayed operational recovery information. Business continuity management provides the organizational foundation for maintaining and restoring priority services, while organizational resilience expands the focus to adaptation, learning, and long term capacity (ISO, 2017, 2019). During disasters, these capabilities depend on external systems and interorganizational coordination. The framework contains six interrelated components: risk intelligence and dependency mapping, public-private information sharing, critical service continuity coordination, infrastructure and supply chain visibility, operational recovery tracking, and resilience learning. These components are not separate stages. They are connected functions that support business continuity and organizational resilience before, during, and after disasters. Together, they help transform fragmented organizational and public-sector information into a shared operational view that supports continuity decisions, coordination, and recovery.

Table 2. Integrated Public-Private COP Framework for Business Continuity and Organizational Resilience

Framework component	Continuity gap addressed	COP function	Decision support value
Risk intelligence and dependency mapping	Limited understanding of hazards, critical activities, suppliers, infrastructure, workforce constraints, and lifeline dependencies.	Map hazards, business impacts, suppliers, infrastructure dependencies, workforce needs, and critical services before disruption.	Stronger continuity planning and clearer preparedness priorities.
Public-private information sharing	Fragmented data across agencies, businesses, infrastructure operators, suppliers, and community partners.	Use agreed reporting fields, validation procedures, access rules, and communication channels for essential operational information.	Improved shared situational awareness and faster coordination.
Critical service continuity coordination	Business continuity plans not linked to community lifeline stabilization.	Identify businesses and services that support food, fuel, healthcare, communications, transportation, shelter, and utilities.	Better alignment between organizational continuity and community stabilization.
Infrastructure and supply chain visibility	Cascading disruption from utilities, transportation, communications, fuel, suppliers, and logistics networks.	Track outage status, restoration priorities, alternate routes, supplier status, inventories, logistics capacity, and bottlenecks.	Greater dependency visibility and more informed restoration decisions.
Operational recovery tracking	Business reopening, infrastructure restoration, workforce return, supplier recovery, and service access tracked separately.	Monitor reopening status, service restoration, recovery delays, continuity gaps, and public-private recovery priorities.	More coordinated operational recovery and lifeline restoration.
Resilience learning and improvement	Lessons from disasters not translated into continuity plans, data-sharing protocols, exercises, or mitigation decisions.	Use after-action reviews, exercises, plan revision, dependency map updates, and COP performance evaluation.	Continuous improvement in organizational and community resilience.

CONCEPTUAL PROPOSITION

The framework is based on the following conceptual proposition: business continuity and organizational resilience during disasters are weakened when organizations lack shared situational awareness, public-private information sharing, infrastructure dependency visibility, supply chain

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

transparency, critical service coordination, and operational recovery tracking. An Integrated Public-Private Common Operating Picture can reduce these gaps by connecting business status, public-sector priorities, infrastructure conditions, supply chain disruption, community lifeline impacts, and recovery progress into a shared decision support environment.

This proposition integrates business continuity management and organizational resilience standards with emergency management doctrine, situational awareness theory, infrastructure interdependency, supply chain resilience, and emergency information systems research (Christopher & Peck, 2004; Endsley, 1995; FEMA, 2017, 2023; ISO, 2017, 2019; Rinaldi et al., 2001; Turoff et al., 2004). It positions business continuity as part of a larger public-private disaster resilience system rather than as a narrow internal organizational function.

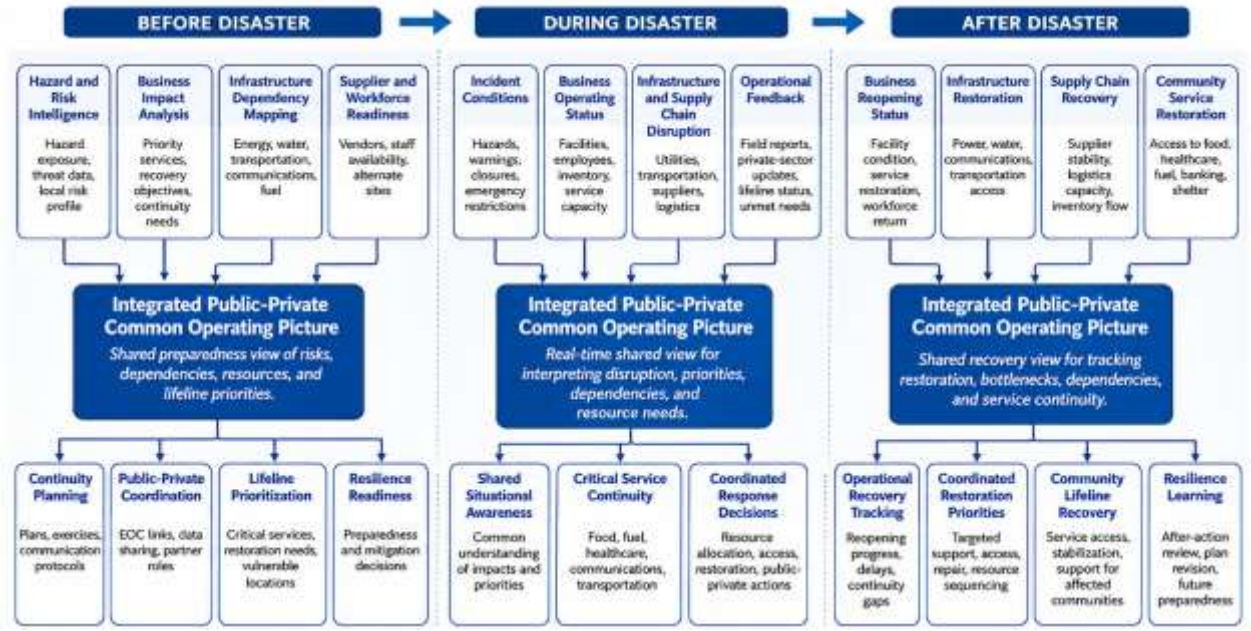


Figure 1. Integrated Public-Private Common Operating Picture Framework Across the Disaster Management Cycle

Note. The figure integrates before disaster preparedness, during disaster continuity coordination, and after disaster operational recovery through a Public-Private Common Operating Picture. It shows how risk intelligence, business impact analysis, dependency mapping, operating status, supply chain disruption, infrastructure restoration, community service restoration, and resilience learning can be connected through one shared decision-support logic.

DISCUSSION

The findings and analysis show that business continuity and organizational resilience during disasters are not only internal organizational responsibilities. They are public-private coordination challenges shaped by infrastructure dependencies, supply chains, community lifelines, information-sharing arrangements, and recovery governance. This matter because organizations often invest in internal continuity plans without fully addressing the external systems that determine whether priority services can actually continue or recover. The first research question asked how business continuity and organizational resilience depend on public-private coordination across the disaster management cycle. The analysis shows that continuity depends on public-private coordination before, during, and after disasters. Before disasters, organizations need risk intelligence, supplier analysis, infrastructure dependency mapping, workforce preparedness, and links with emergency management agencies. During disasters, organizations need timely information about hazards, restrictions, road closures, utility outages, public safety conditions, and resource constraints. After disasters, they need coordinated information about infrastructure restoration, workforce return, supplier stabilization, customer access, financial recovery, and community lifeline restoration. The second research question asked what continuity gaps emerge when organizations lack shared situational awareness, infrastructure dependency visibility, supply chain information, and coordination with emergency management partners. The findings identify four recurring gaps. Situational awareness gaps occur when public and private organizations cannot develop a shared understanding of operational conditions. Dependency visibility gaps occur when organizations do not fully understand how their operations depend on external infrastructure and supply chain systems. Coordination gaps occur when public and private organizations lack established procedures for exchanging information and aligning decisions. Recovery tracking gaps occur when business reopening, infrastructure restoration, supplier recovery, workforce return, and community service restoration are not monitored together. The third research question asked how an Integrated Public-Private COP can strengthen critical service continuity, organizational resilience, and operational recovery before, during, and after disasters. The framework responds by integrating six components and by organizing them across the disaster management cycle. Before disasters, the COP supports hazard awareness, business impact analysis, dependency mapping, supplier readiness, emergency communication protocols, and public-private coordination procedures. During disasters, it integrates incident conditions, business operating status, infrastructure disruption, supply chain constraints, resource availability, and community lifeline impacts. After disasters, it tracks business reopening, service restoration, recovery delays, infrastructure dependencies, and resilience learning. The framework also contributes by repositioning the COP as more than an emergency response display. In many emergency management discussions, the COP is associated mainly with incident response, command coordination, or EOC operations. This article extends the COP into business continuity and organizational resilience across the full disaster management cycle. Before disaster, the COP supports preparedness, risk intelligence, and dependency mapping. During disaster, it

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

supports shared situational awareness, continuity coordination, and resource prioritization. After disaster, it supports operational recovery tracking, restoration sequencing, and resilience learning. The framework further connects business continuity with infrastructure interdependency and supply chain resilience. Traditional continuity planning may focus on internal recovery strategies, but disasters often expose external dependency failures. Rinaldi et al. (2001) show that infrastructure disruptions can cascade across interconnected systems, while Christopher and Peck (2004) and Sheffi and Rice (2005) show that supply chain resilience depends on visibility, flexibility, collaboration, and recovery capability. By integrating infrastructure and supply chain visibility into the COP, the proposed framework helps organizations move beyond isolated continuity planning toward networked continuity planning. Finally, the framework supports public-private trust and role clarity. A Common Operating Picture does not automatically produce common situational understanding. Users also need trust, role awareness, shared interpretation, and communication tools (Steen-Tveit & Munkvold, 2021). This is especially important in public-private coordination because organizations may have different missions, data sensitivities, legal responsibilities, and operational priorities. A public-private COP must therefore be supported by governance arrangements, including data sharing agreements, access controls, reporting standards, privacy safeguards, validation procedures, and joint exercises.

POLICY AND PRACTICE IMPLICATIONS

The framework has implications for emergency management policy, business continuity planning, organizational resilience, public-private coordination, community lifeline stabilization, and operational recovery. Its value depends not only on the design of a shared information system but also on the governance arrangements, data sharing agreements, training programs, exercises, and decision-making structures that allow public and private partners to use information effectively. For emergency management agencies, the framework suggests that private sector continuity information should be integrated into preparedness, response, and recovery planning. EOCs should not only track public-sector incident information. They should also understand which businesses support community lifelines, which critical services are disrupted, which infrastructure dependencies are delaying restoration, and which private-sector resources may support response and recovery. This requires pre-disaster coordination with utilities, healthcare systems, logistics providers, food distributors, telecommunications providers, fuel suppliers, pharmacies, transportation operators, and major employers. For business continuity managers, the framework suggests that continuity planning should move beyond facility level plans and internal recovery time objectives. Organizations should map dependencies on utilities, suppliers, workforce access, transportation, communications, fuel, public safety, and community conditions. They should also identify how their services support community lifelines. A grocery distributor, pharmacy, fuel supplier, hospital, telecommunications provider, bank, or construction firm may be both an affected organization and a critical partner in community recovery. For public-private governance, the framework highlights the need for information-sharing agreements, common reporting templates, data validation procedures, access rules, privacy safeguards, cybersecurity protections, and role clarity before disasters occur. Sensitive private sector information should not be shared casually. However, essential operational information can be shared through defined protocols that protect confidentiality while supporting situational awareness and decision-making.

For exercises and training, the framework suggests that business continuity exercises should include public sector partners, infrastructure operators, and community lifeline scenarios. Emergency management exercises should include private-sector operating status, supply chain disruption, workforce limitations, utility dependencies, business reopening constraints, and critical service continuity. This would help both sides test whether the COP actually supports decisions rather than only displaying information.

LIMITATIONS AND FUTURE RESEARCH

This article is conceptual and document based. It does not test the proposed Public-Private Common Operating Picture Framework through field data, interviews, exercises, simulations, statistical analysis, or formal case studies. The framework should therefore be understood as a structured model for future research and practice rather than as an empirically validated system. The study uses selected standards, doctrine, guidance, and literature rather than an exhaustive systematic review. The source base was selected for conceptual relevance to business continuity, organizational resilience, public-private coordination, COP development, Community Lifelines, infrastructure interdependency, supply chain resilience, and emergency information systems. Future research should expand the source base, compare additional governance contexts, and test whether the framework improves decision-making in practice. The framework also assumes a level of public-private trust, data governance, and technical capacity that may not exist in all jurisdictions or sectors. Some organizations may be reluctant to share operational data because of commercial sensitivity, legal exposure, cybersecurity concerns, reputational risk, or privacy requirements. Public agencies may lack the staff, technology, or procedures needed to collect, validate, and interpret private-sector continuity information during fast-moving incidents. Implementation would therefore require careful governance, phased adoption, and sector-specific adaptation. Future research should test the framework through public-private emergency exercises, EOC simulations, practitioner interviews, sector specific case studies, and pilot COP applications. Studies could examine which continuity data are most useful during disasters, how private-sector information can be protected while supporting emergency coordination, whether shared dependency mapping improves continuity decisions, and whether public-private COPs reduce resource duplication, improve lifeline restoration, or accelerate operational recovery. Future studies should also adapt the framework for sectors such as healthcare, utilities, logistics, higher education, hospitality, finance, and retail supply chains.

CONCLUSION

This article examined business continuity and organizational resilience as public-private coordination challenges across the disaster management cycle. By reframing the study as a qualitative document based conceptual analysis, the article clarifies its methodological basis and avoids presenting sector examples as formal empirical cases. The central argument is that business continuity during disasters should not be understood only as an internal organizational planning function. Although internal continuity plans, business impact analysis, recovery strategies, employee communication procedures, and alternate operating arrangements are essential, they are not sufficient when disasters disrupt transportation, utilities, communications, suppliers, workforce access, public safety, healthcare systems, and community lifelines. The analysis found that business

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

continuity gaps are often external dependency, information sharing, coordination, lifeline stabilization, and recovery tracking problems. The proposed framework integrates six connected components: risk intelligence and dependency mapping, public-private information sharing, critical service continuity coordination, infrastructure and supply chain visibility, operational recovery tracking, and resilience learning. Together, these components show how a COP can help public agencies, businesses, infrastructure operators, healthcare systems, logistics providers, suppliers, nonprofit organizations, and community partners develop a shared operational view of risks, disruptions, dependencies, resources, service continuity, and recovery progress. The main contribution of the article is to reposition business continuity as a public-private disaster resilience function. Traditional continuity planning often focuses on internal organizational recovery, while emergency management doctrine often focuses on public sector coordination. This article connects the two by showing that business continuity, community lifeline stabilization, and operational recovery are interdependent. If tested and implemented responsibly, the proposed framework can help reduce fragmented information, strengthen public-private coordination, improve critical service continuity, support community lifeline stabilization, and accelerate operational recovery before, during, and after disasters.

REFERENCES

1) Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27-40. https://doi.org/10.3316/QRJ0902027
2) Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa
3) Christopher, M., & Peck, H. (2004). Building the resilient supply chain. The International Journal of Logistics Management, 15(2), 1-14. https://doi.org/10.1108/09574090410700275
4) Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. Public Administration Review, 67(s1), 189-197. https://doi.org/10.1111/j.1540-6210.2007.00827.x
5) Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1), 32-64. https://doi.org/10.1518/001872095779049543
6) Federal Emergency Management Agency. (2017). National Incident Management System (3rd ed.). U.S. Department of Homeland Security. https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf
7) Federal Emergency Management Agency. (2023). Community Lifelines implementation toolkit (Version 2.1). U.S. Department of Homeland Security. https://www.fema.gov/sites/default/files/documents/fema_lifelines-toolkit-v2.1_2023.pdf
8) International Organization for Standardization. (2017). ISO 22316:2017: Security and resilience - Organizational resilience - Principles and attributes. https://www.iso.org/standard/50053.html
9) International Organization for Standardization. (2019). ISO 22301:2019: Security and resilience - Business continuity management systems - Requirements. https://www.iso.org/standard/75106.html
10) Kapucu, N. (2006). Interagency communication networks during emergencies: Boundary spanners in multiagency coordination. The American Review of Public Administration, 36(2), 207-225. https://doi.org/10.1177/0275074005280605
11) Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11-25. https://doi.org/10.1109/37.969131
12) Sheffi, Y., & Rice, J. B., Jr. (2005). A supply chain view of the resilient enterprise. MIT Sloan Management Review, 47(1), 41-48. https://web.mit.edu/scresponse/repository/Sheffi_Rice_SC_View_of_the_Resilient_Enterprise_Fall_2005.pdf
13) Steen-Tveit, K., & Munkvold, B. E. (2021). From common operational picture to common situational understanding: An analysis based on practitioner perspectives. Safety Science, 142, Article 105381. https://doi.org/10.1016/j.ssci.2021.105381
14) Tierney, K. J. (2007). From the margins to the mainstream? Disaster research at the crossroads. Annual Review of Sociology, 33, 503-525. https://doi.org/10.1146/annurev.soc.33.040406.131743
15) Turoff, M., Chumer, M., Van de Walle, B. A., & Yao, X. (2004). The design of a dynamic emergency response management information system. Journal of Information Technology Theory and Application, 5(4), 1-36. https://aisel.aisnet.org/jitta/vol5/iss4/3/

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: SK Monirul Islam Mahadi