Cybersecurity Maturity Framework for International Airports in Malaysia: A Systematic Literature Review (SLR)

Suzaliana Samuri[1], Mohd Fared Abdul Khir[2,] , Zahari Mohd Amin[3], and Mohammad FakhrulNizam Mohammad[4]

[1,2]Faculty of Science and Technology,
Universiti Sains Islam Malaysia (USIM), 71800, Nilai, Negeri Sembilan, Malaysia
[3]Faculty of Information Management,
UiTM Selangor Branch, Puncak Perdana Campus, 40150 Shah Alam, Selangor, Malaysia
[4]Malaysian Institute of Aviation Technology (MIAT), Universiti Kuala Lumpur,
47200 Shah Alam, Selangor, Malaysia

Received Date: 15 September 2023
Acceptance Date: 20 September 2023
Published Date: 1 November 2023

Abstract. This paper presents an approach for conducting a systematic literature review on the Cybersecurity Maturity Framework (CSMF) specific to international airports in Malaysia. The systematic review comprises three stages: identification, screening, and included. Rigorous screening of results was accomplished by applying predetermined inclusion and exclusion criteria. This systematic literature review comprehensively explains the prevalent frameworks, models, and standards for evaluating cybersecurity maturity. The insights derived from this review substantially informed the development of a cybersecurity maturity framework tailored to international airports in Malaysia.

Keywords: Systematic literature review, cybersecurity framework, cybersecurity maturity framework, cybersecurity maturity framework, information management.

1 Introduction

In the modern landscape, cybersecurity stands out as a paramount sector. The surge in cybercrime occurrences has compelled organizations to adopt robust security programs more systematically (Calvin NOBLES, 2022). During the year 2022, CyberSecurity Malaysia's Cyber999 assistance center documented a cumulative count of 7,292 cyber incidents across eight distinct categories of incidents, namely spam, intrusion, malicious code, denial of service, fraud, intrusion attempts, content-related issues, and vulnerability reports. This marked a reduction of 2,724 incidents from the previous year's tally of 10,016 in 2021. The most frequently reported incidents were online fraud, malicious code, and intrusion.

In the realm of aviation safety, cybersecurity plays a pivotal role (Lykou et al., 2018). In pursuit of consistent, dependable, and sustainable service delivery, airports prioritize growth, efficiency, safety, and security. This study addresses a pertinent issue: the absence of a cybersecurity maturity framework (CSMF) tailored for airports that local international airports can readily adopt or reference. While various research endeavors have outlined the fundamental attributes that gauge cybersecurity maturity, there is a gap in the literature regarding pinpointing the precise amalgamation of factors necessary to establish a secure organizational environment. Furthermore, a step-by-step methodology for creating a comprehensive CSMF has yet to be extensively explored. The essence of this study rests upon the need to shed light on the crucial interplay between technology, human factors, and processes, which collectively contribute to attaining benefits and realizing success in cybersecurity endeavors (Edwards, 2016).

Numerous studies highlight the financial sector as the most susceptible to cyber risks and fraud (Lagazio et al., 2014; Leukfeldt et al., 2017). However, the aviation industry faces significant vulnerability and is increasingly becoming a focal point for cyberattacks due to its perceived susceptibility (Meyer, 2018). Holding an extensive reservoir of personal and sensitive information, the aviation sector is responsible for safeguarding a substantial amount of data. Pertinent statistics indicate a staggering volume of data generated by airlines, correlating with approximately 4,358 million passengers, underscoring the aviation industry's status as a prime target for cybercriminals (Meyer, 2018).

2 Background and Related Work

The International Air Transport Association (IATA) has characterized cybersecurity as encompassing a range of tools, policies, security measures, guidelines, risk management strategies, training protocols, best practices, assurance mechanisms, and technologies designed for safeguarding the cyber environment and an organization's assets. Despite robust systems in numerous airports to counter prevalent hacking risks, there has been a tendency to overlook a comprehensive strategy for determining an appropriate cybersecurity maturity model that can effectively evaluate their level of cybersecurity readiness. Moreover, the airport industry is seen as the pioneer in the adoption of advanced technologies given the increasing number of air travelers (Lykou, Anagnostopoulou, and Gritzalis, 2019); at the same time, it is regarded as a highly regulated industry that continuously improves on the level of security is needed and justifiable.

Numerous cybersecurity maturity frameworks are at the disposal of cybersecurity professionals within the industry to assess the cybersecurity maturity of organizations. These established frameworks enable the determination of an organization's current cybersecurity maturity level, providing a foundation for charting a path toward achieving the desired level of maturity. Despite the critical role of a cybersecurity framework in safeguarding organizations against cyber threats, airports often need help formulating an appropriate framework for enhancing their cybersecurity maturity.

With a clear framework, airports find it easier to make well-informed investments in the proper security measures. Ineffectively implemented security measures lead to subpar cybersecurity and lower cybersecurity maturity. By investing in state-of-the-art security measures, organizations can shield themselves from cyberattacks leading to data breaches and financial losses. An airport might self-assess and certify its cybersecurity posture using the CSMF.

2.1 Cybersecurity Framework and Cybersecurity Maturity Framework

Industry professionals employ established cybersecurity frameworks to evaluate cyber risks and ascertain the cybersecurity maturity level within their organizations. Among the frequently utilized cybersecurity frameworks are shown in Table.

Table 1: Frequently Utilized Cybersecurity Frameworks

Category	**Title**	**Source**
Framework	NIST Cybersecurity Framework	The US National Institute of Standards and Technology
	ISO/IEC 27000 Family	The International Organization of Standardization and the International Electrotechnical Commission
	CIS Critical Security Control	Center of Internet Security
	Control Objectives of Information Technologies (COBIT)	Information Systems Audit and Control Association (ISACA)
Maturity Model	National Initiative for Cybersecurity Education Capability Maturity Model (NICE)	The US National Institute of Standards and Technology
	Community Cybersecurity Maturity Model (CCSMM)	UTSA Center for Infrastructure Assurance and Security
	Cybersecurity Capability Maturity Model (C2M2)	US Department of Energy
	Open Information Security Management Maturity Model (OISM3)	The Open Group

2.2 Cybersecurity Maturity Level

Cybersecurity maturity levels serve as a valuable tool for technology airports, aiding them in assessing their present cybersecurity status and identifying areas that require attention to reach their desired maturity level. This framework can offer a comprehensive understanding of their cybersecurity posture and the deficiencies that must be addressed in their journey towards achieving their target maturity level Abdullahi Garba et al. (2020).

The level of cybersecurity maturity is gauged by implementing effective cybersecurity and data protection measures within an organization. The effectiveness of these controls, in turn, hinges on the extent of cybersecurity investments allocated to mitigate identified cyber risks. Understanding these cybersecurity maturity levels is particularly crucial for technology startups, as it empowers management to allocate cybersecurity investments judiciously. This allows them to tailor their cybersecurity measures to align with the airports' current and desired maturity levels, ensuring an appropriate and well-fitted cybersecurity strategy.

According to Ngoc et al. (2016), 12 cyber security maturity models have been identified as having three to five maturity levels. From a maturity scale of one to five, an airport with level one in the maturity scale has the lowest cyber security posture with fragile cyber defenses, which makes the airport susceptible to cyber-attacks. On the other hand, an airport with a four on the maturity scale has an above-average cyber security posture with solid defenses against malicious perpetrators. Since every country may have differences in terms of the environment and regulatory requirements, it is pertinent to ensure that the adoption of the framework would be able to fulfill the general or specific needs of the industry (in this case, the airport industry).

3 Systematic Literature Review

A systematic literature review was done to identify the frameworks, models, and standards commonly employed for evaluating cybersecurity maturity. The main objectives are to 1) find literature published about the cybersecurity maturity framework, and 2) to find the variables involved in the cybersecurity maturity framework. This systematic review adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). PRISMA aims to improve the transparency and quality of systematic reviews by providing a structured framework for reporting the entire review process (Liberati et al., 2009). To fulfill the requirements of PRISMA, the required sections have structured this paper, the PRISMA flow diagram, as shown below.

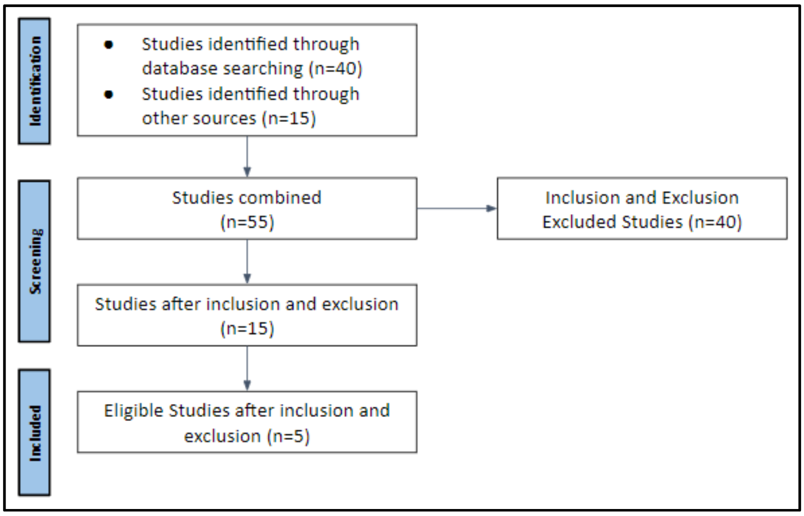

Identification
Screening
Included
Studies identified through database searching (n=40)
Studies identified through other sources (n=15)
Studies combined (n=55)
Inclusion and Exclusion Excluded Studies (n=40)
Studies after inclusion and exclusion (n=15)
Eligible Studies after inclusion and exclusion (n=5)

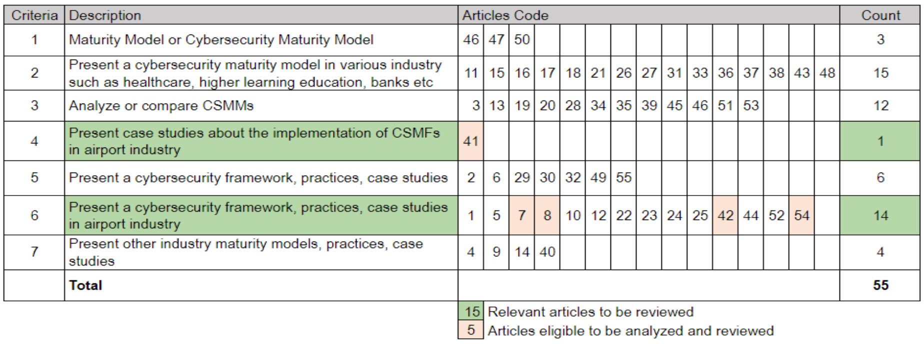
Figure 1: SLR flow diagram using PRISMA

This SLR model was divided into three stages: identification, screening, and included. During the identification stage, several databases were chosen for the literature search. These databases were chosen based on the most popular and highly regarded as an essential source of information searching and retrieval. The screening stage is where the process of inclusion and exclusion takes place. The studies found may not be accurate to the needs of this research and have been excluded from the list of literature, only precise and suitable literature is included in the analysis. The last stage is included, where the eligible studies were analyzed. The information found was used to produce the result of the research.

3.1 Identification

This study gathered research articles from the following digital databases: Science Direct, ResearchGate and IEEE. This study targeted research articles from 2018 to 2022 using the following keywords: ‘‘Cybersecurity Framework’’; ‘‘Cybersecurity Maturity, ‘‘Cybersecurity Framework’’ AND ‘‘Airports’’; ‘‘Cybersecurity Maturity Framework’’ AND ‘Airports’’. As a result of the articles search, 55 related articles were retrieved from the identified four digital databases and the other identified sources. All papers were further analyzed to ensure that there was no duplication. Although duplicates of articles are difficult to ascertain, it is suggested that the publication of articles for SLR consisting of the data extractor or repetition in the extractions must be reported (Liberati et al., 2009). As such, there were 55 related articles qualified for consideration in this study (See Table 2).

Table 2: Criteria for the practical screening and List of qualified articles



Criteria	Description	Articles Code															Count
1	Maturity Model or Cybersecurity Maturity Model	46	47	50													3
2	Present a cybersecurity maturity model in various industry such as healthcare, higher learning education, banks etc	11	15	16	17	18	21	26	27	31	33	36	37	38	43	48	15
3	Analyze or compare CSMMs	3	13	19	20	28	34	35	39	45	46	51	53				12
4	Present case studies about the implementation of CSMFs in airport industry	41															1
5	Present a cybersecurity framework, practices, case studies	2	6	29	30	32	49	55									6
6	Present a cybersecurity framework, practices, case studies in airport industry	1	5	7	8	10	12	22	23	24	25	42	44	52	54		14
7	Present other industry maturity models, practices, case studies	4	9	14	40												4
	Total																**55**

15	Relevant articles to be reviewed
5	Articles eligible to be analyzed and reviewed

3.2 Screening

This section summarizes this study's inclusion and exclusion criteria to ensure a targeted search concerning the research questions. Inclusion and exclusion criteria provide that the selected studies are relevant and related to the current research. This criterion is vital to systematic review as it will determine the most accurate literature accessed in this SLR. The criteria defined in this stage was only for articles in journals or proceedings written in English and full-text articles by searching using relevant keywords in the title, abstract or content of the paper (See Table 3). The screening stage, or practical screening (Okoli & Schabram, 2010), ensures that only relevant articles are selected for analysis (Kitchenham et al., 2010).

Table 3: Inclusion and Exclusion Criteria

No	Criteria	Decision
1	Keywords existed in the title, abstract, or content of the paper	Inclusion
2	Papers from Journals articles and reports	Inclusion
3	Full-text article	Inclusion
4	Papers that are duplicated within the searched documents and sources	Exclusion
5	Papers are written other than in the English language	Exclusion
6	Papers published before the year 2000	Exclusion

Based on the listing of articles in Table 2, it was discovered that 15 relevant articles met the criteria defined in this stage, which are the articles labeled 41, 1, 5, 7, 8, 10, 12, 22, 23, 24, 25, 42, 44, 52 and 54. Summary details of the 15 articles are as follows:

Table 4: List of screened articles

No	Article ID	Author, year	Title	Framework Used	Industry
1	41	Malhotra et al. (2021)	Cyber Security Maturity Model Capability at The Airports	Cybersecurity Capability Maturity Model Certification (CCMMC)	Aviation/ Airports
2	1	Suciu et al. (2018)	Cyber-attacks – the Impact over Airports Security and Prevention Modalities	Airports Cyber-attacks Prevention Methodology (DDoS Attacks & Blended Attacks)	Aviation/ Airports
3	5	Ramon et al. (2018)	Cybersecurity Literature Review and Efforts Report	(i) NIST Cyber-Physical Systems Framework; (ii) DHS Cybersecurity Capability Maturity Model (C2M2); (iii) Center for Internet Security's (CIS); (iv) Critical Security Controls (CSC); (v) OWASP Application Security; (vi) Verification Standard (ASVS); (v) NIST Cybersecurity Framework (CSF)	Transporta tion/ Land
4	7	Lykou et al. (2018)	Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls	(i) European Norm (EN) 16495 standard for Air Traffic Management; (ii) International Society of Automation (ISA)/ International Electrotechnical Commission (IEC)-62443; (iii) National Institute of Standards and Technology (NIST)-Special Publication 800-53 Security and privacy controls; (iv) NIST 800-82 Guide to Industrial Control Systems (ICS) Security	Aviation/ Airports
5	8	Lykou et al. (2018)	Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience	(i) Technical Good Practices; (ii) Organizational Good Practices (iii) Policies and Standards	Aviation/ Airports
6	10	Hyodong Ha and Ook Lee. (2019)	An Empirical Study on Information Integration System Maturity Model for an Airport	Information Integration System Maturity Model using CMMI	Aviation/ Airports
7	12	Koroniotis et al. (2020)	A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports	Not specify	Aviation/ Airports
8	22	Florido-Benítez (2020)	Identifying cyber security risks in Spanish airports	Not specify	Aviation/ Airports
9	23	Aruna Rajapaksha and Dr. Nisha Jayasuriya (2020)	Smart Airport: A Review on Future of the Airport Operation	Airport 4.0	Aviation/ Airports

No	Article ID	Author, year	Title	Framework Used	Industry
10	24	IATA	Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation	(i) International Instruments and Documents; (ii) European Regulations and Documents; (iii) National Documents and Guidance; (iv) Aviation Industry Cyber Specific Documents; and (v) Other Relevant Cyber Industry Framework	Aviation/ Airports
11	25	Hall et al. (2021)	Advancing Cyber Resilience in Aviation: An Industry Analysis	(i) Strategic Approach; (ii) Tactical Approach; (iii) Operative Approach; (iv) Technical Approach	Aviation/ Airports
12	42	Ukwandu et al. (2021)	Cyber-Security Challenges in the Aviation Industry: A Review of Current and Future Trends	Not specify	Aviation/ Airports
13	44	Global Syndicate for Mobility Cybersecurity (GSMC)	Securing the Skies: The Importance of Cybersecurity in the Air Mobility Sector	Not specify	Aviation/ Aerospace
14	52	Nobles et al (2022)	The Need for a Global Aviation Cybersecurity Policy	Not specify	Aviation/ Airports
15	54	Murphy et al 2015	Guidebook on Best Practices for Airport Cybersecurity	Not specify	Airports

Most papers scrutinize the adoption of cybersecurity measures and optimal methodologies to enhance cyber resilience. The analysis comprehensively assesses security deficiencies across various domains, encompassing technical best practices, organizational protocols, policies, and standards. Specifically, article 41 (Malhotra et al., 2021) is a case study article that explicitly discusses the implementation of CSMF in the airport industry. Meanwhile, the other 14 articles addressed the airport industry's general cybersecurity framework, practices or case studies.

3.3 Included

This stage aims to analyze the articles reviewed using the SLR method. In ensuring the articles to be analyzed and reviewed are mainly related to the purpose of this study, several criteria statements were set to filter the related articles, as shown in Table 5. A more refined filtering step followed the initial screening process to ensure that the most appropriate papers were chosen for inclusion in the review. The purpose of the criteria statement is to ensure the articles selected are related to the cybersecurity framework and cybersecurity maturity framework. As described by Anwar (2015), this filtering process involves the application of relevance criteria. Based on the final article analysis criteria, five articles were eligible to be analyzed and reviewed: articles 41, 7, 8, 42, and 54. Papers are deemed irrelevant if they meet any of the following criteria:

Table 5: Relevance Criteria

No	Criteria	Decision
1	Its focus is not on the cybersecurity framework or cybersecurity maturity framework	Exclude
2	It does not mention the cybersecurity framework or cybersecurity maturity framework	Exclude
3	It does not have any explanation on the cybersecurity framework or cybersecurity maturity framework its content	Exclude
4	The framework is not in a cyber-related area	Exclude

4 Findings

This study's data analysis was performed based on the output of the SLR methods that had retrieved five relevant articles identified as articles 41, 7, 8, 42 and 54, as stated in Section 3.2. PRISMA method is a widely used approach used in previous SLR studies, such as in the establishment of a cybersecurity framework for technology startups (Marican et al., 2023), the assessment of IR 4.0 readiness tool (Demong et al., 2021) and use of agent-based modeling in the visitor management system (Štekerová, Zelenka and Kořínek, 2022) is adopted to guide the retrieval of relevant information.

Article number 7 discusses the measures and best practices of cybersecurity measures to enhance the resiliencies of cyber strategy at the airport (Lykou, G. et al., 2018). It is a comprehensive study that covers several areas of discussion on technical and organizational practices inclusive with their requirement for the inclusion of standards and policies. The study proposes the importance of security awareness, which is essential in emerging new technologies. In the same year, article number 8 was written by Lykou et al. (2018), specifically focusing on cyber resilience controls and mitigation of threats. As Lykou G. et al. (2018) suggested, article number 54 also indicates the importance of developing cybersecurity policies to enhance airports' cybersecurity strategies. Although both studies suggested the same, this study found that there are still huge gaps that need to be filled, which are the need for the elements for the discussion on the established cybersecurity framework.

Earlier, Ukwandu et al. (2021) addressed integrating and embedding IT tools in the aviation industry into some mechanical devices, which has triggered some concerns about security issues within the industry. Their study provided more motivation for establishing the cybersecurity framework in the airport industry. The scope of the study equipped the cybersecurity stakeholders in the aviation industry to initiate more proactive actions in securing their industry from the cyber incidents that might affect the industry and its customers. This aligns with the earlier study by Murphy R.J. et al. (2015) that the raised awareness of cybersecurity issues would let the airport industry be more proactive in overcoming this issue. For instance, many industries, including airports, have mobilized various action plans accompanying the cybersecurity strategy, such as appointing a Chief Information Security Officer (CISO), continuous employee training, technical countermeasures strategy, policies and procedures establishment, etc. In addition to the lack of studies addressing the cybersecurity issues within the airport industry, a review of the article also identified that there are countable studies that highlighted the actual condition of the industry. However, the need to understand the actual situation in the industry has been equipped by Malhotra et al. (2021). According to Malhotra, the aviation industry had been regarded as an easy target by hackers, therefore standing at a higher potential risk. This may hold as the industry is perceived to be keeping highly sensitive and personal data of various profiles of customers.

5 Conclusion

The issues and challenges of ensuring the higher protection of organizations and industry surround the physical or infrastructure context, information and data security. This study addresses the limitations of past studies on the need for the availability and existence of a cybersecurity framework within the airport industry. Undoubtedly, many studies focus on establishing and executing the framework, but this study proved its huge gaps by conducting SLR of previous studies between 2018 and 2022. Several studies discussed cybersecurity from the analyzed article; however, most of the studies are inclined towards focusing on other cybersecurity concerns, such as its issues and challenges, the recommendations for best practices, mitigation control, and countermeasures. Therefore, there is a need for more studies focusing on establishing a cybersecurity maturity framework specifically for the airport industry. Establishing a cybersecurity maturity framework would benefit the industry by allowing them to assess their risk level, understand organization security posture and healthiness and enable the involved organizations to quantitatively measure their return on their IT investment (Marican et al., 2023). Hence, this study had its novel contributions and could be one of the first to address these vast gaps within cybersecurity and the airport industry. In addition to successfully identifying the gaps in the lack of cybersecurity framework in the airport industry, future studies would have a practical contribution. For instance, this study also found out that several industry-based cybersecurity frameworks could be adopted to assess the maturity of airport cybersecurity levels, such as the International Organization for Standardization (ISO)IEC 27001, National Institute of Standards and Technology (NIST), Cyber Security Capability Maturity Model (C2M2), Capability Maturity Model Integration (CMMI) and Center for Internet Security (CIS) framework. Therefore, this study proposes that there could be more opportunities to address the gaps identified by identifying the proper cybersecurity maturity framework exclusively defined and established for the airport industry. Since this study only extracts articles from a limited number of databases, which are Science Direct, ResearchGate and IEEE, related articles published in the other databases may not be seen in the analysis. Thus, expanding the research to include other databases is also recommended. As the focus of this study is to identify the previous studies found in establishing a cybersecurity maturity framework for the airport, other researchers interested in further similar types of studies may benefit from the discussion in this study.

Acknowledgments

Acknowledgments are placed before the references. Add information about grants, awards, or other types of funding that you have received to support your research.

References

Abdullahi Garba, A., Musa Bade, A., Yahuza, M., &amp; Nuhu, Y. (2020). Cybersecurity Capability Maturity Models&nbsp; Review and application domain. International Journal of Engineering &amp;amp; Technology, 9(3), 779. https://doi.org/10.14419/ijet.v9i3.30719

Adhikari, S. (2020). An analysis of AIAA aviation cybersecurity framework in relation to NIST, COBIT and DHS Frameworks. AIAA AVIATION 2020 FORUM. https://doi.org/10.2514/6.2020-2930

Advancing Cyber Resilience in Aviation: An Industry Analysis. World Economic Forum. (n.d.). Retrieved June 12, 2022, from https://www.weforum.org/whitepapers/advancing-cyber-resilience-in-aviation-an-industry-analysis

Anwar, N. (2015). The Impact of Information Technology Infrastructure Flexibility on Strategic Use of Information Systems. Pacific Asia Conference on Information Systems (PACIS), 3, Paper 271.

Al-Fedaghi, S., &amp; Haider, A. (2015). System integration: Case study of an airport information system. The Proceedings of the 2nd International Conference on Industrial Application Engineering 2015. https://doi.org/10.12792/iciae2015.058

Aviation cybersecurity strategy - ICAO. (n.d.). Retrieved June 12, 2022, from https://www.icao.int/cybersecurity/documents/aviation%20cybersecurity%20strategy.en.pdf

Building cybersecurity capability, maturity, resilience - NIST. (n.d.). Retrieved June 11, 2022, from https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/TueAM2_2_CMMI.pdf

Calvin Nobles, C., Burrell, D., & Waller, T. (2022). The need for a global aviation cybersecurity defense policy. Land Forces Academy Review, 27(1), 19–26. https://doi.org/10.2478/raft-2022-0003

Cybersecurity Capability Maturity Model (C2M2), version 2.0, July 2021. (n.d.). Retrieved June 11, 2022, from https://c2m2.doe.gov/C2M2%20Version%202.0%20July%202021.pdf

Compilation of cyber security regulations, standards, and guidance ... (n.d.). Retrieved June 12, 2022, from https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regulations-standards-and-guidance_3.0.pdf

Demong, N.A.R. et al. (2021) ‘Industry 4.0 readiness assessment tool: a conceptual framework from social well-being perspective’, Romanian Journal of Information Technology and Automatic Control, 31(1), pp. 53–64. Available at: https://doi.org/10.33436/v31i1y202104.

IATA - fact sheet - cyber security. (n.d.). Retrieved June 11, 2022, from https://www.iata.org/en/iata-repository/pressroom/fact-sheets/fact-sheet---cyber-security/

Identifying cyber security risks in Spanish airports. cyber security: A ... (n.d.). Retrieved June 12, 2022, from https://www.researchgate.net/publication/349711898_Identifying_cyber_security_risks_in_Spanish_airports_Cyber_Security_A_Peer-Reviewed_Journal

Kitchenham, B. et al. (2010) ‘Systematic literature reviews in software engineering – A tertiary study’, Information and Software Technology, 52, pp. 792–805. Available at: https://doi.org/10.1016/j.infsof.2010.03.006.

Liberati, A. et al. (2009) ‘The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration’, Journal of Clinical Epidemiology, 62(10), pp. e1-34.

Lykou, G., Anagnostopoulou, A., &amp; Gritzalis, D. (2018). Implementing cyber-security measures in airports to improve Cyber-Resilience. 2018 Global Internet of Things Summit (GIoTS). https://doi.org/10.1109/giots.2018.8534523

Lykou, G., Anagnostopoulou, A., &amp; Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors, 19(1), 19. https://doi.org/10.3390/s19010019

Malhotra, Ojaswini; Dey, Sharmistha; Foo, Ernest; and Helbig, Mardé, "Cyber Security Maturity Model Capability at The Airports" (2021). ACIS 2021 Proceedings. 55.

Marican, M.N.Y. et al. (2023) 'Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review', IEEE Access, 11(August 2022), pp. 5442–5452. Available at: https://doi.org/10.1109/ACCESS.2022.3229766.

Murphy, R. J., Sukkarieh, M., Haass, J., &amp; Hriljac, P. M. (2015). Guidebook on best practices for airport cybersecurity. Transportation Research Board.

N. T. Le and D. B. Hoang, ''Can maturity models support cyber security?'' in Proc. IEEE 35th Int. Perform. Comput. Commun., Dec. 2016, pp. 1–7.

Rea-Guaman, A. M., Sanchez-Garcia, I. D., Feliu, T. S., & Calvo-Manzano, J. A. (2017). Maturity models in cybersecurity: A systematic review. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI). https://doi.org/10.23919/cisti.2017.7975865

Štekerová, K., Zelenka, J. and Kořínek, M. (2022) 'Agent-Based Modelling in Visitor Management of Protected Areas', Sustainability (Switzerland), 14(19). Available at: https://doi.org/10.3390/su141912490.

Suciu, G., Scheianu, A., Vulpe, A., Petre, I., &amp; Suciu, V. (2018). Cyber-attacks – the impact over airports security and prevention modalities. Advances in Intelligent Systems and Computing, 154–162. https://doi.org/10.1007/978-3-319-77700-9_16

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of Cybersecurity Maturity Assessment Methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. JOIV : International Journal on Informatics Visualization, 4(4), 225. https://doi.org/10.30630/joiv.4.4.482