SMS Best Practice/Good Practice Submission			
State whether this is a Best or Good Practice:		Best Practice	
ANSP	HungaroControl	Date of submission	June 30th 2025
Contact Details			

SoE Study Area	SA 6.1 Hazards to operations are assessed.
BP/GP title	Safety Assessment of Information Security Risks
In use since	since March 2025
ANSPs using this practice (for BP specifically)	None
Key Words	Safety Risk Assessment, Information Security

Cybersecurity is generally gaining more attention, but critical infrastructures, such as aviation and air traffic management are prominent domains. This induced the making of (EU) 2023/203 […] laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety […]. As mandated by the regulation: "*In addition to the management system referred to in point ATM/ANS.OR.B.005, the service provider shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks* ***which may have an impact on aviation safety***.".

However, the Regulation does not specify how the impact on aviation safety should be assessed. Simply treating the security threats as safety threats by inputting them into the conventional safety assessments – which are generally designed for assessing accidental events as opposed to deliberate malicious acts – are proven to be problematic in the following manner:

- the risk controls are not separated between the security and safety sides, their effectiveness is hard to assess,
- since the largest severity is often reached from security events, using conventional risk matrixes, even for low probabilities the risk shows as very significant, especially compared to other (safety) risks.

This necessitates the creation of a new methodology in order to assess the impact of security threats on aviation safety. Based on GM1 IS.AR.200, the methodology follows a Bow-tie approach according to Figure 1.

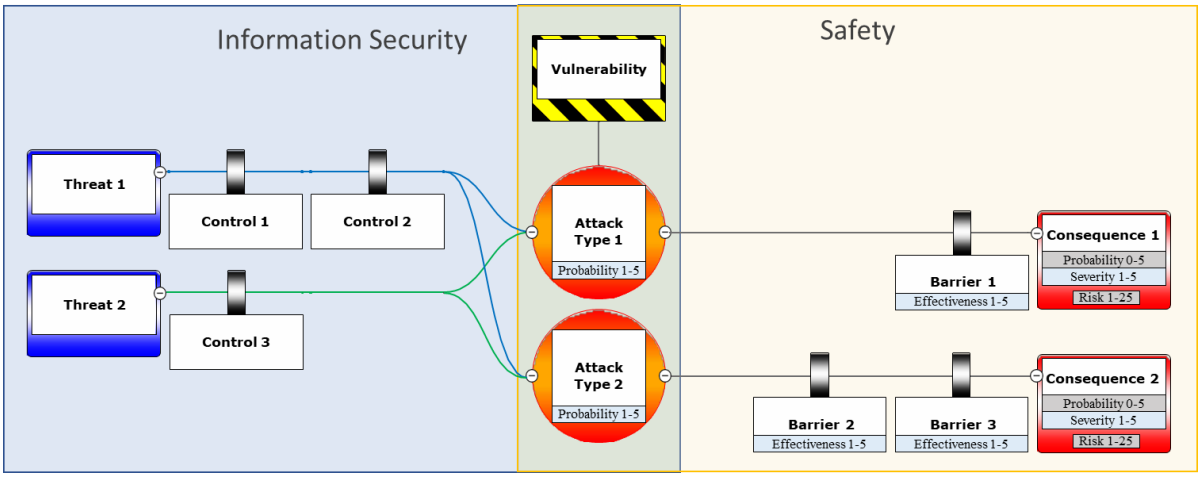

Figure 1. Overview of methodology

The methodology begins with the assessment of information security risks. This assessment may originate from a requirement from a regulation or standard, and should consist of a database of vulnerabilities and threats. Then the appropriate attack types are identified, and their probabilities are determined. This, by definition, is the probability, of a specific attack happening from that specific threat, against all controls on the information security side. An attack can originate from more than one threats, and one threat can cause more than one attack types. Once the attack has taken place, the barriers on the safety side might still be able to eliminate or mitigate the effect. These barriers originate from the architecture of the ATM functional system (people, equipment, procedure). Their effectiveness is assessed on a scale from 1-5, where 1 has no effect whatsoever on the attack, and 5 is completely able to stop the attack's consequences. Consequence in this sense is interpreted as a safety event. Its probability is calculated by taking the probability of the attack and reducing that with the effectiveness of the barrier. This specific formula only allows the probability of the attack at maximum, when the barrier's effectiveness is low (1) and a low, but non-zero probability when the barrier is at its most effective state. The consequence is then assigned a severity, based on the technical occurrence severity scale from EUROCONTROL's RAT methodology, allowing for comparison with historical event data, as RAT is employed for assessing occurrences. Final risk is then calculated independently from RAT, as a product of probability and severity, in a qualitative manner, on a scale of 1 – 25. Risk classification, shown in Table 1, is based on the same risk classes as safety risks (even though instead of a risk matrix, here a product is used).

Table 1. Risk classification

Value	Risk class
0 – 7	acceptable
7,01 - 9	conditionally acceptable
9,01 - 13	not recommended
13,01 - 25	not acceptable

The assigned risk class, aligning with the methodology for safety risks, means different management level required for initiating necessary actions and risk acceptance. In practice, this assessment is recorded in a tabular form.

Validation of the new methodology took place in the spring of 2025. The functional system was divided to technical systems, based on our internal classification used for technical occurrence reporting. The input for the information security side was an information security risk assessment, which is periodically carried out. All threats identified there have been assessed for all technical systems, by involving cybersecurity, safety, and technical experts. The validation brought valuable experience, e.g. for the tuning of the barrier effectiveness scale. As a result, the complete, present risk level of all the technical systems are arranged in a database.

The methodology for assessing safety effects of information security risks is integrated in the change management process. All notifications of changes internally require ticking a field of cybersecurity involvement, which is validated by the cybersecurity team. If a change is found to be relevant in this aspect, then they prepare the safety side, by selecting the appropriate system and threats. Then, by the coordination of the safety team, the technical experts assess how the current risk level is modified due to the change. The current risk level is also updated periodically, when an information risk assessment is carried out.

Another interesting outcome of the validation exercise was the inclusion of such deliberate malicious acts, that do not impact our functional system directly, but can impact our operation indirectly. Such threats include GPS spoofing, laser attacks, radar jamming, etc. These were out of scope for information security risk assessments, but can serve as an addition for the organization's comprehensive risk overview. The new methodology allowed for assessing these risks, and by including operational experts, their operational effects were identified.

The development of the methodology lasted from September of 2024 to February of 2025, with the close collaboration of two safety experts and one cybersecurity expert. The validation involved eight technical experts covering the all domains of the functional system, including those that were previously out of the scope of cybersecurity. A total of 33 systems were analyzed. Furthermore, three operational experts were involved in the assessment of operational effects of selected threats.

Although the methodology was only recently introduced, the organization's understanding of how cybersecurity-related threats may impact aviation safety has already improved. Security and safety are no longer viewed as separate domains, the cross-functional collaboration between cybersecurity, safety, and technical teams has strengthened, leading to more comprehensive risk identification and mitigation strategies. Integration into the change management process assures that cybersecurity aspects are considered to the necessary extent for all changes and the risk level remains up to date. The Safety Management System has been improved by the inclusion of risks that were previously outside its scope, ensuring a more comprehensive safety approach.

By submitting this document, your organisation is willing for the proposed Best or Good Practice to be shared with other ANSPs.

For Best Practices, this document should be sent together with the SoE in SMS questionnaire, to: soe_2025@eurocontrol.int **by 30th June 2025 at the latest**.

Submissions for consideration as Good Practices may be sent by the above date. They may also be identified during the survey interview sessions with the assessment team, following which a Good Practice submission document will be requested.