CHAPTER 2
LEGAL RELATIONS: FROM THEORY TO PRACTICE

Economic Security Documentation System in Civil Aviation Enterprises: The Case of Airports

Zinaida Zhyvko[1], Mykhailo Zhyvko[2]

[1]Doctor of Science (Economics), Professor, Professor of the Department of Aviation Management, Ukrainian State Aviation Academy, Kropyvnytskyi, Ukraine, ORCID: https://orcid.org/0000-0002-4045-669X
[2]Ph.D. (Law), Junior Researcher, Scientific Center of Innovative Research, Pussi, Estonia, ORCID: https://orcid.org/0000-0002-0099-3562

Citation:
Zhyvko, Z., & Zhyvko, M. (2025). Economic Security Documentation System in Civil Aviation Enterprises: The Case of Airports. *Public Administration and Law Review*, (3(23), 52–64. https://doi.org/10.36690/2674-5216-2025-3-52-64

Received: August 26, 2025
Approved: September 28, 2025
Published: September 30, 2025

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC 4.0) license

OPEN ACCESS

Abstract. *Airports operate as complex socio-technical systems where financial, operational, and safety risks intersect; yet the documentary foundations that translate incidents into measurable economic learning remain weakly integrated and unevenly disclosed. The aim of the article is to develop and substantiate a conceptual Airport Economic Security Documentation System (AESDS) by specifying essential document types and their interactions across the strategic–tactical–operational hierarchy, and by mapping how publicly disclosed artifacts at EU airports relate to financial stability, fraud prevention, and risk resilience. The methodology is a web-based documentary review - without interviews - covering eight EU operators (Schiphol, Frankfurt/Fraport, Groupe ADP, Vienna/Flughafen Wien, daa/Dublin, ANA-Portugal, Athens, Prague), limited to materials on official websites and investor portals (annual/governance/ESG reports, policies, supplier/partner codes, SMS/operational regulations). Artifacts were recorded if explicit, current, and linked to governance oversight; public visibility was then assessed along the incident → costing → closure chain. Across the sample, board-anchored ERM and ethics/vigilance systems are widely disclosed, while operational documents that evidence economic-impact tracing - standardized incident-to-impact costing forms, revenue-assurance SOPs, and closure KPIs - are rarely public. Governance disclosures (e.g., Schiphol's COSO-aligned ERM; Vienna's audit-committee oversight; daa's ERM-ESG-ethics integration) confirm a robust top-down scaffolding, but the financial translation layer remains opaque online. The public record thus reveals an asymmetric disclosure pattern: high visibility for incident capture (SMS, whistleblowing), moderate for governance closure, and low for costing/impact artifacts - the critical link from events to economic learning. This pattern reflects commercial sensitivity rather than the absence of practice and motivates an AESDS maturity construct grounded in documentary presence, minimum content, ownership/refresh cycles, and evidence-of-use thresholds. A validated AESDS should integrate strategic policies, tactical control designs (risk registers, revenue-assurance, supplier oversight, incident-to-impact procedures), and operational evidence (checklists, scorecards, costing forms, dashboards), with expert consensus used to finalize minimum content and feasible thresholds for airports of different sizes. Such standardization would enhance transparency, risk resilience, and compliance efficiency while enabling rigorous cross-airport evaluation of documentation maturity and its performance payoffs.*

Keywords: *airport governance; economic security; internal documentation; enterprise risk management; revenue assurance; supplier risk; safety management system; incident-to-impact costing; EU airports.*

JEL Classification: L93, G32, D 73, M48, H56

Formulas: 0; fig.: 0; table: 8; bibl.: 22

Introduction. Airports represent complex socio-technical systems that integrate financial, operational, and security dimensions within an environment characterized by high uncertainty and strict regulatory control. Ensuring economic security in civil aviation enterprises is a multifaceted task that involves not only financial protection against internal and external threats but also the development of a robust internal documentation system that regulates decision-making, risk management, and control procedures. In recent years, the significance of internal documentation has increased due to the intensification of hybrid threats, cyber incidents, and financial irregularities in transport infrastructure sectors. Moreover, the International Civil Aviation Organization (ICAO), the European Union Aviation Safety Agency (EASA), and national authorities have progressively emphasized the need for coherent internal policies, standards, and protocols that align with ISO 31000 (Risk Management), ISO 9001 (Quality Management), and ISO 37001 (Anti-bribery Management Systems).

The problem lies in the fragmented approach to documentation and the lack of standardized frameworks for integrating economic security management into internal corporate policies of airports. Many airports rely on outdated administrative documents that do not correspond to the dynamic risk landscape of the aviation industry. Therefore, it is essential to design a systematic documentation model that strengthens resilience, accountability, and efficiency of economic security management.

Literature Review. The issue of economic security in civil aviation enterprises has recently drawn increasing scholarly and regulatory attention, especially as airports face complex financial, operational, and cybersecurity risks. However, the integration of internal documentation systems within the economic security management framework remains underexplored.

According to the International Civil Aviation Organization (ICAO, 2018), the Safety Management Manual (Doc 9859) establishes a foundation for risk-based management and continuous improvement within civil aviation enterprises. The manual emphasizes a performance-oriented documentation culture - policies, procedures, risk registers, and audit records - that ensures traceability and accountability. Nevertheless, while ICAO defines the documentation requirements for safety and operational risk management, it does not specifically address economic or financial security documentation. This gap limits the ability of airports to align their internal regulatory frameworks with broader enterprise risk management (ERM) and anti-fraud systems.

At the European level, the European Union Aviation Safety Agency (EASA, 2023), through the Easy Access Rules for the Basic Regulation (EU Regulation 2018/1139), highlights the importance of systematic documentation for compliance, reporting, and risk oversight. The regulation defines documentation requirements primarily for safety, maintenance, and operational processes. Similarly, Regulation (EU) No 376/2014 on the reporting, analysis, and follow-up of occurrences in civil aviation focuses on safety occurrences and data protection obligations (European Union, 2018). However, the economic consequences of such events - such as operational disruptions, compensation payments, or financial fraud - remain outside

the scope of these regulatory frameworks. Thus, airports lack a unified documentation model that bridges economic and operational risk domains.

The International Organization for Standardization (ISO, 2018) through ISO 31000:2018 Risk Management - Guidelines provides a universal framework applicable to airports as complex organizations. ISO 31000 stresses the documentation of all stages of risk management - identification, analysis, evaluation, treatment, monitoring, and communication - as evidence of due diligence and decision-making transparency. Integrating this approach into aviation-specific contexts can support the development of economic security documentation systems. However, research by Mihus (2023) and Motuzenko (2024) shows that many transport enterprises, including airports, apply risk documentation inconsistently across departments, lacking integration between financial, compliance, and operational records.

Industry associations have also recognized this challenge. The Airports Council International (ACI, 2024) in its ESG Task Group Paper on Performance and Risk Management Metrics highlights that a mature documentation framework contributes to financial transparency, environmental accountability, and economic resilience. The International Air Transport Association (IATA, 2018; 2022) further underscores the need for standardized cybersecurity documentation within aviation enterprises, including risk assessment templates, supplier oversight forms, and incident reports. These materials directly affect economic security, as cyber incidents may lead to operational paralysis, loss of revenue, or reputational damage. Yet, few studies - such as Rodrigues and Fonseca (2021) - systematically link cybersecurity documentation with financial protection mechanisms in airports.

From a regulatory economics perspective, the ICAO (n.d.) Airport Economics Manual (Doc 9562) provides guidelines on airport charges, cost recovery, and transparency principles. While the manual supports financial integrity and accountability, it does not define how internal documents - such as policies, tariffs, cost allocation methods, or contract registers - should be organized into a comprehensive economic security system. This leaves airports to interpret economic documentation individually, leading to heterogeneity and fragmentation across jurisdictions.

Scholars such as Kozachenko and Ponomarov (2018) argue that economic security management should rely on a structured internal documentation hierarchy that aligns strategic, tactical, and operational decisions. Meanwhile, Vynnyk (2022) emphasizes that documentation culture forms the backbone of economic resilience, ensuring that each managerial action is supported by a regulatory, procedural, and evidence-based foundation. Despite these conceptual insights, empirical research on airport-specific documentation systems remains scarce. Most studies either address general enterprise security or focus exclusively on aviation safety management, leaving a gap in understanding how documentation contributes to economic stability, anti-fraud control, and risk resilience.

Although civil aviation standards increasingly emphasize risk-based management and robust documentation, a coherent airport-level framework linking internal documents to economic security is still missing. Foundational texts prioritize safety management systems and related records (policies, procedures, risk registers,

performance monitoring), yet they stop short of detailing how documentation should safeguard financial integrity, anti-fraud controls, and resilience of revenues and costs within airport enterprises (ICAO, 2018; ISO, 2018; EASA, 2023).

As a result, airports often maintain parallel - and weakly connected - document streams: regulatory compliance files aimed at safety oversight and, separately, managerial documents for budgeting, contracting, and cost control; the absence of an integrating architecture hinders traceability of decisions from risk identification to financial outcomes (European Union, 2018; ICAO, 2018).

Moreover, while guidance on cybersecurity and ESG has matured, it is seldom coupled with the financial governance artifacts that actually absorb and mitigate losses (e.g., supplier-risk clauses, incident-to-impact costing protocols, fraud response playbooks), leaving a methodological gap between cyber guidance and economic protection (IATA, 2018, 2022; Airports Council International, 2024).

The Airport Economics Manual clarifies principles of charges, transparency, and cost recovery, but it does not prescribe how internal policies, SOPs, registers, and dashboards should be structured as a single economic-security documentation system, perpetuating heterogeneous practices across jurisdictions (ICAO, n.d.). Scholarly work notes the importance of documentation culture and ERM alignment, yet evidence remains conceptual; rigorous, comparative studies quantifying how documentation maturity affects measurable economic outcomes - loss reductions, fraud incidence, recovery speed, or continuity metrics - are scarce (Mihus, 2023; Rodrigues & Fonseca, 2021).

Consequently, the literature lacks a validated Airport Economic Security Documentation System (AESDS) model that integrates safety-derived risk processes with financial governance, specifies roles and artifacts across strategic, tactical, and operational layers, and demonstrates statistically the performance payoffs of documentation maturity. This gap not only limits theoretical development but also constrains practitioners who need deployable templates, role matrices, and KPIs that connect compliance documentation to economic resilience in real airport settings.

Aims. This study seeks to design and substantiate a conceptual Airport Economic Security Documentation System (AESDS) by specifying the essential types, functions, and interactions of internal documents across the strategic–tactical–operational hierarchy, and by mapping how publicly disclosed artifacts at major EU airports relate to financial stability, fraud prevention, and risk resilience within airport governance structures.

Methodology. We conducted a web-based documentary review of eight EU airport operators - Royal Schiphol Group (NL), Fraport/Frankfurt (DE), Groupe ADP/Paris (FR), Flughafen Wien/Vienna (AT), daa/Dublin (IE), ANA-Aeroportos de Portugal/Lisbon (PT), Athens International Airport (GR), and Prague Airport (CZ). Sources were limited to official websites and investor portals (annual and sustainability reports, governance statements, codes of conduct, supplier/partner codes, and SMS/operational regulations). For each operator, we recorded whether economic-security-relevant artifacts were (a) explicit (clearly named and scoped), (b) current (dated/editioned), and (c) linked to oversight (e.g., board or audit-committee

responsibility). We then assessed public visibility along the incident → costing → closure chain to determine whether disclosures support traceable economic-impact management; interviews and non-official sources were not used.

Results. Across the eight operators, governance-level frameworks and ethics/vigilance controls are widely disclosed, whereas operational artifacts that would evidence economic-impact tracing - standardized costing forms, revenue-assurance SOPs, and closure KPIs - are largely absent from public sources.

Systematization of international and national standards. Royal Schiphol Group publicly details a COSO-aligned risk-management cycle - identification, appetite setting, management, monitoring, and reporting - anchored in Executive and Audit Committee oversight (Royal Schiphol Group, 2025, pp. 102-109). The framework is presented as an integrated approach to strategic, operational, financial, and compliance risks and includes a maturity lens for process capability; however, document-level templates for loss quantification (e.g., incident-to-impact costing) are not published alongside the framework, leaving the financial translation layer opaque to external readers (Royal Schiphol Group, 2025).

Vienna Airport's annual report and governance filings likewise formalize internal control and risk management under the Austrian Corporate Governance Code with explicit Audit Committee responsibilities and periodic external assessment of effectiveness (Flughafen Wien AG, 2024; 2025). These disclosures demonstrate board-anchored ERM, yet they do not expose operational artifacts that would show how incidents are costed, closed, and re-fed into financial controls.

DAA's Annual Report 2024 and its ESG Strategy 2024-2030 emphasize the integration of ESG, ethics, and ERM, including rollout of standardized risk processes and governance of procurement and IT security at board-committee level (daa, 2025, pp. 56-61; daa, 2025b, pp. 6-9). This signals a maturing nexus between ERM and commercial risk; still, public materials stop short of publishing costing/closure protocols that would allow external verification of economic-loss management.

Groupe ADP provides a comprehensive Ethics & Compliance Code of Conduct and a Vigilance Plan describing value-chain risk identification, prevention, and mitigation measures, plus whistleblowing architecture (Groupe ADP, 2020; 2022; 2024/2025 URD synopsis). These texts evidence a formal ethics program (code, procedures, e-learning, third-party assessment, alert system) that is structurally relevant to economic security via fraud prevention and supplier risk oversight (Groupe ADP, 2023).

Athens International Airport publicly posts a Business Partners' Code of Conduct that addresses sanction screening, anti-money-laundering expectations, and continuity/incident planning obligations for partners; AIA also publishes board-approved sustainability and governance policies, indicating adoption cycles and oversight (Athens International Airport, 2024a; 2024b; 2024c). This combination articulates supplier-facing expectations that intersect directly with financial protection (e.g., AML/CTF, continuity) (Athens International Airport, 2024d).

Table 1. Publicly disclosed artifacts by operator (representative, non-exhaustive)

Operator (country)	ERM/ICFR disclosure	Ethics & vigilance artifacts	SMS / occurrence references	Supplier/partner controls
Royal Schiphol Group (NL)	ERM cycle, risk appetite, committee oversight (Annual Report 2024)	Code referenced within governance system	—	—
Flughafen Wien AG (AT)	Governance report; Audit Committee oversight; external assessment	Compliance officer reporting to Supervisory Board	—	—
daa (IE)	ERM–ESG–ethics integration; procurement & IT security oversight	Ethics program under ESG strategy	—	Procurement oversight signaled
Groupe ADP (FR)	URD includes governance and vigilance references	Code of conduct, whistleblowing, vigilance plan	—	Third-party assessment and vigilance
Athens International Airport (GR)	Board-approved policies; sustainability governance	Corporate code; anti-fraud/anti-corruption; whistleblowing	—	Business Partners' Code (AML, sanctions, continuity)
Fraport/Frankfurt (DE)	—	—	SMS Regulation (EU 2018/1139; 139/2014; 376/2014)	—
Letiště Praha (CZ)	ESG governance references	Compliance Ethics Line (whistleblowing)	—	Partner measures reported at high level

Notes: Dashes indicate that no directly relevant artifact was found on public pages within the scope of this review; absence of public disclosure does not imply absence of internal practice. Sources: Schiphol (Royal Schiphol Group, 2025); Vienna (Flughafen Wien AG, 2024; 2025); daa (daa, 2025; 2025b); Groupe ADP (2020; 2022; 2023; 2025 URD excerpt); Athens International Airport (2024a; 2024b; 2024c; 2024d); Fraport AG (2024; 2023); Letiště Praha (2023; 2025).
Source: systematized by the author

Prague Airport discloses a Compliance Ethics Line (confidential reporting portal) and provides ESG reporting that references governance structures and partner-related initiatives, suggesting ongoing institutionalization of ethics and procurement controls, even if granular operating procedures are not public (Letiště Praha, 2023; 2025).

Fraport publishes binding SMS Regulations for Frankfurt Airport referencing Regulation (EU) 2018/1139, 139/2014, and participation in occurrence reporting consistent with EU 376/2014 (Fraport AG, 2024; 2022/2023). The documents define safety governance, hazard identification, change management, and key-figure reporting; nevertheless, publicly accessible materials do not specify how safety incidents are translated into financial impact and how recovery outcomes are captured within ERM/finance systems (Fraport AG, 2024; see also General Airport Regulations cross-reference).

Table 2. Public visibility of the "economic-impact tracing" chain (incident → costing → closure)

Chain element	Typical public evidence across sample	Observed visibility (web only)
Incident capture (safety/ethics/whistleblowing)	SMS regulations; whistleblowing portals	High (Fraport SMS; Prague Ethics Line; ADP vigilance)
Impact quantification (costing taxonomy, approval trail)	Standardized costing form; risk/finance SOP	Low (not published in any sampled site)
Governance closure (KPIs, audit closure, lessons learned)	Audit committee reporting; KPI dashboards	Moderate at governance level (Schiphol, Vienna, daa), but low at operational template level

Source: systematized by the author

Comparative Modeling. The comparative modeling stage operationalizes the Airport Economic Security Documentation System (AESDS) as a hierarchical, interacting set of documentary artifacts and governance routines, and then tests whether variation in this system is associated with measurable differences in economic-security outcomes across airports. Conceptually, AESDS is defined as a three-level documentary architecture - strategic → tactical → operational - in which upstream artifacts (e.g., Economic Security Policy; Risk Appetite & Tolerance) set intent and constraints, mid-stream artifacts (e.g., Fraud Risk Assessment; Revenue-Assurance SOP; Procurement/Third-Party SOPs; Loss Event Database specification; KPI Compendium) design the control system, and downstream artifacts (e.g., checklists, SoD matrices, incident costing forms, supplier scorecards, dashboards) provide executional evidence. The interaction logic assumes that strategic clarity increases the coherence of tactical design, tactical completeness conditions the quality of operational execution, and operational evidence feeds back to tactical review and strategic oversight through KPI dashboards, audits, and periodic policy refresh.

Table 3. AESDS Hierarchical Interaction Map (Concept → Measurement → Use)

AESDS level	Core artifacts (examples)	Interaction role	Measurement anchors (examples)	Use in models
Strategic	Economic Security Policy; Risk Appetite & Tolerance; Economic Continuity Policy	Sets intent and quantitative guardrails for economic risk	Existence; last approval date; linkage to KPIs and audit committee minutes	Inputs to maturity score; instrument for policy refresh frequency
Tactical	Fraud Risk Assessment; ERM risk register (economic subset); Revenue-Assurance SOP; Procurement & Third-Party SOP; Incident-to-Impact Costing Procedure; Loss Event DB spec; KPI Definition Book; IA Program	Designs controls and analytics; defines data structures; mandates thresholds	Minimum-content compliance; refresh cadence; cross-references to incidents/audits/KPIs	Inputs to maturity; binary/coverage flags for key artifacts
Operational	Control narratives & checklists (P2P/O2C/CapEx); SoD matrices; exception logs; supplier scorecards; incident costing forms; dashboards	Generates executional evidence; closes the loop via KPIs and lessons learned	Coverage rates (% incidents costed; % spend scored; % controls tested); SLA compliance	Coverage covariates; evidence-of-use intensities

Source: systematized by the author

Empirically, the stage translates this architecture into a maturity score and a set of binary/coverage indicators that can be tested against observable outcomes (loss ratios, disruption hours with financial impact, fraud incidence per transaction volume, audit late-closure rates, tariff dispute counts). To avoid tautological measurement, maturity is derived only from documentary presence, quality anchors (minimum content fields), ownership/refresh cycles, and evidence-of-use thresholds (e.g., share of incidents with completed costing forms), not from the outcomes themselves. The comparative design adopts a multi-method approach: regression models with robust standard errors and appropriate link functions (OLS/GLM/Poisson/NegBin), matched comparisons (e.g., propensity score matching on size, ownership, and network role), and mini-case process tracing to connect specific artifact introductions with before/after patterns in losses and recoveries. Robustness checks include outlier treatment (winsorization), alternate operationalizations (e.g., log-loss, per-capita/per-revenue scaling), and multicollinearity diagnostics (VIF).

The hypothesis set posits that higher AESDS maturity and the presence of specific tactical/operational artifacts are associated with improved economic-security performance:

• H1 (Systemic effect). A 10-point increase in AESDS maturity correlates with a lower loss ratio (losses/revenue), ceteris paribus.

• H2 (Process translation). Airports with a standardized Incident-to-Impact Costing Procedure exhibit shorter recovery time (hours to business-as-usual) and higher insurance recovery rate.

• H3 (Supply-chain containment). Greater supplier-risk coverage (share of spend under scorecards with cyber/fraud clauses) correlates with fewer disruption-with-loss events.

• H4 (Assurance intensity). Presence of a formal Revenue-Assurance SOP and exception log with thresholdscorrelates with lower revenue-leakage incidence.

Table 4. Variables and Model Specification (Implementation-Ready)

Construct	Variable	Type	Definition/Construction	Model family (example)
AESDS maturity	AESDS_Maturity	Continuous (0–100)	Sum of 10 domains × 0–4, rescaled	OLS/GLM on LossRatio
Tactical artifact	IncidentCosting_Std	Binary	Formal, approved incident-to-impact costing procedure	OLS/log-linear on RecoveryHours
Operational coverage	SupplierCoverage	%	Spend under scorecards & clauses / total addressable spend	Poisson/NegBin on DisruptionsLoss
Operational coverage	CostingCoverage	%	Incidents with completed costing form / total incidents	OLS/GLM on LossRatio
Assurance intensity	RevAssure_SOP	Binary	Approved revenue-assurance SOP with test plan	OLS/GLM on RevenueLeakageRate
Controls	Size_Pax; Ownership; HubRole; GDPpc; WeatherRisk	Mixed	Traffic volumes; governance type; hub dummy; macro proxy; exposure proxy	Entered in all models
Outcomes	LossRatio; RecoveryHours; DisruptionsLoss; RevLeakageRate; AuditLateClosure	Mixed	As reported/derived from public docs or internal records if available	As per hypothesis

Source: systematized by the author

Model estimation proceeds with robust SEs; VIF < 5 is enforced; sensitivity tests include winsorization (1% tails) and alternative scaling. Matched comparisons (e.g., high-maturity vs. low-maturity airports matched on size/ownership/hub role) provide non-parametric corroboration. Mini-cases (3-4 airports) document the introduction of a specific artifact (e.g., Revenue-Assurance SOP) and trace mechanisms - changes in exception patterns, audit findings closure rates, and trend inflections in loss/ leakage metrics-thereby supporting causal interpretation without over-reliance on regression assumptions.

Table 5. Evidence-of-Use Metrics and Thresholds

Artifact group	Evidence metric	Baseline threshold	Rationale
Policies (strategic)	Update within 12 months; board minutes link	100%	Maintains top-down currency
SOPs (tactical)	Planned tests executed	≥ 80%	Demonstrates operationalization
Registers/DB	Coverage of relevant events	≥ 90%	Ensures analytic completeness
Supplier scorecards	Share of spend covered	≥ 80%	Controls supply-chain exposure
Incident costing	Forms completed on time	≥ 90%	Enables timely financial learning

Source: systematized by the author

Collectively, this Stage delivers estimated effect sizes (e.g., ΔLossRatio per 10 maturity points), identification of high-leverage artifacts (those with statistically robust associations to outcomes), and a narrative account of mechanisms through mini-cases, linking documentation to behavior change and measurable resilience.

Validation. The validation stage subjects the AESDS model - its artifact set, minimum content standards, evidence-of-use metrics, maturity rubric, and hypothesized linkages - to expert scrutiny and consensus building using a multi-round Delphi process. The goal is to assess adequacy (does the model cover what matters?), coherence (do elements fit together logically and operationally?), and scalability (can diverse airports implement it across sizes and ownership forms?) while converting practitioner feedback into a consensus edition.

A panel of 15–21 experts is assembled to balance perspectives: airport CFOs or economic-security leads; ERM heads; internal auditors; procurement/contracting leaders; cyber/OT security representatives; and at least one civil-aviation regulator and one industry association expert (e.g., ACI/IATA). Prior to Round 1, panelists receive a concise AESDS pack: artifact catalogue with minimum fields, maturity rubric with scoring anchors, sample evidence-of-use thresholds, and a short memo summarizing Stage-3 effect sizes and mini-case insights. Rounds are structured to elicit breadth first, then convergence, while minimizing dominance and anchoring effects through anonymized feedback.

Table 6. Delphi Design and Flow

Round	Core task	Instrument	Output
1 (Elicit)	Rate relevance/clarity of artifacts, fields, metrics; propose additions	5-point Likert grids + open comments	Median ratings; free-text suggestions
2 (Converge)	Re-rate after seeing group medians/IQR and rationale	Feedback report; revised grids	Reduced dispersion; candidate inclusions/exclusions
3 (Decide)	Finalize artifact set, weights for maturity rubric, and thresholds	Shortlist with conflicts; weighting exercise	AESDS v1.1 Consensus Edition (artifact list, RACI, weights, thresholds)

Source: systematized by the author

Consensus rules are pre-declared to maintain methodological integrity: (a) IQR ≤ 1.0 on 5-point relevance for inclusion; (b) Kendall's W ≥ 0.70 across domains as panel-level agreement; (c) Lawshe's CVR applied to "essential" fields within artifacts to determine minimum content. Disagreements trigger focused prompts in Round 2 and, if necessary, decision notes documenting the rationale for retaining divergent items (e.g., niche artifacts that smaller airports can adopt at Level-2 maturity).

Table 7. Consensus Criteria and Decision Policy

Criterion	Definition	Threshold	Decision policy
Relevance dispersion	Interquartile range on relevance	IQR ≤ 1.0	Include; else revisit in Round 2
Panel concordance	Kendall's W across domains	W ≥ 0.70	Accept weights; else re-weight discussion
Essentiality	Lawshe CVR for fields	≥ critical value by N	Field retained in minimum content
Implementability	Expert rating of feasibility	≥ 4/5 median	If < 4, downgrade to optional/advanced

Source: systematized by the author

To assess scalability, the panel rates each artifact on feasibility across airport sizes and regulatory contexts and recommends minimal viable adaptations (e.g., consolidated templates for smaller airports; modular KPI sets). Disagreements about evidence-of-use thresholds (e.g., 90% vs. 80% incident-costing coverage) are resolved by pairing risk-based justifications (impact of late costing on recovery learning) with resource constraints, producing tiered thresholds (baseline vs. stretch) for different maturity levels.

Table 8. Validation Evidence Matrix (What "Validated" Means)

AESDS component	Validation questions	Evidence types	Acceptance signal
Artifact set	Is anything missing or redundant?	Round-1/2 ratings; comments	≥ 90% artifacts meet IQR ≤ 1
Minimum content	Are mandatory fields sufficient and auditable?	CVR on fields; examples	CVR ≥ cut-off; exemplar templates
Evidence-of-use	Are metrics fair and outcome-linked?	Feasibility & outcome linkage ratings	Median feasibility ≥ 4; retained
Maturity rubric	Do weights reflect risk contribution?	Weighting exercise; Kendall's W	W ≥ 0.70; stable weights
Scalability	Can small/large airports implement?	Feasibility by airport class	≥ 80% endorse tiered pathways

Source: systematized by the author

The last stage concludes with AESDS v1.1 (Consensus Edition) - a refined artifact list and weighted maturity rubric, agreed minimum content (per artifact), evidence-of-use thresholds (tiered where needed), and implementation guidance (roles, refresh cycles, sample templates). A short validation appendix documents unresolved minority views and recommended future evidence (e.g., publishing non-sensitive templates to strengthen public auditability). This closing transparency maintains academic rigor while yielding practitioner value.

Together, this Stages produce quantified associations between documentation maturity and economic-security performance; a consensus-ratified AESDS that is adequate (coverage), coherent (fit among levels), and scalable (tiered adoption); and a deployable toolkit - artifact templates, maturity-scoring guide, KPI dictionary, and evidence-of-use checks - that enables airports to implement the model, track progress, and demonstrate transparency, risk resilience, and compliance efficiency in a manner consistent with scholarly standards and operational realities.

Discussion. Together, these publicly available artifacts depict a robust top-down scaffolding for economic security. Schiphol's COSO-aligned risk framework, Vienna's corporate-governance architecture, and daa's integration of ethics/ESG with ERM illustrate board-anchored control systems that—in principle - should encompass fraud risk, procurement integrity, cyber-financial exposures, and continuity (Royal Schiphol Group, 2025; Flughafen Wien AG, 2024; daa, 2025; daa, 2025b). Supplier governance is also increasingly codified: Groupe ADP's vigilance plan and code of conduct, Athens' Business Partners' Code, and Prague's whistleblowing system collectively evidence maturing third-party oversight, a cornerstone of economic security given airports' reliance on concessions, ground handling, and complex supply chains (Groupe ADP, 2020; 2022; 2023; Athens International Airport, 2024a; 2024b; 2024c; Letiště Praha, 2023). Finally, Fraport's SMS regulations demonstrate alignment with EU safety law and a reporting culture that should produce incident datasets amenable to cross-functional learning (Fraport AG, 2024; 2023).

However, the tactical and operational documentary strata most probative for economic-impact tracing remain non-public. Across operators, I found no published, standardized templates for incident-to-impact costing, revenue-assurance SOPs and exception logs with financial thresholds, or audit-closure KPIs tied to loss reduction. This opacity likely reflects commercial sensitivity rather than an absence of practice; nonetheless, it limits independent verification of how governance structures translate incidents into measurable financial learning. For web-only research designs, this implies that governance-level readiness can be benchmarked rigorously, while claims about control efficacy or return-on-controls must be framed as inferences from governance signals (policy dates, committee oversight, vigilance reach) rather than direct observation of operational documentary evidence.

Conclusion. This web-based documentary study of EU airport operators shows a consistent governance backbone for economic security - board-anchored ERM frameworks, ethics and whistleblowing systems, supplier/partner codes, and SMS regulations - publicly disclosed across multiple sites (e.g., Schiphol, Vienna, daa; ADP vigilance; Athens partner code; Prague ethics line; Fraport SMS). These artifacts

demonstrate mature top-down arrangements that, in principle, support fraud prevention, procurement integrity, cyber-financial risk oversight, and continuity within airport enterprises.

At the same time, the operational layer that traces economic impact is largely non-public: standardized incident-to-impact costing forms, revenue-assurance SOPs (with exception thresholds), and audit-closure KPIs tied to loss reduction are rarely published on airport websites. As a result, the public record exhibits high visibility for incident capture (SMS, whistleblowing), moderate visibility for governance closure signals (committee oversight, high-level KPIs), and low visibility for impact quantification artifacts - the critical link from events to financial learning and control improvement. This asymmetry is captured in the incident → costing → closure chain: high for capture, low for costing, and only moderate for closure at governance level.

Given this transparency boundary, the study's main empirical finding is an asymmetric disclosure pattern: robust, comparable evidence exists for strategic and governance instruments, whereas tactical and operational documentation most probative of economic-loss management remains internal. This implies that web-only benchmarking can reliably assess readiness at the governance tier, but any claims about control efficacy or return-on-controls must be expressed as inferences rather than direct observations.

Methodologically, the analysis motivates a structured AESDS maturity construct grounded in documentary presence, minimum content, ownership/refresh cycles, and evidence-of-use thresholds - independent of outcome metrics - and a comparative modeling design to test associations between documentation maturity and economic-security outcomes (loss ratios, disruption hours, fraud incidence, closure rates), with appropriate robustness checks (e.g., GLM/Poisson models, matching, sensitivity tests).

Finally, the study concludes that a validated Airport Economic Security Documentation System (AESDS) should integrate strategic, tactical, and operational artifacts and be refined through expert consensus (Delphi) to ensure adequacy, coherence, and scalability; producing a consensus edition with weighted rubric, minimum content, and evidence-of-use thresholds would enable airports to implement the model and demonstrate transparency, risk resilience, and compliance efficiency despite limits on public disclosure.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this article are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Airports Council International – North America. (2024). *Environment, Social, and Governance: An introduction to performance and risk management metrics for North American airports* (White paper). https://shorturl.at/pBoZj
2. Athens International Airport. (2024a). *Business partners' code of conduct*. https://shorturl.at/sFGAC
3. Athens International Airport. (2024b). *Sustainability policy*. https://shorturl.at/gNlqp
4. Athens International Airport. (2024c). *Summary of the company's operation regulation*. https://shorturl.at/1OVtn
5. daa. (2025). *Annual report & accounts 2024*. https://shorturl.at/ePjp6
6. daa. (2025b). *ESG strategy 2024–2030*. https://tinyurl.com/4f4rjrv3
7. European Union Aviation Safety Agency. (2023). *Easy Access Rules for the Basic Regulation (Regulation (EU) 2018/1139)*. https://tinyurl.com/54s8srh3
8. European Union. (2014). *Regulation (EU) No 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation*. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2014/376/oj/eng eur-lex.europa.eu
9. European Union. (2018). *Regulation (EU) 2018/1139* (Basic Regulation). EUR-Lex. https://eur-lex.europa.eu/eli/reg/2018/1139/oj/eng eur-lex.europa.eu
10. Flughafen Wien AG. (2024). *Annual report 2024*. https://viennaairport.com/jart/prj3/va/uploads/data-uploads/IR/2025/VIE_GB_2024_EN.pdf
11. Flughafen Wien AG. (2024). *Consolidated corporate governance report*. https://tinyurl.com/5y6k894x
12. Fraport AG. (2023). *General Airport Regulations (C2.2)*. https://sslapps.fraport.de/webportalAVS/pdf/General-Airport-Regulations.pdf
13. Fraport AG. (2024). *SMS regulation of Fraport AG and FRA-Vorfeldkontrolle GmbH (C4.6)*. https://sslapps.fraport.de/webportalAVS/pdf/Sms-regulations.pdf
14. Groupe ADP. (2020). *Charter for the processing of ethics and compliance-related alerts*. https://tinyurl.com/2rxksuvd
15. Groupe ADP. (2025). *Universal registration document 2024*. https://tinyurl.com/5ye3p6ht
16. International Air Transport Association. (2020/2022). *Compilation of cybersecurity regulations, standards & guidance applicable to civil aviation* (White paper). https://tinyurl.com/bdcmz8r5
17. International Civil Aviation Organization. (2018). *Safety Management Manual (SMM), Doc 9859 (4th ed.)*. https://store.icao.int/en/safety-management-manual-doc-9859
18. International Civil Aviation Organization. (2025). *Airport economics manual (Doc 9562)*. https://www.icao.int/
19. International Organization for Standardization. (2018). *ISO 31000:2018 Risk management—Guidelines*. https://www.iso.org/standard/65694.html
20. Letiště Praha, a.s. (2023). *ESG report of Prague Airport Group 2023*. https://tinyurl.com/52pdtysw
21. Letiště Praha, a.s. (2025). *Compliance Ethics Line*. https://www.prg.aero/en/compliance-ethics-line
22. Royal Schiphol Group. (2025). *Annual report 2024*. https://tinyurl.com/y3jp8nb2