Terrorism – Studies, Analyses, Prevention, 2026, no. 9: 398–406

https://doi.org/10.4467/27204383TER.26.016.23799

Varia

Civil aviation security in practice – security systems, control and operational resilience

Bohdan Paszukow
Securitas Services

Civil aviation security is one of the cornerstones of the global transport system. Consistent procedures, modern tools and well-designed security systems contribute to its improvement. As part of the AVSEC (aviation security) programmes, standards and practices are being developed to prevent acts of unlawful interference, strengthen the resilience of infrastructure and ensure a high level of risk control. Particular states and international organisations adopt different models for organising their security systems – ranging from centrally managed to more decentralised models based on operator responsibility. This diversity of approaches is particularly evident when comparing the solutions used in the European Union and the United States.

Assessment of civil aviation security quality in the United States and the European Union

When conducting a quality assessment of the aviation security, particularly for a global corporation engaged in the protection of people and property

in various domains, it is essential to understand how particular regions structure their aviation security frameworks. The United States and the European Union both pursue the same overarching goals which are preventing terrorist incidents and ensuring the safety of passengers, staff, and infrastructure. However, their implementation differs in terms of how the security system is managed, the approach to drafting and enforcing regulations, and the mechanisms of supervising operators. The European Union is based on detailed, uniform technical standards and procedures. The United States prefer a more centralised model, with a strong role for the Transportation Security Administration (TSA) and a greater emphasis on outcomes- and effectiveness-based solutions rather than rigid procedural requirements. The EU therefore adopts a normative approach, while the US takes an efficiency-based approach, which involves different ways of organising and monitoring the AVSEC systems.

The TSA, which assumed direct responsibility for aviation security in the US, was established as part of the Department of Homeland Security following the events of 11 September 2001. It sets uniform screening requirements, issues federal security directives, and manages checkpoint operations at most airports. This centralised approach allows rapid adaptation to emerging threats through directive changes. Oversight is conducted through federal inspections, covert testing, and incident driven updates to procedures. The American regulatory system focuses on and includes detailed requirements for passenger and baggage screening, staff vetting, and access control. It emphasises uniformity and speed of response, with federal agencies directly accountable for compliance.

The EU model is built on harmonisation across multiple sovereign states, which must implement common AVSEC standards while retaining their own administrative structures and national responsibilities.

Regulation (EC) No 300/2008[1] provides the baseline framework for aviation security across the EU, setting common rules for screening, access control, and cargo security. These rules are supplemented by detailed implementing acts that specify performance standards. Enforcement is carried out by national authorities within each Member State, but the European Commission plays a central role in oversight. It conducts

[1] *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* (Official Journal of the EU L 97/72 of 9 IV 2008).

inspections, requires annual compliance reporting, and ensures that Member States apply the common rulebook consistently. A distinctive feature of the EU system is the ECAC Common Evaluation Process (CEP), which provides standardised laboratory testing of security equipment against agreed performance criteria. This ensures comparability of equipment approvals across Member States and avoids fragmented national assessments. Therefore, the EU model allows Member States to meet the baseline requirements while maintaining crossborder consistency through harmonised standards and EU Commission oversight.

A key strength of the EU's aviation security regulatory regime is the standardisation of security measures. EU legislation allows resources and efforts to be focused on the areas of most risk, while providing a framework for close cooperation between Member States, regulatory authorities, aviation industry and other stakeholders involved in AVSEC. Common platforms and coordination mechanisms such as SAGAS (Security Advisory Group for Aviation Security), which operates within the European Commission, or industry organisations representing the private sector, such as ASSA-i (Aviation Security Services Association – International), play a key role in this process.

In addition, the EU regulatory system supports quality control and compliance monitoring mechanisms to ensure consistent operational and regulatory oversight.

Although the EU and US approaches differ in terms of governance structure, regulatory style and supervisory mechanisms, in practice they are converging through transatlantic cooperation. The US Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA) maintain bilateral agreements to avoid duplicative certifications and align technical procedures. This cooperation extends into security, where mutual recognition of certain controls and certifications helps streamline compliance for global operators.

Assessment of physical security measures in the EU civil aviation

Compliance assessments serve as the backbone of aviation security. They provide a structured way to verify that airports, airlines, and associated

service providers adhere to international and national regulations, as well as other national local civil aviation authorities.

Assessments methods, their scope and criteria evolve in response to emerging threats, technological advancements, and lessons learned from past incidents and audits. This evolution concerns both the methods used to identify risks and the tools employed to analyse them. This process also takes place within the framework of the AVSEC international cooperation network, which encompasses institutions such as International Civil Aviation Organization (ICAO), the European Commission, TSA, EASA, as well as industry organisations and associations. It is this network that facilitates the exchange of information, the updating of standards and the adaptation of risk assessment methods to a globally changing risk environment.

One of the most critical components of compliance assessment is the monitoring of access control systems. Airports are complex environments with multiple restricted zones. Processes of civil aviation security quality control verify that only authorised personnel have access to sensitive areas, identification systems, biometric checks, and surveillance technologies are functioning correctly and that procedures for issuing and managing access credentials are effective. This prevents unauthorised entry, which could compromise aircraft, passengers, or cargo.

Equally important is the evaluation of passenger and baggage screening procedures. Compliance assessments ensure that screening technologies such as X-ray machines, explosive detection systems, and body scanners are properly calibrated and maintained. Quality control also involves observing the performance of security personnel, checking whether they follow protocols consistently, and identifying gaps in training or vigilance.

Cargo and supply chain security is another significant area of assessment. It covers the procedures for screening, storing, and transporting cargo. It is checked whether the suppliers and contractors adhere to approved security practices and that there is a clear chain of custody for all goods entering the aircraft environment.

Security is only as strong as the people implementing it, and therefore, quality control processes emphasise continuous education, drills, and evaluations. Personnel must be prepared not only to respond effectively to suspicious behaviour, emergencies, or attempted breaches. Compliance

assessments often include simulated scenarios to test readiness and resilience.

Risk management and incident reporting systems play a crucial role. Compliance assessments ensure the effective operation of mechanisms for identifying vulnerabilities function effectively, promptly, reporting incidents, and implementing corrective actions. Quality control processes track how quickly and effectively organisations respond to identified risks, whether through procedural changes, technology upgrades, or enhanced training. This creates a feedback loop where lessons learned strengthen overall physical securityin aviation.

Technology integration is another key component. As part of the compliance assessment, checks are carried out to ensure that surveillance systems, biometric identification, and automated access controls are installed and are actively monitored and maintained. Quality control ensures that data from these systems is used effectively to detect anomalies and prevent breaches.

Observations are one of the most immediate and practical tools in the compliance assessment process. By conducting onsite inspections, auditors and inspectors can directly observe how security procedures are implemented in real time. For example, they may watch how access control points are managed, whether identification checks are consistently applied, or how baggage screening is conducted. Observations might reveal eventual discrepancies between procedures and practice.

Document validation complements observations by ensuring that the organisation's policies, manuals, and records align with regulatory requirements. This involves reviewing training records to confirm that personnel have received the required instruction, checking incident logs to verify that breaches are reported and investigated, as well as validating certifications to ensure equipment meets standards. Without accurate and uptodate documentation, even the best operational practices can drift into noncompliance. Moreover, document reviews provide evidence that the organisation is not only compliant today but has systems in place to remain compliant over time.

Interviews with personnel help gauge their level of understanding of risk, their attitudes to work, and readiness for action. Speaking with frontline staff such as security officers might reveal whether training has been effective and whether employees feel confident in applying protocols. Interviews with management can uncover how

Terrorism – Studies, Analyses, Prevention
2026, no. 9: 395–406

seriously leadership prioritises security and whether there is a culture of accountability. Importantly, interviews often highlight areas that documents and observations cannot capture, for instance, whether staff feel comfortable to execute their activities especially during peak hours or whether the procedures for reporting suspicious activity are clear and the communication channels are trusted.

Testing protocols can be divided into overt and covert methods. Overt testing includes scheduled drills, such as evacuation exercises or controlled access challenges, where staff are aware they are being evaluated. These tests measure compliance under observed conditions and help organisations refine their procedures. Covert testing, often referred to as red teaming, involves simulating realworld threats without prior notice, for example, attempting unauthorised access or introducing prohibited items through checkpoints. Covert tests are invaluable because they reveal how systems perform under genuine stress, without the artificiality of a staged exercise. Together, overt and covert testing ensure that physical security measures are not only compliant on paper but effective against actual threats.

Ultimately, the assessment of compliance and security quality control in civil aviation serve to establish a layered security system. Regulatory adherence, access control, screening, cargo security, personnel training, risk management, and technology integration together form a comprehensive shield against threats. This approach ensures that physical security in civil aviation remains at an acceptable level. It protects passengers, staff, and assets maintaining public confidence in air travel at the same time.

The use of artificial intelligence to ensure civil aviation security

In order to enhance the efficiency, accuracy and adaptability of aviation security systems to changing threats and operational conditions, artificial intelligence (AI) is increasingly being integrated into them.

Passenger and baggage screening technologies now use machine learning algorithms to detect prohibited items more effectively than traditional X-ray systems. The AI-driven tools can analyse vast amounts of imaging data, recognise patterns and characteristics of risks, and flag anomalies with greater precision, reducing the likelihood of human error. Similarly, biometric identification systems at airports, such as facial

recognition and fingerprint scanning, rely on AI to match identities quickly and securely, streamlining passenger flow while maintaining strict access control.

AI is used in surveillance and monitoring systems. Modern CCTV (closed circuit television) networks are enhanced with AI-powered analytics that can detect suspicious behaviour, unattended baggage, or unauthorised access in real time. This proactive capability allows security personnel to respond faster and more effectively to potential threats. In cargo and supply chain security, AI tools are used to track shipments, verify authenticity, and identify irregularities during their transport.

In practice, AI is not replacing traditional security measures but augmenting them. Human oversight remains essential, as AI systems must be continuously tested, validated, and monitored to ensure they perform reliably under diverse conditions. The combination of human expertise and AI-driven tools creates a layered defence system that strengthens aviation security without compromising safety standards.

Components of a corporate aviation security programme

Aviation has a global dimension, and therefore corporate AVSEC programmes must align with international standards, regional directives, and national civil aviation authority requirements. This regulated environment shapes every aspect of the programme, from policy development, operational execution to quality control carried out by external authorities. Organisations also establish internal quality control mechanisms that include document validation, operational observations, structured interviews with staff, and both overt and covert testing protocols. By embedding these processes into daily operations, organisations can identify gaps early, correct deficiencies, and demonstrate to regulators that they are meeting or exceeding required standards. This proactive compliance culture is a hallmark of aviation security and is less common in other private security sectors, where oversight may be less stringent.

Aviation security threats evolve, and organisations within the security programme must invest in training, awareness, and skill development at all levels. Frontline staff need regular refresher courses on screening procedures, while management must be trained in crisis response and regulatory updates. Capacity building also extends to technological

adaptation, ensuring that staff can operate advanced screening equipment and respond to emerging cyber threats. This emphasis on continuous learning ensures that the organisation remains resilient in the face of new challenges, and at the same time it reflects the dynamic nature of corporate aviation security compared to more static private security environments. Most private security programmes are limited to the local or national context and do not require such a high level of international coordination.

Equally important is the role of global network sharing and collaboration between organisations operating in the aviation sector. Corporate AVSEC programmes benefit from participating in global networks that share intelligence, best practices, and lessons learned. Whether through industry associations, regulatory working groups, or bilateral partnerships, this exchange of information allows organisations to anticipate emerging threats, adopt proven strategies, and align their practices with global standards.

Security and cybersecurity audits for critical infrastructure facilities – potential errors

On 3 April 2026, the amendment to the Act on the National cybersecurity system[2] came into force. Its aim was to bring national regulations into line with the EU's NIS2 Directive[3] by expanding obligations for critical infrastructure (CI) operators. The new law will affect significant number of entities, including operators across energy, transport, healthcare, and digital services.

One of these obligations is to carry out external information system security audits. The effectiveness of audits in strengthening the resilience of CI depends on the organisation's approach to such an audit.

Above all, audits should not be viewed merely as a box-ticking exercise. The NIS2 Directive emphasises continuous risk management, not just periodic checks. Organisations should embed audit findings into their

[2] *Act on the National cybersecurity system* (Journal of Laws of 2026, item 20, as amended).

[3] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)* – (Official Journal of the EU L 333/80 of 27 XII 2022).

cybersecurity strategy, ensuring improvements are sustained rather than temporary.

Another critical error is ignoring supply chain and third-party risks. The NIS2 Directive requires operators to assess risks from vendors and service providers. Many CI systems rely on external contractors responsible for software, hardware, or system maintenance. If audits fail to evaluate these dependencies, attackers may exploit weak links outside the organisation's direct control.

It is very important that obligations relating to incident reporting and response are met. The NIS2 Directive requires timely reporting of cybersecurity incidents to national authorities. If audits do not test incident response capabilities such as escalation paths, communication protocols, and coordination with regulators, organisations may fail during a real crisis. Audits should include simulations to verify readiness. Finally, organisations should align audits with resilience planning.

The Critical Entities Resilience (CER) Directive[4] complements the NIS2 Directive by focusing on physical and operational resilience of critical entities. If audits only cover technical cybersecurity without considering broader resilience measures like system redundancy, disaster recovery, and crosssector coordination – CI may remain exposed to systemic risks.

In summary, Poland's mandatory external audits of CI security are a powerful tool, but only if approached strategically. Taking a rigorous approach to regulatory compliance, addressing supply chain risks, ensuring governance accountability within the management system, testing incident response, and integrating resilience planning are essential steps.

Building resilience to threats in civil aviation in the EU – recommendations

Building civil aviation resilience to threats within EU countries requires a comprehensive and layered approach that balances regulatory oversight, technological innovation, and human preparedness. At the core of the system, strict adherence to international and European aviation

[4] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC* – (Official Journal of the EU L 333/164 of 27 XII 2022).

security regulations provides the foundation. However, resilience goes beyond compliance, as it requires proactive risk management and the ability to adapt quickly to evolving threats.

One of the most important elements is the integration of advanced technology. Surveillance systems enhanced with AI, biometric identification for passenger processing, and automated cargo screening tools all contribute to detecting and mitigating risks more effectively. Continuous training and competency assessments of personnel remain indispensable.

Security threats are often transnational, and system resilience depends on timely intelligence exchange between national authorities, airlines, and airports. Furthermore, digital systems underpin nearly every aspect of aviation operation, which is why cybersecurity is so important, including the protecting networks from intrusion and ensuring continuity of operations in the face of cyberattacks.

Resilience to threats is built through a culture of continuous improvement. Incident reporting, auditing, and feedback loops allow vulnerabilities to be identified and corrected swiftly. What works is a layered defence where regulation, technology, human expertise, and cooperation reinforce one another. Neglecting any of these pillars would weaken the system, but when combined, they create a robust shield that ensures aviation in EU countries remains secure, adaptable, and trusted by the public.

One of the biggest challenges in protecting airports against terrorism and sabotage is detecting insiders. They may act out of ideology, coercion, or financial motivation, and their activities can be difficult to detect. Certain standards are currently in place in this regard, but it is essential to further strengthen them in order to build resilience. In this regard, the minimum standards set out in Regulation (EC) No 300/2008 currently apply. These include, among other things, strict background checks of employees, continuous monitoring of staff with access to restricted areas, and mandatory training in security awareness. Airports are required to implement access control systems, conduct random screening of staff, and enforce reporting mechanisms for suspicious behaviour. To build resilience, it is essential to reinforce these guidelines.

Experts argue that more emphasis should be placed on security culture encouraging employees to remain vigilant, report concerns, and understand the risks posed by colleagues who may misuse their privileges.

Organisations should create environment in which employees feel responsible for safety and are fully aware of risks.

Using solutions from the EU civil aviation sector to build resilience to hybrid threats in maritime and rail transport

Hybrid threats, those that blend physical, cyber, informational, and even legal-instrumental tactics, pose a growing challenge to transport CI. Maritime ports and rail networks, much like airports, are highly interconnected systems whose operation can be disrupted through sabotage, including cyberattacks, disinformation campaigns, or insider manipulation. While each sector has its own operational realities, the EU civil aviation acquis offers a mature framework of resilience practices that can be adapted to strengthen maritime and rail security.

One of the most valuable lessons from aviation is the risk-based, layered approach to security. Aviation combines multiple layers of defence from passenger screening and cargo checks to access control and surveillance. This principle can be applied to maritime and rail transport by tailoring controls to critical nodes such as port terminals, signalling centres, and freight depots. Operators should adopt flexible, intelligence-led measures that reflect the open nature of ports and rail networks.

Another transferable strength is access control and credentialing discipline. Aviation requires strict background checks, continuous monitoring of restricted areas, and random screening of staff with access to these areas. In maritime and rail, similar measures can safeguard control rooms, maintenance yards, and cargo handling facilities. Importantly, insider risk management must go beyond one-time vetting, incorporating behavioural monitoring and periodic re-assessment to detect changes in staff circumstances or vulnerabilities.

Equally critical is the security culture embedded in aviation. Continuous training, scenario-based exercises, and mandatory reporting of suspicious behaviour help to create a workforce that is alert and prepared for threats. Maritime and rail operators can benefit from adopting this culture, ensuring that employees understand hybrid threats and feel empowered to act when anomalies arise. Joint drills across sectors involving operators, regulators, and emergency services can simulate hybrid scenarios, strengthening the ability to response.

Terrorism – Studies, Analyses, Prevention
2026, no. 9: 395–406

It is worth noting, however, that not all practices that work effectively in aviation will necessarily work in the maritime and rail transport sectors. This applies, for example, to airport checkpoints. Copy pasting these solutions into open maritime and rail environments would create bottlenecks without addressing the unique vulnerabilities of these sectors. Similarly, overreliance on technology without governance and human oversight can leave systems exposed to adversarial manipulation. The siloed responsibilities must be replaced with joint command structures and interoperable protocols across agencies.

By combining aviation's proven frameworks with sector-specific adaptations, the EU can build a robust shield against hybrid campaigns that target its critical transport lifelines.

Bohdan Paszukow

Specialist in civil aviation, author of scientific publications on airport security and control in civil aviation.

Contact: bohdan.paszukow@gmail.com