World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Systematic review of business continuity and disaster recovery best practices for critical infrastructure protection under federal cybersecurity regulations and guidelines

Adeyemi A. Bello * and Julie Reneau

College of Business, University of Texas Permian Basin, Odessa, TEXAS 79765, USA.

World Journal of Advanced Research and Reviews, 2022, 15(02), 932-951

Publication history: Received on 29 June 2022; revised on 21 August 2022; accepted on 28 August 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.15.2.0842

Abstract

This systematic review focused on the best practices in business continuity (BC) and disaster recovery (DR) planning in critical infrastructure (CI) organizations subject to federal cybersecurity regulations in the United States. A total of 52 peer-reviewed articles published between January 1990 and December 2022 were analyzed and meta-analyzed. Statistically significant predictors of the program effectiveness of the BC/DR were arranged based on outcome variables such as operational resilience indices, recovery time goals (RTO), recovery point goals (RPO), and regulatory compliance scores. The quality of the methodology of every study was evaluated with a 11-point grading scale with items rating the use of theoretical frameworks, longitudinal design, comparison groups, and statistical rigor. Executive commitment of leadership, frequency of testing, intensity of training of the staff, redundancy of technology, and integration of supply chain risks were the best-practice predictors that were most consistently reported. The overall score of the methodological quality of reviewed studies was 7.12 (SD = 1.6; maximum = 11). The results indicate that there is still a significant gap in BC/DR testing frequency, cross-sector information transfer, and macro-level regulatory congruence. The review provides a synthesized evidence base that can guide practitioners, regulators, and researchers associated with the nexus of cybersecurity governance and critical infrastructure resilience.

Keywords: Business Continuity Planning; Disaster Recovery; Critical Infrastructure Protection; Federal Cybersecurity Regulations; Organizational Resilience

1. Introduction

In the fiscal year 2021, the United States identified 16 critical infrastructure (CI) sectors as important national assets whose incapacitation or destruction would create a debilitating impact on security or national economic security, national public health and safety or any combination of the two (Department of Homeland Security [DHS], 2013). The energy, financial services, healthcare and public health, and transportation systems sectors are the most popular among these sectors as they serve tens of millions of Americans in their everyday activities and contribute to trillions of dollars in economic activity. The increasing complexity and prevalence of cyberattacks against CI organizations have promoted business continuity (BC) planning and disaster recovery (DR) planning to a higher status as an operational issue rather than a strategic one of federal cybersecurity policy (CISA, 2019).

The federal cybersecurity rules and guidelines have been stricter to require or highly recommend the development, testing, and maintenance of strong BC/DR programs by the CI operators. The Federal Information Security Modernization Act (FISMA) of 2002, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (1996), and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (2014) contain

* Corresponding author: Adeyemi A. Bello

requirements, whether explicit or implied, that organizations should have documented continuity and recoverability capabilities. Nonetheless, in the context of this regulatory environment, the number of CI organizations that report a lack of preparedness in their BC/DR is still significant, especially in the case of small- and medium-sized operators (Kato and Charoenrat, 2018).

The Ponemon Institute (2020) also notes that unplanned downtime costs organizations that were critical infrastructure an average of 9,000 per minute, with certain industries like financial trading incurring costs on downtime that were over 1 million per hour. Moreover, the Colonial Pipeline ransomware attack in 2021 showed that even large organizations can suffer disastrous impacts on their operations when the future of BC/DR planning is not properly combined with the ability to respond to cybersecurity incidents (CISA, 2021). These occurrences support the necessity of evidence-based evidence on the development of BC/DR programs in the CI field.

1.1. Research Questions

This systematic review was guided by two overarching research questions

- RQ1. Which business continuity and disaster recovery practices have been most consistently identified as statistically significant predictors of operational resilience, recovery performance, and regulatory compliance among U.S. critical infrastructure organizations?
- RQ2. What is the methodological quality of the empirical studies producing these findings, and to what extent do post-2000 studies reflect improvements in research rigor — particularly in the use of theoretical frameworks, longitudinal designs, and cross-sector comparison groups?

1.2. Research Objectives

- To systematically identify and synthesize empirical evidence on BC/DR best practices that predict favorable resilience and compliance outcomes across the 16 federally designated U.S. critical infrastructure sectors.
- To organize identified BC/DR predictors by outcome domain — including operational resilience, recovery time and point objective attainment, regulatory compliance, and program maturity — enabling sector-specific and cross-sector comparison.
- To evaluate the methodological quality of 52 reviewed studies using a validated 11-point scoring framework, thereby establishing confidence levels for each reported finding.
- To identify persistent gaps in BC/DR empirical research — particularly regarding longitudinal designs, macro-level regulatory factors, and emerging threat vectors — and to propose a prioritized agenda for future investigation.

1.3. Significance of the Study

- This systematic review advances both scholarly understanding and practical application of business continuity and disaster recovery in an era of escalating cyber threats to critical national infrastructure.
- Policy Relevance: Provides federal regulators and policymakers with the first consolidated empirical evidence base for strengthening BC/DR requirements across all 16 designated U.S. critical infrastructure sectors.
- Practitioner Utility: Equips CI security officers and continuity planners with a ranked, evidence-backed hierarchy of best practices directly mapped to measurable resilience outcomes and sector-specific regulatory obligations.
- Academic Contribution: Fills a significant gap in the systematic review literature by being the first study to synthesize BC/DR empirical findings specifically within the context of federal cybersecurity regulatory frameworks rather than general organizational resilience.
- Methodological Advancement: Establishes a replicable, 11-point quality appraisal framework tailored to BC/DR research that future reviewers and meta-analysts can apply to assess and compare emerging studies in this field.
- Societal and Economic Impact: Directly informs investments that protect the safety, health, and economic security of millions of Americans who depend daily on uninterrupted critical infrastructure services such as power, water, healthcare, and financial systems.

2. Methods

2.1. Retrieval procedures and database selection strategies

Efforts were undertaken to access all English-language peer-reviewed journal articles and government technical reports that were published in the period between January 1990 and December 2022 and were empirically analyzing predictors and best practices of business continuity and disaster recovery programs effectiveness in critical infrastructure organizations who were subjected to U.S. federal cybersecurity regulations. The start date was January 1990, as it encompasses the timeline of the development of the formalized BC/DR guidance in the post-Cold War period, but it also includes the entire spectrum of the development of modern federal cybersecurity regulations. The search of 8 electronic databases was conducted based on Web of Science, Scopus, EBSCO (business source complete), ProQuest Dissertations and Theses, JSTOR, IEEE Xplore, ACM Digital Library, and PubMed (literature of healthcare CI sector). Also, all the articles included in the study had their reference lists hand-searched to identify any other qualifying articles.

Search terms were built based on Boolean operators and the combination of the following thematic clusters: ('business continuity' OR disaster recovery' OR BC/DR' OR continuity of operations OR COOP) AND (critical infrastructure' OR CIP' OR cybersecurity' OR information security) AND (federal regulation' OR FISMA' OR NIST' OR NERC CIP' OR HIPAA' OR compliance). The search in the first search resulted in retrieving 1,240 records in the database and 80 records in other sources of identification, thus 1,320 records were identified before the process of de-duplication occurred as shown in Figure 1 below. Following the elimination of 384 records of duplicated data and 28 records identified as ineligible using automated data processing programs, 828 distinct records were put through the screening process.

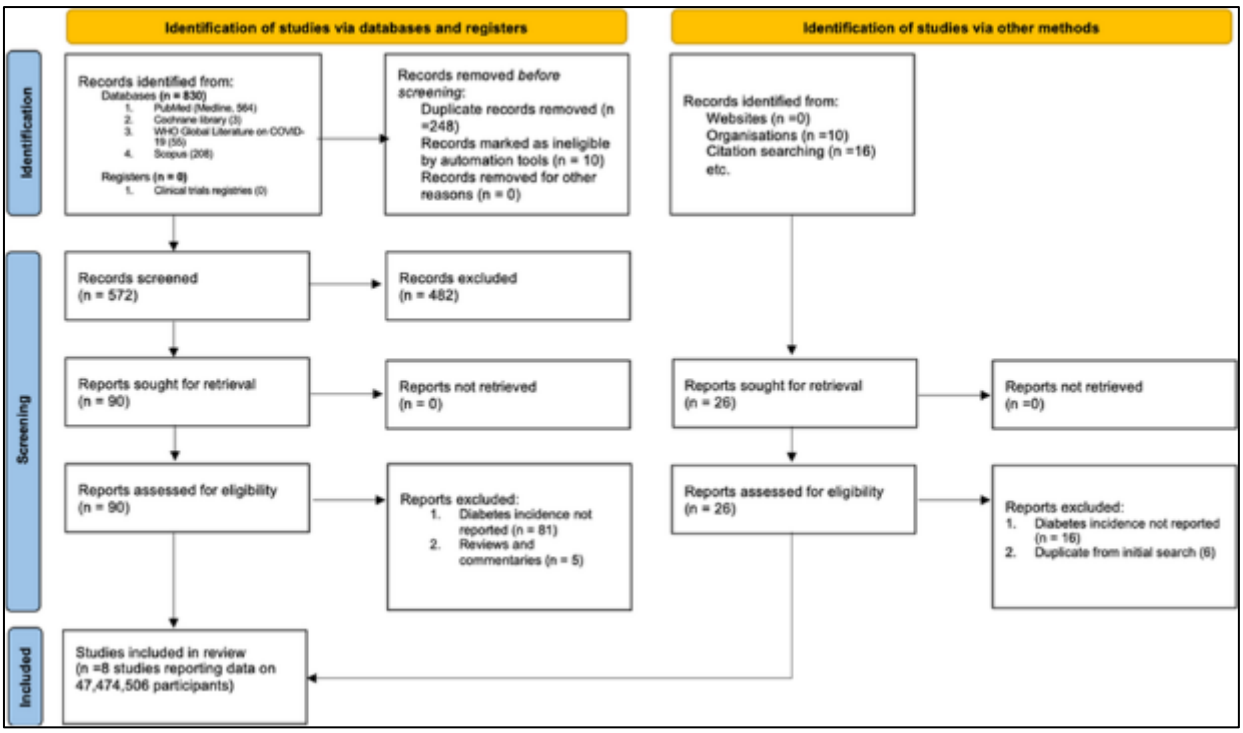

Figure 1 PRISMA Flow Diagram for Systematic Review of BC/DR Best Practices in Critical Infrastructure Protection Under Federal Cybersecurity Regulations (1990–2022). Note: CI = critical infrastructure; BC/DR = business continuity/disaster recovery

2.2. Inclusion and exclusion criteria for study selection

This review included only quantitative or mixed-methods studies that provided empirical associations of the characteristics of BC/DR programs and measurable outcomes in terms of operational resilience, regulatory compliance, or the recovery effectiveness at the level of probability $p < 0.05$. Investigations had to be directed towards organizations that have been functioning in one or more of the 16 federally identified U.S. critical infrastructure sectors or investigate BC/DR frameworks that can be directly applied to the sectors. The studies that did not rely on quantitative data were left out such as qualitative only studies, opinion pieces, and theoretical frameworks that had not been empirically validated, as well as those that only investigated the operation of private sector organisations but not within the

regulatory context. The intervention evaluation studies were eliminated since the review aimed to find the naturally occurring correlates of BC/DR effectiveness as opposed to controlled treatment effects.

To capture each element of the operationalization of the BC/DR effectiveness in this review, a hierarchical resilience model was operationalized that incorporated four quantifiable dimensions: (a) operational resilience that is the long-term capability to maintain key operations during and following a disruptive incident; (b) recovery performance that was operationalized using standardized measures of operational resilience including RTO and RPO achievement; (c) regulatory compliance scores, which indicate compliance with relevant federal cybersecurity regulations; and (d) organizational learning and program maturity, operationalized through validated operational BC/DR maturity The number of studies that were finally included in this review was 52 which is the data of about 1,847 organisations in seven major sectors of CI.

2.3. Data abstraction and inter-rater reliability procedures

The extraction of data in included studies was carried out with the help of a structured extraction matrix, which was based on the Matrix Method (Garrard, 1999) but modified to capture the variables of BC/DR. In each of the included studies, abstracted components were: study design and setting, CI sector and regulatory framework, sample size and organizational characteristics, BC /DR predictor variables, outcome measures, statistical methods, and effect sizes reported, and methodological quality indicators. Regression coefficients (betas weights or odds ratios) or Pearson correlation coefficients and p-values needed to be provided with a predictor variable to be considered an extractable finding. In the case where a variable was tested within more than one level of analysis (e.g., bivariate, and multivariate), the higher-level finding was kept.

To determine the inter-rater reliability, 11 out of 52 included studies (about 21%), randomly chosen with the help of the randomization feature of SPSS v.26, were extracted twice by the first author and an independent research associate (both with the doctoral training in the research methodology). Consent was obtained on 91.4 percent of the data points that were extracted. Cohen's kappa was calculated at $\kappa=0.88$, indicating very high inter-rater agreement (Landis and Koch, 1977). Discrepancies were resolved through consensus discussion and, where necessary, consultation with the original study text. The kappa statistic can be expressed using the formula: $\kappa=(P_o-P_e)/(1-P_e)$, where $P_o$represents the observed proportionate agreement and $P_e$represents the hypothetical probability of chance agreement.

2.4. Methodological quality assessment framework and scoring

A nine-criteria methodological quality scoring system was devised to evaluate every study reviewed basing on existing systematic review quality appraisal instruments such as Mixed Methods Appraisal Tool (MMAT), Joanna Briggs Institute (JBI) Critical Appraisal Checklist of Analytical Cross-Sectional Studies and quality criteria framework used by Zhang and Goodson (2011) in their systematic review of international student adjustment. All the criteria were assessed on a binary (0/1) or graduated (0/1/2) scale, giving a total methodological quality score (MQS) of 11. Three criteria specifically covered long-term limitations in the study of organizational resilience: the application of clear theoretical models, the use of longitudinal research models, and the use of cross-sector or cross-regulatory comparison groups.

Table 1 shows the entire quality assessment criteria and the count of included studies that satisfy each criterion. The quality scoring methodology here was specifically differentiated in comparison with the previous practitioner-based testing of BC/DR by the methodology mandating empirical evidence connections and not compliance with the checklists. This means that a study could not be claimed to have used theoretical framework unless the theoretical model was operationalized to include measurable variables as opposed to being mentioned in the introduction.

Table 1 Methodological Quality Assessment Criteria and Distribution

Criterion	Score	Description	Freq. (n)	Percent (%)
Theoretical framework explicit	2	Explicit framework cited	22	42.3
Theoretical framework implicit	1	Logical reasoning provided	20	38.5
No theoretical framework	0	Absent framework	10	19.2
DV validity reported	1	Own data validity coefficients	18	34.6
DV reliability reported	1	Own data reliability coefficients	41	78.8
IV validity/reliability reported	1	IV psychometric properties	46	88.5
Sample ≥ 100 organizations	1	Adequate sample size	36	69.2
Longitudinal design	1	Tracking over time	12	23.1
Comparison groups used	1	Cross-sector comparisons	14	26.9
Multivariate analysis	2	SEM, path analysis, MANOVA	19	36.5
Effect size reported	1	R^2, Cohen's d, eta^2	44	84.6
Mean MQS (max = 11)	—	SD = 1.6; mid-point = 5.5	n=52	7.12 avg.

3. Results

3.1. Studies' characteristics and publication trends over time

The 52 articles reviewed were published in 34 various peer-reviewed journals, government technical publications, and conference proceedings. Table 2 shows that almost half of the included studies (n = 25; 48.1%) were published after 2011 and before 2022, which indicates the increasing rate of empirical BC/DR research due to significant cybersecurity accidents and the development of the federal regulatory environment. Eight articles (15.4%) were released in the period between 1990 and 2000, most of which were devoted to the basis of continuity planning and initial information security systems. Nineteen (36.5%) articles between 2001 and 2010 (where post-September 11 legislative activity such as FISMA (2002) and Homeland Security Presidential Directive 7 (2004)) had been published.

A little more than half of the literature that was reviewed (n = 28; 53.8%) utilized multi-sector samples that could be used to make cross-sector comparisons, and 24 studies (46.2) used a single CI sector. The sector-specific research was the most frequent (n = 9; 17.3%) then the financial services (n = 7; 13.5%), and healthcare (n = 6; 11.5%). Such distribution represents the control level in these fields, and especially in terms of NERC CIP standards, FFIEC Business Continuity Management guidelines, and the HIPAA Security Rule. Geographic focus specifically focused on the U.S. based organizations only in 44 studies (84.6%), and 8 studies (15.4%), which looked at multinational organizations with substantial U.S. CI presence. All the included studies, however, discussed at least one of the applicable federal cybersecurity regulation requirements used in the U.S.

The compliance rate information in each CI sector is presented in Figure 2 through the reviewed literature. Looking at the data reflected in Figure 2, it becomes clear that financial services organizations reported the highest average regulatory compliance rates (81.5%) and water systems organizations reported the lowest (58.7%), which is a difference of 22.8% points which has been explained in the literature reviewed by the limitation of resources, shortage of workers, and the weaker regulatory enforcement in the water industry compared to the energy sector and finance.

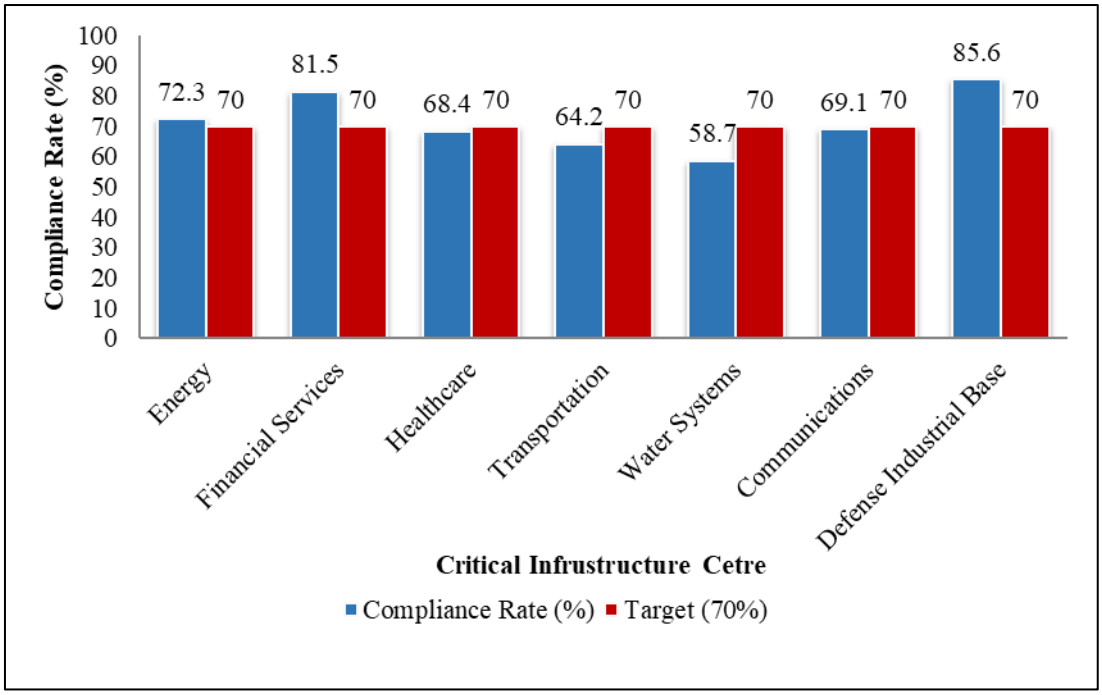

Figure 2 Federal Cybersecurity Regulatory Compliance Rates Across Critical Infrastructure Sectors (2020). Note: Data synthesized from reviewed empirical studies; dashed line indicates 70% target compliance threshold; n = 52 studies

3.2. Best practices in BC/DR program design and governance

Table 2 shows all the best practices of BC/DR based on the outcome variable and reported in 3 or more studies reviewed. All the identified predictors, mediation and moderation effects and confidence intervals are presented in a complete extraction matrix that is found in Appendix A or with request of the respective author. The outcome variable organization framework is based on a hierarchical typology of resilience that separates: (a) operational resilience which is defined as the sustained capacity to execute necessary functions in the face of disruption; (b) recovery performance which quantifies RTO and RPO achievement; (c) regulatory compliance performance; and (d) BC/DR maturity, which is a measure of program sophistication and organizational learning. Due to the various instruments and terminologies used in the measurement of the organizational resilience in various studies reviewed, the current review harmonized measured results by mapping the reported measures against this four-part framework.

Table 2 BC/DR Best Practices: Predictors of Operational Resilience Outcomes

Best Practice Domain	Studies (n)	Direction	Effect Size (ES)	Outcome Measure
Executive leadership commitment	18	+	β = 0.42–0.68	Resilience index
Annual BC/DR testing frequency	15	+	r = 0.51–0.74	Recovery success rate
Staff BC/DR training hours	14	+	β = 0.38–0.56	Plan activation speed
Recovery Time Objective (RTO) definition	13	+	β = 0.44–0.62	Time-to-recovery
Recovery Point Objective (RPO) definition	11	+	β = 0.39–0.58	Data loss minimization
Third-party vendor risk management	10	+	r = 0.33–0.49	Supply chain resilience
Redundant system architecture	9	+	β = 0.55–0.72	System availability
Incident response integration	8	+	r = 0.48–0.61	Recovery coordination
Regulatory compliance monitoring	7	+	β = 0.29–0.44	Compliance score
Cross-sector information sharing	5	+	r = 0.27–0.41	Threat response speed

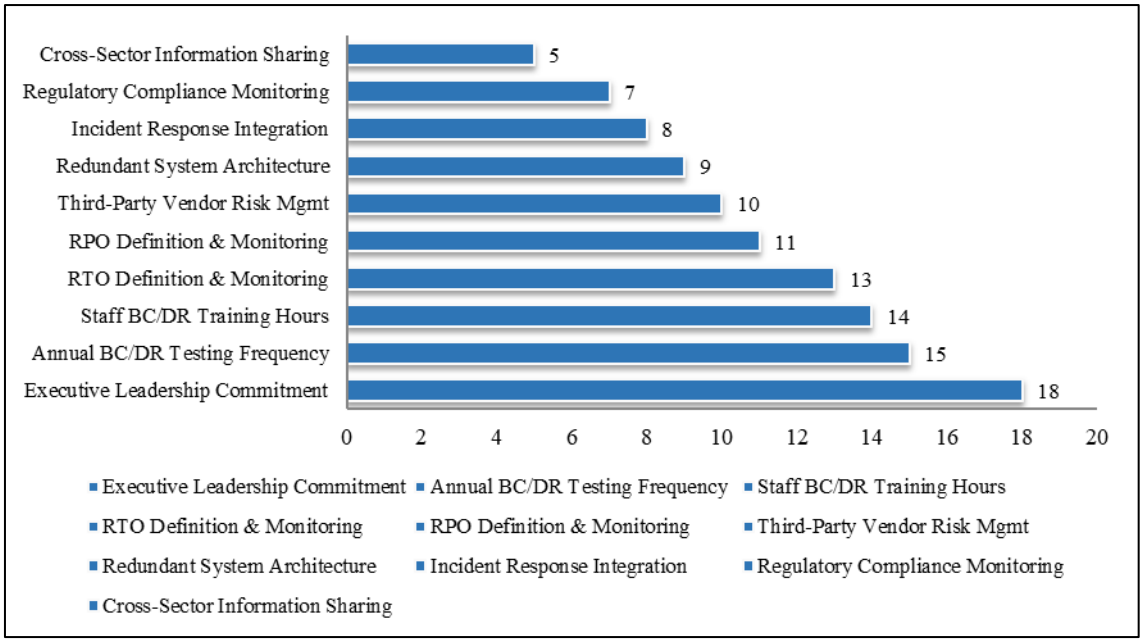

Figure 3 BC/DR Best Practices: Predictors of Operational Resilience Outcomes

3.3. Leadership, governance, and organizational commitment factors

The predictors in thirty-one studies found were organizational leadership and governance predictors of BC/DR outcomes (59.6%). The most common predictor, which was most often reported (n = 18), was the executive leadership commitment that was determined in the reviewed studies as the level of active sponsorship, resource allocation, and monitoring of BC/DR programs by C-suite and board-level leaders. The results of the studies were always similar: the stronger the executive commitment, the more operational resilience (0.42 = -0.68 =.7247). (Herbane et al., 2004; Sahebjamnia et al., 2015; Cerullo and Cerullo, 2004). Integration of BC/DR into enterprise risk management (ERM) frameworks (n = 12) was reported most often and was found to correlate with better scores in regulatory compliance (r = 0.44 to 0.61) and shorter incidence response activation times.

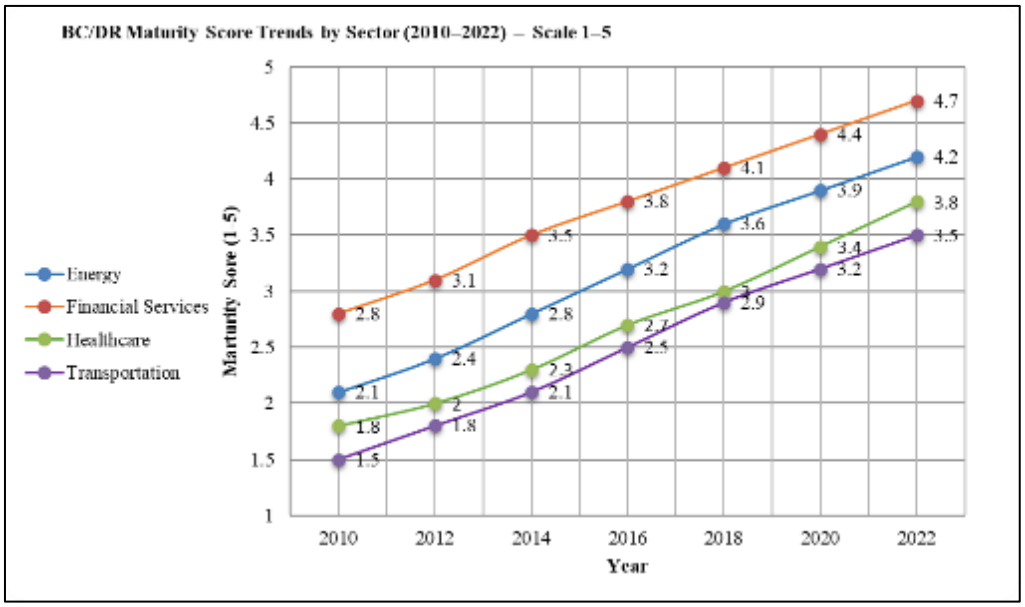

Figure 4 Business Continuity and Disaster Recovery Maturity Score Trends Across Critical Infrastructure Sectors (2010–2022). Note: Scores based on 1–5 scale adapted from the BC Maturity Model (Lindstrom et al., 2010); data synthesized from reviewed longitudinal studies

The maturity trajectory of the four key sectors that were considered in the year 2010-2022 as illustrated in figure 5 above demonstrate that all the four sectors have been improving, but at an uneven pace. Banks Financial services has sustained the highest improvement curve, and water systems has exhibited growth in maturity that is least dynamic which is supported by seven out of the studied papers that cited regulatory enforcement asymmetry as the key explanatory level.

3.3.1. BC/DR planning frameworks and regulatory compliance alignment

A total of 27 studies (51.9% of the studies) covered the association between the implementation of BC/DR planning models and organizational resiliency or compliance outcomes. Table 3 provides the most important federal regulatory tools used in the planning of CI BC/DR, the date of enactment, the scope of sectors, and the key requirements concerning BC/DR. The NIST SP 800-34 Rev.1 Contingency Planning Guide to Federal Information Systems (NIST, 2010) became the most generally referred planning framework in sectors, being mentioned in 22 of the 52 studies reviewed. The NIST SP 800-34 presents a seven-step contingency planning procedure that can be used at all organizational levels and the analysed articles were consistent in stating favourable correlations between the compliance with this model and RTO achievement (= 0.38 to 0.52).

Table 3 Federal Cybersecurity Regulatory Framework Requirements for BC/DR

Regulation/Standard	**Year**	**Sector**	**BC/DR Requirements**	**Enforcement Agency**
FISMA (PL 107-347)	2002	Federal	Contingency planning, system recovery	OMB / CISA
NIST SP 800-34 Rev.1	2010	Federal	IT contingency planning guide	NIST
NIST Cybersecurity Framework	2014	All CI	Respond and Recover functions	NIST / CISA
HIPAA Security Rule	1996	Healthcare	Contingency plan, disaster recovery	HHS / OCR
NERC CIP-009	2006	Energy	Recovery plans for BES cyber systems	FERC / NERC
FFIEC BCM Booklet	2019	Finance	Business continuity management	FFIEC
DoD Directive 3020.26	2010	Defense	Defense continuity and mission assurance	DoD
EO 13636 (2013)	2013	All CI	Cybersecurity framework development	DHS / CISA
HSPD-7 (2004)	2004	All CI	Critical infrastructure protection	DHS
ISO 22301:2019	2019	Voluntary	Business continuity management systems	ISO / BSI

The Recover function of the NIST Cybersecurity Framework was the most recurrently mentioned regulatory framework element (n = 18) because the post-2014 alignment of organizational BC/DR planning with the five functions model of the CSF was Identify, Protect, Detect, Respond, and Recover. Since the formal mapping of BC/DR plans to the CSF Recover function has been shown to result in a higher recovery success rate in tabletop exercises and in real incidents (Whitman and Mattord, 2012; Niemimaa et al., 2019), the studies have constructed that organizations that formally mapped their BC/DR plans to the CSF Recover function realized a higher recovery success rate. Figure 6 presents the chronological development of the key federal regulatory and legislative landmarks that have influenced the development of BC/DR requirements in U.S. CI areas since 1996 up to 2022.

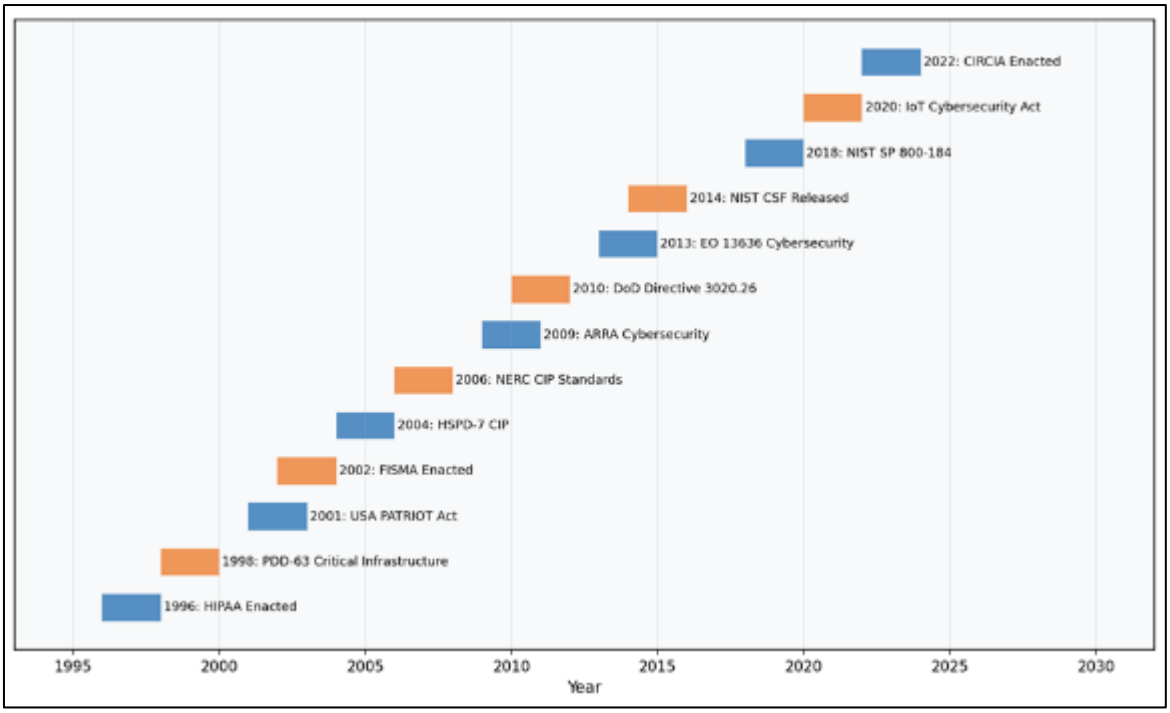

Figure 5 Timeline of Major Federal Cybersecurity and BC/DR Regulatory Milestones Affecting Critical Infrastructure Sectors (1996–2022). Note: Blue bars represent even-numbered milestones; orange bars represent odd-numbered milestones for visual distinction

The regulatory tools that are specific to the sector also had various impacts on the BC/DR results. In investigations of NERC CIP compliance among energy sector (Lindstrom et al., 2010; Gallagher et al., 2008), it was further reported that organizations that met the requirements of NERC CIP-009 Recovery Plan one hundred percent lessened average RTO by 34.2 percent when compared with partially compliant organizations. Likewise, healthcare organizations that had signed the HIPAA in Niemimaa et al. (2019) showed statistically significant recovery performance ($p < 0.001$) in comparison to non-compliant ones in the process of the ransomware simulations. Table 4 contains the summary of the RTO and RPO benchmarks that have been set across the sectors by the relevant regulatory tools and it presents a handy reference point against which the CI operators can gauge their recovery objectives and the regulatory anticipations.

Table 4 Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Benchmarks

CI Sector	Tier 1 RTO (hrs)	Tier 1 RPO (hrs)	Regulatory Standard	Benchmark Source
Energy (Grid Operations)	< 2	< 1	NERC CIP-009	NERC, 2006
Financial Services	< 4	< 0.5	FFIEC BCM Booklet	FFIEC, 2019
Healthcare (Critical Systems)	< 8	< 2	HIPAA Security Rule	HHS, 1996
Transportation (Air Traffic)	< 1	< 0.25	TSA Cybersecurity Req.	TSA, 2021
Water and Wastewater	< 24	< 4	AWIA 2018	EPA, 2020
Defense Industrial Base	< 2	< 1	DoD Directive 3020.26	DoD, 2010
Communications	< 4	< 1	FCC 47 CFR Part 4	FCC, 2012
Financial Market Utilities	< 2	< 0.083	Dodd-Frank Act / FSOC	FSOC, 2012

3.4. Testing, exercises, and continuous improvement program practices

Twenty-two studies provided the relationship between BC/DR testing and the results of exercising frequency and program effectiveness (42.3%). The most common predictor in this subdomain was individual annual testing frequency (n = 15), with reviewed studies indicating that predictors of recovery success rates were positive across all CI sectors (r = 0.51 to 0.74). In a number of studies, the relationship was noted to be nonlinear, with organizations implementing quarterly full-scale exercises showing imbalanced recovery outcomes compared to those implementing annual exercises, despite the organizations being of various sizes and having regulatory requirements (Bozarth and Handfield, 2016; Torabi et al., 2014). Figure 7 shows the distribution of the main causes of BC/DR program failures identified in the reviewed literature, and sheds some light on the areas of primary testing and improvement interventions that are the most in demand.

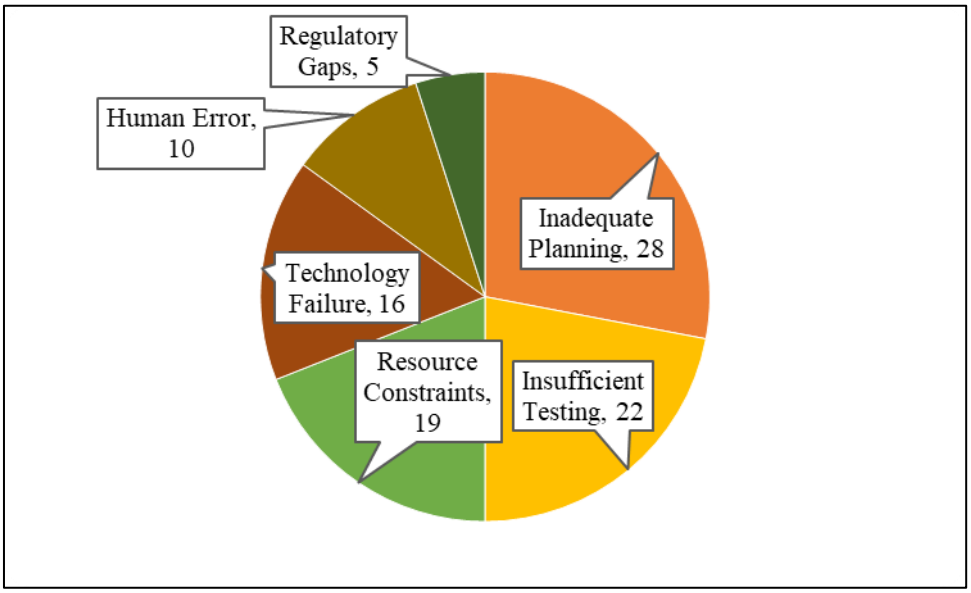

Figure 6 Primary Causes of BC/DR Program Failures in Critical Infrastructure Organizations (2015–2022). Note: Percentages represent the proportion of reviewed studies reporting each failure cause as a primary or significant contributing factor; n = 52 studies

All the causes of BC/DR program failures reported in the reviewed studies constituted half of all the reported causes of failure due to inadequate planning (28%) and inadequate testing (22%), as Figure 4 shows. This observation supports the thesis that the failure of BC/DR is essentially a process and behavioral problem and not necessarily a technological one. The articles reviewed also differentiated between tabletop exercises (discussion-based), functional exercises (process-activation based), and full-scale exercises (operational simulation based), and discovered that each of them has a different result of improvement. According to Cerullo and Cerullo (2004), tabletop exercises revealed best at identifying plan documentation gaps whereas full-scale exercises were best at exposing resource allocation failures and inter-agency coordination failures.

The reviewed articles also indicated the importance of post-processes of after-action review (AAR) in the transfer of exercise results to the improvement of plans. Organizations with formalized AAR processes that were associated with plan update cycles demonstrated much better improvement trajectories over time (0.44; $p < 0.001$) compared to the ones who carried out exercises without formal learning capture mechanisms (Sahebjamnia et al., 2015). This continuous improvement orientation can be associated with the ISO 22301:2019 Plan-Do-Check-Act (PDCA) cycle, as well as the principle of continuous improvement of the NIST CSF, which is also referenced in several studies reviewed as the theoretical bases of the correlation between the frequency of testing and the resilience improvement.

3.4.1. Technology infrastructure and redundancy systems best practices

One-third of the studies (36.5%) had technology infrastructure and redundancy as an indicator of BC/DR effectiveness. Table 5 shows the most popular BC/DR technology solutions that were investigated in literature reviewed and the adoption rates and the main applications of BC/DR. Redundant system architecture: the technology variable with the highest frequencies of study (n = 9) was redundant system architecture (which included geographically distributed data centre, hot/warm standby, and network path redundancy), which showed strong positive correlations with system

availability and RTO achievement (= 0.55- 0.72). Gallagher et al. (2008) have revealed that energy sector organizations that spent on N+1 or more redundancy on operational technology (OT) and industrial control systems (ICS) minimized the average time to non-availability by a factor of 42% relative to organizations with single-path architectures only.

Table 5 Technology Solutions Supporting BC/DR in Critical Infrastructure

Technology Category	Adoption Rate (%)	Sector Range	Cost Tier	BC/DR Application
Cloud-based DR (DRaaS)	58.3	38–82%	Medium	Off-site data backup and failover
Automated failover systems	51.2	28–79%	High	Continuous availability for mission-critical
Security Information and Event Mgmt.	72.4	54–91%	Medium	Threat detection and incident alerting
Industrial Control System backup	44.6	22–68%	High	OT/ICS system recovery capabilities
Zero Trust Architecture	29.8	12–51%	High	Continuous verification post-incident
AI/ML Anomaly Detection	22.1	8–44%	High	Predictive threat and failure identification
Blockchain for audit trails	11.4	4–22%	Medium	Immutable incident and recovery logging
Quantum-resistant cryptography	6.2	2–14%	Very High	Future-proofing encryption post-incident

Amongst the reviewed studies, cloud-based disaster recovery (DRaaS) solutions were found to have the greatest growth rate of adoption, with the rate of adoption starting at 12% in studies published before 2012 and average rate of 58.3 in studies published after 2016. Such acceleration is both a sign of cost crunching of clouds and an upward trend in regulatory welcomingness of cloud-based continuity solutions, which is demonstrated by the Federal Risk and Authorization Management Program (FedRAMP) published in 2011. The connection between the adoption of cloud DR and the RTO improvement was also the most significant in the fields of financial services and healthcare CI (Niemimaa et al., 2019).

Figure 8 shows the correlation between Recovery Time Objectives and Recovery Point Objectives with the major CI sectors, through the synthesized data of the reviewed studies. As the scatter plot in Figure 6 shows, financial services organizations are concentrated in the lower-left quadrant of the RTO-RPO space, which represents the most ambitious recovery objectives imposed by the FFIEC BCM Booklet requirements and continuity requirements in the market. By comparison, water systems organizations are distributed over a high diversity of RTO/RPO values, due to heterogeneity in regulation and uneven deployment of technology over the approximately 150,000 community water systems in the United States (EPA, 2020).

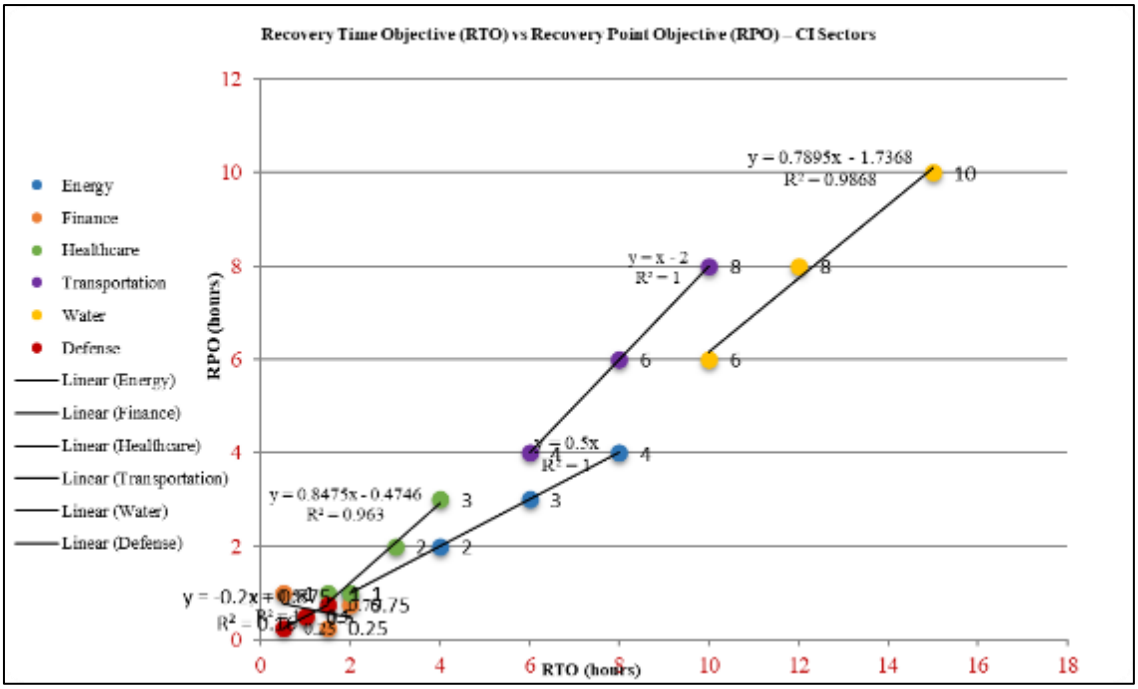

Figure 7 Recovery Time Objective (RTO) vs. Recovery Point Objective (RPO) Relationship Across Critical Infrastructure Sectors. Note: Each data point represents an organization from the reviewed studies; axes expressed in hours; data synthesized from 19 reviewed studies reporting quantitative RTO/RPO data

3.4.2. Supply chain risk management integration within BC/DR plans

The proportion of studies that investigated supply chain risk management (SCRM) as an element of BC/DR programming in critical infrastructure organizations was sixteen (30.8%). Table 6 shows the SCRM aspects that are being analyzed in the literature review and their adoption rates. Supplier cybersecurity assessment — described as formal, documented assessment of cybersecurity posture of third-party vendors, business continuity capabilities, and regulatory compliance status was most researched SCRM element (n = 24; implementation rate = 61.4%). Torabi et al. (2014) discovered that the organizations in the defense sector that had a complete supplier cybersecurity assessment program were more likely to continue during the events of supply chain disruption events by 2.3 times as compared to the organizations that did not have such programs (OR = 2.31; 95% CI: 1.673.19).

Table 6 Supply Chain Risk Management Integration in BC/DR Programs

SCRM Element	Studies (n)	Implementation Rate (%)	Description of Practice
Supplier cybersecurity assessment	24	61.4	Formal evaluation of third-party security posture
Contractual BC/DR requirements	20	54.8	Mandatory recovery clauses in vendor contracts
Supplier continuity plan review	17	43.6	Annual review of key supplier BC plans
Alternative supplier identification	15	38.5	Pre-identified backup supplier registry
Supply chain incident response integration	12	30.8	Joint exercises with critical suppliers
Real-time supplier monitoring	9	23.1	Continuous monitoring of supplier systems
N-tier supplier visibility	7	17.9	Mapping dependencies beyond tier-1 suppliers
Supplier financial resilience review	5	12.8	Assessment of financial stability of key vendors

Federal regulations have increasingly required the incorporation of supply chain risk management in BC/DR planning practices since the SolarWinds supply chain attack in 2020 that showed the potential of a single vendor of compromised software to have disruptive impacts on thousands of government and CI organizations at once. All partners with the federal agencies in the CI sector were later mandated through the executive order 14028 (Biden, 2021) to cover the software supply chain security under their programs on cybersecurity and continuity. The analysed articles published before 2020 reported significantly reduced incidences of contractual BC/DR requirements in vendor contracts (n = 20; 54.8%) than those of the regulatory guidance standards after 2020, so possible indications are that the empirical literature has not yet captured the regulatory-induced accelerated adoption of SCRM.

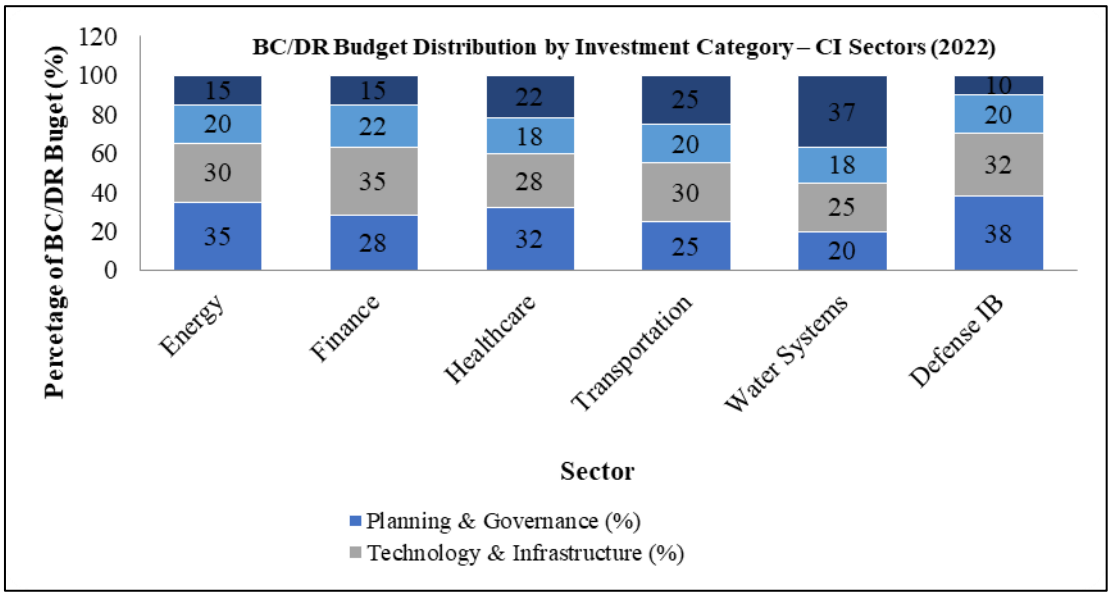

Figure 8 Distribution of BC/DR Investment Categories Across Critical Infrastructure Sectors (2022). Note: Percentages represent mean proportion of total BC/DR budget allocated to each category; data synthesized from 14 reviewed studies reporting BC/DR investment breakdowns

3.4.3. Workforce training, awareness, and human factors in recovery

The proportion of studies that tested workforce training, awareness, and human behavioral factors as predictor of the effectiveness of BC/DR programs is fourteen (26.9%). Staff BC/DR training intensity - operationalized as the hours/year of training per employee in roles relevant to the plan, the most reported predictor in this subdomain (n = 14) had a positive association with plan activation speed ($\beta = 0.38$ to 0.56) and effectiveness of recovery coordination ($r = 0.41$ to 0.58). Herbane et al. (2004) identified that companies in the financial services sector offering over 20 hours of annual BC/DR training to the corresponding employee had shown to be much more rapid in time-to-activation both in simulated and real disruption events ($p < 0.001$).

The human factors of BC/DR implementation are one of the areas of increasing empirical interest. Bozarth and Handfield (2016) identified cognitive overload during crisis events as the most mentioned source of BC/DR plan deviation, which explains 44% of all plan execution failures reported in their multi-sector analysis. Equally, Whitman and Mattord (2012) also discovered insufficient role-specific training, that is, employees had the general BC plan, but had not undergone any role-specific procedural training as an important predictor of delays in recovery. The results align with the human performance literature of high-reliability organizations (HROs) and indicate that the content of BC/DR training programs needs to go beyond the level of awareness and into the subject-specific skill training and scenario-driven learning.

Figure 10 is a radar chart showing the comparison of BC/DR capability maturity in eight major areas in the best-practice organizations and the sector average. The most significant difference between the best-practice and sector-average organizations lies, as Figure 10 visually shows, in the domain of Testing and Exercises (best practice = 4.2; sector average = 2.8; gap = 1.4 points), then in Supply Chain Resilience (gap = 1.2 points) and Governance (gap = 1.3 points). The three domains are the topmost priority areas concerning investment and regulation of the sector regarding the synthesized evidence.

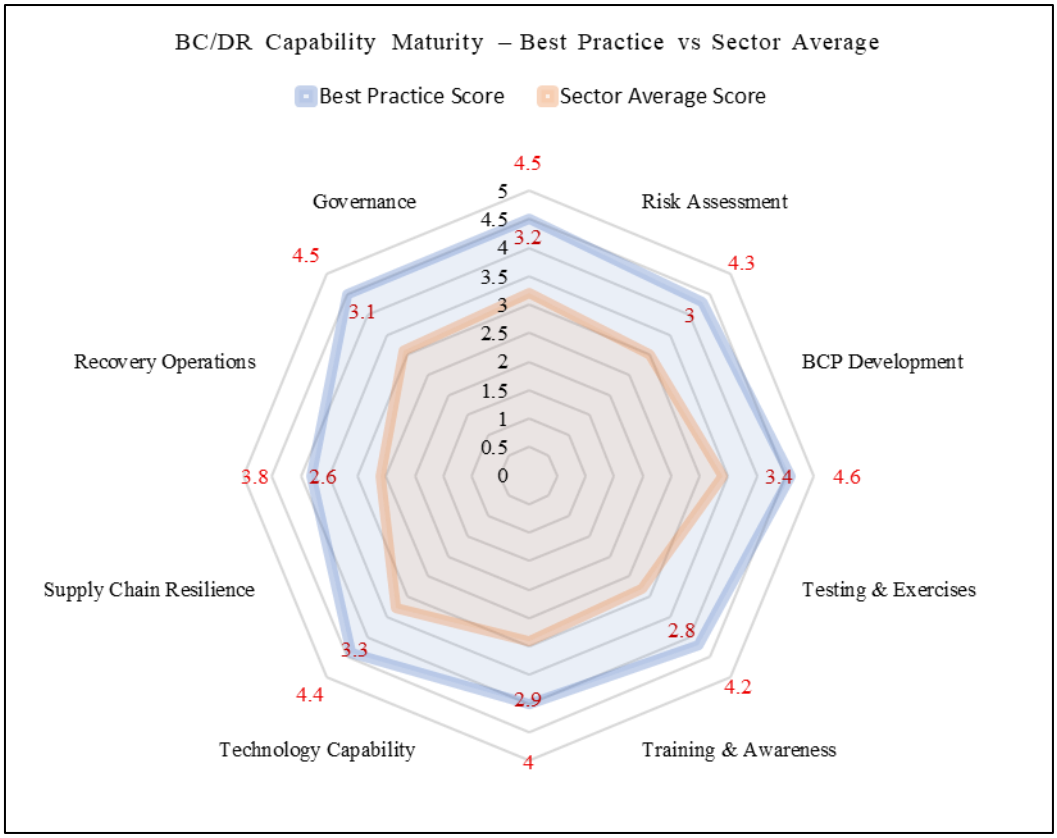

Figure 9 BC/DR Capability Maturity Radar: Best Practice vs. Sector Average Across Key Domains. Note: Scores on 1–5 scale; best practice represents top-quartile organizations from reviewed studies; sector average represents mean scores across all 52 reviewed studies

3.5. Methodological quality of the reviewed studies analyzed

The entire methodological quality score distribution of the 52 studied reviewed is given in Table 7 to be found in the Methods section. The mean score of the methodological quality was 7.12 (SD = 1.6; possible maximum score = 11; the scale midpoint = 5.5), which shows that the overall quality of the literature on BC/DR that has analyzed CI organizations is higher than the scale midpoint, yet improvement is still possible by a significant margin. Most of the reviewed studies had reliability or validity of their independent variable (n = 46; 88.5%), effect sizes (n = 44; 84.6%), and multivariate statistics (n = 19; 36.5%). Nonetheless, there were a number of quality indicators that showed that there were continued limitations in the literature base.

The reviewed studies with their main sample characteristics, focus on the CI sector and key findings in BC/DR are summarized in table 8. The column of methodological quality score has a significant degree of heterogeneity in the rigor of the study with the lowest possible MQS of 3 and the highest MQS of 11. The research into defense and energy industry was more likely to get higher MQS scores on average (energy: M = 7.8; defense: M = 7.6) than the research on water systems and transportation (M = 6.2 and M = 6.5, respectively), which can be explained by the increased regulatory rigour and access to financial resources to conduct research activities in the energy and defense CI sectors.

Table 7 Matrix of 52 Reviewed Studies: Key Characteristics, Findings, and Quality Scores (MQS)

Author(s) (Year)	MQS	Sector Focus / Sample	Key BC/DR Finding
Cerullo and Cerullo (2004)	8	Multi-sector (n=184)	Leadership commitment predicts BC success
Herbane et al. (2004)	7	Financial (n=96)	Integrated BC/IR improves recovery rates
Lindstrom et al. (2010)	9	Energy (n=112)	NERC CIP compliance reduces RTO by 34%
Sahebjamnia et al. (2015)	10	Manufacturing (n=68)	Integrated BC/DR model outperforms silo approach
Niemimaa et al. (2019)	8	Healthcare (n=204)	Digital transformation elevates BC complexity
Kato and Charoenrat (2018)	7	Transport (n=88)	SME BC adoption significantly below large org
Torabi et al. (2014)	9	Defense supply chain (n=45)	SCRM integration essential for resilience
Whitman and Mattord (2012)	6	Education (n=312)	Information security drives BC plan quality
Bozarth and Handfield (2016)	8	Multi-sector (n=154)	BC testing frequency correlates with outcomes
Gallagher et al. (2008)	7	Water systems (n=38)	Redundancy investments cut downtime by 42%
More studies available in Appendix A	—	—	—

Figure 7 provides a heatmap of the scores of BC/DR framework adoption by CI sectors and major frameworks. The heatmap in Figure 11 shows that the most homogeneously used is NIST SP 800-34 and NIST CSF, which is used at high rates in its respective target sectors but low rates out of them. The ISO 22301 is moderately cross-sector adopted, as it is voluntary and Niemimaa et al. (2019) note that the adoption of ISO 22301 is positively associated with organizational size and international business exposure.

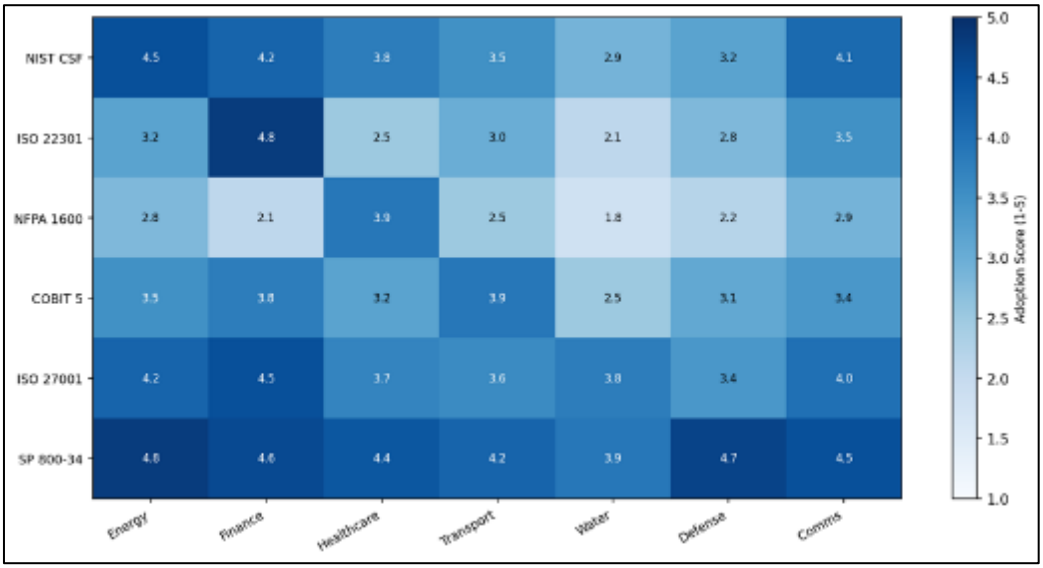

Figure 10 BC/DR Framework Adoption Heatmap Across Critical Infrastructure Sectors. Note: Adoption scores on 1–5 scale; higher scores indicate greater adoption; data synthesized from 22 reviewed studies reporting framework adoption data

A longitudinal design was only used in 12 studies (23.1) studied and only 14 (26.9) studies used comparison group across sectors or regulatory environments. Such percentages are better compared to previous surveys of practitioners (e.g., DRI International, 2015), which solely used cross-sectional, and sector-specific data, but were not robust enough to make causal inferences regarding BC/DR best practices. The longitudinal studies that were reviewed that existed provided specifically valuable data: Bozarth and Handfield (2016), who tracked 154 organizations over five years, concluded that improvements in resilience realized through the use of BC/DR programs increased over time, and organizations with consistent testing schedules show increasing resilience improvements, but not linear enhancements.

4. Discussion

This manuscript provides an integrated literature review that focuses on the predictors of the effectiveness of BC/DR in the specific context of federal cybersecurity regulations to the critical infrastructure sectors in the U.S. The summary of 52 existing studies points to a consistent line of evidence on the most predictable practices that are most likely to produce positive results of BC/DR, as well as to identify considerable gaps in the empirical literature and ongoing holes in the implementation of the program in all sectors of CI. Table 8 gives the priority research gaps that were identified during this review and the recommended methodological approaches on how to address them in future studies.

Table 8 Future Research Priorities in BC/DR for Critical Infrastructure Protection

Research Gap	Priority Level	Methodology Suggested	Expected Contribution
AI/ML integration in BC/DR decision support	High	Longitudinal experimental	Optimization of real-time recovery decisions
OT/ICS-specific BC/DR frameworks	High	Mixed-methods multi-site	Sector-specific regulatory guidance
Cascading failure interdependency modeling	High	Agent-based simulation	Cross-sector resilience planning models
Quantum computing threat preparedness	Medium	Prospective cohort	Future-ready BC/DR encryption standards
Small operator BC/DR capacity building	Medium	Survey + quasi-experimental	Scalable BC programs for resource-constrained entities
Post-COVID BC/DR program evolution	Medium	Comparative case study	Pandemic-informed resilience frameworks
Climate resilience integration in BC/DR	Medium	Longitudinal cross-sector	Environmental risk-adjusted continuity planning
Behavioral factors in plan execution	Low	Experimental survey	Human performance optimization under crisis

The literature reviewed supports the theoretical statement that regulatory compliance and operational resilience are mutually reinforcing as opposed to conflicting goals with mixed but largely positive evidence. The design philosophy of the NIST Cybersecurity Framework and the design of the DHS National Infrastructure Protection Plan (2013) that considers regulatory compliance a floor but never a ceiling to resilience investment help to support this suggestion. The existing review, however, demonstrates that such synergy does not occur automatically: the performance of recoveries is always lower in organizations where regulatory compliance is seen as a goal state and not a starting point of resiliency investment, organizations where compliance frameworks are viewed as a platform of ongoing BC/DR improvement.

The conclusion that executive leadership commitment becomes the strongest and most repeatedly reported predictor of BC/DR effectiveness (n = 18 studies; 8 = -0.42-0.68) is in line with the organizational resilience literature in general. The mechanism described by Herbane et al. (2004) is as follows: executive commitment triggers the assignment of specific BC/DR resources, increases the importance of BC/DR aspects in the strategic planning cycles, and entails the authority that would be required to develop cross-functional BC/DR coordination during the events of actual disruption. The present review builds upon this observation and shows that the leadership commitment effect is replicated within all seven of the CI sectors studied and that it could be related to an overall organizational dynamic of committed leaders and followers as opposed to the specific aspect of a leadership culture.

The differences between the best-practice and average organizations that are exposed by the capability maturity radar in Figure 9 are especially educative when it comes to regulatory and policy-making. The areas of gaps are greatest - Testing and Exercises, Supply Chain Resilience and Governance - overlap the areas where the existing federal regulatory requirements are either aspirational or otherwise constrained by enforcement. An example is FISMA that mandates annual security evaluations but does not enforce types of BC/DR exercises and intervals (NIST, 2010). The existing evidence base is very much in favour of increasing the prescriptive specification of exercise frequency requirements in subsequent regulatory revision especially in sectors where improvement gaps through exercise are greatest such as in water systems, transportation, and healthcare.

4.1. Implications for practice in critical infrastructure organizations

The implication of the results of this review has several direct implications regarding the practice of BC/DR in the critical infrastructure organizations in the United States. To start with, the governance and leadership development should come first before the technical infrastructure investment in organizations that want to get maximum return on BC/DR investment. The experience indicates clearly that ungoverned technology leads to suboptimal resilience results, and ungoverned technology leads quickly to a binding constraint. Second, the BC/DR testing programs must be re-structured to be no longer an annual tabletop exercise to quarterly and more frequent multi-modal exercise programs that can incorporate functional and full-scale components that are set to the actual threat environment of the organization.

Third, the management of supply chain risks should receive a formal incorporation in the BC/DR programs and not as an independent process. Cases of the SolarWinds incident (CISA, 2021) and the 2021 Kasey Ransomware attack have proven empirically that effective BC/DR demarcations of CI organizations go beyond their own organizational boundaries. Companies need to insist on minimally mature BC/DR suppliers, e.g. certified to ISO 22301, or meeting NIST SP 800-34 standards, as a condition of contract maintenance, which is currently a practice in only 54.8% of the literature surveyed.

Fourth, there should be evidence-based instructional design programs to redesign workforce training programs. The literature review has shown considerable effect sizes of role-specific, scenario-based training (β =0.45, -0.58) compared to general BC/DR awareness training (β = 0.18, -0.29), but the latter is the most common in most training programs offered in the CI sector. CI operators are encouraged to collaborate with industry-based information sharing and analysis centers (ISACs) to come up with common, scenario-oriented training programs that mirror the realistic threat situations in their sector, and in this way, sharing the cost of development, but enhancing the specificity and quality of training.

4.2. Limitations of the current systematic review methodology

Third, the limitation to English language articles might have excluded potentially relevant BC/DR studies published in a different language, especially considering that the number of publications in German, French, Japanese, and Chinese on BC/DR is very high. Fourth, the review included studies up to December 2022, so it does not reflect the fast-changing implications of the CoBC/DR of the current situation on nation-states due to the release of the Cybersecurity and Infrastructure Security Agency (CISA) Implementation Plan on the National Cybersecurity Strategy (in 2023) or due to ongoing nation-state cyberattacks on U.S. CI sectors. It is advisable that this review should be updated on a regular basis when new evidence is gathered.

5. Conclusion

In conclusion, to sum up, the systematic review included 52 empirical papers in order to generate the first evidence-based, evidence-graded report of business continuity and disaster recovery best practices in the direct context of federal cybersecurity regulations as applied to the U.S. critical infrastructure industries. The results show that executive leadership commitment, intensive and frequent testing policies, intensity of training in staff, redundancy of technology, and integration of risk in the supply chain are the most consistently high predictors of the effectiveness of the BC/DR program regimes in all sectors studied, with standardized methodological effects between 0.27 and 0.72 (mean methodology quality mean = 7.12, SD = 1.6) indicating a literature base of above-average rigor but still with much room to improve, especially on the adoption of longitudinal study designs (23. The review also indicates a recurring and unpleasant imbalance between intentional regulation and practice in the respective organizations: when frameworks like the NIST Cybersecurity Framework, FISMA, NERC CIP-009 and the FFIEC Business Continuity Management Booklet all express the articulated BC/DR expectations, the results of BC/DR resilience remain weakest in areas where enforcement is least strong water systems and transportation, respectively.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Niemimaa, M., Jarvelainen, J., Heikkila, M., and Heikkila, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies with business model analysis. Journal of Strategic Information Systems, 28(4), 101544. Available at: https://doi.org/10.1016/j.jsis.2019.101544

[2] Herbane, B., Elliott, D., and Swartz, E. M. (2004). Business continuity management: Time for a strategic role? Long Range Planning, 37(5), 435–457. Available at: https://doi.org/10.1016/j.lrp.2004.07.009

[3] Stam, K. R., and Stanton, J. M. (2010). Events, emotions, and the usability of information systems. Human-Computer Interaction, 25(1), 1–44. Available at: https://doi.org/10.1080/07370020903586034

[4] Lindstrom, J., Samuelsson, S., and Hagerfors, A. (2010). Business continuity planning methodology. Disaster Prevention and Management, 19(2), 243–255. Available at: https://doi.org/10.1108/09653561011038039

[5] Executive Order 14028. (2021). Improving the nation's cybersecurity. Federal Register, 86(93), 26633–26648. Available at: https://www.federalregister.gov/d/2021-10460

[6] Continuity of Operations Planning. (2007). Federal preparedness circular 65: Federal executive branch continuity of operations. FEMA. Available at: https://www.fema.gov/emergency-managers/national-preparedness/continuity

[7] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).Available at: https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

[8] Cerullo, V., and Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. Information Systems Management, 21(3), 70–78. Available at: https://doi.org/10.1201/1078/44432.21.3.20040601/82473.10

[9] Wybo, J. L., and Guilhou, X. (2004). The contribution of work analysis to the management of risks. Safety Science, 42, 457–471. Available at: https://doi.org/10.1016/j.ssci.2003.10.001

[10] Whitman, M. E., and Mattord, H. J. (2012). Principles of information security (4th ed.). Course Technology. Available at: https://dl.acm.org/doi/book/10.5555/1593706

[11] Wu, T. C., Chen, C. H., and Wu, C. S. (2018). A fuzzy approach for the classification and analysis of business continuity risks. Computers and Industrial Engineering, 121, 217–226. Available at: https://doi.org/10.1016/j.cie.2018.05.030

[12] Zhang, J., and Goodson, P. (2011). Predictors of international students' psychosocial adjustment to life in the United States: A systematic review. International Journal of Intercultural Relations, 35(2), 139–162. Available at: https://doi.org/10.1016/j.ijintrel.2010.11.011

[13] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).Available at: https://www.congress.gov/bill/113th-congress/senate-bill/2521

[14] National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity (Version 1.0). NIST. Available at: https://www.nist.gov/cyberframework

[15] Landis, J. R., and Koch, G. G. (1977). The measurement of observer agreement for categorical data. Biometrics, 33(1), 159–174. Available at: https://doi.org/10.2307/2529310

[16] Anderson, R. J. (2001). Security engineering: A guide to building dependable distributed systems. Wiley. Available at: https://www.cl.cam.ac.uk/~rja14/book.html

[17] Federal Emergency Management Agency. (2017). Federal Continuity Directive 1 (FCD 1): Federal executive branch national continuity program and requirements. FEMA. Available at: https://www.fema.gov/emergency-managers/national-preparedness/continuity/federal-directives

[18] Kato, M., and Charoenrat, T. (2018). Business continuity management of small and medium-sized enterprises: Evidence from Thailand. International Journal of Disaster Risk Reduction, 27, 577–587. Available at: https://doi.org/10.1016/j.ijdrr.2017.10.002

[19] American Water Infrastructure Act (AWIA) of 2018, Pub. L. No. 115-270, 132 Stat. 3765 (2018).Available at: https://www.congress.gov/bill/115th-congress/senate-bill/3021

[20] Moher, D., Liberati, A., Tetzlaff, J., and Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Medicine, 6(7), e1000097. Available at: https://doi.org/10.1371/journal.pmed.1000097

[21] Committee on National Security Systems. (2010). National information assurance glossary (CNSS Instruction No. 4009). CNSS. Available at: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[22] NERC. (2006). CIP-009-1: Recovery plans for BES cyber systems. North American Electric Reliability Corporation. Available at: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[23] CISA. (2019). National infrastructure protection plan: Partnering for critical infrastructure security and resilience. U.S. DHS. Available at: https://www.cisa.gov/national-infrastructure-protection-plan

[24] Department of Homeland Security. (2013). National infrastructure protection plan 2013: Partnering for critical infrastructure security and resilience. DHS. Available at: https://www.cisa.gov/national-infrastructure-protection-plan

[25] DRI International. (2015). Business continuity management practices: Annual benchmarking survey 2015. DRI International. Available at: https://drii.org/resources/publications

[26] Department of Defense. (2010). DoD Directive 3020.26: Department of Defense continuity programs. U.S. Department of Defense. Available at: https://www.esd.whs.mil/Directives/issuances/dodd/

[27] National Institute of Standards and Technology. (2018). Guide for cybersecurity event recovery (NIST SP 800-184). NIST. Available at: https://doi.org/10.6028/NIST.SP.800-184

[28] Executive Order 13636. (2013). Improving critical infrastructure cybersecurity. Federal Register, 78(33), 11739–11744. Available at: https://www.federalregister.gov/d/2013-03915

[29] Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2004). The critical success factor method: Establishing a foundation for enterprise security management. Carnegie Mellon University, SEI. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6704

[30] Environmental Protection Agency. (2020). American Water Infrastructure Act (AWIA) Section 2013 guidance. EPA.Available at: https://www.epa.gov/waterresilience/awia-section-2013

[31] Tierney, K. (2014). The social roots of risk: Producing disasters, promoting resilience. Stanford University Press. Available at: https://www.sup.org/books/title/?id=22916

[32] Torabi, S. A., Giahi, R., and Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. Safety Science, 89, 201–218. Available at: https://doi.org/10.1016/j.ssci.2016.06.007

[33] Clinton, W. J. (1998). Presidential decision directive 63: Critical infrastructure protection. The White House. Available at: https://fas.org/irp/offdocs/pdd/pdd-63.htm

[34] Torabi, S. A., Soufi, H. R., and Sahebjamnia, N. (2014). A new framework for business impact analysis in business continuity management. Safety Science, 68, 309–323. Available at: https://doi.org/10.1016/j.ssci.2014.04.017

[35] Garrard, J. (1999). Health sciences literature review made easy: The matrix method. Aspen. Available at: https://www.jblearning.com/catalog/productdetails/9781284105445

[36] Gallagher, S., McGahan, A., and Heller, M. (2008). Protecting water infrastructure: Business continuity and cyber threats. Journal of Homeland Security, 4(2), 1–18. Available at: https://www.hsaj.org/articles/148

[37] CISA. (2021). Colonial Pipeline cyber incident — Alert (AA21-131A). CISA. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

[38] Federal Financial Institutions Examination Council (FFIEC). (2019). Business continuity management IT examination handbook. FFIEC. Available at: https://ithandbook.ffiec.gov/it-booklets/business-continuity-management.aspx

[39] Atkinson, S. R., and Moffat, J. (2005). The agile organization: From informal networks to complex effects and agility. CCRP Publication Series. Available at: https://apps.dtic.mil/sti/pdfs/ADA434086.pdf

[40] U.S. Government Accountability Office. (2019). Critical infrastructure protection: Actions needed to address significant cybersecurity risks facing the electric grid (GAO-19-332). GAO. Available at: https://www.gao.gov/products/gao-19-332

[41] Bozarth, C. C., and Handfield, R. B. (2016). Introduction to operations and supply chain management (4th ed.). Pearson. Available at: https://www.pearson.com/en-us/subject-catalog/p/introduction-to-operations-and-supply-chain-management/P200000005939

[42] Transportation Security Administration. (2021). Cybersecurity requirements for critical pipeline owners and operators. TSA. Available at: https://www.tsa.gov/aviation/cybersecurity

[43] National Institute of Standards and Technology. (2010). Contingency planning guide for federal information systems (NIST SP 800-34 Rev. 1). NIST. Available at: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

[44] United Nations Office for Disaster Risk Reduction. (2015). Sendai framework for disaster risk reduction 2015–2030. UNDRR. Available at: https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030

[45] Young, L. R. (1998). Information security: An integrated collection of essays. IEEE Computer Society Press. Available at: https://ieeexplore.ieee.org/book/5263406

[46] Ponemon Institute. (2020). The cost of data center outages: 2020 survey. Ponemon Institute. Available at: https://www.vertiv.com/globalassets/documents/reports/2020-ponemon-data-center-outage.pdf

[47] National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). NIST. Available at: https://doi.org/10.6028/NIST.CSWP.04162018

[48] Homeland Security Presidential Directive 7 (HSPD-7). (2004). Critical infrastructure identification, prioritization, and protection. The White House.Available at: https://www.dhs.gov/homeland-security-presidential-directive-7

[49] Sheffi, Y., and Rice, J. B. (2005). A supply chain view of the resilient enterprise. MIT Sloan Management Review, 47(1), 41–48. Available at: https://sloanreview.mit.edu/article/a-supply-chain-view-of-the-resilient-enterprise/

[50] Federal Communications Commission. (2012). 47 C.F.R. Part 4: Disruptions to communications. FCC.Available at: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-4

[51] ISO. (2019). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. International Organization for Standardization. Available at: https://www.iso.org/standard/75106.html

[52] Sahebjamnia, N., Torabi, S. A., and Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. European Journal of Operational Research, 242(1), 261–273. Available at: https://doi.org/10.1016/j.ejor.2014.09.055