ISSN: 2586-6036
JWMAP website: http://accesson.kr/jwmap
doi: http://dx.doi.org/10.13106/jwmap.2026.vol9.no2.123

A Study on Measures to Strengthen the Continuity of Information and Data Communication Resources Based on the Corporate Disaster Management Standard[i]
- Focusing on a Technical and Governance Comparison of Private and Public Data Center Fire Cases and Integrated Improvement Measures -

Woo-Yang HEO[1], Un-Gi JOO[2]

1. First Author Researcher, Department of Industrial Engineering, Sunmoon University, Korea.
Email: hwy007@naver.com
2. Corresponding Author Professor, Department of Industrial Engineering, Sunmoon University, Korea.
Email: ugjoo@sunmoon.ac.kr

Received: March 23, 2026. Revised: March 29, 2026. Accepted: March 30, 2026.

Abstract

Purpose: This study aims to analyze how data center and cloud service disruptions can escalate into broader social disasters and to propose measures to strengthen the continuity of information and data communication resources through an improved Business Continuity Management System (BCMS). **Research design, data, and methodology**: To this end, a continuity assessment framework comprising seven analytical domains, including business impact analysis, risk assessment, utility protection, communication, and training, was constructed on the basis of the revised Corporate Disaster Management Standard. Using a comparative case study design, this study analyzes the 2022 Pangyo private platform data center fire and the 2025 Daejeon public data center fire. **Results**: The findings show that both cases revealed common vulnerabilities in the management of interdependencies among resources and in the verification of practical recovery training. The private sector demonstrated relatively high technical agility in the service recovery process, but governance linkages and inter-organizational coordination were limited. In contrast, the public sector had a more formalized response system, but empirical validation at the operational level of redundancy and resource failover procedures was found to be insufficient. **Conclusions**: This study concludes that digital continuity cannot be secured through simple technical redundancy alone and should instead be supported by an integrated BCMS that combines infrastructure resilience, utility protection, governance coordination, and crisis communication across both the public and private sectors. These findings provide practical implications for strengthening continuity planning in digital service environments.

Keywords: Corporate Disaster Management Standard, Business Continuity Management System, Data Center Fire, Digital Continuity, Crisis Communication

JEL Classification Code: M15, L86, H12

1. Introduction

1.1 Background and Necessity

As messaging, payment, mobility, identity verification, and administrative functions have become deeply embedded in everyday life, interruptions to digital services have become a social risk issue. Accordingly, large-scale disruptions can trigger a chain of effects that goes beyond direct service failure, including economic losses, behavioral confusion, unequal burdens on

vulnerable users, and long-term erosion of trust. In this environment, the continuity of information and data communication resources needs to be approached not merely as a narrow IT maintenance issue but as a disaster management issue.

The practical importance of this shift is clearly revealed in large-scale data center outages. When the core physical environment of a data center is damaged by fire, power, cooling, network access, orchestration tools, and service availability can all be affected in a cascading manner. Continuity planning that fails to integrate facility control, service prioritization, authority, and communication is bound to remain fragmented. This paper therefore focuses on data center fire incidents as concrete situations in which technical and governance vulnerabilities simultaneously emerge and interact.

1.2. Purpose, Scope, and Research Questions

The purpose of this paper is to reinterpret the revised Corporate Disaster Management Standard from the perspective of digital continuity and to derive measures for strengthening the continuity of information and data communication resources through a comparison of private and public data center fire cases. The scope of the study is limited to interpreting the major elements of the standard for the digital service environment and comparatively analyzing the 2022 Pangyo private data center fire and the 2025 Daejeon public data center fire. The analysis focuses on the process by which physical failures cascade into service interruptions and on differences in technical response, operational coordination, crisis communication, and recovery priorities during that process.

To this end, this study sets the following research questions.

First, which elements of the Corporate Disaster Management Standard operate as key factors when a physical failure spreads into a system-wide service interruption?

Second, what differences do the private and public cases show in terms of technology, coordination, and communication?

Third, in what directions can the revised Corporate Disaster Management Standard be supplemented and applied to secure the digital continuity of information and data communication resources?

In addition, this study sets the following research hypotheses.

Hypothesis 1. The more faithfully the core elements of the Corporate Disaster Management Standard are implemented, the higher the continuity performance of information and data communication resources will be.

Hypothesis 2. The higher the level of utility protection and the distribution of control systems, the lower the possibility that physical failures will spread across services as a whole.

Hypothesis 3. The more integrally technical response and organizational governance operate, the higher the performance of service recovery and user trust maintenance in data center disaster situations will be.

2. Theoretical Background

2.1. Standard-Based Continuity Logic

The Corporate Disaster Management Standard structures continuity activities across prevention, preparedness, response, recovery, performance evaluation, and improvement. In digital environments, its particularly important contributions lie in business impact analysis (BIA), risk assessment, documented information, communication, and training. BIA requires organizations to define MTPD, MBCO, RTO, and RPO. These indicators jointly specify how long an organization can tolerate disruption, what minimum level of service must be maintained, how quickly recovery should be achieved, and to what point information must be restored (International Organization for Standardization, 2019; Ministry of the Interior and Safety, 2025a).

RTO and RPO are particularly important in digital service environments. RTO means the target time by which a product, service, or activity must be resumed after an interruption. RPO means the point in time to which information must be restored in order to resume normal activities. In practice, RPO expresses the acceptable data loss window on a time basis. In continuously changing systems such as transaction systems, operational logs, and real-time statistics, a low RPO value is strategically very important. The ideal direction for the most critical services is to bring the RPO as close to zero as possible through real-time synchronization, distributed architecture, and highly resilient failover design (International Organization for Standardization, 2019).

The standard also explicitly addresses essential support utilities such as electricity and communications (Ministry of the Interior and Safety, 2025a). In the data center environment, servers and storage cannot be separated from power, cooling, and environmental controls. A battery room fire, electrical failure, or cooling loss can quickly escalate into a service-level crisis. Therefore, utility protection should be understood not merely as a facility management issue but as a prerequisite control for the continuity of information resources (International Organization for Standardization, 2019; Ministry of the Interior and Safety, 2025a).

2.2. Digital Well-being and Trust

This paper introduces digital well-being as a complementary analytical lens. Here, digital well-being refers to a state in which disruptions to users' daily functioning, trust, and psychological stability are

minimized through the maintenance or restoration of essential digital services. Based on this definition, continuity performance cannot be evaluated solely on the basis of server availability. It must also account for whether users receive timely and reliable information, whether alternative channels are accessible and clear, and whether uncertainty and exclusion are effectively reduced during the disruption period (Jang, 2015; Jang, Kim, & Yoo, 2018; Lee, 2021). Furthermore, recent research published in this journal has demonstrated that digital environments directly influence workers' well-being and productivity through factors such as information overload, technostress, and blurred work-life boundaries (Cha & Seo, 2025). This reinforces the need to conceptualize continuity not only in technical terms but also in relation to digital well-being.

Table 1. Analytical Domains Reconfigured from the Standard for Digital Continuity

Domain	Core Concern	Interpretation in This Study
BIA	MTPD, MBCO, RTO, RPO, dependency mapping	Defines recovery priorities, acceptable data loss windows, and minimum service levels
Risk Assessment	Physical, cyber, and operational disruption scenarios	Links batteries, power, cooling, tools, and vendor dependencies into compound risk scenarios
Utility Protection	Survivability of power, cooling, and communications	Treats facility stability as a direct control for service continuity
Operational Tools	Monitoring, deployment, access control, key management	Examines whether the control plane can survive even when the primary site is disrupted
Communication	Internal/external communication and alternative channels	Evaluates timeliness, authority, and channel diversity
Documented Information	Recovery procedures, approval paths, logs, evidence	Examines whether documents are executable rather than merely symbolic
Training/Evaluation	Rehearsal, corrective action, continuous improvement	Tests whether continuity assumptions are actually achievable

3. Research Design and Case Summary

3.1. Research Method

This study uses a multiple-case comparative design and relies on official materials, government announcements, explanatory materials, and summaries of major investigations that can be cross-validated against one another (Kakao, 2022; Kakao Corp., 2023; Ministry of Science and ICT, 2022; Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025). The seven analytical domains presented in Table 1 serve as the comparative framework. The purpose of this study is not to judge legal compliance but to identify recurrent mechanisms of discontinuity and derive operationally useful improvement measures.

3.2. Private Case: Company K and the Pangyo Fire

The 2022 Pangyo fire was an incident that had a major impact on a leading private platform operator whose services had become deeply embedded in everyday life (Ministry of Science and ICT, 2022). According to public materials, long-duration disruptions occurred in many services, including messaging, after the fire (Kakao, 2022; Kakao Corp., 2023). This case suggests that even when data redundancy is secured, actual recovery may be delayed if key operational tools such as orchestration, monitoring, deployment, and access control are concentrated at the damaged site. It also confirmed that in platform service environments, user expectations and social evaluations are strongly shaped by non-technical response elements such as user notifications, estimated recovery times, and compensation policies (Kakao Corp., 2023).

From a business continuity perspective, the Pangyo fire is important because it shows that redundancy at the data level and recoverability at the operational level do not necessarily coincide. Furthermore, the disruption of convenience services can quickly spread across everyday activities such as ordering, reservations, payment, authentication, and communication, causing social confusion. This case is therefore a representative example showing that, in a society with deepening digital

dependence, service continuity can be directly linked to the well-being of individuals and society (Kakao, 2022; Kakao Corp., 2023).

3.3. Public Case: Institution G and the Daejeon Fire

The 2025 Daejeon fire affected a government data center supporting Government24 and related public services (Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025). Unlike the private case, the public case differed in that it affected functions connected with administrative rights, identity-related procedures, and inter-agency coordination. Accordingly, recovery involved not only technical restoration but also priority grading management, public accountability, and the management of alternative channels for citizens and institutions (Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025).

The public case illustrates the continuity challenges of digital government. Dependencies do not end within a single institution. Central systems, local government functions, public portals, and identity-related services are linked through chains of institutional and technical relationships. For this reason, the complexity of governance itself operates as a continuity variable (Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025).

Table 2. Comparison of Responses to Private and Public Data Center Fires

Comparison Axis	Private Case: Company K / Pangyo	Public Case: Institution G / Government24	Interpretive Point
Command System	Internal emergency governance and rapid company-side coordination	Formal government-led coordination involving graded recovery decisions	Agility vs. formal coordination
Recovery Priority	Rapid normalization of user-visible service functions	Phased recovery of essential public services and linked systems	Service-centered vs. public-duty-centered recovery
Communication Style	Apologies, user guidance, compensation, trust messages	Official briefings, phased recovery notices, public guidance	Brand/user communication vs. administrative accountability
Alternative Channels	Relatively limited emphasis on offline alternatives	Strong emphasis on alternative channels and linked administrative pathways	Public continuity requires visible alternatives beyond digital interfaces
Governance Complexity	A single corporate chain including vendor dependencies	Multi-agency coordination across central and local institutions	Inter-agency dependency is stronger in the public case
Post-incident Emphasis	Trust recovery and reliability enhancement	Management of recovery status and institutional improvement	Different strengths that can be recombined
Common Vulnerability	Utility failures and concentration of the control plane affect recovery	Utility failures and cross-system interdependencies affect recovery	Technology and governance must be addressed together

4. Results of Comparative Analysis

4.1. Common Failure Mechanisms

The first recurrent mechanism is the cascading spread of utility failures into service failures. In both cases, the disruptions could not be understood merely at the software or application level. Batteries, power, cooling, and environmental controls determined whether systems could continue operating and whether restart would proceed in an orderly or disorderly way. Continuity planning that separates facilities from services fails to capture this causal chain.

The second mechanism is the concentration of the control plane. Even if data replication and backup environments exist, rapid recovery is not guaranteed if monitoring systems, deployment tools, key management functions, access control, and decision-making authority are concentrated in a single vulnerable location. Therefore, the survivability of the control plane should be treated not as an additional engineering feature but as a core continuity requirement.

The third mechanism is insufficient verification of communication and rehearsal capabilities. When large-scale disruptions occur, organizations must simultaneously deal with technical recovery, public inquiries, media attention, and institutional oversight. If templates, approval authority, and alternative channels

have not been verified in advance, recovery problems expand beyond infrastructure issues into crises of trust. Even when internal BIA records are not publicly disclosed, the gap is evident from the published recovery timelines alone. In the private case, the fire was extinguished in about eight hours, and core messaging was partially restored about two hours later, but broad service normalization required approximately 127.5 hours (Kakao, 2022; Kakao Corp., 2023). In the public case, it was reported that Grade 1 systems required about 840 hours (35 days) to reach 100% recovery (Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025). Although official service-specific RTO/RPO targets were not disclosed, these observations suggest a substantial gap between the recovery times generally expected for critical digital services and the actual recovery times.

4.2. Differential Strengths and Weaknesses

The private case shows a relative strength in service-centered agility. It is oriented toward restoring user-visible functions quickly and managing the aftermath through apologies, service updates, and compensation (Kakao, 2022; Kakao Corp., 2023). However, its weakness lies in the possibility that, although services appear to be distributed and individually recoverable, the core functions that actually govern orchestration, monitoring, deployment, access control, and operational decision-making may remain centralized. In such a structure, attempts to restore individual services rapidly may not lead to stable overall recovery. On the contrary, if the central control functions are damaged or constrained, recovery can become more complicated, slower, and harder to coordinate than the visible service structure initially suggests. This interpretation is consistent with the observed delays in full service normalization despite partial functional recovery in the Pangyo case (Kakao, 2022; Kakao Corp., 2023).

The public case shows relative strengths in formal coordination, phased prioritization, and the operation of alternative channels. Because public services are linked to administrative rights, identity-related procedures, and inter-agency responsibilities, the recovery process tends to proceed within a more explicit framework of accountability and priority management (Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025). At the same time, however, the complexity of inter-agency dependencies and the possibility of delay associated with formal approval and reporting structures appear as weaknesses. In other words, the public model may provide greater procedural clarity, but it may also face slower execution when many institutional actors must move together, as reflected in the extended recovery durations reported in the public case (Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025).

These results suggest that the two sectors should not be viewed in terms of superiority or inferiority, but rather as possessing different continuity assets and different structural vulnerabilities. Private organizations tend to provide technical agility, rapid user-facing response, and flexible communication, whereas public organizations tend to provide formal accountability, explicit prioritization, and alternative service-channel logic. The key design question, therefore, is not which model is better in absolute terms, but how the strengths of both models can be combined while reducing their respective weaknesses. A more resilient continuity model would need to preserve the agility of service-centered recovery while also ensuring that the control functions required for stable recovery are sufficiently distributed, transparent, and governable (Kakao, 2022; Kakao Corp., 2023; Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025).

Table 3. Root Causes and Standard-Based Implications

Root Cause	Observed Pattern	Main Result	Standard-Based Implication
Cascade from utilities to services	Battery/power incidents spread into broad service disruptions	Broad outages and prolonged sequential recovery	Facility controls, utility rehearsals, and recovery priorities need to be integrated
Control plane concentration	Tools, credentials, or authority are not sufficiently distributed	Failover is delayed despite redundancy	Monitoring, deployment, access, and key management must be distributed across multiple sites
Weak communication verification	It has not been demonstrated that templates and backup channels were actually rehearsed under outage conditions, and uncertainty expanded while recovery continued for about 127.5 hours in the private case and about 840 hours for Grade 1 systems in the	As outages persisted for a non-trivial duration, user confusion, rumors, distrust, and guidance delays intensified	The executability of the communication system needs to be reviewed as a core control item

	public case		
Incomplete scenario rehearsal	Formal plans existed, but compound scenarios were not repeatedly validated against actual recovery timelines	Decision cycles slowed and a visible gap emerged between benchmark continuity expectations and actual TTR	Procedural verification and post-incident corrective action need to be linked to checking the realism of RTO/RPO assumptions

4.3. Cross-Benchmarking with International Cases

International benchmark cases reinforce the same lessons. Morgan Stanley's response to 9/11 suggests that when emergency procedures and role allocation are structured in advance, even extreme situations can reduce delays in initial response and enable organized transition (55korea88, 2024). Nokia's and Ericsson's preparations after the Philips fire offer another important lesson. Recognizing a disruption is not enough; alternative design, procurement, and operational options must exist (Latour, 2001). In both cases, continuity outcomes depended more on validated actions and prepared alternatives than on symbolic plans (55korea88, 2024; Latour, 2001).

These international benchmark cases are important because they show that the mechanisms observed in domestic data center cases are neither isolated nor culturally specific. Rehearsal, dependency mapping, and the availability of alternatives are universal continuity variables. Their importance is even greater in the digital realm, where coupling among systems is high and failures spread quickly, affecting larger numbers of users.

Table 4. Comparison of Domestic and International Benchmarks

Case	Preparation in Advance	Immediate Response	Observed Result	Implication
Morgan Stanley (9/11)	Repeated training and working manuals	Immediate execution of action under pressure	Greatly reduced life-safety damage and secured operational continuity more quickly	Pre-structured procedures and role systems help reduce delays in initial crisis response
Nokia (Philips fire)	Alternative design and procurement capability	Rapid escalation and reconfiguration	Business impact was controlled	BIA must be extended to the supply chain
Ericsson (Philips fire)	Fragile alternatives and excessive dependence on assumptions	Delayed adaptation	Losses expanded	Assumptions must be validated in advance
Company K (2022)	Some redundancy existed, but operational tools were concentrated	Messaging was partially restored about 10 hours after ignition, but broad recovery was delayed by orchestration weaknesses	Full normalization required about 127.5 hours, and about 105,000 damage claims and KRW 27.5 billion in compensation were reported	Data redundancy alone is insufficient without resilient control tools, and the quantified recovery gap needs to feed back into BIA targets
Institution G (2025)	Complex public-service linkages and graded priorities	Official recovery and public guidance proceeded in parallel while Grade 1 services were prioritized	One injury and zero deaths were reported, Grade 1 systems reached 100% recovery after about 840 hours (35 days), and reported losses were about KRW 9.5-10.0 billion	Critical service continuity needs to include explicit recovery objectives linked to public channel design and recovery governance

Note: Compiled from Latour (2001), Kakao (2022), Kakao Corp. (2023), Ministry of the Interior and Safety (2025b), and Seoul Metropolitan Government (2025).

4.4. Interpretation of the Research Hypotheses

Taken together, the domestic and international case comparisons confirm that differences in continuity performance observed in data center disaster situations are not accidental phenomena but are closely related to the level of prior preparedness, dependency management, utility protection, distribution of operational control systems, crisis communication, and rehearsal (International Organization for Standardization, 2019;

Kakao, 2022; Kakao Corp., 2023; Ministry of the Interior and Safety, 2025a, 2025b; Seoul Metropolitan Government, 2025; Latour, 2001). On this basis, the research hypotheses established in this study can be interpreted as follows.

First, the hypothesis that the more faithfully the core elements of the Corporate Disaster Management Standard are implemented, the higher the continuity performance of information and data communication resources will be can be interpreted as being generally supported. The case analysis showed that simple data redundancy alone was insufficient and that actual recoverability increased only when business impact analysis (BIA), risk assessment, documented recovery procedures, utility protection, crisis communication, training, and evaluation worked together (International Organization for Standardization, 2019; Ministry of the Interior and Safety, 2025a). This suggests that continuity performance may depend less on the presence of isolated technical elements than on how integrally the core elements of the standard are implemented.

Second, the hypothesis that the higher the level of utility protection and the distribution of control systems, the lower the possibility that physical failures will spread across services as a whole can also be interpreted as being largely supported. The Pangyo fire case showed that even when data-level redundancy exists, recovery can be delayed if core operational functions such as orchestration, monitoring, deployment, and access control are concentrated at the damaged site (Kakao, 2022; Kakao Corp., 2023). This means that, in addition to physical utilities such as power, cooling, and communication paths, the distribution of the operational control system itself is an important condition for securing the continuity of information and data communication resources. In other words, technical redundancy and distributed operational control should be understood not as separate issues but as complementary continuity factors (International Organization for Standardization, 2019; Kakao, 2022; Kakao Corp., 2023).

Third, the hypothesis that service recovery and user trust maintenance performance will be higher when technical response and organizational governance operate in an integrated manner can also be interpreted as being supported. The private platform case showed the importance of technical recovery capability and operational agility, while the public case revealed the importance of formal reporting systems, operation of alternative channels, role allocation, and stakeholder coordination (Kakao Corp., 2023; Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025). International benchmark cases also reconfirmed that continuity outcomes depend more heavily on actually validated actions, prepared alternatives, and repeated rehearsals than on symbolic planning (Latour, 2001). Accordingly, digital continuity is not secured merely by the resilience of technical infrastructure; it can be achieved more stably when combined with governance capabilities that enable organizations to share information, coordinate decisions, and manage external trust during crises.

However, because this study is a qualitative comparative case study based on publicly available materials, these hypotheses are not presented as statistically tested causal claims. Rather, they should be understood as theory-informed hypotheses examined through comparative case evidence and used to derive analytically grounded implications. Even so, the common mechanisms repeatedly identified across domestic and international cases suggest that the Corporate Disaster Management Standard can provide a meaningful analytical framework and practical implications for strengthening the continuity of information and data communication resources (International Organization for Standardization, 2019; Ministry of the Interior and Safety, 2025a; Latour, 2001). On the basis of this interpretation, the next chapter proposes BCMS improvement measures for strengthening digital continuity.

5. Integrated Improvement Measures

5.1. Governance and Incident Command System

A digital continuity model should define incident command roles before an incident occurs. Technical recovery, public or customer response, external liaison, security and access control, and compensation/legal functions should be separated by role but integrated at the command level. In particular, a workable authority matrix is important in after-hours conditions, degraded conditions, and inter-agency environments.

5.2. Architecture and Low-RPO Design

Core services should move toward geographic redundancy and low-RPO operation. The strategic direction for the most sensitive services is to bring the RPO close to zero. This is realistic only when real-time synchronization, resilient networks, and active-active or equivalent distributed architectures are supported by the survivability of operational tools and explicit operating procedures (International Organization for Standardization, 2019). In other words, the continuity objective is not merely faster restart but the joint preservation of service state and executable control capability. The fact that the recovery times observed in both cases were measured in days rather than in the short timeframes generally expected for high-criticality digital services makes the need for this transition even clearer (Kakao, 2022; Kakao Corp., 2023; Ministry of the Interior and Safety, 2025b; Seoul Metropolitan Government, 2025).

5.3. Utilities, Tools, and Documentation

Utility protection needs to be treated as a core control that determines the continuity of information and data communication resources (Ministry of the Interior and Safety, 2025a). Accordingly, physical and technical risk factors such as battery room fires, electrical failures, cooling loss, and communication path failures should be assumed not as isolated incidents but as parts of compound scenarios. In addition, operational tools such as monitoring, deployment, key management, access control, and logging should avoid single-site dependency structures and be designed to remain continuously available even in multi-site environments. At the same time, documented information should not remain at a merely formal level but should be specified as executable documents that can actually operate during crises. To this end, it is necessary to clearly define not only recovery sequences, role allocation, approval procedures, and alternative channels, but also the methods for collecting and preserving verifiable evidence such as logs, decision records, and notification histories generated during incident response and recovery (International Organization for Standardization, 2019; Ministry of the Interior and Safety, 2025a).

5.4. Rehearsal and Crisis Communication

More importantly, it is necessary to verify in an integrated manner whether the core assumptions of the continuity plan actually hold under conditions in which technical failover, authority execution, and internal and external communication operate simultaneously. Initial notifications, periodic updates, recovery notices, and post-incident improvement announcements should be templated in advance. For organizations that have public contact points, call-center operating logic, offline alternative routes, and inter-agency communication systems also need to be reviewed within the same analytical framework. In addition, prior studies published in this journal have addressed disaster awareness, disaster preparedness, and competency development, while also showing that field-based safety training is more effective than lecture-based instruction in strengthening risk-prevention behaviors (Park et al., 2023; Kim & Joo, 2025). These findings reinforce the argument that continuity planning in digital service environments should rely not only on formal documentation but also on executable, scenario-based rehearsal. The value of rehearsal lies in checking whether the core assumptions of the continuity plan still hold even under conditions where technical, organizational, and social pressures operate simultaneously (Latour, 2001; Ministry of the Interior and Safety, 2025a).

Table 5. Integrated Roadmap for Strengthening BCMS in Digital Service Environments

Stage	Main Deliverable	Execution Focus	Example Indicator
Current-State Diagnosis	Asset/service inventory and dependency map	Visualizes dependencies among facilities, data, vendors, and tools	Completion rate of critical service inventory
BIA and Risk Analysis	MTPD, MBCO, RTO, RPO, and compound scenarios	Reaches agreement on continuity objectives and identifies utility/control-plane dependencies	Target agreement rate; scenario coverage
Strategy Design	Geographic redundancy, low-RPO architecture, distributed control plane	Separately designs data redundancy and tool survivability	Reduction rate of single points of failure
Plan and Channel Design	Recovery procedures, authority matrix, communication templates	Prepares executable procedures and alternative channels	Time to first notice; procedure update rate
Training and Improvement	Integrated rehearsal and corrective-action loop	Validates assumptions and closes gaps after training	Post-training corrective-action implementation rate; corrective-action completion rate

6. Discussion

6.1. Policy and Well-being Implications

Data center disasters should be treated as socio-technical disruptions that affect service rights, public trust, and everyday functioning. As dependence on digital platforms and public portals increases, continuity policy needs to move closer to critical infrastructure policy. In particular, in areas where private and public services are intertwined, minimum expectations regarding recovery objectives, rehearsal, and dependency mapping need to be clarified more explicitly (International Organization for

Standardization, 2019; Ministry of the Interior and Safety, 2025a).

The well-being perspective makes clear why the quality of communication matters. Even if a service is technically restored, if users are not adequately informed, are excluded, or remain in uncertainty, it is only partially restored from the perspective of social functioning. Therefore, continuity includes not only the speed of technical repair but also the quality of guidance, the accessibility of alternatives, and the reduction of anxiety during the disruption period (Jang, 2015; Lee, 2021).

6.2. Implications for Doctoral-Level Research

Based on the framework derived through qualitative cross-case comparison, this study suggests an agenda for in-depth future research applying Mixed Methods Research. Doctoral-level follow-up research requires the following stepwise expansion. This staged research agenda is intended to address the present study's limitation in empirical validation and to test the robustness, transferability, and practical utility of the proposed framework across sectors and disaster types.

First, it is necessary to derive the importance and priorities of the major components of the Corporate Disaster Management Standard through Delphi analysis targeting expert groups and, on that basis, conduct a survey of practitioners to build a "Digital Continuity Maturity Model (D-CMM)" (Jang, 2015; Jang, Kim, & Yoo, 2018). Specifically, quantitative maturity measurement is needed across seven domains, including the level of organizational policy, the adequacy of budget allocation, the currency of asset inventories, the level of agreement on RTO/RPO, and outsourced-risk management.

Second, in the deepening stage of follow-up research, it is necessary to verify the structural relationships among these factors through structural equation modeling (SEM), setting the technology and governance indicators proposed in this study as independent variables and users' functional accessibility and psychological well-being (Digital Well-being) during disasters as dependent variables. This would make it possible to explain more systematically how continuity performance affects the maintenance of citizens' daily life and the recovery of social trust beyond simple technical restoration (Lee, 2021).

Third, such a quantitative approach can contribute to developing the Corporate Disaster Management Standard from a simple set of recommended guidelines into a measurable key performance indicator (KPI) system (Jang, 2015; Lee, 2021). As a result, follow-up research has academic significance in identifying the empirical utility of the advancement of disaster management systems for user trust, functional accessibility, and digital well-being.

7. Conclusion

This study reconfigured the Corporate Disaster Management Standard with a focus on information and data communication resources and conducted a comparative analysis of private and public data center fire cases. The analysis identified three recurrent vulnerabilities: (1) the cascading spread of utility failures, (2) the concentration of control-plane assets, and (3) insufficient verification of communication and rehearsal capabilities. In parallel, it identified complementary strengths: service-centered recovery agility in the private sector, and formal coordination, phased prioritization, and alternative channel operation in the public sector.

The central finding Is that continuity In critical digital service environments is not a matter of choosing between technical redundancy and administrative procedures. Rather, it requires an integrated BCMS that simultaneously combines technical agility, facility resilience, executable authority, pre-validated procedures, and stakeholder-oriented communication. In this integrated view, continuity is achieved not by any single layer but by the alignment of infrastructure, operations, and governance under real-world stress conditions.

From a practical standpoint, the results imply that organizations should move beyond siloed continuity planning and design for the survivability of both service state and control capability. This includes distributing operational control functions, strengthening utility protection as a core control, institutionalizing executable authority structures, and validating communication and rehearsal processes under compound conditions.

From a policy and societal perspective, continuity should be understood not only as an infrastructure concern but also as a mechanism for protecting trust, functional accessibility, and digital well-being. As digital dependence deepens, failures in data centers can rapidly escalate into social disruptions; therefore, continuity policy should be aligned more closely with critical infrastructure policy. Although the present analysis focuses on fire incidents, the proposed framework is also applicable to other compound disruption scenarios, including power outages, cooling failures, communication path disruptions, cyber-physical failures, and multi-vendor dependency breakdowns. In practical terms, this framework may be used not only in large platform companies and public institutions but also in hospitals, financial services, cloud operators, logistics systems, and other digitally dependent organizations.

This study has limitations in that it relies on publicly available materials and examines only two cases. Accordingly, the findings should be interpreted as analytically grounded rather than statistically generalized. Nevertheless, by identifying recurrent mechanisms across cases and linking them to actionable design principles, this study provides a publishable conceptual framework and a practical roadmap that organizations can apply when

designing and improving digital continuity.

References

55korea88. (2024, March 5). The miracle of Morgan Stanley, disaster preparedness training, and safety insensitivity [Blog post]. *Naver Blog*. https://blog.naver.com/55korea88/223373897852

Cha, S. S., & Seo, B. (2025). Digital disconnection psychology: Impact on workplace wellbeing and productivity. *Journal of Wellbeing Management and Applied Psychology, 8*(2), 39–47. https://www.accesson.kr/jwmap/v.8/2/39/55530

International Organization for Standardization. (2019). *ISO 22301:2019 security and resilience—Business continuity management systems—Requirements*. ISO. https://www.iso.org/standard/75106.html

Jang, M. H. (2015). *A study on the development and evaluation of a business continuity management index (BCMI) for domestic firms* (Doctoral dissertation, Soongsil University). https://www.dbpia.co.kr/journal/detail?nodeId=T13687676

Jang, M. H., Kim, K. S., & Yoo, H. J. (2018). A study on the development and evaluation of the business continuity management index (BCMI). *Journal of the Korean Production and Operations Management Society, 29*(1), 95–114. https://doi.org/10.21131/kopoms.29.1.201802.95

Kakao. (2022, December 8). 1015 outage retrospective: Service platform layer redundancy [Technical session, if(kakao)dev2022]. https://if.kakao.com/2022/session/108

Kakao Corp. (2023, September 14). Kakao publishes stability report [Press release]. https://www.kakaocorp.com/page/detail/10624

Kim, H.-D., & Joo, Y.-H. (2025). The impact of field-based safety training on workers' risk-prevention behaviors. *Journal of Wellbeing Management and Applied Psychology, 8*(5), 81–88. https://www.accesson.kr/jwmap/v.8/5/81/57645

Latour, A. (2001, January 29). Trial by fire: A blaze in Albuquerque sets off major crisis for cell-phone giants. *The Wall Street Journal*. https://www.wsj.com/articles/SB980720939804883010

Lee, S. W. (2021). *The effects of ISO 22301 and ISMS certification on business continuity performance: Focusing on corporate culture and processes* (Doctoral dissertation, Soongsil University). https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=DIKO0015870171

Ministry of Science and ICT. (2022, October 16). Regarding the Pangyo data center fire [Press release]. https://www.korea.kr/news/pressReleaseView.do?newsId=156530927

Ministry of the Interior and Safety. (2025a, June 16). *Corporate disaster management standard* (Notice No. 2025-42). https://www.law.go.kr/LSW/admRulInfoP.do?admRulSeq=2100000006535

Ministry of the Interior and Safety. (2025b, September 27). Response to the fire disruption in administrative information systems enters full-scale recovery mode [Press release]. https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?nttId=120966

Park, H.-M., Kim, T.-H., Kim, J.-Y., Kim, J.-E., Park, G.-E., Baek, J.-W., Shin, Y.-J., & Kim, Y.-M. (2023). Nursing students' disaster awareness, disaster preparedness, and disaster nursing competency. *Journal of Wellbeing Management and Applied Psychology, 6*(4), 51–61. https://doi.org/10.13106/jwmap.2023.Vol6.no4.51

Seoul Metropolitan Government, Digital City Bureau, Information Systems Division. (2025, October 29). Current Seoul Metropolitan Government response to the fire at the National Information Resources Service. https://news.seoul.go.kr/gov/archives/571648