Terrorism – Studies, Analyses, Prevention, 2026, no. 9: 375–393

https://doi.org/10.4467/27204383TER.26.015.23798

Varia

The civil aviation security system as an example of strengthening critical infrastructure resilience

Karol Dymek

Independent author

https://orcid.org/0009-0004-3946-8695

Introduction

After more than a decade of working in the field of civil aviation security at various levels within organisations conducting or supervising aviation activities – including serving as a quality control auditor at both the European and national levels – I have become convinced that no solutions exist that can guarantee a one hundred percent security. The pace of change in today's world is giving rise to new threats and new sources from which they originate. The media are increasingly reporting on threats to online banking, on social media account hacks aimed at spreading disinformation in connection with the war in Ukraine, and on fire, for example in shopping centres[1] or in courier shipments that catch

[1] *Zarzuty w związku z pożarem hali przy ul. Marywilskiej 44* (Eng. Charges relating to the fire at the shopping centre on Marywilska Street 44), Prokuratura Krajowa, 12 V 2025, https://www.gov.pl/web/prokuratura-krajowa/zarzuty-m44 [accessed: 15 III 2026].

fire[2]. The aviation industry, which is regarded as one of the safest modes of transport, is not immune to incidents that pose a threat, despite its high level of regulation and numerous security procedures. It should be borne in mind that airlines and airports are part of critical infrastructure (CI). There are many specialist professional groups within the aviation industry whose role is to ensure the smooth and safe operation of the entire system. To make this possible, aviation activities are subject to strict legal regulations, numerous rules and procedures.

It is said in the industry that most aviation regulations are written in blood. The event that changed the modern world and had a major impact on the approach to civil aviation security was the attack on the World Trade Center carried out on 11 September 2001[3].

In civil aviation, safety and security are of paramount importance. Air disasters – when they occur – often have international implications, given that the aircraft carries passengers from many different countries. The Pan Am airline has learnt the hard way that even minor breaches of safety regulations can have disastrous consequences. The company went bankrupt, partly as a result of the plane crash near the Scottish town of Lockerbie when a bomb exploded in checked-in luggage stored in the hold[4].

Civil aviation security is not limited to the elements that are immediately visible to travellers, such as the presence of security staff in the terminal or security checks on passengers and their luggage. Aviation security constitutes a complex ecosystem, encompassing suppliers

[2] *Akt oskarżenia w sprawie aktów sabotażu na rzecz rosyjskiego wywiadu* (Eng. Indictment in the case of acts of sabotage on behalf of the Russian intelligence services), Prokuratura Krajowa, 16 I 2026, https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-w-sprawie-aktow-sabotazu-na-rzecz-rosyjskiego-wywiadu [accessed: 15 III 2026].

[3] K. Izak, *Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA*, "Przegląd Bezpieczeństwa Wewnętrznego" 2021, no. 25, pp. 341–369. https://doi.org/10.4467/20801335PBW.21.033.14310.

[4] B. Makowski, I. Mazurek, *Zamach w Lockerbie. Kto stał za śmiercią 270 ofiar?* (Eng. The attack in Lockerbie. Who was responsible for the deaths of 270 victims?), Polskie Radio 24, 21 XII 2025, https://polskieradio24.pl/artykul/2236228,zamach-w-lockerbie-kto-stal-za-smiercia-270-ofiar [accessed: 15 III 2026]; M. Walków, *30 lat od jednego z największych zamachów w lotnictwie cywilnym* (Eng. Thirty years on from one of the worst civil aviation disasters), Business Insider Polska, 21 XII 2018, https://businessinsider.com.pl/wiadomosci/30-lat-od-jednego-z-najwiekszych-zamachow-w-lotnictwie-cywilnym/2p7f04t [accessed: 15 III 2026]; D. Cowan, *Lockerbie bombing suspect appears in court*, BBC, 16 XII 2023, https://www.bbc.com/news/uk-scotland-67659046 [accessed: 15 III 2026].

to airports (e.g. duty-free shops, fuel suppliers) and aircraft (e.g. catering), as well as logistics companies handling air cargo and many more. All of this forms interconnected supply chains that often extend beyond the airport grounds, reaching as far as the manufacturers of the goods in question.

My professional experience shows that the entities mentioned above have various approaches to security of goods and facilities. Particular sectors operate within different legal and financial frameworks, which means they have different priorities when it comes to security. In practice, it is sometimes the case that even meeting the basic requirements set out in the regulations concerning security[5] can be difficult for them. These requirements concern, among other things, the development of appropriate procedures, the determination of the point at which in-flight supplies or cargo become traceable and from which a restricted-access regime must be ensured, the conduct of analyses regarding groups of people who may have unsupervised access to goods and security-restricted areas, as well as the carrying out of background checks on staff, which will be discussed later in the article.

Security and safety

To begin with, it is worth clarifying the meanings of the terms 'security' and 'safety' in the aviation context. These words are often used interchangeably, which can lead to misunderstandings within the industry, as they refer to different areas.

The term *safety* refers to operational safety, i.e. the safe conduct of aviation operations both on the ground and in the air. In this context, *safety* in English concerns the prevention of accidents and incidents in the broadest sense. In simple terms, it is the aviation equivalent of health and safety at work, covering protection against threats arising from both animate and inanimate factors, i.e. threats beyond human control caused by human factor, as well as errors in organisational management, etc.

[5] This concerns the regulations regarding both international, e.g. *Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security* (Official Journal of the EU L 299/1 of 14 XI 2015), and national regulations, e.g. *Regulation of the Minister* of *Infrastructure of 2 December 2020 on the National Civil Aviation Security Programme* (Journal of Laws of 2021, item 774).

Security in English, on the other hand, refers to a set of measures taken to counter deliberate and unlawful acts. Staff carrying out aviation security tasks include, among others, those conducting security checks, as well as Police and Border Guard officers. These operations in the field of security are not limited to activities carried out exclusively by specialist services, but also include the use of security measures by staff, such as physically securing goods exempt from screening during their transport.

In everyday practice, safety and security at the airport go hand in hand. Every aircraft crew member, airport employee and person carrying out duties within the airport is obliged to comply with the requirements relating to both operational safety and aviation security.

An example of the difficulties involved in using terminology accurately can be seen in the content published on the International Civil Aviation Organization (ICAO) website. Their often inaccurate translation from English into Polish, e.g. using browser-based translation tools, leads to a blurring of the terminological distinctions between concepts. For example, in the case of documents relating to security culture – which I will discuss in more detail later – automatic translation tools incorrectly translate 'security' as 'bezpieczeństwo' rather than 'ochrona'. Therefore, the term 'screening' (kontrola bezpieczeństwa) that I have mentioned should be translated as 'kontrola ochrony', but in Polish such a phrase does not exist in the context in question and would sound absurd.

For this reason, it is particularly important to adopt a critical approach to information sources, to use AI-based tools and translation services with caution, as well as to properly understand and distinguish between security and safety regulations. The fact that certain policies, procedures and mechanisms can be effectively applied in both the security and safety domains may present an additional complication, but it can also be a significant advantage.

Consequently, the similarities in the meaning of both terms in Polish may cause confusion among those attempting to explore these two issues.

A few words on the legal basis for security

Law concerning aviation and its protection has an international scope. Common standards are derived from legislation adopted by the ICAO.

At its core is the Convention on International Civil Aviation[6] of 1944, also known as Chicago Convention, regulating civil aviation worldwide. It has established the ICAO, an organisation authorised to draft international aviation legislation. The Chicago Convention comprises as many as 19 annexes covering a wide range of topics, including civil aviation security (Annex 17)[7]. In addition, the ICAO publishes a manual for states and organisations implementing civil aviation security regulations[8], which is a restricted-access document.

In Poland, the regulations are governed by the Chicago Convention, however, due to Poland's membership in the European Union, regulations of the European Commission and the Council of Europe on civil aviation security apply within Polish territory. The legal basis for the civil aviation security system is the *Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002*[9]. In this regulation, an interpretation for the application of Annex 17 to the Chicago Convention was established. It harmonises the requirements relating to key elements of the civil aviation security system across the entire EU. In addition to setting out the general scope of Member States' responsibilities, this act also stipulates the obligation to adopt detailed implementing acts at national level. Annex I to this regulation[10] lists 12 aspects of civil aviation security, including airport security, aircraft security, as well as cargo and mail security.

The Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security of 2008 can be regarded as a kind of constitution for civil aviation security in the EU, for which implementing regulations had to be issued. The most important of them is

[6] *Convention on International Civil Aviation, signed in Chicago on 7 December 1944* (Journal of Laws of 1959, no. 35, item 212, as amended).

[7] *Annex 17 to the Convention on International Civil Aviation Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Civil Aviation Authority, https://ulc.gov.pl/_download/prawo/prawo_miedzynarodowe/konwencje/Zalacznik_17_Ochrona_lotnictwa_wydanie_12_zm_18.pdf [accessed: 15 III 2026].

[8] *Aviation Security Manual* (Doc 8973 – Restricted), 2022, ICAO, https://www.icao.int/aviation-security-policy-section/SecurityManual [accessed: 15 III 2026].

[9] Official Journal of the EU L 97/72 of 9 IV 2008.

[10] *Annex I Basic standards for safeguarding civil aviation against acts of unlawful interference (article 4) to the Regulation of the European Parliament and of the Council of 11 March 2008 on common rules...*

the *Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security*.

In turn, this regulation was supplemented by the *Commission Implementing Decision C(2015) 8005 final of 16 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security containing information, as referred to in point (a) of Article 18 of Regulation (EC) No 300/2008*[11]. This decision has not been published in the Official Journal of the EU. The provisions contained therein are of a sensitive nature and are directed on a limited access basis to specific entities and persons holding positions in the civil aviation security system.

At the level of national law, the most important piece of legislation concerning the civil aviation security is the *Act of 3 July 2002 – Aviation Law*[12]. Section IX, *Civil Aviation Security*, sets out the civil aviation security requirements within the national legal framework. However, the essential part of these regulations consists of statutory powers to issue implementing acts specifying the detailed requirements. These include:

- *Regulation of the Minister of Infrastructure of 2 December 2020 on the National Civil Aviation Security Programme*,
- *Regulation of the Minister of Infrastructure of 5 November 2020 on the National Quality Control Programme in the field of civil aviation security*[13],
- *Regulation of the Minister of Infrastructure of 26 July 2021 on the National Civil Aviation Security Training Programme*[14].

It is precisely these regulations that supplement the aforementioned requirements of the European regulations I mentioned earlier. They form three pillars on which the civil aviation security system is based.

[11] Civil Aviation Authority, https://ulc.gov.pl/prawo/prawo-uni-europejskiej/prawo-ue-akty-prawne/ochrona-lotnictwa/3-decyzja-wykonawcza-komisji-c-2015-8005-z-dnia-16-listopada-2015-r-ustanawiajaca-szczegolowe-srodki-w-celu-wprowadzenia-w-zycie-wspolnych-podstawowych-norm-ochrony-lotnictwa-cywilnego-zawierajaca-informacje-o-ktorych-mowa-w-art-18-lit-a-rozporzadzenia-we [accessed: 15 III 2026].

[12] Consolidated text, Journal of Laws of 2025, item 1431, as amended.

[13] Consolidate text, Journal of Laws of 2023, item 1204.

[14] Journal of Laws of 2013, item 1147.

Act of unlawful interference

In the international law, acts of terrorism against civil aviation are referred to as acts of unlawful interference (AUI)[15]. Article 2(20) of the Aviation Law sets them out in detail and defines them as unlawful and deliberate acts involving:

a) use of violence against a person on board an aircraft during flight, where such an act may endanger the safety of that aircraft,
b) destruction of an aircraft or causing damage to it that renders it unable to fly or may pose a threat to the safety of that aircraft,
c) placement on board an aircraft of an object, device or substance that may endanger the health or lives of passengers or crew, or destroy the aircraft or cause damage to it that could prevent it from flying or pose a threat to the safety of the aircraft during flight,
d) hijacking of an aircraft, with or without crew and passengers on board, including for the purpose of using the aircraft as a means of carrying out a terrorist attack from the air,
e) destruction or damage of ground-based or on-board aviation equipment, the disruption of its operation, or the use of violence against a person operating such equipment, where this causes a significant disruption to air traffic or a threat to civil aviation safety,
f) dissemination of false information that poses a threat to persons and property in the field of aviation,
g) destruction or serious damage to airport facilities, the disruption of their operation, or the use of violence against a person operating such facilities, where this causes a significant disruption to air traffic or the operation of the airport, or poses a threat to the civil aviation security.

The seven AUI categories listed above form the basis for defining the threats against which the civil aviation is protected. Establishing an international framework for these acts and incorporating it into national legal systems facilitates effective countermeasures against such threats, as well as the criminalisation of behaviour by individuals who either carry out or plan AUI. Criminal liability for such acts is provided for under, among others, Art. 212 of the Aviation Law, as well as Art. 115, Art. 166, Art. 173 and Art. 174 of the Criminal Code[16].

[15] *Annex 17 to the Convention on International Civil Aviation...*, p. 15.

[16] *Act of 6 June 1997 – Criminal Code* (consolidated text, Journal of Laws of 2025, item 383, as amended).

Security Management System

In today's world, management systems to boost an organisation's efficiency are becoming increasingly important. Without an integrated management system for the organisation, including its security, the ability to respond effectively and proactively to threats arising in the external environment is lost. To this end, it is necessary to adopt a structured approach based on assessing existing resources, identifying weaknesses in the security system, managing risk (or rather risks), promoting security culture, and ensuring a high standard of human resources involved in the system (training, appropriate staff selection). Equally important is the effective flow of internal information as well as cooperation with the authorities and external services.

In the structure and requirements of legislation developed over more than 80 years, one can discern the outline of a strong aviation protection system. However, the full implementation of these principles and providing them with robust legal framework is a key element in building a strong system within a broader context. The cornerstone of an effective security management system (SeMS)[17], as with any modern management system, is the development of appropriate security policies approved and implemented by the management of the entity in which SeMS operates. These policies should set out objectives and priorities for security.

An important element of these policies is the establishment of requirements for procedures to respond to security threats and incidents, including guidelines for communication with both the relevant internal services and the public administration authorities responsible for crisis response. At the same time, it is essential to ensure that adequate human, infrastructural and technical resources are in place.

Another pillar of SeMS is risk management based on the identification of risks and the implementation of measures to control and minimise them. These activities are complemented by mechanisms for monitoring the effectiveness of security measures, quality control and the system's continuous improvement.

One of the more recent elements introduced into civil aviation security regulations is the concept of security culture, understood as building trust among employees, promoting appropriate attitudes and behaviours, and encouraging the reporting of incidents and irregularities.

[17] *Aviation Security Manual* (Doc 8973 – Restricted)...

It was on these principles, among others, that the Polish implementing regulations were drawn up, namely the ones mentioned earlier:

- *National Civil Aviation Security Programme* governing policy areas and setting out detailed requirements relating to risk-based measures and purely protective measures,
- *National Training Programme* governing the scope of competence requirements for those involved in the security system,
- *National Quality Control Programme* governing the area of monitoring compliance with legal requirements, and consequently its quality.

From a practical point of view, it makes sense to identify the key components that, in my opinion, are essential for building an effective SeMS. One of them is to create the role of a security manager – someone responsible not only for implementing the system, but also for its operation and development. The person in this role should have a genuine, rather than merely formal, ability to influence change and make key decisions in the area of security. There are examples where a security manager is appointed within an organisation, yet the person in that role has no real authority within the organisational structure. In such situations, despite their commitment, sense of responsibility and willingness to act, security manager lacks the tools to effectively manage security. It is therefore essential, when establishing the role of security manager, to ensure that they are granted formal and practical powers to manage financial and human resources in the area of security. Only such a framework allows the security system to function effectively.

The organisation should implement consistent security policies, standards and procedures that are endorsed and actively supported by senior management. These documents should clearly define security objectives, identify key threats and take into account the context in which the organisation operates.

Nowadays, there is an increasing emphasis on a modern, risk-based approach to security. This is due to the rapidly changing and wide range of threats, which require regular identification, assessment and re-analysis. Risk management involves assessing the impact of risks on an organisation and consciously implementing appropriate safeguards to achieve an acceptable level of risk.

There is no single universal risk assessment tool – the choice of tool should be tailored to the nature of the organisation, while adhering to the principles of simplicity and usability. It should be also emphasised that it is impossible to eliminate risk entirely, and that the concept of zero

risk remains unrealistic. Therefore, informed acceptance of certain level is required.

In practice, when developing policies and procedures, there is often a problem of unreflective copying of solutions that are not always appropriate to the specific nature of a given entity. The problem is not the use of ready-made templates , but the inability to adapt them to one's own objectives, risks, and available resources.

Effective security management also requires innovation and creativity. The process or risk owner, being the person most familiar with the realities of the organisation, should initiate, or at least approve, the identified risks and the methods used to mitigate them. At the same time, it is worth emphasising that simple tools, when implemented properly and thoughtfully, can deliver very good results.

At the stage of developing procedures and designing SeMS, it is necessary to take into account the methods of responding to identified threats, incidents and breaches that may occur in day-to-day operations. Protective measures should serve a preventive and deterrent function. However, it is equally important to prepare personnel to respond appropriately in the event of an incident. Employees should know how to activate the response system and which services – including the Police or other public authorities – should be engaged.

To illustrate the importance of properly preparing infrastructure and personnel for safety purposes, the experience of aviation security screeners from several years ago may serve as an example. The case concerned the security screeners activation of a procedure for neutralising a potential threat involving an improvised explosive device (IED) found in a shipment during security check. Formally, the activities were carried out in accordance with the applicable procedures of the registered agent[18]. However, it turned out that carrying them out was significantly hindered due to the location of the X-ray machine in which the shipment was being scanned. The package became stuck inside the machine, which was positioned at a considerable height, making it impossible to use the bomb disposal robot and causing complications in conducting further pyrotechnic operations.

[18] Regulated agent means an air carrier, agent, freight forwarder or any other entity who ensures security controls in respect of cargo or mail. See: Article 3(26) of the *Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules...*

This highlighted the inadequacy of emergency procedures in relation to the actual infrastructural and technical conditions, as well as the need to ensure operational continuity. A schematic approach consisting of suspending operations, evacuating personnel and waiting for the appropriate services to arrive may lead to serious organisational, operational and financial consequences resulting from disruptions to service delivery.

Human resources

The key component of the security system, yet at the same time its most vulnerable and threat-susceptible element, is the human factor. For this reason, civil aviation security regulations place considerable emphasis on personnel vetting, particularly of individuals involved in implementing security measures such as screening, access control, surveillance and patrols, as well as employees with unescorted access to protected areas and facilities[19].

Current regulations provide for two levels of **background checks** for aviation and airport personnel, candidates and other individuals who have access to among other things, the airport's restricted areas. The standard background check includes verification of identity, employment and education history covering at least the previous five years, as well as confirmation of a clean criminal record, including from countries where the person resided during that period. The enhanced background check is carried out with the involvement of the competent services, in particular the Border Guard, and consists of determining – including on the basis of operational or intelligence information – the existence of negative premises.

Background check procedures are carried out on a regular basis, at least every five years, although the validity of particular elements is verified more frequently – every three years for standard background check procedure and annually for enhanced background check. This process involves significant organisational resources, particularly in the case

[19] See e.g. chapter 11 of the *Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures...*; section IX of the *Act of 3 July 2002 – Aviation Law...*; *Regulation of the Minister of Infrastructure of 2 December 2020 on the National Civil Aviation Security Programme...*

of airports, where it encompasses staff from numerous entities operating within their area, numbering anywhere from several to over a dozen thousand people. It is worth emphasising that the obligation to conduct background checks also applies to individuals with unrestricted access to critical aviation ICT systems and data, as part of protection against cyber threats. Such personnel are treated analogously to persons who have unescorted access to specially protected areas of an airport.

Experience shows that even the most advanced procedural and technical solutions cannot replace properly background-checked and security-aware personnel responsible for the operation of key infrastructure components. Although the background check requires time and resources, it not only helps reduce risk but also enables the rapid identification of any potential adverse information concerning personnel.

This mechanism, developed within the international aviation sector, would require appropriate adaptation to national conditions and legal order to be effectively implemented in other CI sectors. Compared with vetting procedures conducted for access to classified information, background checks of personnel in the aviation industry are carried out within a relatively short timeframe, which is their significant advantage. However, in the context of high staff turnover, even this period is sometimes perceived as an organisational challenge.

The second key pillar of an effective security system is the **qualifications and competencies of personnel**. In the field of civil aviation security, there is a comprehensive training system tailored to the scope of responsibilities of particular groups of employees – from senior management and middle managers to individuals directly involved in the implementation of security measures. An important element is also the training aimed at raising security awareness among employees who do not perform direct security-related duties but operate in an environment requiring heightened vigilance.

Security culture[20] constitutes a set of standards, values, attitudes and principles relating to security, which are the foundation of the organisation's daily functioning and are reflected in the actions and behaviour of all its members. Security should not be viewed solely as the task of specialised services, but as a shared responsibility encompassing all

[20] *Security Culture*, International Civil Aviation Organization, https://www.icao.int/security-culture [accessed: 15 III 2026].

levels of the organisational structure – from operational staff to senior management.

In practice, security culture connects individual elements of the security system. Without developing it, even the best-designed procedures, systems and technical measures may prove ineffective. A lack of understanding of the purpose of security leads to it being viewed merely as a set of rules and prohibitions that are therefore not accepted or properly implemented. In this sense, the security culture is the driving force of the security system.

In recent years, insider threats[21] have been receiving increasing attention within the civil aviation. This term refers to deliberate and intentional actions taken by individuals with authorised access to an organisation, which may lead to acts of sabotage, subversion or unlawful interference.

Countering internal threats can be based on a combination of several complementary mechanisms, such as background checks, security awareness training, fostering a security culture, information campaigns and the implementation of systems for reporting irregularities. When used in combination, these elements significantly strengthen the organisation's resilience to threats posed, for instance, by employees who are becoming radicalised, in the broadest sense of the word.

Quality control

SeMS is based on Plan–Do–Check–Act (PDCA) concept[22], also known as the Deming cycle, which treats security as a continuous process. This approach involves planning security measures, implementing them, assessing their effectiveness, as well as introducing corrective and improvement measures. Once a risk analysis has been carried out, objectives have been set and appropriate protective measures have been implemented, it is necessary to check whether the system is functioning as intended.

[21] Ibid.

[22] See in more detail: *PDCA – Klucz do ciągłego doskonalenia i skutecznego zarządzania procesami* (Eng. PDCA – The key to continuous improvement and effective process management), Instytut Doskonalenia Produkcji, https://www.doskonalenieprodukcji.pl/blog/pdca-klucz-do-ciaglego-doskonalenia-i-skutecznego-zarzadzania-procesami [accessed: 15 III 2026].

In the literature, the terms 'compliance monitoring' and 'quality control' are used interchangeably, primarily due to terminological discrepancies in the translations of legal acts. In the national legal order, the term quality control[23] has become established in the context of civil aviation security, and this is the term that will be used in the remainder of this study.

Over the years, civil aviation has developed a comprehensive quality control system in the field of security. Although it is based on commonly used control and audit methods, its nature is similar to the approach familiar from the field of cybersecurity. Particular emphasis is placed on continuous monitoring, identifying vulnerabilities and responding swiftly to evolving threats, rather than merely on periodic assessments of compliance with established requirements.

Quality control in the civil aviation constitutes a multi-level system for verifying that Member States, airports, air carriers and other system participants meet at least the basic security requirements. Supervisory powers are exercised at various levels: at international level by the ICAO, at the European Union level by the European Commission, in Poland by the President of the Civil Aviation Authority, whereas at the level of individual aviation entities – by the internal auditors.

The multi-level nature of this system, as well as the possibility for auditors from different Member States to participate in joint audits carried out together with the European Commission inspectors, are conducive to exchange the knowledge and good practices. In addition, European Union regulations provide for mechanisms enabling the European Commission's inspectors to share the results of the audits carried.

Compared to other Member States, Poland has developed an extensive system of certified internal auditors, while at the same time attempting to transfer control mechanisms and practices to the level of aviation operators. This solution strengthens the coherence of the security system and increases its resilience through systematic inspections and the implementation of corrective actions.

The basic control methods in the field of civil aviation security include audit, inspection, security testing and survey.

[23] *Regulation of the Minister of Infrastructure of 5 November 2020 on the National Quality Control Programme in the field of civil aviation security*.

An audit is an announced activity and covers all the security measures applied in a given entity.

The inspection consists in the verification of selected elements of the security system, especially the so-called directly linked security measures, the correct application of which can only be confirmed by their joint assessment.

Security testing constitute unannounced and covert verification activities, such as attempts to bring in prohibited articles by security, gain unauthorised access to restricted areas or unauthorised board an aircraft. This can be compared to the pentests known from cybersecurity.

The above forms are complemented by survey, which consists in the assessment of a specific security measure and is carried out by the competent aviation authority as part of the oversight exercise.

In practice, unannounced control methods, such as inspections and security testing, are of particular value in the evaluation of the civil aviation security system. Thanks to them, information about the functioning of the security system in everyday conditions are obtained, through the use of CCTV recordings, interviews with employees performing their activities without notifying them.

Although important from the point of view of the overall assessment of operations and system compliance, audits are more effective in the analysis of broad areas of the organisation's functioning. At the same time, both civil aviation security audits and inspections often require significant organisational effort and time, involving multi-person teams for many working days to get a complete picture of the functioning of the security system.

It should be emphasised that in the event of non-compliance or deviations from the applicable regulations and procedures, it is necessary to implement adequate remedial measures and launch a corrective action programme. The aim of these activities is to remove identified vulnerabilities of the security system as quickly as possible.

The implementation of a corrective programme requires full support from the person responsible for security, understanding of the entire process, and taking responsibility for effectively removing identified deficiencies. At the same time, it is necessary to take into account the principles of the security culture in order to clearly communicate the objectives of corrective actions and to obtain real support from employees and cooperating organisational units.

Finally, attention should be paid to one more element included in the *National Quality Control Programme*[24], which can be considered innovative, which does not appear directly in the international regulations on the civil aviation security. We are talking about security exercises, which significantly relate to crisis management issues and the implementation of business continuity plans. According to the mentioned programme, each airport is obliged to conduct annual exercises, which most often consist of simulating an attempt to carry out AUI and activating crisis management teams as well as checking the response procedures in force in a given airport. These exercises are carried out, depending on the agreed scope, in cooperation with air carriers, other entities conducting aviation activities, the airport security service, as well as state services operating at the airport, especially the Border Guard, the Police and the Internal Security Agency.

Security of civil aviation and security of critical infrastructure

The analysis of the *National Critical Infrastructure Protection Program 2023*[25] and its annex entitled *Standards for ensuring the smooth functioning of critical infrastructure – good practices and recommendations*[26] indicates that many of the solutions proposed in it are consistent with the mechanisms used in the civil aviation security system. This is positive, as the civil aviation security system is one of the most developed and formalised infrastructure security systems, and it is based on a multi-level approach to risk management and the continuous improvement of security procedures.

At the same time, some recommendations contained in the aforementioned national CI Protection Program are merely good practices in nature, which may limit the extent of their implementation by CI operators. It seems justified to introduce selected solutions through higher-level normative acts, which would allow for their uniform and consistent application. This applies in particular to issues related to human resource management in safety and security systems, such as the development

[24] Ibid.

[25] *Narodowy Program Ochrony Infrastruktury Krytycznej* (Eng. National Critical Infrastructure Protection Program), Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb-en/national-critical-infrastructure-protection-program [accessed: 15 III 2026].

[26] Ibid.

of personnel competencies or the strengthening of employee verification mechanisms, especially for those having access to critical elements of infrastructure. Experience of the civil aviation sector indicates that appropriate selection, training and continuous improvement of personnel competencies constitute one of the pillars of an effective security system.

Equally important is the development of security culture, which involves building threat awareness and a sense of responsibility for safety and security among all system participants. This means the need to carry out systematic training, informational and organisational activities aimed at strengthening attitudes conducive to identifying and reporting potential threats.

It should also be emphasised that although conducting security audits is recommended in policy documents concerning the protection of CI, in practice these activities often focus on assessing formal compliance and analysing documentation. Meanwhile, the effectiveness of the security system depends on its functioning in operational conditions. For this reason, activities such as exercises and security testing using AUI simulation, become particularly important, as they make it possible to verify an organisation's actual ability to respond to crisis situations.

Summary

Due to their location in the transport sector, civil airports are one of the key areas of CI. Civil aviation experience of operating in a highly regulated environment with a particularly developed SeMS can be used to strengthen the resistance of other elements of CI.

Most of the regulations currently in force in security area focus on activities carried out in operational, restricted zones and in their critical parts. This applies not only to civil aviation and airports, but also to other crowded public spaces. In the face of modern threats, the protection of infrastructure that is used by large population centres and to which access is almost unrestricted, such as stations, metro stations, venues of mass events, etc. should be a priority and needs continuous improvement. In this context, it is worth recalling the attack on Brussels Airport in Zaventem

in 2016[27], which – like many other terrorist attacks – was carried out in the public area of the airport's departure hall.

It seems reasonable to conduct frequent specialist training for security services, including, among others, intervention techniques or the use of weapons. At the same time, it is advisable to expand the course content to include, for example, behavioural profiling, which teaches the identification of potentially dangerous behaviour and taking adequate actions at the earliest possible stage of threat development, addressed to a wide group of employees, such as conductors and transport drivers.

The increasingly frequent presence of armed guards and officers from various services in public spaces, including streets and transport hubs, is an important element of preventive measures. In this context, it is worth considering the greater use of service dogs trained both for patrol operations and for detecting explosives. This involves organisational, formal and legal challenges, but the operational and preventive potential of such a solution is large, especially in the context of threats related to unattended luggage. The presence of handlers with trained dogs on patrols can not only contribute to the rapid identification of potential threats but also deter potential perpetrators of acts of terrorism or sabotage. Consequently, this can reduce the risk of incident escalation and shorten the response time of the services, including the time required to evacuate the area at risk.

Another aspect is the assessment of effectiveness of the implemented protection measures in relation to the most frequently identified terrorist threat scenarios. It is essential to take actions to identify potential vulnerabilities and test existing solutions. It is also recommended to repeat such checks periodically.

In my opinion, the following can significantly contribute to increasing the level of CI protection:

- actively undertaking actions aimed at exchanging experiences,
- developing cooperation between entities operating in different sectors,
- building awareness of the need for changes and the evolution of security systems,
- creating and using effective tools for the supervision and review of the security system, based on solid legal foundations.

[27] M. Zieliński, *Zamachy terrorystyczne w Brukseli* (Eng. Terrorist attacks in Brussels), Polska Zbrojna, 22 III 2016, https://polska-zbrojna.pl/Mobile/ArticleShow/18869 [accessed: 28 III 2026].

These actions would promote the transfer of good practices present in civil aviation to other areas affecting the proper functioning of the state and society, and they are also consistent with the concept of continuous improvement of safety and security systems, as well as increasing the resilience of CI to contemporary threats.

Karol Dymek

Specialist with over twenty years' experience in the security. For over 18 years, he has been involved in civil aviation security, also as a national auditor in the Civil Aviation Authority. He currently works as an internal auditor at one of the largest airports in Poland.

Contact: dymek.karol@gmail.com