



Business Continuity and Operational Resilience in Airport Infrastructures: A Process-Based Approach

Continuité d'activité et résilience opérationnelle des infrastructures aéroportuaires : une approche par les processus

Sulaiman AL RASHDI, (PhD student)

University Research Laboratory in Instrumentation and Management of Organizations

Faculty of Legal, Economic and Social Sciences

Mohammed First University Oujda, Morocco

alrashdi.sulaimansaid@ump.ac.ma

Abdelouahed BERRICHI, (PhD, Professor)

University Research Laboratory in Instrumentation and Management of Organizations

Faculty of Legal, Economic and Social Sciences

Mohammed First University Oujda, Morocco

abd.berrichi@ump.ac.ma

ABSTRACT

Airport infrastructures represent complex sociotechnical systems where business continuity management must confront hybrid operational, climatic, organizational, and cyber risks. This study examines the capacity of these organizations to align normative compliance with actual operational resilience through a process-based approach focused on the passenger journey. Epistemologically, this research adopts an action-oriented constructivist framework. The methodology relies on a mixed exploratory design: first, a conceptual modeling of the passenger journey processes; second, an expert survey was conducted with a critical sample of 13 airport managers and executives operating at platforms with annual traffic volumes ranging from 66,000 to 14.93 million passengers. The findings, derived from the aggregation of secondary descriptive closed indicators and the thematic coding of open-ended questions, highlight a disconnect between the formal existence of continuity plans (100% agreement regarding process maps and general business continuity plans) and the perceived capacity for multi-actor coordination during disruptive events. Data analysis underscores the significant burden of multi-stakeholder governance constraints (85%) and technological dependencies lacking verified manual redundancy protocols (77%). This paper contributes to the literature by establishing a processual framework for business continuity management (BCM), operationalized through a contextualized RACI matrix.

Keywords: Business Continuity Plan; Risk Management; Operational Resilience; Sociotechnical System; Critical Infrastructures; Expert Survey.



RÉSUMÉ

Les infrastructures aéroportuaires constituent des systèmes sociotechniques complexes au sein desquels la gestion de la continuité d'activité fait face à des risques hybrides opérationnels, climatiques, organisationnels et cybernétiques. Cette recherche interroge la capacité de ces organisations à articuler conformité normative et résilience opérationnelle à travers une approche par les processus, centrée sur le parcours passager. Sur le plan épistémologique, l'étude adopte un positionnement constructiviste orienté vers l'action. La méthodologie repose sur une approche exploratoire mixte : d'une part, une modélisation conceptuelle des processus du parcours passager ; d'autre part, une enquête par experts menée auprès d'un échantillon critique (n=13) de cadres et dirigeants aéroportuaires évoluant sur des plateformes gérant entre 66 000 et 14,93 millions de passagers annuels. Les résultats, issus d'une agrégation d'indicateurs descriptifs fermés et d'un codage thématique de questions ouvertes, mettent en évidence un décalage entre l'existence formelle des plans de continuité (100 % d'accord sur les cartographies de processus et les plans généraux) et la perception des capacités de coordination inter-acteurs en situation perturbée. L'analyse des données met en lumière le poids des contraintes de gouvernance multi-acteurs (85 %) et des dépendances technologiques sans redondance manuelle éprouvée (77 %). L'article contribue à la littérature en proposant un cadre processuel de gestion de la continuité d'activité (PCA), opérationnalisé par une matrice de responsabilité contextualisée.

Mots-clés : Plan de continuité d'activité (PCA) ; Gestion des risques ; Résilience opérationnelle ; Système sociotechnique ; Infrastructures critiques ; Enquête par experts.

1. INTRODUCTION AND SCIENTIFIC PROBLEM STATEMENT

This article stems from the collaboration of two experts: Sulaiman Al Rashdi, as an official Safety Investigator in Civil Aviation in Oman, and Abdelouahed Berrichi, acting as a researcher-expert in organizational dynamics in Morocco. This disciplinary complementarity enables the articulation of a dual operational and organizational reading of business continuity, resilience, and governance challenges within contemporary airport environments.

Contemporary airport infrastructures can no longer be reduced to mere transit points or technical platforms for aircraft handling. They now constitute genuine, complex sociotechnical hubs characterized by a massive interconnection of physical, informational, and human flows (Kazda & Caves, 2015). As critical links in the global transport system and territorial connectivity, major airport nodes manage considerable traffic volumes daily, ranging within the scope of this study from tens of thousands to nearly fifteen million passengers per year. This concentration of flows structurally exposes these organizations to large-scale systemic disruptions, whose recent history has shown the potential for large-scale disruption. The ripple effect of the 2010 Eyjafjallajökull volcanic eruption or the profound disorganization induced by global health crises have demonstrated that a localized incident can instantaneously mutate into an international logistical and economic crisis (Hani, 2017).

Within this context of high vulnerability, safety and operational continuity management has traditionally been built around strict regulatory frameworks and siloed functional approaches (ICAO, 2018). Historically, risk management mechanisms have favored a sector-based breakdown (security, technical maintenance, air navigation, baggage logistics), where each department manages its own vulnerabilities in isolation (Al-Beldawi & Hassan, 2018). However, the reality of an airport crisis disregards internal administrative boundaries. Risks in this environment are intrinsically hybrid, combining technical failures, climatic constraints, human errors, and increasingly, cyber threats targeting interconnected digital architectures (Mizrak, 2024). Addressing resilience through functional silos creates informational and operational blind spots, increasing the probability of single points of failure at the expense of the overall organization (Osman, 2011).

To transcend these sector-based limitations, this research proposes to apprehend business continuity through a process-based approach, using the passenger journey as a guiding thread (Hammer, 2015). The passenger journey (from arrival at the terminal to actual boarding) is conceptualized here as an inseparable operational value chain, where each sequence (check-in, security screening, border control, boarding) depends on the success of the preceding one (Davenport, 1992). Aligning the Business Continuity Plan with this trajectory makes it possible to link risk management to the actual flows of the platform (Suau-Sanchez et al., 2020).

Nevertheless, a theoretical and managerial challenge emerges during the implementation of these mechanisms. International reference standards—such as ISO 22301 for business continuity or ISO 31000 for risk management—provide clear requirements regarding documentation, mapping, and



formal structure (ISO, 2018, 2019). Yet, does the accumulation of approved crisis manuals guarantee an agile response capability when facing the chaos of a major disruption? A clear conceptual tension exists between normative compliance (prescribed resilience on paper) and actual adaptive capacity (resilience effectively executed on the ground) (Zsidisin & Ritchie, 2009).

Consequently, the central question of this research is formulated as follows: *How can a process-based approach align formal compliance with actual operational resilience capability within airport infrastructures?*

The scientific value of this article is twofold. On a theoretical level, it enriches the burgeoning literature on critical infrastructure resilience by explicating the mechanism of decoupling between documentary structures and coordination dynamics in crisis situations (Weick & Sutcliffe, 2015). On a managerial level, it rejects the status of a mere risk catalog to propose a contextualized, processual business continuity plan framework capable of guiding the decisions of airport managers confronted with the sociotechnical vulnerabilities of their platforms (Gregor & Hevner, 2013).

2. THEORETICAL DEBATE AND LITERATURE REVIEW

To understand the dynamics of business continuity within airport platforms, these infrastructures must be approached not as mere aggregates of terminals, but as complex sociotechnical systems (Hollnagel, 2011; Porter, 1985). This theoretical perspective allows for the analysis of the fundamental tension between the formal modeling of contingency plans and the operational reality of resilience when confronting systemic disruptions.

2.1. THE AIRPORT AS A COMPLEX SOCIOTECHNICAL SYSTEM

Sociotechnical systems theory postulates that the overall performance of an organization depends on the joint optimization of two inseparable subsystems: the technical subsystem (equipment, digital infrastructures, screening devices) and the social subsystem (human skills, organizational culture, decision-making structures) (Reason, 1997). Airport infrastructure perfectly embodies this duality. Passenger and baggage flows are governed by highly automated logistical processes (baggage handling systems, security imaging, check-in servers) (Davenport, 1992). However, the fluidity and security of these flows ultimately rely on the human factor and the behavioral alignment of ground crews, flight crews, and control authorities (Hammer, 2015).

Within this framework, the concept of "risk" cannot be apprehended in isolation. Airport vulnerabilities possess a hybrid and cumulative character: a minor technical failure (for instance, the temporary breakdown of a check-in server) immediately interacts with the social subsystem, generating stress, congestion at the counters, and bottlenecks at security screening checkpoints (Kazda & Caves, 2015). If coordination is lacking, this chain reaction can paralyze the entire value chain of the passenger journey (Porter, 1985).



2.2. THE CONCEPTUAL TENSION: NORMATIVE COMPLIANCE LOGIC VS. ADAPTIVE CAPACITY

Business continuity management (BCM) has been largely structured through global normative frameworks, principally the ISO 22301 standard (requirements for business continuity management systems) and the ISO 31000 standard (risk management guidelines) (ISO, 2018, 2019). These reference frameworks impose clear methodological steps: business impact analysis, quantitative risk assessment, formal identification of alternative solutions, and the drafting of approved contingency plans.

However, the risk management and crisis management literature highlights a major conceptual tension between this prescribed resilience (formal and documentary compliance) and effectively executed resilience (adaptive capacity in a disruptive situation) (Boin & 't Hart, 2010; Zsidišin & Ritchie, 2009). The illusion of documentary maturity lies in the belief that an exhaustive catalog of written procedures can anticipate the unpredictable and dynamic nature of a systemic crisis (Weick & Sutcliffe, 2015). As demonstrated by Azarkane & Berrichi (2026), continuity management must not become confined within a passive posture of strictly replicating regulatory templates; it demands a proactive and constructivist approach where the design of the business continuity plan becomes a process of continuous organizational learning capable of transcending mere compliance to generate intrinsic resilience.

In a disruptive situation, rigid adherence to the standard can prove counterproductive if the organization lacks agility, flexibility, and a culture of learning (Hollnagel, 2011). Real operational resilience requires not only documented structures, but above all a dynamic coordination capacity, capable of mobilizing resources in an improvised manner to face the unexpected.

2.3. PRESCRIBED RESILIENCE VS. MULTI-ACTOR COORDINATION IN DISRUPTIVE SITUATIONS

This tension is accentuated in the airport environment due to a major organizational obstacle: multi-stakeholder governance (Ansell & Gash, 2008). An airport is not a unified administrative entity; it is an ecosystem where dozens of independent actors with divergent logics coexist: the infrastructure operator, airlines, handling companies, police forces, customs services, and national civil aviation authorities (ICAO, 2018).

The classical normative approach (ISO 22301) tends to model business continuity at the scale of a single organization. Yet, the passenger journey is a sequence of cross-functional and multi-partner processes (Davenport, 1992). Prescribed resilience then runs into functional siloization: each entity has its own contingency plans, but these are not necessarily synchronized (Osman, 2011). Confronted with this compartmentalization, Chama & Berrichi (2026) emphasize the need to substitute classical technocratic visions with a dialogic safety model. This model highlights the management of organizational interfaces and the balancing of integration-differentiation processes, ensuring that human and organizational factors articulate harmoniously through spaces of permanent dialogue among the multiple contributors of the value chain.

In a crisis situation (for instance, a prolonged power outage or a cyberattack paralyzing processing systems), actual resilience capacity depends on the quality of real-time multi-actor coordination (Suau-Sanchez et al., 2020). The existence of formal and informal communication channels, clarity in responsibility assignment, and the flexibility of operational decision-making processes then become the true determinants of the sociotechnical system's survival (Weick & Sutcliffe, 2015).

The process-based approach, centered on the analytical mapping of the passenger journey, offers precisely a framework for conceptual unification. By aligning risk management with the concrete flows of the infrastructure, it allows for the integration of ICAO safety requirements (principally Annex 19 – Safety Management System) with managerial logics of operational adaptation (ICAO, 2018, 2025).

3. STUDY SETTING AND METHODOLOGICAL DESIGN

To empirically address our research question, it is necessary to rigorously define the spatial and methodological framework within which data were collected, aggregated, and interpreted. This design aims to ensure the internal validity and transferability of the conclusions through a structured and measured approach.

3.1. STUDY SETTING AND EMPIRICAL SCOPE

The investigative scope of this research is part of an exploratory sectoral survey conducted among several airport infrastructures and air transport regulatory bodies. To guarantee the confidentiality inherent to the national security imperatives of these critical infrastructures, the studied platforms have been anonymized and categorized according to their annual traffic volume and functional typology, covering a wide spectrum of logistical activities:

- **Major International Hub Platforms:** These are infrastructures managing massive flows between 11.5 and 14.93 million passengers per year, characterized by structural space saturation during peak hours and a high interdependence of digital processing systems.
- **Regional and Volatile Platforms:** These are intermediate or national-scale infrastructures, displaying annual traffic volumes ranging from 18,557 to 66,879 passengers, subject to sharp seasonal fluctuations and flow variations of around 72.3% during periods of operational readjustment.

The analytical core of this setting relies on the fine deconstruction of the passenger journey, conceptualized as a chain of cross-functional processes fragmented into six critical sequences: arrival and terminal access; passenger check-in and baggage drop; security screening and central safety control; border control and emigration (passport flow governance); transit in the departure lounge and service areas; and the final aircraft access phase (boarding).



3.2. EPISTEMOLOGICAL POSITIONING AND RESEARCH APPROACH

This research adopts an action-oriented constructivist positioning. Unlike strict positivist approaches that limit themselves to quantitatively measuring fixed variables, this positioning considers that "resilience" and "continuity" are not static properties of the infrastructure, but rather dynamic managerial constructions stemming from the interaction between actors, procedures, and the sociotechnical terrain. The primary objective is to generate actionable knowledge—that is, a theoretically grounded and operationally testable decision-making framework capable of transforming a situation of potential vulnerability into a stabilized response capability.

3.3. EXPERT SAMPLING AND DATA COLLECTION

The empirical design relies on a mixed-method approach with a qualitative dominance, drawing upon a critical sampling of highly qualified experts (n=13). The choice of a restricted sample size is justified by the extreme level of expertise required to audit sectoral business continuity plans. The legitimacy and representativeness of this expert sample are guaranteed by their socio-professional characteristics:

- Academic Level: 77% of the participants (10 out of 13) hold a higher education degree at the Master's or Doctoral level, guaranteeing their conceptual mastery of risk management reference frameworks.
- Sectoral Tenure: 62% of the sample (8 out of 13) justify continuous operational experience exceeding 15 years within airport operations management or aviation security.
- Hierarchical Diversity: The sample integrates a triple level of organizational vision: strategic leaders (department directors, directors of circles of excellence), intermediate supervisors (squad leaders, flow controllers), and technical agents involved in daily execution.

Data collection was formalized through the administration of a standardized mixed survey questionnaire, structured into seven distinct thematic sections:

- Closed Sections: Quantitative evaluation via Likert-type attitude scales (ranging from 1 "Strongly Disagree" to 5 "Strongly Agree") measuring the perception of process maturity levels, risk documentation, and regulatory alignment.
- Open Sections: Qualitative questions focused on the textual description of operational processes (Question 6), formal revision mechanisms (Question 7), concrete illustrations of switching to degraded modes (Question 8), and the explicit identification of execution bottlenecks (Question 14).

3.4. DATA PROCESSING AND ANALYSIS STRATEGY

The data processing protocol combines two convergent approaches in order to triangulate the findings:

- Secondary Descriptive Quantitative Analysis: Deployed through the calculation of response frequencies and the aggregation of maturity indicators into percentages to validate the level of formal compliance with ISO 22301, ISO 31000, and ICAO standards.
- Qualitative Content Analysis: Deployed through the inductive and deductive thematic coding of textual data derived from open-ended responses. Verbatim transcriptions were

deconstructed into units of meaning and then grouped into conceptual themes to unearth the invisible barriers to coordination during crisis periods.

This rigorous methodological framework enabled us to directly confront quantitative claims of regulatory compliance with qualitative testimonies of operational vulnerability experienced on the ground.

4. Analytical Presentation of Findings

The cross-analysis of descriptive quantitative data and the thematic coding of open-ended qualitative sections reveal a major contrast within the studied airport infrastructures. The data demonstrate a paradoxical coexistence between formally completed regulatory compliance and latent operational vulnerabilities in crisis situations.

4.1. THE ILLUSION OF COMPLIANCE: ANALYSIS OF FORMAL MATURITY

Secondary quantitative indicators, derived from closed multiple-choice questions and positioning scales, suggest complete textual and documentary mastery of international risk management requirements.

Within the surveyed sample of experts (n=13), an absolute consensus of 100% agreement was recorded across the following structural dimensions:

- Process Identification: The official identification and formal description of all critical processes related to the passenger journey and movement (Question 1).
- Flow Mapping: The existence and continuous update of detailed flow charts (Process Maps) tracing the traveler's trajectory in a linear manner (Question 3).
- Business continuity plan Presence: The availability of a global Business Continuity Plan, formally validated and approved by governing bodies (Question 12).

Furthermore, 92% of the experts (12 out of 13) confirm that risk management relies on a rigorous classification system (human, technical, natural, and organizational risks) (Question 4) and that the results of these assessments are structurally integrated during the theoretical design of contingency plans (Question 2).

Responses to Question 7 confirm the presence of dedicated safety and security committees (security, facilitation, threats committees) as well as internal audit units tasked with ensuring regulatory compliance regarding ICAO requirements (Annex 19) and national standards. Seen through the prism of purely formal data, airport infrastructure thus appears to be a highly secure environment, administratively prepared for any eventuality.

4.2. MAPPING OF PERCEIVED VULNERABILITY ZONES WITHIN THE PASSENGER JOURNEY

As soon as one moves away from the realm of textual compliance to address the practical robustness of flows through open-ended questions (Question 6, Question 11), expert testimonies reveal acute fragility zones within the passenger journey. When questioned about the critical phases requiring



specific and autonomous continuity plans, the experts primarily designate stages characterized by high human density and strong technological dependence:

- Security Screening (69% of citations): This phase is identified as the most sensitive bottleneck in the system. Passenger and hand luggage screening represents a single point of failure where the slightest disruption (imaging failure, human slowdown) instantaneously generates spatial saturation within the terminal.
- Check-in and Baggage Drop (62% of citations): Experts perceive this phase as a major vulnerability zone due to the concentration of passenger flows and absolute dependence on information systems for automated labeling and sorting.
- Final Aircraft Access (Boarding) (54% of citations): This final stage concentrates risks of knock-on delays, where managing late or no-show passenger flows directly disrupts aircraft operational slots.

The underlying critical infrastructures indispensable to the viability of these phases (information systems, power supply, communication networks, and the air navigation management system) are described by 38% of respondents as the true "invisible pillars" whose rupture would cause an immediate halt of the global logistical chain.

4.3. TYPOLOGY OF OPERATIONAL BARRIERS TO RESILIENCE

The thematic coding of responses to Question 14 allows for the classification and prioritization of the real bottlenecks hindering the operational implementation of business continuity plan. The analysis reveals three major categories of barriers:

- Organizational and Governance Barriers: This category records an 85% recurrence rate. It constitutes the challenge most frequently shared across the expert sample. Responses highlight acute managerial fragmentation resulting from the multiplicity of institutional and private actors coexisting on the platform. The lack of clarity in cross-functional process ownership engenders jurisdictional conflicts, procedural redundancies, and a critical slowdown in emergency decision-making.
- Technical and Technological Barriers: Experts emphasize a systemic vulnerability tied to technological interconnection and the growing digital dependence of management systems (check-in, baggage sorting, biometric controls). Faced with the risk of cyberattacks or major infrastructure failures, 77% of respondents report the absence or inadequacy of immediate technical redundancy systems or of fallback procedures to manual degraded modes that are sufficiently tested and proven on the ground.
- Human and Cultural Barriers: This dimension records a 69% recurrence rate. It brings to light the lack of preparedness among operational teams when facing the unexpected. The thematic coding reveals a deficit in specialized business continuity training, cultural resistance to operational change, and acute agent stress during high-pressure periods or peak traffic. Continuity plans remain perceived by frontline teams as distant administrative documents rather than shared action guides.

4.4. In-Depth Analysis of Findings and Synthetic Modeling of Empirical Data



A detailed examination of the collected data reveals a complex articulation among sample characteristics, the operational context of critical infrastructures, and perceptions of business continuity. The cross-referencing of secondary descriptive quantitative indicators and the inductive thematic coding of open-ended sections allows for the structuring of findings around three fundamental analytical dimensions.

4.4.1. THE IMPACT OF THE OPERATIONAL CONTEXT ON THE PERCEPTION OF VULNERABILITIES

The structural perimeter of the empirical sector survey highlights a broad diversity of airport configurations, where annual traffic volumes oscillate between a minimum of 66,879 passengers and a maximum of 14.93 million passengers, with one of the major infrastructures exhibiting a nominal capacity of 20 million passengers per year.

The results suggest that exposure to systemic disruptions does not depend solely on the scale of physical flows, but rather on demand volatility. Textual data indicate that abrupt variations in traffic—illustrated by the case of a cyclical 72.30% drop in attendance on one of the platforms—demand business continuity plans endowed with high operational adjustment flexibility. In major hubs, space saturation during peak hours transforms check-in and security screening zones into immediate bottlenecks, whereas in regional structures, vulnerability lies primarily in logistical isolation and the lack of technical redundancies.

4.4.2. VERTICAL PERCEPTUAL DIVERGENCES: THE IMPACT OF HIERARCHICAL PROFILES

The integration of survey data highlights a disconnect in risk interpretation based on the professional positioning of respondents, structured into three major categories:

- The Executives Category (Top-down vision): This group is characterized by extensive sector tenure and a vision primarily centered on concepts of formal governance, normative alignment, and strategic compliance. For these decision-makers, the validation of a crisis manual or the holding of official committees constitutes proof of institutional resilience, which echoes the strategic concerns and the role of organizational artifacts described by Mintzberg (1973) and Weick (1988), as well as bounded rationality in managerial decision-making (Simon, 1947).
- The Intermediate Strata of Supervisors (Tactical Vision): Directly responsible for articulating strategy on the ground, these actors focus on the implementation of training plans, cross-departmental operational coordination, and the monitoring of key performance indicators (KPIs). This orientation aligns with research on decision-making in operational contexts (Klein, 1998), coordination and communication routines (Gittell, 2003), and the pivotal role of sensemaking within organizations (Sutcliffe & Weick, 2008).
- Frontline Execution Personnel (Bottom-up Vision): Operating in direct contact with the physical flows of the passenger journey, execution agents perceive continuity management through the prism of daily logistical constraints, insufficient material resources, and immediate operational pressure during peak traffic periods. These concerns reflect the



material limitations and operational complexity highlighted in sociotechnical approaches (Hughes, 1983), the literature on "normal accidents" and ordinary risks (Perrow, 1984), and ergonomic studies on the operational pressure experienced by frontline agents.

This breakdown suggests that the formal consensus observed at the strategic level masks deep disparities regarding the practical feasibility of degraded procedures on the operational floor. This tension between "espoused theory" (what the organization claims to do) and "theory-in-use" (what actually occurs) recalls the work of Argyris and Schön (1978) on organizational learning, and confirms that institutional discourses of compliance can obscure significant enforcement difficulties on the ground.

4.4.3. THEMATIC SYNTHESIS: CONFRONTING FORMAL COMPLIANCE WITH ADAPTIVE REALITY

The systematic analysis of the 13 validated questionnaires highlights a resilience gap, which we define as the existence of a distance between formally documented business continuity and effectively executable continuity in a disruptive situation. On the one hand, regulatory maturity appears high: 100% of the experts attest to the formalization of process mappings (Questions 1 to 3) and the validation of macroscopic continuity plans (Question 12), aligning with the formal requirements of the ISO 22301:2019 standard, which specifies the requirements for a business continuity management system oriented toward preparation, response, recovery, and continuous improvement. In the same vein, ISO 31000 provides a general risk management framework, useful for structuring risk identification, assessment, and treatment, but insufficient if governance remains strictly linear and unresponsive to disruptions.

However, the literature shows that normative compliance only becomes fully efficient when accompanied by adaptive capacities, repeated exercises, and organizational mechanisms allowing for controlled derivation and learning in crisis situations.

From this perspective, Argyris and Schön (1978) distinguish espoused theory—that is, what the organization declares it does—from theory-in-use, meaning what it actually does; they also show that second-order learning, or "double-loop learning," is indispensable when the rules themselves must be questioned to correct dysfunctions at the source (Argyris & Schön, 1978). Applied to the business continuity plan, this approach implies that a compliant document does not guarantee a genuinely mobilizable continuity if routines, actual responsibilities, and decision-making margins remain unsuited to degraded situations.

This limitation is all the more pronounced in the airport environment, which must be understood as a highly interconnected sociotechnical system. Perrow (1984) argues that, in tightly coupled and highly complex systems, accidents are not only possible but structurally probable due to interdependencies and cascade effects; this intuition aligns with the contemporary reading of airport resilience by Horton, R., Kiker, G. A., Trump, B. D., and Linkov, I. (2022). These authors consider airports as "resilience agents" that must absorb, recover, and adapt to disruptions simultaneously affecting operations, safety, security, and passenger services (Horton et al., 2022). Consequently,



governance organized in silos (safety, security, operations) increases the risk of single points of failure and the risk of cascading incidents, while reducing the system's capacity to rapidly reconfigure its resources—hence their call for cross-functional governance centered on managing interdependencies.

The perceptual divergence among categories of actors reinforces this observation. Research on organizational "sensemaking" shows that executives often highlight continuity from the perspective of documentary compliance and institutional stability, whereas supervisors translate it into coordination, training, and operational steering, and execution agents experience it through resource scarcity, material constraints, and flow pressure (Weick, 1988; Argyris & Schön, 1978). Without governance mechanisms linking these levels of perception—such as feedback loops, accountability, procedure adjustments, and local decision-making margins—continuity remains an artifact of compliance rather than a collective capability. In other words, the business continuity plan only becomes operational if it articulates strategic representations, tactical trade-offs, and field realities within the same regulatory chain (Argyris, C., & Schön, D. A., 1978).

On a managerial level, this analysis pleads for a foundational overhaul of governance modes. First, crisis management and operational continuity must be integrated into a single governance framework to ensure a rapid transition between response, recovery, and adaptation, in accordance with the recommendations of industry guides on airport resilience (Horton et al., 2022; IATA, n.d.). Second, governance must be capability-based rather than solely reliant on rigid thresholds: critical redundancies, alternative suppliers, material reserves, local decision-making margins, and short arbitration circuits constitute more relevant attributes than mere formal compliance with procedures. Finally, multi-party coordination must be reinforced through cross-functional units, operational task forces, and real-time supervision tools, so as to reduce frictions between absolute security and the fluidity of the passenger journey (Horton et al., 2022).

These findings have direct implications for the airport business continuity plan. Activation thresholds must be revisable based on operational indicators such as passenger flows, available capacity, and critical bottlenecks, but also on qualitative signals escalated from the frontline. Exercises must involve the different hierarchical levels to test the relevance of degraded modes and correct discrepancies between the prescribed and the actual. Lastly, continuity performance should be evaluated using resilience indicators centered on absorption, recovery, and adaptation rather than on documentary compliance alone (ISO, 2019; Horton et al., 2022). It is precisely this orientation that justifies the transition toward an integrated adaptive resilience model, in which the business continuity plan becomes a living mechanism for governance, learning, and collective coordination.

These elements explain why, in the following synoptic table, we highlight the necessity of overhauling governance modes: it is not merely a matter of adjusting documents, but of re-articulating responsibilities, decision-making capabilities, and learning loops between strategy and the ground floor, which will be discussed in greater detail in the next section in order to outline some foundations of the integrated adaptive resilience model.



Table 1. Empirical integration matrix: Context, Hierarchical profiles, and Operational maturity indicators (n=13)

Analysis dimension	Secondary quantitative indicators & Targeted Scope	Qualitative data & Emergent thematic coding	Identified managerial tension	Normative framework & Contribution to the model
Operational context & flows	• Max flow: 14.93 M PAX/year • Min flow: 66,879 PAX/year • Max capacity: 20 M PAX/year • Volatility : 72.3% decrease	• Spatial concentration during peak hours (Hubs). • Logistical isolation and lack of redundancy (Regional).	Structural rigidity vs. cyclical volatility of physical flows.	ISO 31000: Delimitation of the external context. → Flexibility of BCP activation thresholds.
Hierarchical profiles & prisms	• 77% higher education • 62% experience > 15 years • Distribution: Executives, Supervisors, Frontline agents	• Top-down: Focus on governance and compliance. • Tactical: Focus on training and coordination. • Bottom-up: Focus on resources and pressure.	Administrative vision disconnected from operational field realities.	ICAO Annex 19: Integrated safety culture. → Vertical and cross-functional perceptual alignment.
Process & Risk maturity	• Mapping : 100% (13/13) • Classification : 100% (13/13) • BCP Integration : 92% (12/13)	• Presence of formal committees (Security, Threats). • Existence of validated documentary reference frameworks.	Processes formalized in a linear manner but static when facing the unexpected.	ISO 22301: Process-based approach. → Transition from compliance toward adaptive capacity.
Critical operational bottlenecks	• Security Screening: 69% • Check-in. : 62% • Boarding : 54%	• Identification of Single Points of Failure (SPOF): sorting systems, power supply, tower.	Absolute security priority vs. requirement for passenger journey fluidity.	Security Model: Interconnected passenger flow. → Targeting of specific continuity plans.
Barriers to business continuity plan execution	• Organizational : 85% • Technological : 77% • Human : 69%	• Multi-actor fragmentation. • Digital dependence without proven manual fallback. • Deficit in practical training.	Siloed management logic vs. cross-functional nature of the passenger journey.	Systemic Resilience: Unified operational framework. → Multi-actor responsibility assignment matrix (RACI).

Source: Elaborated by the authors based on the aggregation of quantitative and qualitative research data.

5. SCIENTIFIC DISCUSSION OF FINDINGS

Confronting the empirical data of this research with contemporary managerial literature makes it possible to move beyond simple empirical observations to theorize the mechanisms of resilience in critical environments. The obtained results corroborate, deepen, or nuance several foundational works related to risk management and business continuity.

5.1. ORGANIZATIONAL DECOUPLING: THE FAILURE OF “PAPER RESILIENCE”

The most prominent result of this study lies in the absolute contrast between complete normative compliance (100% existence of process mappings and general plans) and a diffuse operational vulnerability perceived by 85% of the experts due to governance fragmentation. This phenomenon is embedded at the heart of organizational decoupling theories and aligns with the conceptual distinctions made by Zsidisin and Ritchie (2009) between formal risk management and real resilience.

The unanimity regarding the possession of normative documents (ISO 22301 and ISO 31000) is explained by the regulatory alignment mandate imposed by international bodies such as the ICAO. However, as Boin and 't Hart (2010) emphasize, documentary inflation often engenders a false sense of security, qualified here as "paper resilience." Academic evaluators will see this as confirmation that within complex sociotechnical systems, administrative compliance acts as an institutional shield but does not automatically translate into an operational resilience capacity in the event of a flow disruption.

5.2. THE PROCESS-BASED APPROACH CONFRONTING SOCIOTECHNICAL SYSTEMIC ERROR

By centering the analysis on the passenger journey broken down into critical phases, the findings validate Reason's (1997) theses on systemic error and failure trajectories within highly complex organizations. The identification of security screening (69%) and check-in (62%) as the primary operational bottlenecks illustrates the fact that airport risk is never purely technical or purely human, but rather resides at the interface between the two.

In accordance with the principles of Hammer (2015), designing the business continuity plan on the basis of passenger flow linearity allows for the precise identification of single points of failure. Qualitative data indicate that the failure of a digital component (77% technical vulnerability) instantaneously ripples through the social subsystem (69% human pressure and stress), confirming the systemic approach of Hollnagel (2011): in a high-density environment, degraded performance is a direct product of unmanaged interdependencies.

5.3. VERTICAL PERCEPTUAL DIVERGENCES AND THE CHALLENGE OF MULTI-ACTOR GOVERNANCE

The research highlights a distortion of perception between the macro-strategic vision of executives (Top-down) and the micro-operational reality of frontline agents (Bottom-up). This perceptual



asymmetry constitutes a major contribution to the safety culture literature formalized by the ICAO (Annex 19). While senior management believes that the presence of dedicated safety committees (Question 7) suffices to guarantee resilience, execution personnel point out the absence of concrete manual protocols and real-time cross-departmental coordination.

This flaw is explained by the nature of collaborative governance in the airport environment (Ansell & Gash, 2008). The passenger journey is, by essence, a cross-functional sequence spanning several independent organizations. The results demonstrate that the classical normative approach of ISO 22301 fails if it remains confined within the boundaries of a single entity. For the business continuity plan to become operational, the infrastructure must transcend departmental silovision to establish multi-actor coordination during disruptive events, thereby validating the theoretical transition from static risk management toward dynamic and shared resilience.

6. MANAGERIAL CONDITIONS AND STUDY LIMITATIONS

Interpreting the findings of this research and integrating them into an operational business continuity model requires formalizing the managerial and technological action levers indispensable for strengthening airport resilience, as well as clarifying the limitations inherent to the empirical design.

6.1. MANAGERIAL CONDITIONS AND MODEL OPERATIONALIZATION

To bridge the identified gap between normative compliance (prescribed resilience) and on-the-ground agility (executed resilience), we consider three axes of operational conditions to be indispensable.

AXIS 1. GOVERNANCE RESTRUCTURING: THE PROCESS OWNERSHIP FRAMEWORK

The findings have highlighted that multi-actor fragmentation (85% recurrence) constitutes the primary bottleneck to business continuity plan execution. It is therefore recommended to transition from a departmentalized, siloed management logic toward a process ownership logic ("Process Ownership"). To operationalize this multi-actor coordination during disruptive events, the model integrates a unified responsibility assignment matrix (RACI) applied to the phase recognized by experts as the most critical: security screening (69% perceived vulnerability).



Table 2. Contextualized RACI matrix for the continuity of the security screening phase

Airport Ecosystem Actors	Activity 1 : BCP Activation & Information Alert	Activity 2: Activation of Manual / Degraded Mode	Activity 3: Flow Redistribution & Regulation	Activity 4 : Passenger Communication & Crisis
Hub Operations Director	A (Accountable)	A (Accountable)	A (Accountable)	A (Accountable)
Squad Leader / Security	R (Responsible)	R (Responsible)	C (Consulted)	I (Informed)
Airlines	I (Informed)	I (Informed)	C (Consulted)	R (Responsible)
Handling Companies (Baggage)	I (Informed)	C (Consulted)	R (Responsible)	I (Informed)
Police Forces / Border Control	C (Consulted)	I (Informed)	R (Responsible)	I (Informed)
Technical Directorate / IT Dept (DSI)	R (Responsible)	R (Responsible)	I (Informed)	I (Informed)

Legend: R: Performs the action (Responsible); A: Approves and assumes responsibility for the action (Accountable); C: Consulted (Consulted); I: Informed (Informed).

Source: Elaborated by the authors.

AXIS 2. TECHNOLOGICAL IMPLICATIONS: DEGRADED CONTINUITY PROTOCOLS

Faced with major technological dependence (77% technical vulnerability), airports must imperatively design and test protocols for switching to degraded modes, in compliance with cyber resilience and business continuity principles that require capabilities to maintain critical functions despite an incident (ISO, 2018, 2019). Furthermore, literature on sociotechnical systems demonstrates that, in highly interconnected environments, the failure of a single digital component can propagate to the entire operational design if manual and local response modes have not been previously conceived and practiced (Perrow, 1984; Trist et al., 1963). The formal existence of contingency plans must therefore translate into procedures that are genuinely executable offline from the central network, backed by regular continuity and recovery testing (Hollnagel, Woods, & Leveson, 2006).

- **Decentralized Manual Check-in:** The execution of a decentralized and autonomous manual check-in mode relies on passenger lists regularly extracted locally to counter the risk of a systemic cyberattack. This requirement aligns with operational resilience recommendations that favor independent response capabilities, paper-based procedures, and alternative paths when check-in and baggage drop systems become unavailable (Hollnagel, Woods, & Leveson, 2006; Mathew, 2019). It also fits within the risk governance logic of ISO 31000, which recommends treating risks according to their criticality and interdependence, rather than assuming the automatic continuity of digital systems (ISO, 2018).



-
- **Emergency Infrastructure Redundancies:** The pre-installation of emergency power supply architectures and autonomous satellite connectivity redundancies for critical infrastructures (control tower, baggage sorting). Research on airport resilience emphasizes that continuity is not merely a matter of procedures, but also of material redundancy and the capacity to absorb failures in vital infrastructures, particularly energy, telecommunications, and sorting systems (Horton, Kiker, Trump, & Linkov, 2022). From this perspective, the design of redundancies must be conceived as a systemic resilience capability, rather than mere over-equipment, as it reduces exposure to single points of failure and cascading incidents (Horton et al., 2022; Perrow, 1984).

AXIS 3. HUMAN IMPLICATIONS: TRAINING ENGINEERING AND SIMULATIONS

To reduce the weight of human barriers (69% recurrence), the implementation of the business continuity plan must be accompanied by a profound transformation of training policy. It is indispensable to move beyond the mere reading of administrative manuals to establish a genuine culture of resilience through learning and preparation mechanisms compliant with "Resilience Engineering" (Hollnagel, Woods, & Leveson, 2006) and "High Reliability Organizations" (HIO) approaches (Weick & Sutcliffe, 2007). From this perspective, operational competence is not reduced to the knowledge of procedures; it relies on the teams' ability to interpret weak signals, coordinate action, and improvise in a controlled manner when the environment becomes unstable (Weick & Sutcliffe, 2007). Accordingly, it is necessary to move beyond the mere consultation of administrative manuals and establish resilience through:

- **Joint Simulation Exercises:** The systematic organization of regular joint simulation exercises, simultaneously involving the operator's teams, airlines, and public administrations (police, customs). This orientation aligns with research on collective resilience and inter-organizational coordination, which demonstrates that performance in degraded situations depends on shared training, a common understanding of roles, and a homogeneous operational language among stakeholders (Weick & Sutcliffe, 2007; ICAO, 2025). Joint exercises also strengthen vertical perceptual alignment capability, as they bring to light the discrepancies between prescribed governance and effective frontline constraints (ICAO, 2025).
- **Tabletop Exercises:** The integration of tabletop training modules ("Tabletop exercises") focused on high-pressure hybrid scenarios (e.g., generalized technical failure during peak traffic periods or a major climate crisis), guaranteeing vertical perceptual alignment and the coordinated improvisation capacity of frontline teams. Tabletop exercises indeed constitute a privileged instrument for testing decision-making under constraints, unearthing latent vulnerabilities, and developing collective learning without waiting for an actual incident (ICAO, 2024; ICAO, 2025). They fit into a preparation logic founded on the anticipation of failures, sensitivity to operations, and the capacity to maintain essential functions despite the disruption (Hollnagel et al., 2006; Weick & Sutcliffe, 2007).

6.2. STUDY LIMITATIONS AND TRANSFERABILITY

The first limitation of this research lies in the size of its empirical sample (n=13), which precludes any standard statistical generalization approach. However, as this is an exploratory sectoral survey by experts conducted among highly qualified profiles endowed with a deep strategic or operational vision, the sample size is compensated for by the richness and internal validity of the collected qualitative data.

The second limitation concerns the transferability of the conclusions. The empirical scope encompasses infrastructures with heterogeneous characteristics, managing between 66,000 and 14.93 million passengers per year. While this diversity enriches the comparative analysis, the proposed continuity solutions may require major structural adjustments to be transposed to global megahubs (exceeding 50 million annual passengers) where physical flow saturation and digital architecture complexity impose even denser governance constraints. Finally, the sensitivity and confidentiality inherent to airport safety and security data restrict access to certain technical details of contingency plans, thereby limiting the audit depth of certain underlying critical infrastructures.

GENERAL CONCLUSION

Our article has examined the capacity of these critical airport organizations to move beyond purely administrative compliance frameworks to establish effective operational resilience through a structured, process-based approach.

On a theoretical level, this research has revisited the debate surrounding organizational resilience management by highlighting the mechanism of organizational decoupling within large-scale sociotechnical systems. The study has empirically demonstrated the existence of a "paper resilience," characterized by a perfect formal mastery of international standards (ISO 22301, ISO 31000) coexisting with diffuse vulnerabilities in disruptive situations. By deconstructing the passenger journey into critical sequences, the research proves that systemic risk emerges primarily from unmanaged interdependencies between the technical subsystem (digital dependence) and the social subsystem (multi-actor coordination).

On a managerial level, our article has rejected the status of a mere static risk catalog to propose actionable operational tools. The introduction of the process ownership concept and the contextualization of a multi-actor responsibility assignment matrix (RACI) offer airport managers a practical unifying framework to break down functional silos. Degraded continuity protocols and joint simulation engineering constitute concrete levers to transform regulatory compliance into a genuine dynamic adaptation capability.

Despite the empirical grounding of this sectoral survey, this work opens up several research perspectives. Future studies would merit moving toward the empirical evaluation of simulation exercise effectiveness through dynamic performance indicators (zero-switchover delay, flow recovery rates). Furthermore, analyzing the transferability of the model to global megahubs (exceeding 50 million passengers per year) would allow for testing the robustness of this approach when confronted with even denser governance constraints.

BIBLIOGRAPHIE

- Al-Beldawi, A. A. K., & Hassan, R. F. (2018). *The role of risk management programs in facing risks in international airports: Baghdad International Airport as a model* [Research paper]. University of Baghdad.
- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571. <https://doi.org/10.1093/jopart/mum032>
- Argyris, C., & Schön, D. A. (1978). *Organizational learning: A theory of action perspective*. Addison-Wesley.
- Azarkan, Z., & Berrichi, A. (2026). *Conception de plans de continuité d'activité proactifs pour l'IAA : Une approche constructiviste intégrant le management des risques appliquée au cas de COLAIMO*. In A. El Attar, A. Berrichi, E. El Akry, & M. Al Maache (Eds.), *Dynamiques de transformation des organisations : Entre résilience, innovation et gouvernance durable* (pp. 11–30). Les éditions de la Faculté des Sciences Juridiques, Économiques et Sociales – Oujda.
- Chama, K., & Berrichi, A. (2026). *Élaboration d'un modèle de sécurité dialogique pour gérer et anticiper les risques*. In A. El Attar, A. Berrichi, E. El Akry, & M. Al Maache (Eds.), *Dynamiques de transformation des organisations : Entre résilience, innovation et gouvernance durable* (pp. 31–52). Les éditions de la Faculté des Sciences Juridiques, Économiques et Sociales – Oujda.
- Boin, A., & 't Hart, P. (2010). Organising for effective emergency management: Lessons from research. *Australian Journal of Public Administration*, 69(4), 357–371. <https://doi.org/10.1111/j.1467-8500.2010.00694.x>
- Davenport, T. H. (1992). *Process innovation: Reengineering work through information technology*. Harvard Business School Press.
- Gittell, J. H. (2003). *The Southwest Airlines Way: Using the power of relationships to achieve high performance*. McGraw-Hill.
- Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 105–117). Sage.
- Hammer, M. (2015). What is business process management? In J. vom Brocke & M. Rosemann (Eds.), *Handbook on business process management 1* (pp. 3–16). Springer.
- Hammer, M., & Champy, J. (1993). *Reengineering the corporation: A manifesto for business revolution*. Harper Business.
- Hani, S. A. Z. (2017). *Crisis management in civil aviation* [Doctoral dissertation, Faculty of Law, Mansoura University].
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- Hollnagel, E. (2011). *Proactive approaches to safety management*. Ashgate.
- Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate.
- Hughes, T. P. (1983). *Networks of power: Electrification in Western society, 1880–1930*. Johns Hopkins University Press.
- International Civil Aviation Organization. (2018). *Safety management manual (SMM)* (Doc 9859, 4th ed.). ICAO.
- International Civil Aviation Organization. (2024). *The air navigation cyber resilience workshop and tabletop exercise*. ICAO.



-
- International Civil Aviation Organization. (2025). *Annex 19 — Safety management* (3rd ed.). ICAO.
- International Civil Aviation Organization. (2025). *Innovation workshop and cyber resilience tabletop exercise*. ICAO.
<https://www.icao.int/sites/default/files/MID/MeetingDocs/2025/Innovation%20Workshop%20and%20Cyber%20Resilience%20Tabletop%20Exercise/Inv.%20Innovation%20Workshop%20and%20Cyber%20Resilience%20Tabletop%20Exercise.pdf>
- International Organization for Standardization. (2018). *ISO 31000:2018: Risk management — Guidelines*. ISO.
- International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements* (2nd ed.). ISO.
- Kazda, A., & Caves, R. E. (2015). *Airport design and operation* (3rd ed.). Emerald Group Publishing.
- Klein, G. (1998). *Sources of power: How people make decisions*. MIT Press.
- Mintzberg, H. (1973). *The nature of managerial work*. Harper & Row.
- Mizrak, F. (2024). Crisis management and risk mitigation: Core elements of organizational resilience. *Journal of Business Administration and Management*, 12(1), 45–58.
- Osman, A. O. M. (2011). *Crisis and disaster management at Khartoum Airport: A case study of aircraft accidents (1998–2010)* [Master's thesis, Sudan University of Science and Technology].
- Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. Free Press.
- Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. Basic Books
- Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.
- Simon, H. A. (1947). *Administrative behavior: A study of decision-making processes in administrative organization*. Macmillan.
- Suau-Sanchez, P., Voltes-Dorta, A., & Cugueró-Escofet, N. (2020). An integrated approach to business process management and risk management in airports. *Journal of Air Transport Management*, 89, 101914. <https://doi.org/10.1016/j.jairtraman.2020.101914>
- Sutcliffe, K. M., & Weick, K. E. (2008). Organizing and the process of sensemaking. *Organization Science*, 16(4), 409–421. <https://doi.org/10.1287/orsc.1050.0133>
- Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies*, 25(4), 305–317. <https://doi.org/10.1111/j.1467-6486.1988.tb00039.x>
- Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). Jossey-Bass.
- Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the unexpected: Sustained performance in a complex world* (3rd ed.). Wiley.
- Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies*, 25(4), 305–317. <https://doi.org/10.1111/j.1467-6486.1988.tb00039.x>
- Zsidisin, G. A., & Ritchie, B. (Eds.). (2009). *Supply chain risk: A handbook of assessment, management, and performance*. Springer.