

BEYOND BUSINESS CONTINUITY: RETHINKING CRISIS AND OPERATIONAL RESILIENCE IN THE DIGITAL ERA

Phuah Chin Hong¹; Akram Abdulraqueeb Sultan Al-Khaled²

Department for People and Organisations, Glasgow School for Business and Society,
Glasgow Caledonian University, Glasgow, UK, in collaboration with IEG Campus,
Malaysia¹; Faculty of Business and Hospitality, Spectrum International University College,
Malaysia².

p.chinhong@student.iegcampus.com¹; akram@siuc.edu.my²

ABSTRACT

Digital transformation has altered the velocity, interdependence, and boundary spanning character of organisational disruption. Contemporary organisations depend on cloud services, automated decision systems, software supply chains, and third-party technology providers, creating conditions in which failures can propagate rapidly across organisational and sectoral boundaries. This conceptual paper synthesises business continuity management (BCM), crisis management, organisational resilience, and digital resilience literature to evaluate the complementary contributions of ISO 22301:2019, NIST SP 800-34 Rev. 1, and COBIT 2019. Five documented disruptions, Maersk/NotPetya, the 2024 CrowdStrike outage, British Airways' 2017 IT disruption, TSB's 2018 migration incident, and Knight Capital's 2012 trading failure, are used as illustrative secondary cases rather than as a formal empirical case study dataset. The synthesis distinguishes framework scope limitations from implementation shortcomings and proposes four conceptual propositions. Its principal contribution is a Five-Layer Operational Resilience Model integrating: (1) governance and accountability; (2) continuity management; (3) technical recovery; (4) crisis leadership and communication; and (5) organisational learning and adaptive resilience. The layers operate recursively, with learning feeding back into governance, continuity assumptions, technical controls, and leadership practice. The paper also extends the model to educational institutions, where continuity of teaching, assessment, research, student services, and institutional communication increasingly depends on learning-management systems, student information systems, cloud and EdTech providers, cybersecurity, and AI enabled services. The analysis suggests that established frameworks provide essential structural foundations but require complementary adaptive, communicative, learning, and ecosystem-governance capabilities. The model is offered for future empirical testing rather than as a validated maturity model.

Keywords: *Operational Resilience; Business Continuity Management; Crisis Management; Digital Resilience; Organisational Resilience; Educational Institutions; ISO 22301; Crisis Communication.*

INTRODUCTION

Digital transformation has fundamentally altered the nature of organisational risk. Cloud computing, artificial intelligence (AI), algorithmically driven processes, platform-based supply chains, and outsourced technology services can increase efficiency while also concentrating dependencies. Disruptions may therefore propagate across organisational boundaries at a speed and scale that challenge assumptions embedded in conventional continuity planning (Pescaroli & Alexander, 2018). The 2017 NotPetya cyberattack caused severe global disruption, while the July 2024 CrowdStrike outage affected approximately 8.5 million Windows devices worldwide (Greenberg, 2018; Microsoft, 2024). These incidents illustrate why resilience increasingly concerns not only recovery of internal assets but continuity of important services within complex digital ecosystems.

Business Continuity Management (BCM) remains an important foundation for identifying disruption impacts, establishing recovery priorities, and preparing continuity arrangements (Niemimaa, 2015). Crisis management addresses a related but distinct problem: how leaders interpret ambiguous events, make decisions under pressure, coordinate people, and communicate with stakeholders when planned assumptions become unreliable (Bundy et al., 2017). Operational resilience extends the focus from restoring assets toward sustaining important services through disruption and adapting where necessary (Bank of England, 2021; Basel Committee on Banking Supervision [BCBS], 2021).

This paper argues that the central challenge is not choosing one resilience framework over another. ISO 22301:2019, NIST SP 800-34 Rev. 1, and COBIT 2019 have different intended scopes and provide complementary forms of discipline. The conceptual problem is how these structural capabilities connect with crisis leadership, sensemaking, communication, collective mindfulness, and organisational learning. The paper therefore develops a Five Layer Operational Resilience Model and asks three questions: (1) what do the three established frameworks explicitly contribute to contemporary operational resilience; (2) what complementary capabilities become visible when major digital disruptions are examined through crisis management and organisational resilience theory; and (3) how can these insights be translated to educational institutions whose core activities increasingly depend on digital ecosystems?

CONCEPTUAL APPROACH AND ANALYTICAL METHOD

The manuscript is explicitly positioned as a conceptual synthesis. It integrates literature and established frameworks to develop a more coherent explanatory architecture rather than testing hypotheses with a primary empirical dataset. The analysis combines four bodies of knowledge: BCM and operational resilience; IT contingency planning and governance; crisis management and communication; and organisational resilience, sensemaking, and learning. This approach is appropriate because the theoretical contribution concerns relationships among capabilities that are dispersed across separate literatures.

The analysis proceeds in four stages. First, the principal constructs are differentiated, and the theoretical perspectives are mapped to specific resilience functions. Second, ISO 22301:2019, NIST SP 800-34 Rev. 1, and COBIT 2019 are compared according to their stated

scope and explicit coverage of governance, continuity, technical recovery, communication, human factors, emerging technology, and third-party dependencies. Third, five disruption cases are used illustratively to examine whether the conceptual gaps identified in the literature are practically meaningful. Fourth, the synthesis is consolidated into the Five-Layer Model and translated to educational institutions.

The five cases were selected purposively because they represent distinct disruption mechanisms and sectors: destructive cyberattack (Maersk), shared third party software failure (CrowdStrike), infrastructure/IT service disruption (British Airways), complex technology migration (TSB), and automated trading malfunction (Knight Capital). Their diversity is useful for conceptual comparison, but they are not treated as a statistically representative sample or as a formally coded multiple case study. Documentary and regulatory sources establish incident facts; the application of resilience frameworks is the authors' analytical interpretation unless formal adoption is documented. Consequently, the paper avoids labelling incidents as an "ISO failure," "NIST failure," or "COBIT failure" without evidence that the organisation formally implemented the relevant framework.

ISO 22301:2019 remains the edition examined because it is the published standard against which the cases and much of the literature considered here developed, and it remains an important reference point for certified BCM practice. A subsequent edition has been under development. The analysis should therefore be read as an assessment of the 2019 edition and its relationship with complementary capabilities, not as a prediction about the content of a future revision.

CONSTRUCT DEFINITIONS AND THEORETICAL INTEGRATION

BCM is defined here as the structured organisational process for identifying disruption impacts, determining continuity priorities, establishing response and recovery arrangements, exercising them, and improving the management system (ISO, 2019; Niemimaa, 2015). Crisis management concerns preparation for and management of events that threaten organisational objectives, legitimacy, stakeholders, or survival and that demand exceptional sensemaking, decision making, coordination, and communication (Bundy et al., 2017). Operational resilience refers to the capability to continue delivering important services within tolerable levels of disruption and to adapt when circumstances exceed expected conditions (Bank of England, 2021; BCBS, 2021). Organisational resilience is broader: the capability to anticipate, cope with, adapt to, and learn from adversity across strategic, behavioural, and operational domains (Duchek, 2020; Hillmann & Guenther, 2021). Digital resilience refers specifically to maintaining and adapting digitally enabled activities amid cyber, technology, data, platform, automation, and digital-supply-chain disruption.

The term Crisis and Operational Resilience (COR) is used in this paper as the authors' integrative conceptual terminology rather than as a universally established discipline. It denotes the combined governance, continuity, technical, leadership, communication, and learning capabilities needed to anticipate, absorb, respond to, recover from, and adapt to severe disruption.

The theoretical perspectives used in the paper perform different functions. Fink's (1986) crisis lifecycle emphasises the prodromal phase and the possibility of recognising warning signals before escalation. Mitroff (2004) connects signal detection, prevention, containment, recovery, and learning. Sensemaking explains how people construct workable interpretations when familiar cues and routines become unreliable (Maitlis & Christianson, 2014; Weick, 1993). High Reliability Organisation (HRO) theory contributes preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience, and deference to expertise (Weick & Sutcliffe, 2015). Situational Crisis Communication Theory (SCCT) contributes a stakeholder centred logic for selecting communication responses according to perceived responsibility and stakeholder expectations (Coombs & Laufer, 2018). Duchek's (2020) capability perspective links anticipation, coping, and adaptation, while Edmondson (2019) explains how psychological safety can support learning and the reporting of weak signals.

Four conceptual propositions follow from this synthesis. Proposition 1: operational resilience is strengthened when governance, continuity management, technical recovery, crisis leadership and communication, and organisational learning are treated as interdependent capabilities rather than independent programmes. Proposition 2: the value of formal BCM and IT governance frameworks depends partly on complementary adaptive capabilities, especially sensemaking, distributed expertise, communication, and the capacity to improvise within clear decision boundaries. Proposition 3: dependence on shared digital providers shifts part of the relevant unit of resilience from individual organisation to the wider technology ecosystem. Proposition 4: organisational learning is recursive: incidents, exercises, and near misses should reshape governance priorities, continuity assumptions, technical controls, and leadership routines.

BUSINESS CONTINUITY MANAGEMENT IN THE DIGITAL ENVIRONMENT

The core BCM principles of business impact analysis (BIA), risk assessment, recovery planning, governance, exercising, and continual improvement remain conceptually important. Digitalisation, however, changes the dependencies that these practices must capture. A service may rely simultaneously on cloud infrastructure, identity services, telecommunications, endpoint software, data platforms, payment services, and outsourced support. Conventional asset centred or linear process maps may therefore understate concentration risk and cascading dependencies (Aven, 2016; Ivanov, 2021; Pescaroli & Alexander, 2018).

Hopkin's (2022) risk management perspective emphasises that risk arrangements should be dynamic rather than static. Linkov and Trump (2019) similarly conceptualise resilience through capacities to absorb, adapt, recover, and anticipate. These ideas extend BCM without displacing it: BIA remains useful, but its unit of analysis increasingly needs to be the important service and its end-to-end ecosystem. Recovery planning remains useful, but it may need to incorporate manual fallback, safe rollback, alternate communication channels, provider failure, and conditions in which automated recovery is unavailable.

The distinction between documented preparedness and demonstrated capability is equally important. Plans can provide cognitive scaffolding and role clarity, but their value depends on realistic exercise, organisational awareness, leadership commitment, and learning.

COVID-19 research showed that organisations often faced disruptions longer and more systemic than conventional scenarios assumed (Bryce et al., 2020). The appropriate conclusion is not that BCM is obsolete, but that contemporary BCM needs to be connected more explicitly to adaptive and ecosystem level capabilities.

Table 1: Business Continuity Management Principles and Digital Era Extensions

BCM principle	Traditional emphasis	Digital-era extension
Business impact analysis	Internal assets, services and processes	End to end digital services; cloud, identity, data and third-party dependencies; concentration risk.
Risk assessment	Identifiable and bounded threats	Cascading, systemic, software supply chain, algorithmic and deep uncertainty scenarios.
Recovery planning	Restoration of systems/facilities	Manual fallback, safe rollback, alternate communications, vendor failure and ecosystem coordination.
Governance/preparedness	Internal ownership and leadership	Executive decision rights plus contractual and third-party resilience accountability.
Continual improvement	Periodic plan review	Exercises, near misses, weak signals and incidents reshape controls, assumptions and culture.

Note: Developed by the authors from the conceptual synthesis of ISO 22301:2019, Niemimaa (2015), Aven (2016), Pescaroli and Alexander (2018), Ivanov (2021), and Hopkin (2022). The digital era extensions reflect the authors' synthesis of how established BCM principles can be adapted to interconnected digital services, third party dependencies, cascading risks, ecosystem coordination, and organisational learning.

CRITICAL EVALUATION OF BCM AND IT-GOVERNANCE FRAMEWORKS

The three frameworks examined operate at different levels. ISO 22301:2019 specifies requirements for a business continuity management system (BCMS) and therefore provides the broadest organisation wide continuity structure. Its Plan–Do–Check–Act logic supports governance, BIA, continuity strategies, exercising, evaluation, and improvement. Its strength lies in scalable management system discipline and the possibility of external certification. Its limitation for the present argument is not that it “fails” to address every digital risk, but that detailed crisis communication strategy, AI specific failure modes, and ecosystem governance require complementary guidance and organisational capabilities.

NIST SP 800-34 Rev. 1 is narrower by design. It provides detailed contingency planning guidance for federal information systems, including BIA, recovery strategies, plan development, testing, training, and maintenance (NIST, 2010). It should not be conflated with the NIST Cybersecurity Framework (CSF) 2.0. The two separate publications from different periods. Organisations may use them together, but this is an organisational integration across NIST resources rather than a single formally integrated framework. NIST CSF 2.0 provides a broader cybersecurity risk management taxonomy, including the Govern function, while SP 800-34 remains focused on information system contingency planning (NIST, 2010, 2024).

COBIT 2019 operates primarily as an enterprise governance and management framework for information and technology. It contributes strategic alignment, accountability, performance management, and continuity-related governance through objectives such as DSS04 Manage Continuity (ISACA, 2018). Its governance orientation is valuable, but detailed crisis execution and technical recovery normally require complementary standards and procedures. The three frameworks should therefore be understood as overlapping but non-equivalent components of a resilience architecture.

Table 2: Comparison of ISO 22301:2019, NIST SP 800-34 Rev. 1, and COBIT 2019

Criterion	ISO 22301:2019	NIST SP 800-34 Rev. 1	COBIT 2019
Primary scope	Organisation-wide BCMS requirements	Information-system contingency planning	Enterprise governance/management of information and technology
Governance coverage	Strong management system governance	Limited relative to enterprise governance frameworks	Strong strategic governance/accountability
Technical recovery depth	Moderate	High within system contingency scope	Moderate; complementary detail normally required
Crisis communication	Limited explicit strategic guidance	Not a principal focus	Not a principal focus
Explicit AI specific guidance	Not explicit in 2019 edition	Not explicit	Limited in core 2019 framework
Human/cultural factors	Leadership, competence and awareness addressed; limited crisis leadership depth	Limited	People/skills considered; limited crisis leadership depth
Third party/ecosystem risk	Can be incorporated; limited ecosystem specific detail	Can address external dependencies at system level	Governance mechanisms relevant; operational detail requires supplementation
Principal contribution	BCMS discipline and assurance	Detailed contingency planning logic	Strategic alignment and accountability
Complementary capability needed	Crisis leadership/communication, ecosystem and emerging technology depth	Enterprise governance, non-IT continuity, crisis leadership/communication	Detailed continuity/recovery design and crisis execution

Note: Developed by the authors from International Organization for Standardization (2019), National Institute of Standards and Technology (2010, 2024), and ISACA (2018). The comparison reflects the published scope and explicit coverage of the frameworks rather than a claim that any framework is universally deficient or was formally implemented in illustrative cases.

This comparison produces a more measured conclusion than a simple gap analysis. Apparent absences often reflect intended scope. Nevertheless, when organisations depend on the three frameworks as part of a broader resilience architecture, crisis communication, adaptive leadership, learning, shared provider concentration, and emerging automated-system risks deserve explicit complementary treatment.

CRISIS MANAGEMENT, COMMUNICATION, AND THE HUMAN DIMENSION

Crisis management becomes particularly important when disruption exceeds assumptions embedded in continuity plans. Bundy et al. (2017) emphasise that crises involve both operational disruption and stakeholder interpretation. Maitlis and Christianson (2014) show that sensemaking is especially important when events are ambiguous and action cannot wait for complete information. These perspectives explain why technically sound recovery procedures may still be insufficient if decision rights are unclear, expertise is ignored, or leaders cannot develop a shared understanding of rapidly changing conditions.

HRO theory reinforces this argument. Preoccupation with failure encourages attention to anomalies before they become major events; sensitivity to operations keeps decisionmakers connected to frontline conditions; and deference to expertise allows authority to migrate toward those with the most relevant knowledge (Weick & Sutcliffe, 2015). These principles are particularly relevant to digitally mediated crises because technical signals may emerge first among engineers, security analysts, vendors, lecturers, administrators, or operational staff rather than senior executives.

Crisis communication is another complementary capability. SCCT is not a compliance standard, and organisations should not be described as “SCCT compliant.” Rather, SCCT provides theoretical expectations concerning responsibility attribution and appropriate communication responses (Coombs & Laufer, 2018). Digital media further increase expectations for rapid, accurate, and transparent updates (Veil et al., 2011). Communication therefore needs to be exercised alongside technical recovery, with designated responsibilities, stakeholder mapping, accessible channels, and processes for updating messages as facts change.

ILLUSTRATIVE CASES OF DIGITAL DISRUPTION

The five cases below are used to illuminate the conceptual argument. They do not establish causal effects of standards and do not assume formal framework adoption unless documented. Each case separates reported incident characteristics from the analytical resilience questions raised by the event.

Maersk and NotPetya (2017)

NotPetya caused extensive disruption across Maersk’s global technology environment. Contemporary reporting described the destruction or disabling of large numbers of endpoints and servers and estimated losses of approximately US\$250–300 million (Greenberg, 2018). The scale of the incident illustrates the difficulty of relying on recovery assumptions designed for localised or partial failures. It also illustrates the importance of manual workarounds and decentralised problem solving when digital systems are widely unavailable.

Through the Five-Layer lens, Maersk raises questions about continuity dependency mapping (Layer 2), recoverability under widespread technical failure (Layer 3), distributed coordination and stakeholder communication (Layer 4), and the conversion of crisis experience into redesigned controls (Layer 5). Public communication during the disruption can be

described as broadly consistent with principles of transparency, but the available evidence does not justify claiming that communication alone produced a superior reputational outcome or formally coding the organisation against SCCT.

CrowdStrike Global Outage (2024)

A faulty CrowdStrike Falcon content update in July 2024 affected approximately 8.5 million Windows devices, according to Microsoft (2024). The outage disrupted organisations across sectors and geographies. The event is analytically important because a common technology provider created correlated disruption among otherwise separate organisations, demonstrating how shared digital dependencies can turn a provider level fault into a cross sector operational event.

The case suggests that BIA and continuity strategies should include shared provider concentration, mass endpoint remediation, deployment safeguards, alternate operating arrangements, and vendor failure scenarios. It also supports Proposition 3: resilience cannot always be analysed solely at the individual-organisation level. Contractual controls, staged release practices, provider recovery arrangements, communication, and cross organisational coordination form part of ecosystem resilience. This observation identifies capabilities requiring attention; it does not establish that ISO, NIST, or COBIT formally failed in affected organisations.

British Airways IT Disruption (2017)

British Airways experienced a major IT disruption in May 2017 that led to extensive flight cancellations and passenger disruption. IAG's 2017 annual reporting identified a material financial impact from the incident (International Airlines Group [IAG], 2017). The case illustrates the importance of critical dependency analysis, alternate processing, operational workarounds, and timely customer communication during service disruption.

The earlier manuscript compared British Airways with Maersk too conclusively. The cases differ in cause, operating context, stakeholders, duration, and available evidence, so they cannot establish that communication caused one organisation to experience a better reputational outcome. A more defensible interpretation is that both cases illustrate the dual nature of resilience: technical restoration and stakeholder communication proceed in parallel. This is consistent with Bundy et al. (2017) and SCCT informed research, which indicate that stakeholder perceptions are influenced by timeliness, accuracy, empathy, and consistency of organisational communication.

TSB Bank Migration Incident (2018)

TSB's 2018 IT migration caused widespread disruption to customer banking services. In 2022, the FCA and PRA imposed a £48.65 million fine for operational risk management and governance failings associated with the migration and subsequent disruption (Financial Conduct Authority [FCA], 2022). Unlike speculative attribution to a particular framework, this

regulatory evidence directly supports the conclusion that governance and operational risk management weaknesses were significant.

The TSB case illustrates the distinction between formal governance and effective execution. Governance structures have limited resilience value if testing is insufficiently challenging, escalation is ineffective, operational information is inaccurate, or senior decisionmakers lack a realistic understanding of service conditions. The case also demonstrates the importance of communication that remains consistent with customer experience. Through the proposed model, TSB therefore connects Layers 1–4 and demonstrates why governance, continuity, technical execution, and communication should not be managed as independent silos.

Knight Capital Algorithmic Trading Failure (2012)

Knight Capital’s 2012 trading incident is particularly relevant to machine speed digital risk. According to the Securities and Exchange Commission (SEC, 2013), a defective software deployment caused millions of erroneous orders and losses exceeding US\$460 million in approximately 45 minutes. Importantly, the SEC also documented warning messages and controlled weaknesses that were not adequately acted upon. The incident should therefore not be interpreted simply as a failure occurring too quickly for human intervention.

Instead, Knight Capital illustrates interaction among automation, deployment governance, monitoring, weak signals, escalation, and human decision making. Machine-speed propagation can compress the acute phase of a crisis, but technical safeguards, deployment controls, kill mechanisms, and meaningful alerts can create opportunities for prevention or containment. This strengthens the paper’s theoretical integration: Fink’s weak signal logic, HRO preoccupation with failure, sensemaking, and technical recovery controls all become relevant. The central resilience question is whether organisations can detect anomalous behaviour, interpret signals correctly, and empower timely intervention before automated processes amplify harm.

Table 3: Illustrative Digital Disruptions and Resilience Questions

Case	Documented disruption	Analytical resilience questions	Observed organisational response / lesson
Maersk / NotPetya	Destructive cyber disruption across global IT	Widespread recoverability; manual fallback; distributed coordination	Illustrates improvisation and learning under extreme technical disruption.
CrowdStrike 2024	Shared update affected ~8.5m Windows devices	Provider concentration; correlated failure; recovery at scale	Highlights ecosystem dependency, staged change and provider and customer coordination.
British Airways 2017	Major IT disruption and extensive cancellations	Critical dependencies; alternate processing; customer communication	Shows technical restoration and stakeholder communication as parallel tasks.

TSB 2018	Migration disruption; later regulatory enforcement	Governance-to-execution gap; testing; escalation; communication	Regulatory findings support significant operational risk and governance weaknesses.
Knight Capital 2012	Defective deployment; >US\$460m loss in ~45 minutes	Warnings; algorithmic safeguards; kill mechanisms; escalation	Shows interaction between machine speed propagation and human/organisational controls.

Note: Developed by the authors from Greenberg (2018), Microsoft (2024), International Airlines Group (2017), Financial Conduct Authority (2022), and Securities and Exchange Commission (2013), interpreted through conceptual resilience literature. The cases are illustrative secondary cases and do not constitute a formally coded empirical case study.

CRITICAL SYNTHESIS: THE FIVE-LAYER OPERATIONAL RESILIENCE MODEL

The illustrative cases and theoretical literature converge on a common point: resilience cannot be reduced to recovery documentation or technical restoration. At the same time, it would be equally misleading to dismiss formal frameworks as merely procedural. Duchek (2020) argues that structured preparation and adaptive capacity can be complementary, while Weick (1993) demonstrates how identity, role clarity, and sensemaking influence action when established routines collapse. The conceptual synthesis therefore treats formal structure as the foundation on which adaptive capabilities operate.

The Five-Layer Operational Resilience Model is the paper's principal contribution. It integrates capabilities that are often governed separately and clarifies the mechanisms connecting them. Layer 1, Governance and Accountability, defines priorities, ownership, tolerances, decision rights, and resource commitments. Layer 2, Continuity Management, translates these priorities into BIA, dependency mapping, strategies, exercises, and workable fallback arrangements. Layer 3, Technical Recovery, supplies prevention, containment, restoration, rollback, monitoring, and cyber-recovery mechanisms. Layer 4, Crisis Leadership and Communication, provides sensemaking, distributed expertise, adaptive decision making, coordination, and stakeholder communication. Layer 5, Organisational Learning and Adaptive Resilience, converts incidents, exercises, near misses, and weak signals into changes in assumptions, culture, governance, controls, and future capability.

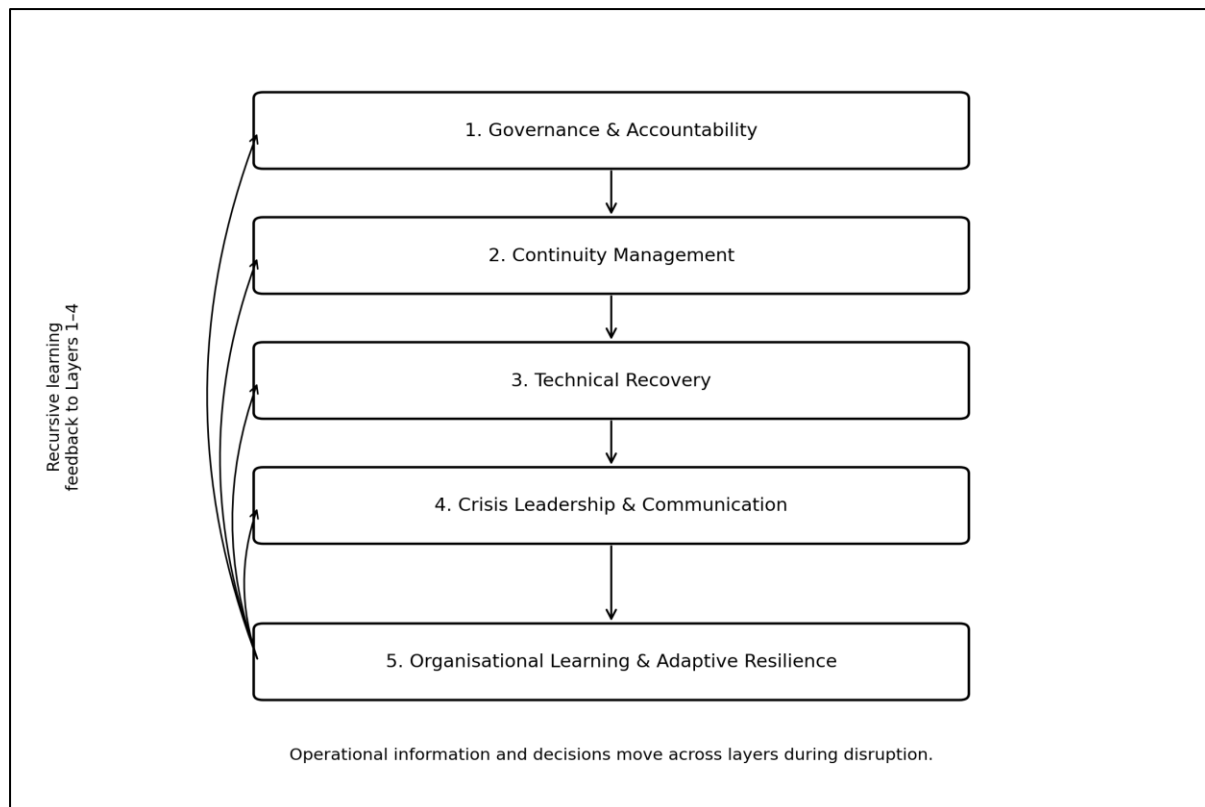
Table 4: Five-Layer Operational Resilience Model: Capabilities, Foundations, and Coverage Gaps

Layer	Focus	Capabilities / mechanisms	Theoretical / practice foundations	Typical coverage gap
1. Governance & Accountability	Priorities, ownership, tolerance, decision rights	Executive oversight; accountability; third party governance; resource allocation	COBIT 2019; BCBS (2021); Bank of England (2021)	Formal governance may not translate into exercised operational capability.
2. Continuity Management	Important services and continuity arrangements	BIA; dependency mapping; strategies; exercises; manual fallback	ISO 22301; BCM literature	Static/internal assumptions may miss fast changing ecosystem dependencies.
3. Technical Recovery	Prevent, contain, restore, rollback or safely degrade	Backups; alternate processing; monitoring; cyber recovery; staged deployment; kill mechanisms	NIST SP 800-34; NIST CSF; resilience engineering	Technical recovery alone does not resolve leadership, communication or ecosystem coordination.
4. Crisis Leadership & Communication	Shared meaning, decisions and stakeholder coordination	Sensemaking; deference to expertise; distributed authority; spokespersons; stakeholder monitoring	Bundy et al. (2017); Coombs & Laufer (2018); Maitlis & Christianson (2014); Weick & Sutcliffe (2015)	Limited explicit strategic treatment in conventional continuity/contingency frameworks.
5. Organisational Learning & Adaptive Resilience	Renew capability after incidents, exercises and near misses	After-action review; psychological safety; weak signal review; assumption testing; capability renewal	Duchek (2020); Edmondson (2019); Mitroff (2004)	Learning may be reduced to procedural correction rather than deeper adaptation.

Note: Developed by the authors from the conceptual synthesis. The five layers are interdependent rather than sequential. Layer 5, Organisational Learning and Adaptive Resilience, provides recursive feedback to Layers 1–4 by translating lessons from incidents, exercises, near misses, and weak signals into changes in governance priorities, continuity assumptions, technical controls, leadership practices, and crisis communication. Operational information and decisions also move across adjacent layers during disruption.

The model is recursive rather than linear. Layer 5 feeds back into Layer 1 by changing priorities, accountability, risk tolerances, and investment; into Layer 2 by revising BIA assumptions, scenarios, dependency maps, and continuity strategies; into Layer 3 by strengthening technical controls, observability, rollback, and recovery architecture; and into Layer 4 by improving leadership routines, escalation, communication, and decision rights. Information also moves upward during disruption: technical telemetry and frontline observations from Layer 3 inform Layer 4 sensemaking; Layer 4 decisions activate or modify Layer 2 continuity arrangements; and material trade-offs are escalated to Layer 1. Conversely,

weaknesses in an earlier layer increase demands on later layers. Incomplete dependency mapping, for example, may create greater need for improvisation, while weak technical safeguards can transform a manageable anomaly into a leadership crisis. Resilience therefore emerges from interaction among the layers rather than from the maturity of any single component. Figure 1 makes these forward linkages and recursive learning loops explicit.



Note: Developed by the authors from the conceptual synthesis. Layer 5 provides recursive feedback to Layers 1–4, while operational information and decisions move across layers during disruption.

Figure 1: Five-Layer Operational Resilience Model

This recursive logic also clarifies the four propositions. Proposition 1 concerns cross-layer integration. Proposition 2 explains why procedural frameworks require adaptive human capabilities. Proposition 3 extends governance and continuity beyond organisational boundaries to shared digital ecosystems. Proposition 4 identifies learning as the feedback mechanism through which the entire architecture evolves. These propositions provide a basis for empirical testing. Operationally, the model can therefore be examined through observable mechanisms: governance ownership and tolerances (Layer 1), tested dependency maps and fallback arrangements (Layer 2), recovery and rollback performance (Layer 3), escalation and stakeholder communication effectiveness (Layer 4), and evidence that lessons alter controls and assumptions (Layer 5). These mechanisms provide an initial basis for future construct development and empirical validation.

IMPLICATIONS FOR EDUCATIONAL INSTITUTIONS

The educational relevance of operational resilience has increased as schools, colleges, and universities have digitised teaching, assessment, administration, research, and student support. Educational institutions commonly depend on learning-management systems (LMS), student information systems (SIS), identity and access services, cloud productivity suites, video platforms, digital libraries, payment systems, research infrastructure, managed security providers, and third party EdTech. Recent research treats cybersecurity in higher education as an institutional and policy challenge rather than a narrowly technical problem and highlights the importance of cyber resilience, awareness, and maturity capabilities (Fouad, 2021; Brezavšek & Baggia, 2025; Chaudhuri & Shoemaker, 2025).

The continuity objective in education is therefore not simply to “restore IT.” An LMS outage during examinations can interrupt assessment; identity-provider failure can block access to multiple services simultaneously; ransomware can affect student records and communications; a cloud or telecommunications outage can prevent remote teaching; and compromised AI enabled services can create integrity, privacy, or decision-quality risks. Educational resilience must consequently be expressed in service terms: continuity of teaching and learning, assessment integrity, research continuity, student welfare, administrative services, and credible institutional communication.

The Five-Layer Model provides practical translation. Governance should identify important educational services, assign ownership, and define tolerable disruption in terms meaningful to students, faculty, administrators, regulators, and partners. Continuity management should map end to end dependencies for teaching, assessment, enrolment, research, and student support. Technical recovery should include secure backups, alternate authentication, learning-content recovery, offline or alternative teaching arrangements, safe software rollback, and tested restoration of student data. Crisis leadership and communication should establish decision rights and accessible channels for students, parents where relevant, staff, regulators, and providers. Organisational learning should convert outages, cyber incidents, exercises, and near misses into changes in pedagogy, architecture, procurement, training, and governance.

AI enabled education creates a further resilience dimension. Generative AI, automated assessment, predictive analytics, and adaptive learning may introduce model, data, availability, integrity, privacy, and third-party dependency risks. The NIST AI Risk Management Framework emphasises governance, mapping, measurement, and management of AI risk across the system lifecycle (NIST, 2023). This does not mean ISO 22301 or NIST contingency guidance has “failed” because it lacks detailed AI prescriptions. Rather, institutions need complementary AI governance and technical controls within Layers 1–3, combined with human oversight, escalation, communication, and learning in Layers 4–5.

Table 5: Application of the Five-Layer Operational Resilience Model to Educational Institutions

Layer	Schools	Universities	Educational ecosystem implication
1. Governance & Accountability	Protect teaching, safeguarding and student/parent services	Define important teaching, research, administration and student support services	Clarify accountability across institutions, ministries, cloud/EdTech providers and partners.
2. Continuity Management	Alternative teaching, attendance and communication arrangements	BIA for LMS, SIS, assessment, identity, research and student services	Maps cross provider dependencies and concentration risk.
3. Technical Recovery	Backups, alternate devices/connectivity and secure restoration	Cyber recovery, alternate authentication, resilient learning/research platforms	Require recovery evidence, staged changes, rollback and interoperable alternatives.
4. Crisis Leadership & Communication	Rapid staff coordination and clear student/parent messages	Distributed decision rights; faculty/student/media/regulator communication	Coordinate incident language, escalation and multiparty communication.
5. Learning & Adaptive Resilience	Embed lessons in drills and staff development	Revise architecture, pedagogy, procurement and training after exercises/incidents	Share lessons and threat intelligence across institutions and sector bodies.

***Note:** Developed by the authors from the Five-Layer Operational Resilience Model and the educational resilience discussion, informed by Chaudhuri and Shoemaker (2025) and relevant continuity, cybersecurity, and resilience literature cited in the manuscript. The applications are conceptual examples for schools, universities, and wider educational ecosystems rather than empirically validated prescriptions.*

DISCUSSION AND SYNTHESIS

The synthesis suggests that operational resilience is best understood as a living organisational capability rather than a static compliance state. ISO 22301 provides management system discipline; NIST SP 800-34 provides detailed information system contingency guidance; and COBIT contributes enterprise governance and accountability. Their differing scopes explain why no single framework explicitly supplies every capability required during complex digital disruption. The practical challenge is integration. Recent cyber resilience maturity research likewise supports moving beyond isolated controls toward integrated organisational capabilities and adaptive assessment (Brezavšek & Baggia, 2025).

The five illustrative cases reinforce different parts of this synthesis. CrowdStrike highlights ecosystem concentration and correlated provider failure; Knight Capital demonstrates the interaction between automated propagation, warning signals, escalation, and human judgement; TSB shows how formal governance and operational execution can diverge; British Airways highlights the parallel requirements of continuity and stakeholder communication; and Maersk illustrates adaptive action under widespread technical disruption. These cases do not demonstrate universal inadequacy of any individual framework. Rather, they illustrate why structural and adaptive capabilities need to operate together.

The Five-Layer Operational Resilience Model provides integrative architecture for these observations. Governance establishes priorities, ownership, tolerances, and decision rights. Continuity management converts those priorities into dependency maps, strategies, exercises, and fallback arrangements. Technical recovery provides prevention, containment, restoration, rollback, and observability. Crisis leadership and communication enable sensemaking, coordination, distributed expertise, and stakeholder engagement. Organisational learning and adaptive resilience convert incidents, exercises, near misses, and weak signals into changes across the other four layers.

The model is therefore recursive rather than sequential. During disruption, operational information moves across layers such as technical telemetry and frontline observations inform crisis sensemaking, leadership decisions activate or modify continuity arrangements, and material tradeoffs are escalated to governance. After disruption, learning feeds back into governance priorities, continuity assumptions, technical controls, leadership routines, and communication practice. Resilience emerges from the interaction of these capabilities rather than from the maturity of any single layer.

IMPLICATIONS

The model has practical implications for organisations and educational institutions. Governance should be supported by operational evidence from severe but plausible exercises, dependency mapping, incidents, near misses, and service performance rather than relying solely on plan completion or audit status. Continuity management should organise analysis around important services and map critical technology, identity, cloud, data, telecommunications, and provider dependencies. Technical resilience should include staged deployment, safe rollback, monitoring, automated safeguards, and kill mechanisms where rapid automated processes can amplify error.

For educational institutions, the relevant service outcomes include continuity of teaching and learning, assessment integrity, research continuity, student welfare, administrative services, and credible institutional communication. Exercises should therefore be designed around service disruption scenarios such as loss of an LMS during assessment, identity provider failure, ransomware affecting student services, cloud or EdTech outages, compromised AI enabled tools, or misinformation during a campus crisis. The objective is to test both technical restoration and the institution's capacity to sustain important educational services.

CONCLUSION

This paper reframes business continuity in the digital era as an integrative resilience problem. ISO 22301:2019, NIST SP 800-34 Rev. 1, and COBIT 2019 provide valuable but differently scoped foundations. The illustrative cases show why contemporary disruption also raises questions of shared digital dependencies, rapid automated propagation, weak signals, sensemaking, crisis communication, and organisational learning. These observations do not demonstrate that the frameworks failed in the organisations examined; they identify where complementary capabilities are required and where implementation deserves scrutiny.

The principal conceptual contribution is the Five-Layer Operational Resilience Model, which integrates governance and accountability, continuity management, technical recovery, crisis leadership and communication, and organisational learning and adaptive resilience. Its central claim is that these capabilities are interdependent and recursive. Learning feeds back into governance, continuity assumptions, technical controls, and leadership practice, while weaknesses in one layer increase demands on the others. The four propositions derived from the synthesis provide a basis for future empirical testing.

Extending the model to educational institutions demonstrates its relevance beyond corporate settings. Continuity of teaching, assessment, research, student services, and institutional trust increasingly depends on resilient digital ecosystems. The model is therefore offered not as a replacement for established standards or as a validated maturity model, but as a conceptual architecture for connecting formal continuity and governance disciplines with the adaptive human capabilities required to sustain important services under changing conditions.

Recommendations

Five recommendations follow directly from the Five-Layer Model. First, organisations should integrate crisis leadership and communication into resilience exercises so that leaders practice interpreting ambiguous information, delegating decisions, coordinating expertise, and communicating accurately with stakeholders (Coombs & Laufer, 2018; Veil et al., 2011).

Second, organisations should strengthen third party and ecosystem resilience by mapping critical dependencies, assessing concentration risk, exercising provider failure scenarios, and incorporating resilience requirements into procurement and contracts. DORA provides a developed regulatory example of third-party ICT risk governance in financial services, while the underlying dependency logic has wider relevance (European Parliament & Council of the European Union, 2022).

Third, organisations should build adaptive decision capability. Psychological safety, collective mindfulness, and deference to expertise can support the reporting and interpretation of weak signals, while scenario exercises should test judgement and improvisation as well as adherence to plans (Duchek, 2020; Edmondson, 2019; Weick & Sutcliffe, 2015).

Fourth, business impact analysis, scenario design, change management, and technical recovery should incorporate machine speed and AI enabled risks, including rapid software deployment, algorithmic error, model or data failure, and situations in which disruption can propagate faster than conventional escalation. Preventive controls, monitoring, staged releases, rollback, and kill mechanisms should complement recovery planning.

Fifth, organisations should institutionalise recursive learning. Lessons from incidents, exercises, and near misses should alter governance priorities, continuity assumptions, technical architecture, procurement, leadership development, and communication practice. This recommendation operationalises Layer 5 and prevents continual improvement from becoming a narrow document maintenance exercise. Together, the recommendations connect the model's five layers to observable organisational practices rather than treating the model as an abstract sequence.

Limitations and Future Research

This paper has four principal limitations. First, it is conceptual and does not empirically validate the Five-Layer Operational Resilience Model. Second, the illustrative cases rely on secondary literature and publicly available organisational or regulatory documentation; the depth and quality of evidence differ among cases. Third, the framework comparison assesses published scope and explicit coverage rather than every way experienced practitioner may combine standards and sector guidance. Fourth, the five cases are concentrated in large, digitally intensive organisations and cannot be assumed to represent small organisations, schools, universities, or all regulatory jurisdictions.

Future research should operationalise the five layers into measurable constructs and test their relationships with resilience outcomes. Cross sector surveys could examine whether balanced capability across the five layers is associated with service continuity, recovery performance, stakeholder trust, or organisational learning. Longitudinal case studies could investigate how governance, technology, leadership, and learning evolve before and after disruption. Comparative studies could examine whether different sectors require different layer configurations. Resilience maturity assessments could identify observable indicators for each layer, while ecosystem studies could test whether provider concentration and inter organisational coordination explain disruption propagation.

Educational settings provide a particularly valuable research agenda. Studies could compare schools and universities in relation to continuity of teaching and assessment, LMS and SIS dependencies, cyber resilience, crisis communication, AI governance, and leadership. Research could also examine whether educational institutions that routinely exercise service-based disruption scenarios recover more effectively and maintain greater stakeholder trust than institutions whose continuity programmes remain primarily document based.

REFERENCES

- Ansell, C., Sørensen, E., & Torfing, J. (2021). The COVID-19 pandemic as a game changer for public administration and leadership? The need for robust governance responses to turbulent problems. *Public Management Review*, 23(7), 949–960.
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.
- Bank of England. (2021). *Operational resilience: Impact tolerances for important business services* (Supervisory Statement SS1/21). <https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-impact-tolerances-for-important-business-services>
- Basel Committee on Banking Supervision. (2021). Principles for operational resilience. *Bank for International Settlements*. <https://www.bis.org/bcbs/publ/d516.htm>

- Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management*, 15(1), 50–59.
- Brezavšek, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems*, 13(1), 52. <https://doi.org/10.3390/systems13010052>
- Bryce, C., Ring, P., Ashby, S., & Wardman, J. K. (2020). Resilience in the face of uncertainty: Early lessons from the COVID-19 pandemic. *Journal of Risk Research*, 23(7–8), 880–887.
- Bundy, J., Pfarrer, M. D., Short, C. E., & Coombs, W. T. (2017). Crises and crisis management: Integration, interpretation, and research development. *Journal of Management*, 43(6), 1661–1692.
- Chaudhuri, A., & Shoemaker, D. (2025). Cyber-attack on schools, steps toward resilience. *EDPACS*. <https://doi.org/10.1080/07366981.2025.2503627>
- Coombs, W. T., & Laufer, D. (2018). Global crisis management: Current research and future directions. *Journal of International Management*, 24(3), 199–203.
- De Haes, S., & Van Grembergen, W. (2020). *Enterprise governance of information technology: Achieving alignment and value in digital organizations* (3rd ed.). Springer.
- Duchek, S. (2020). Organizational resilience: A capability based conceptualization. *Business Research*, 13(1), 215–246.
- Edmondson, A. C. (2019). *The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth*. Wiley.
- European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. *Official Journal of the European Union*, L 333, 1–79.
- Financial Conduct Authority. (2021). *Building operational resilience* (Policy Statement PS21/3). <https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience>
- Financial Conduct Authority. (2022, December 20). *TSB fined £48.65m for operational resilience failings*. <https://www.fca.org.uk/news/press-releases/tsb-fined-4865m-operational-resilience-failings>
- Fink, S. (1986). *Crisis management: Planning for the inevitable*. American Management Association.

- Fouad, N. S. (2021). Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. *Journal of Cyber Policy*, 6(2), 137–154. <https://doi.org/10.1080/23738871.2021.1973526>
- Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
- Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews*, 23(1), 7–44.
- Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate.
- Hopkin, P. (2022). *Fundamentals of risk management: Understanding, evaluating and implementing effective enterprise risk management* (6th ed.). Kogan Page.
- International Airlines Group. (2017). *Annual report and accounts 2017*. <https://www.iairgroup.com/>
- International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience, Business continuity management systems, Requirements*. ISO.
- ISACA. (2018). *COBIT 2019 framework: Governance and management objectives*. ISACA.
- Ivanov, D. (2021). Supply chain viability and the COVID-19 pandemic: A conceptual and formal generalisation of four novel challenges. *International Journal of Production Research*, 59(12), 3535–3552.
- Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience*. Springer.
- Maitlis, S., & Christianson, M. (2014). Sensemaking in organizations: Taking stock and moving forward. *Academy of Management Annals*, 8(1), 57–125.
- Microsoft. (2024, July 20). *Helping our customers through the CrowdStrike outage*. <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>
- Mitroff, I. I. (2004). *Crisis leadership: Planning for the unthinkable*. Wiley.
- National Institute of Standards and Technology. (2010). *Contingency planning guide for federal information systems (Special Publication 800-34 Rev. 1)*. <https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final>
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1)*. <https://doi.org/10.6028/NIST.AI.100-1>

- National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. <https://doi.org/10.6028/NIST.CSWP.29>
- Niemimaa, M. (2015). Interdisciplinary review of business continuity from an information systems perspective: Toward an integrative framework. *Communications of the Association for Information Systems*, 37, 69–96.
- Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, 49, 208–216.
- Pescaroli, G., & Alexander, D. (2018). Understanding compound, interconnected, interacting, and cascading risks: A holistic framework. *Risk Analysis*, 38(11), 2245–2257.
- Securities and Exchange Commission. (2013, October 16). *In the matter of Knight Capital Americas LLC (Administrative Proceeding File No. 3-15570)*. <https://www.sec.gov/litigation/admin/2013/34-70694.pdf>
- Sutcliffe, K. M., Vogus, T. J., & Dane, E. (2016). Mindfulness in organizations: A cross-level review. *Annual Review of Organizational Psychology and Organizational Behavior*, 3, 55–81.
- Veil, S. R., Buehner, T., & Palenchar, M. J. (2011). A work in process literature review: Incorporating social media in risk and crisis communication. *Journal of Contingencies and Crisis Management*, 19(2), 110–122.
- Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, 38(4), 628–652.
- Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the unexpected: Sustained performance in a complex world* (3rd ed.). Wiley.

Appendix 1: Acronyms and Abbreviations

Acronym	Full term
AI	Artificial Intelligence
BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BIA	Business Impact Analysis
COBIT	Control Objectives for Information and Related Technologies
COR	Crisis and Operational Resilience (authors' integrative term)
CSF	Cybersecurity Framework
DORA	Digital Operational Resilience Act
FCA	Financial Conduct Authority
HRO	High Reliability Organisation
ICT	Information and Communications Technology
ISO	International Organization for Standardization
LMS	Learning Management System
NIST	National Institute of Standards and Technology
SCCT	Situational Crisis Communication Theory
SEC	U.S. Securities and Exchange Commission
SIS	Student Information System