*Proc. of the European Safety and Reliability Conference (ESREL 2026)*
*Edited by* José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva, Monica Santamaria and Chiara Turco
© 2026 ESREL 2026 Organizers. *Published by* Research Publishing, Singapore.
ISBN: 978-981-94-6718-1 | doi: 10.3850/ESREL2026061419_esrel26-p27657-cd

# Operationalising Trust in the Sky: An Institutional Analysis of EASA Part-IS Implementation

Edouard van den Heuvel

*Amsterdam Business School, University of Amsterdam, the Netherlands.*
*E-mail: edouard.vandenheuvel@uva.nl*

Riana Steen

*Department of Safety, Economics and Planning University of Stavanger, Norway.*
*E-mail: riana.steen@uis.no*

Maria Papanikou

*Faculty of Technology,, Amsterdam University of Applied Sciences, the Netherlands.*
*E-mail: m.papanikou@hva.nl*

**Abstract**
The European Aviation Safety Agency (EASA) Part-IS regulation requires EU airlines to integrate information security into existing aviation safety frameworks, aiming to improve regulatory consistency, organisational resilience, and overall aviation safety. Despite its significance, limited empirical insight exists into the preparedness of airlines to implement and demonstrate compliance with Part-IS. This study examines implementation readiness using publicly available information, reflecting the perspective of external stakeholders. A systematic document review and regulatory gap analysis are applied to six purposively selected European airlines representing variation in business models, governance structures, and geographic coverage within the EASA jurisdiction. The analysis focuses on six high-priority clauses according to IS.I.OR regulation and assesses the alignment between publicly disclosed governance arrangements, security risk management practices, and procedural measures and regulatory requirements. The findings indicate that all sampled airlines have established basic information security structures and initiated preparatory activities. From an institutional perspective, organisational responses largely reflect compliance with formal regulatory demands and partial alignment with industry norms, while information security remains unevenly embedded in organisational practices. However, publicly available information rarely addresses aviation-specific security risk assessments, the integration of information security into occurrence reporting systems, or the existence of formal Information Security Management Manuals. This lack of transparency constrains external evaluation of regulatory readiness and may affect stakeholder confidence. The study contributes a transparent and replicable approach for assessing implementation readiness in security-sensitive and highly regulated domains and highlights the need for structured procedural development and clearer public disclosure to demonstrate compliance and strengthen trust in aviation safety and security.

*Keywords*: Aviation safety, EASA Part-IS, Cybersecurity, Regulatory readiness, Information Security Management, Resilience.

## 1. Introduction

Aviation is a highly regulated industry where continuous introduction and amendment of regulations are essential to maintaining safe and secure operations. Research on Performance-Based Regulation (PBR) highlights how risk-management principles underpin mandated management systems in aviation, such as the Safety Management System (SMS), which became a regulatory requirement in the early 2010s (ICAO, 2018). SMS provides a structured framework for managing safety through continuous improvement, with core components including policy, risk management, safety assurance, and safety promotion.

Such frameworks demonstrate that systematic risk-based governance contributes significantly to operational safety in aviation, However, as technological advancement reshapes the sector, new classes of risks—particularly

cyberthreats—have emerged, exposing airlines to attacks from cybercriminals, state-sponsored actors, and hacktivists (Ukwandu et al., 2022). In response, the European Union introduced Part Information Security (Part-IS), administered by the European Union Aviation Safety Agency (EASA), providing a regulatory framework for information-security management across the aviation ecosystem.

However, despite the foundational work on SMS and broader PBR approaches, critical questions remain about the integration of digital and operational safety systems. While SMS has long addressed operational hazards, the literature provides limited insight into how information-security management systems (ISMS) can be embedded effectively within existing safety governance frameworks. Only a few studies systematically examine how cyber-risk considerations are operationalised in aviation-specific contexts (Fonseca-Herrera, Rojas, & Florez, 2021). This creates a dilemma: if ISMS adoption mirrors SMS practices, how can airlines ensure that cyber and physical safety risks are addressed holistically? And if current guidance is insufficient, what additional mechanisms are required to achieve effective integration and operational resilience?

The purpose of this paper is to examine the implementation of EASA Part-IS within European aviation and identify potential implementation gaps. This study builds on previous SMS research, which generally focused on operational hazards but typically neglecting the interdependence between operational and digital risks. ISMS integration introduces a new dimension: information security as an inherent component of overall safety assurance. As we demonstrate, examining regulatory texts, sector guidance, and public airline disclosures allows for identifying structural and organisational barriers that may obscure critical implementation challenges. Consequently, generalized approaches to information security risk management can lead to inaccurate assessments of sector readiness and misaligned resource allocation.

To occupy this niche, the study employs a structured analytical framework based on three observable indicators: (i) aviation-specific probability–severity matrices for cyber-risk assessment, (ii) explicit mapping between information-security events and safety-occurrence reporting under Regulation 376/2014 (ECCAIRS), and (iii) inclusion of safety-impact criteria within change-control documentation. This framework not only operationalises the contextualisation gap but also enables systematic comparison across airlines.

Finally, this study leverages authoritative regulatory texts, sectoral guidance, and public airline disclosures as empirical material. These sources are particularly valuable because they capture the regulatory intent, sector-wide expectations, and current organisational practices, offering a representative view of European aviation's preparedness for Part-IS. Through these paths, the research highlights how integrated governance of information security and operational safety can enhance overall sector resilience. The findings therefore provide both theoretically informed and practically actionable foundation for ensuring cyber-resilient aviation operations.

## 2. Theoretical Framing

### 2.1 *Regulatory response to rising digital threats*

Digitalisation has enhanced airline operations, from flight planning to passenger services, while increasing cyber risks and systemic vulnerabilities. Aviation cybersecurity is both a technical and institutional challenge (Björck, 2004; Kurt & Gerede, 2018; Melin et al., 2018). Robust frameworks like Part-IS establish harmonised, aviation-specific security standards to protect critical information assets and promote operational resilience. Its principles—availability, integrity, and confidentiality—ensure that data is accurate, accessible, and protected, forming the foundation of effective information-security management (NIST, 2022; von Solms & van Niekerk, 2013).

Although the terms information security and cybersecurity are often used interchangeably, they differ in scope. Information security focuses on protecting the data itself and the human and procedural dimensions surrounding it, whereas cybersecurity encompasses broader technical measures that defend digital infrastructures and networks. In aviation, these domains are inseparable, as security systems and risks can compromise operational safety (Paraschi et al. 2022). For example, in the Aircraft Control Domain (ACD) of flight-management and navigation systems, breaches pose direct threats to flight safety. Hence, the cross-domain and multi-layered nature of aviation security reinforce the

need for systematic, comprehensive, and enforceable protection measures. Regulatory harmonization under Part-IS is therefore a prerequisite for sustained digital resilience in the aviation sector, highlighting the institutional perspective.

### 2.2. *Institutional theory*

The institutional theory perspective provides a robust framework for analysing the interaction between organizations and their broader institutional environments (Scott, 2005; Tina Dacin et al., 2002), emphasizing the significance of legitimacy, isomorphic pressures, and the balance between stability and change (DiMaggio & Powell, 2000). This lens enables better understanding of the complex dynamics within societal and regulatory contexts, offering insights into how external norms, rules, and expectations shape organizational structures and practices. As a theoretical lens, it views organisations as actors embedded in broader environments shaped by formal rules, professional norms, and shared belief systems.

These influences are commonly structured into three pillars: a) the regulative pillar with formal legal and regulatory mandates that organisations must adhere to, such as specific clauses of Part-IS and related EASA guidance; b) the normative pillar with professional standards, role expectations, and industry best practices that determine how compliance is enacted; c) the cultural-cognitive pillar on shared understandings, values, and routines that embed compliance behaviour into everyday organisational life.

Recent research on institutional theory, according to David et al. (2019) moved from studying how organizations become similar to examining institutional change, such as new laws, products, and occupations. This expansion has strengthened the framework, but challenges remain. Key issues include reconciling different decision-making models and better understanding how socio-cultural forces interact with entrepreneurial actions.

## 3. Methodology

### 3.1. *Research design*

This study uses a qualitative approach based on publicly available documents, combining systematic document analysis (Bowen, 2009), with regulatory gap analysis to examine how European airlines are preparing for the EASA Part-IS regulation. The regulatory gap analysis benchmarks publicly disclosed practices against specific Part-IS requirements to identify areas of alignment and deficiency, while focusing on authoritative sources ensures transparency and supports replicability. The design mirrors the perspective of IT auditors, who are responsible for providing independent assurance on governance, risk management, and compliance structures.

### 3.2. *Data sources and sampling strategy*

Two main categories of data were analysed to address the research objectives: authoritative regulatory and guidance (AU & G) documents and public disclosures (PD) from European airlines. Table 1 outlines the specific documents included in these categories. These documents collectively defined the intended scope, objectives, and operationalization of Part-IS requirements, with data primarily drawn from the 2024 reporting year and supplemented by available 2025 updates.

Table 1. Study's documents.

| Source | Document |
|---|---|
| AU & G | The complete legal text of Commission Implementing Regulation (EU) 2023/203 (Part-IS). |
| AU & G | The EASA Easy Access Rules for Information Security, relevant international standards such as ISO/IEC 27001. |
| AU & G | The NIS 2 Directive, the ICAO Safety Management Manual, and sector-specific guidance from EUROCONTROL and ENISA. |
| PD | Airlines annual reports, sustainability/ESG reports. |
| PD | Corporate governance statements & risk and compliance disclosures. |
| PD | Publicly released Information Security Management System (ISMS) policies. |

A purposive sampling strategy (Suri, 2011) was employed to select six European airlines for in-depth analysis. This selection aimed to ensure diversity across critical dimensions, including business models (full-service, low-cost, and cargo

operators), governance structures (single carriers versus multi-brand airline groups), and geographic coverage within the EASA jurisdiction. The selected organisations were: Lufthansa Group, Air France–KLM, International Airlines Group (IAG – British Airways/Iberia), Ryanair Holdings, easyJet, and Cargolux Airlines International. A key criterion for inclusion was the public availability of sufficient documentation pertaining to governance, risk management, compliance, or information security.

### 3.3. *Data analysis and procedures*

The data analysis followed a structured three stage qualitative process designed to link regulatory requirements with theoretical interpretation. In the first stage, a codebook was developed using a combined deductive and inductive approach. The initial coding structure was derived from six high priority EASA Part IS clauses IS.I.OR.200 to 255 and was then refined through iterative analysis to capture emergent themes and sector specific characteristics identified in the airline documents.

In the second stage, each coded segment was assigned one or more institutional pillar tags, regulative, normative, or cultural cognitive, to examine not only formal compliance with regulatory requirements but also the extent to which information security appeared embedded in organisational practices and understanding.

The third stage involved thematic analysis, in which coded data were clustered into core domains such as governance, risk assessment, and incident reporting. This was followed by a regulatory gap analysis that benchmarked publicly disclosed practices against EASA Part IS and ISO IEC standards and classified the level of alignment as aligned, partially aligned, or not evidenced.

### 3.4. *Transparency and ethical considerations*

The study was designed to ensure methodological transparency and replicability. Analytical decisions were traceable through a structured codebook and institutional pillar tagging, which linked interpretations directly to regulatory clauses and documented evidence. The analysis explicitly recorded the absence of evidence in public disclosures, clarifying that a classification of not evidenced reflected limited transparency rather than confirmed non implementation.

The findings also pointed to a sector wide transparency gap that complicated external assessment of Part IS observable readiness. While airlines commonly signalled alignment with formal regulatory requirements, publicly available material provided limited insight into operational practices, including aviation specific risk assessment, Information Security Management Manuals, and the integration of information security events into safety reporting. This constraint limited external verification of readiness and affected stakeholder confidence.

## 4. Findings

Our analysis reveals three key themes regarding European airlines' observable readiness for Part-IS implementation. First, implementation patterns emerged, including governance-first approaches, adaptations of existing ISO/IEC 27001 frameworks, and gradual integration of information security into safety management systems. Second, we examined preparatory activities, inferring progress from indirect indicators like governance alignment and policy updates, particularly where explicit Part-IS statements or roadmaps were absent. Finally, the cross-case analysis identified readiness gaps, highlighting the need for aviation-specific risk assessments, integrated occurrence reporting, defined roles, dedicated Information Security Management Manuals (ISMMs), and contextualization of generic ISO frameworks.

### 4.1. *Alignment of Part-IS Requirements with Industry Practices*

Part IS builds on ISO IEC 27001, adding aviation-specific requirements for governance, risk assessment, reporting, documentation, and personnel. Airlines show varying degrees of commitment to information security, with limited evidence of risk management implementation. "Aligned" indicates complete compliance evidence, "partially aligned" refers to disclosures lacking aviation context, and "not evidenced" means no relevant public information. Findings prioritize key clauses as follows:

- IS.I.OR.200 – Information Security Management System (ISMS): Lufthansa Group and Air France–KLM reference established ISMS frameworks in ESG

reports, but without explicit links to aviation safety. Ryanair describes an "information security framework" within its corporate governance report yet omits operational or safety-specific integration.

- IS.I.OR.205 – Information Security Risk Assessment: Risk disclosures are common but focus on financial or operational categories. No carrier publishes a probability–severity risk-classification method for aviation-related information security hazards. IAG references "cyber risk management" but without methodological detail.
- IS.I.OR.230 – External Reporting Scheme: Compliance with Regulation (EU) No 376/2014 is acknowledged by Lufthansa Group, IAG, and Cargolux, but none explicitly integrate information security incidents into occurrence reporting procedures in their public documentation.
- IS.I.OR.240 – Personnel Requirements: Cargolux identifies a CISO with operational authority over freight security. easyJet names a security leadership role but omits scope and reporting lines. Larger groups list accountable executives but rarely detail competency frameworks or verification processes.
- IS.I.OR.250 – Information Security Management Manual (ISMM): No ISMM is publicly available. Lufthansa Group and Air France–KLM imply its existence through governance diagrams, but without procedural transparency.
- IS.I.OR.255 – Changes to the ISMS: Change control is mentioned generically in IT governance contexts (e.g., easyJet, IAG) but is not linked to ISMS changes with aviation safety considerations.

### 4.2. *Emerging Implementation Patterns*

The analysis reveals three dominant patterns in how airlines approach the implementation of the Part-IS requirements.

One pattern is characterised by a governance-first orientation, where early emphasis is placed on formal accountability structures, executive role designation, and high-level policy statements. This approach reflects an initial organisational response to regulatory expectations, in which information security is positioned within senior management and corporate governance arrangements. Public disclosures in such cases tend to emphasise responsibility allocation rather than operational practice, and they provide limited insight into how designated roles exercise authority or interact with safety management processes under Part-IS.

A second pattern concerns the adaptation of existing information security frameworks, particularly among airlines operating certified management systems. Carriers with ISO/IEC 27001 certification, such as Lufthansa Group and easyJet, appear to extend established structures to address Part-IS requirements, drawing on familiar controls, documentation practices, and assurance mechanisms. These adaptations remain largely generic in publicly available material and show limited evidence of translation into aviation-specific contexts, such as hazard-based risk assessments that link information security threats to operational safety.

The third pattern involves the incremental integration of information security governance into existing safety management systems. Airlines such as Air France–KLM and Cargolux appear to embed information security responsibilities within established safety structures, aligning Part-IS-related activities with existing reporting, oversight, and assurance processes. This mode of integration emphasises organisational continuity and coherence, while Part-IS-specific artefacts, including dedicated Information Security Management Manuals, are less visible in public disclosures.

### 4.3. *Preparations, approach, and implementation strategies*

Publicly available material shows that none of the sampled airlines has issued a Part-IS-specific readiness statement, implementation roadmap, or formal declaration of compliance intent. The absence of such documents does not in itself imply a lack of internal activity, as preparation for regulatory compliance in security-sensitive domains often takes place without public communication. Information security measures, governance changes, and risk assessments are frequently treated as confidential, which can limit what organisations choose to disclose. At the same time, the lack of explicit reporting constrains the ability of external stakeholders to assess the state of observable readiness and

introduces uncertainty regarding the scope, maturity, and timing of implementation efforts.

In the absence of direct evidence, indications of preparatory work can instead be inferred from indirect signals in corporate reporting. Several airlines refer to the alignment of internal governance structures with evolving regulatory requirements in environmental, social, and governance disclosures, which likely encompass Part-IS alongside other regulatory initiatives. Structural changes within organisations provide further indications, such as the establishment of information security committees with direct reporting lines to executive management, suggesting increased formalisation of oversight. Other airlines refer to updates of operational policies that incorporate aviation-specific cybersecurity requirements without explicitly naming Part-IS, reflecting a tendency to frame compliance activities in broader or more generic terms. References to cross-domain coordination mechanisms, including joint safety and security committees, further indicate attempts to integrate information security considerations into existing organisational structures and management processes.

### 4.4. *Implications for Readiness*

The gap analysis reveals that while foundational ISMS elements are present across the sector, full Part-IS alignment will require: documented aviation-specific risk assessment methodologies and integrated incident reporting linking information security to occurrence reporting; transparent role definitions and competency verification for key personnel; dedicated ISMMs and ISMS change control processes tied to safety outcomes. Airlines with ISO/IEC 27001 certification are structurally advantaged but must close the contextualisation gap. This "contextualisation gap" refers to the difference between generic ISMS structures-often based on ISO/IEC 27001-and the aviation-specific tailoring needed to address hazards, integrate with occurrence reporting, and link change control to safety outcomes. The limited public disclosure of Part-IS preparations may be a strategic choice, but it reduces sector-wide transparency and hinders external benchmarking. If regulatory authorities introduce mandatory public compliance statements, operators without documented, aviation-specific frameworks will face compressed timelines for compliance demonstration.

## 5. Discussion

The discussion is organised around the three institutional pillars, regulative, normative, and cultural cognitive, followed by cross cutting reflections on transparency, regulatory coherence, and implications for practice and theory.

Across all six airlines, the findings indicate strong alignment with the regulative pillar. Formal governance structures, designated accountable executives, and high-level information security statements are consistently visible in corporate disclosures. This pattern reflects the dominant role of coercive regulatory pressure in aviation, where compliance is mandatory and publicly scrutinised (Meyer and Rowan, 1977; Scott, 2005). Airlines appear structurally prepared in that responsibility, oversight, and reporting lines are defined and linked to emerging security requirements.

At the same time, this alignment is largely procedural. As observed during earlier regulatory transitions, particularly the introduction of Safety Management Systems (ICAO, 2013; Kurt and Gerede, 2018), formal structures tend to precede operational integration. Pillar tagging shows that much of the documented activity remains at the level of formal acknowledgement rather than demonstrable practice. Rules are recognised and governance frameworks are in place, but limited public evidence shows how these arrangements influence daily operations. In institutional terms, regulative conformity supports legitimacy without necessarily indicating embedded effectiveness.

The normative pillar highlights the role of professional standards and shared frameworks in shaping organisational behaviour. Here, the findings suggest partial alignment. Many airlines rely on established standards such as ISO IEC 27001 and the NIS 2 Directive, which offer mature governance principles and technical controls. However, these frameworks are intentionally generic and require adaptation to aviation specific and to safety contexts. The analysis shows that such adaptation remains uneven. While some airlines demonstrate structured approaches to risk management and

training, explicit links between information security controls and flight safety hazards are rarely made public. This pattern is consistent with previous research showing that sector specific integration often lags behind formal certification (Melin et al., 2018; Fonseca Herrera et al., 2021). Without stronger normative convergence through shared guidance, professional communities, or industry benchmarks, the diffusion of consistent Part IS practices is likely to remain fragmented.

The cultural cognitive pillar represents the least developed dimension of institutionalisation. Public disclosures provide limited evidence that information security has become a taken for granted organisational value comparable to safety. Instead, it is often presented as a specialised or technical function rather than a cross-cutting element of operational decision making. Indicators such as the absence of publicly available Information Security Management Manuals, limited integration of cyber incidents into occurrence reporting, and scarce reference to aviation specific risk classification suggest that cultural embedding is still emerging. Similar dynamics were observed during early phases of SMS implementation, when formal systems were introduced before safety values were fully internalised (Gerede, 2015). In this sense, information security appears to be at an early stage of cultural institutionalisation.

A theme that cuts across all three pillars is the transparency gap. None of the sampled airlines publishes a Part IS readiness statement, implementation roadmap, or detailed procedural disclosure. While restricted disclosure is understandable in a security sensitive domain, it constrains external assessment and weakens sector wide learning. From an institutional perspective, organisations perform the formal aspects of compliance while limiting visibility into practice (Meyer and Rowan, 1977). This separation reduces opportunities for benchmarking and mutual learning across the industry. Moderated transparency mechanisms, such as structured readiness statements or thematic reporting, could support comparison without exposing sensitive information and are consistent with the public interest role of aviation oversight.

For regulators, the findings indicate that coercive instruments alone are unlikely to achieve full institutionalisation of Part IS. While enforcement establishes baseline compliance, sustained integration depends on normative and cultural support. Interpretive guidance, capacity building initiatives, and cross industry forums can help translate regulatory requirements into operational practice. Guidance from EASA that illustrates how information security management can be integrated with existing safety management systems may support contextualisation and promote more consistent implementation across the sector.

## 6. Conclusion and final remarks

This study examined how European airlines are preparing for EASA Part IS implementation and how these efforts reflect institutional processes of regulatory adoption. By combining systematic document analysis with pillar tagging, the research assessed governance structures, procedural measures, and the integration of information security into organisational practices using only publicly available data. The findings show that airlines are structurally prepared: formal governance arrangements, designated accountable executives, and references to international standards are consistently visible. However, the translation of these formal structures into aviation-specific operational practice remains uneven. Evidence of integrated risk management, dedicated Information Security Management Manuals, and cultural embedding of information security is limited, revealing a gap between procedural compliance and deeper institutionalisation.

These findings have several implications. Structurally, airlines have created the foundations for Part IS compliance, but achieving full regulatory maturity will require more than formal alignment. Effective implementation depends on the convergence of coercive, normative, and cognitive forces: regulatory compliance must be supported by professional norms, shared guidance, and cultural adoption. Regulators and auditors can facilitate this process by providing interpretive guidance, capacity-building, and moderated transparency mechanisms that enable benchmarking without compromising sensitive information. The results also underscore the importance of integrating information security management with existing safety management systems to ensure both operational safety and digital trust.

The study has limitations. It relies exclusively on public disclosures, which may underrepresent internal practices, and does not capture real-time organisational behaviour or employee perceptions. The transparency gap observed highlights that some regulatory activities may be underway but remain unreported, limiting external verification. Future research could address these gaps by combining public document analysis with field studies, interviews, or surveys to capture internal practices and perceptions. Comparative studies across jurisdictions could further explore how Part IS implementation interacts with national regulatory frameworks, and longitudinal research could track their co-evolution.

**References**


Bjorck, F. (2004). Institutional theory: a new perspective of research into IS/IT security in organisations. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences,* IEEE.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40.

David, R. J., Tolbert, P. S., & Boghossian, J. (2019). Institutional theory in organization studies. *Oxford research encyclopedia of business and management*.

DiMaggio, P. J., & Powell, W. W. (2000). The iron cage revisited institutional isomorphism and collective rationality in organizational fields. *Economics meets sociology in strategic management* (pp. 143-166). Emerald Group Publishing Limited.

Fonseca-Herrera, O., Rojas, A., & Florez, H. (2021). A model of an information secutiry management system based on NTC-ISO/IEC 27001 standard. *Procedia Computer Science, 192*, 4804-4813.

Gerede, E. (2015). A study of challenges to the success of the safety management system in aircraft maintenance organizations in Turkey. *Safety Science, 73*, 106-116.

ICAO (2013). Safety Management Manual. Third Edition. International Civil Aviation Organization. Available online at https://www2023.icao.int/SAM/Documents/2017-SSP-GUY/Doc%209859%20SMM%20Third%20edition%20en.pdf

ICAO (2018). Safety Management Manual. Fourth Edition. International Civil Aviation Organization. Available online at https://www.icao.int/safety-management/guidance-material.

Kurt, Y. & Gerede, E. (2018). An assessment of aviation management system applications from the new institutional theory perspective. *Uluslararası Yönetim İktisat ve İşletme Dergisi, 14*(1), 97-122.

Melin, U., Axelsson, K., & Löfstedt, T. (2018). Understanding an integrated management system in a government agency- focusing institutional carriers. *International Conference on Electronic Government*, 15-28.

Meyer, J. & Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *Americal Journal of Sociology, 83*(2), 340-363.

Morgan, H. (2022). Conducting a qualitative document analysis. The Qualitative Report, 27(1), 64-77.

NIST (2022). Cybersecurity-A critical component of Industry 4.0 implementation. National Institute of Standards and Technology. Available online at https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-critical-component-industry-40-implementation

Paraschi, E.P., Georgopoulos., A., & Papanikou, M. Safety and security implications of crisis-driven austerity HRM practices in commercial aviation: a structural equation modelling approach. *Safety Science, 147*, 105570.

Scott, W. R. (2005). Institutional theory: Contributing to a theoretical research program. Great minds in management: The process of theory development, 37(2), 460-484.

Suri, H. (2011). Purposeful Sampling in Qualitative Research Synthesis. Qualitative research journal, 11(2), 63-75.

Tina Dacin, M., Goodstein, J., & Richard Scott, W. (2002). Institutional theory and institutional change: Introduction to the special research forum. Academy of Management Journal, 45(1), 45-56.

Ukwandu, E., Ben-Farah, M., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., & Bellekens, X. (2022). Cybersecurity challenges in the aviation industry: A review of current and future trends. *Aerospace, 9(*3), 1–23.

von Solms, R. & van Niekerk, J. (2013). From information security to cybersecurity. *Computers and Security, 38*, 97-102.