*Proc. of the European Safety and Reliability Conference (ESREL 2026)*
*Edited by* José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 *Published by* Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26514-cd

# Strengthening cybersecurity in regional governmental units

Marie Hudcová

*Department of Military Science Theory (K-105), University of defence, Czech Republic. E-mail: marie.hudcova@unob.cz*

Alena Oulehlová

*Department of Military Science Theory (K-105), University of defence, Czech Republic. E-mail: alena.oulehlova@unob.cz*

The implementation of Directive (EU) 2022/2555 (NIS 2) and the adoption of Act No. 264/2025 Coll. on cybersecurity introduce new obligations for public administration and significantly increase demands on cybersecurity governance. This article analyses the impact of the new cybersecurity legislation on regional governmental units in the Czech Republic.

The study identifies key risk areas related to the performance of obligations of regulated service providers, including increased administrative burden, insufficient funding, lack of methodological guidance, and unclear terminology. A semi-quantitative risk analysis is applied to assess the severity and acceptability of these risks. The results show that increased administrative burden represents an unacceptable risk, while insufficient funding and lack of methodological support are conditionally acceptable but may significantly hinder effective implementation. The findings highlight the need for strengthened institutional support, adequate funding, and clearer regulatory guidance to ensure compliance with cybersecurity requirements.

*Keywords*: risk analysis, security measures, cybersecurity, regional governmental units.

## 1. Introduction

The rise of information technology brings greater efficiency to both the private and public sectors, but also greater vulnerability. With the increasing digitization of the private and public sectors, cyber dependence on information systems, communication networks, and cloud services is increasing.

This growing dependence is particularly significant for so-called regulated service providers, i.e. entities whose services are essential for the functioning of society or the state. These include not only public administration bodies, but also sectors such as energy (e.g. power grids), transport (e.g. railway systems), digital infrastructure (e.g. internet service providers), and healthcare systems. In the context of this article, the focus is primarily on regional governmental units, specifically regional authorities and municipalities with extended powers, which represent administrative units within the Czech Republic responsible for regional governance and delegated state administration. Regional authorities and municipalities with extended powers represent key tiers of subnational public administration, performing both self-governing and delegated state functions.

With the growing number of cyber security incidents not only in the Czech Republic but also in the European Union, the NIS 2 Directive was adopted. Directive 2022/2555 of the European Parliament and of the Council of the European Union on measures to ensure a high common level of cybersecurity across the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (hereinafter referred to as "NIS 2"), (European Union 2022), Act No. 264/2025 Coll., on cybersecurity and other implementing regulations. These normative legal acts reflect modern information systems, the

management of their security and resilience to security incidents and attacks, primarily by establishing new obligations for the private and public sectors (Czech Republic 2025).

The NIS 2 Directive aims to eliminate significant differences between European Union member states in terms of cybersecurity by establishing minimum rules governing the functioning of the coordination regulatory framework, thanks to an update of the list of sectors and activities to which cybersecurity obligations apply. The NIS 2 Directive focuses on harmonizing cybersecurity in European Union member states, particularly in terms of the level of detail and method of supervision. Furthermore, the NIS 2 Directive distinguishes between highly critical sectors and other critical sectors, which significantly expands the scope of NIS 2 implementation to a larger part of the sector. At the same time, NIS 2 emphasizes cooperation between European Union member states to ensure cybersecurity. It also introduces obligations to report incidents, maintain the continuity of essential services, and ensure the security of networks and information systems. The aim of the NIS 2 Directive is to protect the European Union and its population from cyberattacks (European Union 2022).

Act No. 264/2025 Coll., on cybersecurity, was approved in response to the NIS 2 Directive. Its aim is to increase the resilience of regulated service providers to cyber threats. The Act also introduces categories of regulated service providers, namely those with higher obligations and those with lower obligations (Czech Republic 2025). Depending on the importance of the regulated service provider, regional governmental units are divided into higher and lower obligation regimes. The higher obligation regime includes, among others, regional authorities, while the lower obligation regime includes, among others, administrative districts of municipalities with extended powers (Czech Republic 2025).

### 1.1. *Technical and security measures for providers of regulated services*

The Cybersecurity Act imposes new technical and security measures on regulated service providers. It introduces 12 new tasks for providers under the lower obligations regime, including municipalities with extended powers, and 24 new tasks for providers under the higher obligations regime, including regional authorities. These tasks include, for example, security measures management systems, the establishment of security roles, risk management, human resources security, and the management of cybersecurity events and incidents (Czech Republic 2025).

## 2. Threats arising from the Cybersecurity Act and implementing regulations for regional governmental units

The aim of the article is to analyse the potential risks inherent in the Cybersecurity Act and its implementing regulations. At the same time, the article aims to create an impact analysis of the adoption of the Cybersecurity Act on regional governmental units. To achieve the objective of the article, municipal authorities with extended powers and regional authorities in the Czech Republic were selected, as they have become providers of regulated services due to the adoption of the Cybersecurity Act and implementing regulations. The article uses the methods of analysis, synthesis, and literature review. Risk analysis and risk assessment procedures were newly created for the purposes of the article, with a semi-quantitative approach to probability estimation being chosen and individual categories and levels of impact, including risk acceptability levels, being defined (see chapter 3. Risk Analysis of the article for more details). The risk analysis was based on the recommendations for the implementation of ISO 31000.

The comment procedure (the term refers to the legislative consultation process in which stakeholders (e.g. government bodies, professional associations, and industry representatives) provide feedback on draft legal regulations before their adoption) on the implementing regulations of Decree No. 410/2025 Coll., on security measures for providers of regulated services under the lower obligations regime (Czech Republic 2025) and Decree No. 409/2025 Coll., on security measures for providers of regulated services under the higher obligations regime (Czech Republic 2025) highlighted several threats that could have a significant impact on the implementation of the Cybersecurity Act and its implementing regulations. The authors of the article reviewed the documents in the comment procedure, on the basis of which threats were identified, particularly from

cases that were not accepted in the legislative process.

### 2.1.*Increased administrative burden*

The comment procedure repeatedly emphasized the significant administrative burden that providers of regulated services under both higher and lower obligations will face. The comments focused in particular on the scope of documentation work, the obligation to regularly update security measures, and the requirement to provide demonstrable training for responsible employees (Government of the Czech Republic 2025).

In addition, providers of regulated services under the higher obligations regime emphasized the difficulty of securing personnel roles in the area of cybersecurity. The consultation process also included requests to ease certain obligations, in particular to extend the intervals between security audits and risk assessments. There were also calls to shorten the intervals for archiving security events, which would be economically unviable on such a scale (Government of the Czech Republic 2025).

### 2.2.*Unclear wording of obligations and terminology*

The comments also highlighted the problem of unclear terminology, specifically the terms "secure communication," "technical asset," "relevant requirements," and "user." There is no precise definition of these terms or what they encompass. In the case of the term "secure communication," it is unclear what can be considered secure communication. Similarly, it is unclear whether mere encryption during message transmission is sufficient or whether end-to-end encryption is always required. In the case of the term "technical asset," it is not clearly defined what a technical asset is in relation to Decree No. 410/2025 Coll (Government of the Czech Republic 2025). Furthermore, the comments point out the ambiguity of the term "relevant requirements" according to Decree No. 410/2025 Coll. The ambiguity of this term is potentially harmful because the provider has no basis for deciding which specific requirements apply to them (Government of the Czech Republic 2025). In the case of Decree No. 409/2025 Coll., clarification and specification of the definition of the term "user" was identified as a fundamental comment in the comment procedure, because the definition could be misinterpreted to mean that the user is the end user of the service (Government of the Czech Republic 2025).

### 2.3.*Insufficient methodological guidance*

During the consultation process for Decree No. 410/2025 Coll., it was recommended that specific methodological materials be created, particularly for providers of regulated services under the lower obligations regime, who often do not have the financial resources to hire companies or other professionals to help them implement the security measures required by the Cybersecurity Act (Seeba, Valgre, and Matulevičius 2025). The methodological material should include sample documentation, procedures, and recommendations for implementing the Cybersecurity Act (Government of the Czech Republic 2025).

### 2.4.*Insufficient funding*

Another topic discussed was the need to secure adequate funding for regulated service providers, who are facing a significant increase in administrative, organizational, and technical obligations without adequate financial coverage for these obligations (Government of the Czech Republic 2025). The consultation process for Decree No. 410/2025 showed that the implementation of the Cybersecurity Act and its implementing regulations will have an impact on providers in the hundreds of thousands to millions of crowns per year, due to the need to create new systematized positions, the need to purchase new technologies, and increased costs for security audits and operational support (Government of the Czech Republic 2025).

### 2.5.*Absence of rules for the safe use of artificial intelligence tools*

The consultation process revealed that the Cybersecurity Act and its implementing regulations do not reflect the growing trend in the use of artificial intelligence. The main threat is the possible leakage of information when text or files are inappropriately entered into publicly available AI systems, which can process and store data in cloud storage outside the EU or store queries for the purpose of further training the model (Winther and Fredriksen 2025; Government of the Czech Republic 2025; Bolgouras, Zarras, Leka et al. 2025).

### 2.6.*Lack of regulatory and impact analysis*

The consultation process for Decree No. 409/2025 Coll. revealed that no regulatory and impact analysis had been carried out. The Office of the Government of the Czech Republic, the Confederation of Industry of the Czech Republic, and the Association of Small and Medium-Sized Enterprises of the Czech Republic describe that the decree imposes tasks beyond the scope of NIS 2 obligations. These impacts have not been assessed (Government of the Czech Republic 2025; Novelli, Casolari, Hacker, Spedicato, Floridi 2024; Bolgouras, Zarras, Leka, et al. 2025).

## 3. Risk Analysis

Six threats were identified based on a review of the comment procedure for the aforementioned decrees. For providers of regulated services under the lower obligations regime, a risk analysis has been prepared focusing on increased administrative burden, unclear wording of (their) obligations and terminology, insufficient methodological guidance, insufficient funding, and the absence of rules for the safe use of artificial intelligence. For providers of regulated services under the higher obligations regime, a risk analysis has been prepared for administrative burden, unclear formulation of (their) obligations and terminology, insufficient funding, absence of rules for the safe use of artificial intelligence, and lack of regulatory and impact analysis.

The aggregate measure of consequences N is determined as a combination of the coefficient of impact on providers ($K_P$) and the coefficient of impact on the public ($K_V$), where the weighting coefficients were set as impacts on providers ($VK_P$=0,4) and impacts on the public ($VK_V$=0,6) according to the following relationship:

$$N = (K_P \times VK_P) + (K_V \times VK_V)$$

**The impact coefficient on the provider ($K_P$)** is determined as the arithmetic mean of three coefficients:

$$K_P = \frac{K_{P1} + K_{P2} + K_{P3}}{3}$$

- $K_{P1}$ = impact coefficient on employees:

Table 1. Impact coefficient on employees

| Level of impact on employees | $K_{P1}$ |
|---|---|
| High | 3 |
| Medium | 2 |
| Low | 1 |

The impact coefficient on employees ($K_{P1}$) expresses the degree of negative impact on employees, particularly in terms of increased stress levels and workload. It reflects the pressures associated with new cybersecurity obligations, including administrative burden and additional security requirements.

- $K_{P2}$ = budget impact coefficient:

Table 2. Budget impact coefficient

| Budget impact | $K_{P2}$ |
|---|---|
| 11-100% increase in expenditure | 3 |
| 4-10% increase in expenditure | 2 |
| 0-3% increase in expenditure | 1 |

The budget impact coefficient ($K_{P2}$) expresses the degree of impact on the budget of the regulated service provider. The wide range in the highest category (11–100%) reflects variability depending on the size and preparedness of individual organizations.

- $K_{P3}$ = coefficient of impact on organizational/process activities:

Table 3. Impact coefficient on organizational/process activities

| Degree of impact on organizational/process activities | $K_{P3}$ |
|---|---|
| High impact | 3 |
| Medium impact | 2 |
| Low impact | 1 |

The impact coefficient on the organization's organizational and process activities ($K_{P3}$) expresses the degree of negative impact on the functioning of the organization's internal processes.

**The impact coefficient on the public ($K_V$)** expresses the degree of negative impact in relation to the functioning of public administration and is determined as the arithmetic mean of four coefficients:

$$K_V = \frac{K_{V1} + K_{V2} + K_{V3} + K_{V4}}{4}$$

- $K_{V1}$ = Service availability coefficient

Table 4. Service availability coefficient

| Degree of impact on service availability | $K_{V1}$ |
|---|---|
| High impact >500 citizens | 3 |
| Medium impact <500 citizens | 2 |
| Low impact <100 citizens | 1 |

The service availability coefficient ($K_{V1}$) expresses the degree of negative impact on the availability of services.

- $K_{V2}$= Personal data protection coefficient

Table 5. Personal data protection coefficient

| Degree of impact on personal data protection | $K_{V2}$ |
|---|---|
| Leakage of highly sensitive data | 3 |
| Leakage of basic personal data of more than 100 individuals | 2 |
| Leakage of basic personal data | 1 |

The personal data protection coefficient ($K_{V2}$) expresses the degree of negative impact on personal data protection.

- $K_{V3}$= Psychological impact coefficient

Table 6. Psychological impact coefficient

| Degree of impact on citizens' mental health | $K_{V3}$ |
|---|---|
| Panic | 3 |
| Fear and uncertainty | 2 |
| No impact | 1 |

The psychological impact coefficient ($K_{V3}$) expresses the degree of impact on citizens' mental health.

- $K_{V4}$ = Time impact coefficient

Table 7. Time impact coefficient

| Time impact | $K_{V4}$ |
|---|---|
| More than one month | 3 |
| One day to one month | 2 |
| Within 24 hours | 1 |

The time impact coefficient ($K_{V4}$) expresses the duration of the threat.

**The risk assessment (R)** for regulated service providers is expressed as the product of the **aggregate magnitude of consequences (N)** and the **probability of occurrence (F)**. A high probability of occurrence of a threat has a quantitative rating of 3, a probable occurrence of a threat has a rating of 2, and an unlikely occurrence has a rating of 1. The reference level of risk acceptability has been set for acceptable risks (0–5⟩, conditionally acceptable risks (5–6 ⟩, and unacceptable risks (6–9). Providers of regulated services under the lower obligations regime will be designated as $R_N$ and those under the higher obligations regime as $R_V$.

### 3.1.*Increased administrative burden*

Increased administrative burden has been identified as an unacceptable risk both for providers of regulated services under the higher obligations regime ($R_V$=8.1) and for providers of regulated services under the lower obligations regime ($R_N$=6.75). The most significant impact will be on employees and on organizational and procedural activities, as the Cybersecurity Act imposes 12 new tasks on providers of regulated services with lower obligations and 24 new tasks on those with higher obligations, including archiving for a period of four years, annual updates of the overview of security measures and evaluation of their effectiveness, and demonstrable training of responsible employees (Czech Republic 2025). Increased administrative demands may also translate into increased operating costs for organizations, particularly in connection with the need for additional staff or consultations with external firms, technical support, or the purchase of appropriate computer hardware and software. The increased administrative burden will have an impact on the public in terms of a possible slowdown in the availability of services (Government of the Czech Republic 2025).

### 3.2.*Insufficient funding*

Insufficient funding was assessed as a conditionally acceptable risk with a value of $R_N$=5.1 for providers of regulated services under the lower obligations regime. For providers of regulated services under the higher obligations regime, insufficient funding was assessed as a conditionally acceptable risk with a value of $R_V$=5.4. Insufficient financial resources will have

a significant impact on administration. The Cybersecurity Act and its implementing regulations significantly increase the personnel, organizational, and technical demands on providers of regulated services without ensuring adequate financial coverage for these obligations. In terms of impact on the public, insufficient funding will not have a direct impact on the public, but it may lead to delays in services, which could cause concern and uncertainty (Government of the Czech Republic 2025).

### 3.3.*Absence of rules for the safe use of artificial intelligence*

For providers of regulated services under both higher and lower obligations, the absence of rules for the safe use of artificial intelligence was assessed as an acceptable risk with a value of $R_V$=4.6 and $R_N$=4.6. The absence of rules for the safe use of artificial intelligence will not have a direct negative impact on employees, the budget, or organizational and procedural activities. The misuse of artificial intelligence tools can have a clear impact on the public, as it can lead to the leakage of highly sensitive information and basic personal data. From a time perspective, this threat is assessed as long-term, as the potential impacts of the misuse of artificial intelligence may require extensive corrective measures (Government of the Czech Republic 2025).

### 3.4.*Insufficient methodological guidance*

Insufficient methodological guidance was assessed as a conditionally acceptable risk with a value of $R_N$=5.4, but only for providers of regulated services under a lower obligation regime, as employees will not have access to clear and consistent guidelines for the implementation of security and organizational measures. The absence of methodology increases the risk of errors, which can have a high impact on the provider's budget, especially if the requirements of the Cybersecurity Act are not met and a fine is subsequently imposed. Insufficient methodological guidance will have a high impact on organizational and procedural activities due to the possible inefficient setting of processes within the organization (Government of the Czech Republic 2025).

### 3.5.*Unclear formulation of obligations and terminology*

Unclear formulation of obligations and terminology may have a high impact on employees of providers of regulated services under both higher and lower obligations, who will find it difficult to correctly interpret the organizational and technical requirements for their organization. Unclear formulation of obligations and terminology for providers of regulated services under the higher and lower obligations regime was assessed as an acceptable risk with values of $R_V$=4.56 and $R_N$=4.82. The impact on the budget is assessed as medium, as the provider may have problems allocating the financial resources necessary to fulfil the imposed obligations, which is closely linked to the impact on organizational and procedural activities due to the complicated planning of investments in cybersecurity based on unclear terminology (Government of the Czech Republic 2025).

### 3.6.*Lack of regulatory and impact analyses*

The absence of regulatory and impact analyses was repeatedly identified as a serious problem during the consultation process for Decree No. 409/2025 Coll. The decree imposes obligations beyond the scope of the NIS 2 Directive, which are highly demanding in economic, operational, and administrative terms. The absence of regulatory and impact analysis was noted among providers of regulated services under the higher obligations regime and it was assessed as a conditionally acceptable risk with a value of $R_V$=5.4. The absence of this analysis also means that the impact of the newly adopted cybersecurity law on staffing, administrative burden, budget, and organizational and procedural activities has not yet been sufficiently assessed. This significantly complicates planning, decision-making on the amount and allocation of both financial and human resources, and preparation for the implementation of legal obligations for providers of regulated services under the higher obligations regime, as they do not have access to an objective assessment of the real impact of the Cybersecurity Act and its implementing regulations. At the same time, the absence of regulatory and impact analysis may pose a significant risk to the public, as the overload on organizations may lead to a long-term

reduction in the availability of services (Government of the Czech Republic 2025).

Table 8. Summary of risk analysis results

| Threat | $R_N$ | $R_V$ | Risk level |
|---|---|---|---|
| Increased administrative burden | 6.75 | 8.1 | Unacceptable |
| Insufficient funding | 5.1 | 5.4 | Conditionally acceptable |
| Absence of rules for the safe use of artificial intelligence | 4.6 | 4.6 | Acceptable |
| Insufficient methodological guidance | 5.4 | – | Conditionally acceptable |
| Unclear formulation of obligations and terminology | 4.82 | 4.56 | Acceptable |
| Lack of regulatory and impact analyses | – | 5.4 | Conditionally acceptable |

## 4. Recommendations for minimizing risks

Based on the risk analysis, acceptable, conditionally acceptable, and unacceptable risks were evaluated. Excessive administrative burden was assessed as unacceptable risk. In the case of unacceptable risks, it is necessary for regional governmental units to adopt systemic measures that are necessary to minimize these risks. In order to minimize the impact of excessive administrative burden, it is necessary to introduce centralized methodological and administrative support for providers of regulated services under both higher and lower obligations. This service should provide methodological support for the implementation of technical and organizational measures.

In order to minimize the impact of the conditionally acceptable risk of insufficient funding, more financial resources need to be allocated. The funds could be provided to regulated service operators in the form of subsidy programs aimed at implementing technical and organizational measures. Furthermore, a minimum financial framework should be introduced for providers of regulated services under both higher and lower obligations.

Insufficient methodological guidance and the lack of regulatory and impact analysis were assessed as conditionally acceptable risks. In order to minimize the impact of insufficient methodological guidance, it is necessary to develop centralized methodological support for providers of regulated services under the lower obligations regime. Methodological materials should include sample documentation, recommended procedures, and practical guidance for the implementation of technical and organizational measures required by the Cybersecurity Act. To minimize the impact of the lack of regulatory and impact analysis, such analyses should be developed at both the national and regional levels and regularly reviewed in light of economic and political changes.

## 5. Conclusion

The analysis of the impact of the implementation of the Cybersecurity Act and its implementing regulations reveals key areas that may have a significant impact on regulated service providers under both higher and lower obligations. The most significant threats identified in the consultation process include increased administrative burden, the absence of rules for the safe use of artificial intelligence, insufficient methodological guidance, insufficient funding, unclear formulation of obligations and terminology, and a lack of regulatory and impact analysis.

A risk analysis was subsequently carried out on the significant impacts, which showed that increased administrative burden is among the unacceptable risks. Conditionally acceptable risks include insufficient methodological guidance, lack of regulatory and impact analyses and insufficient funding. Acceptable risks include unclear formulation of obligations and terminology and the absence of rules for the safe use of artificial intelligence.

The results of the analysis indicate that sufficient funding needs to be secured, personnel capacities need to be strengthened, and a regulatory and impact analysis needs to be carried out to objectively assess the economic, organizational, and personnel impacts. Without these steps, the requirements of the Cybersecurity Act and its implementing regulations cannot be effectively met.

Although the analysis focuses primarily on regional governmental units, the findings are also relevant for other regulated service providers on which public administration depends, such as

energy, transport, and digital infrastructure sectors.

**References**

European Union. 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union.

Czech Republic. 2025. Act No. 364/2025 Coll., on Cyber Security (Zákon č. 364/2025 Sb., o kybernetické bezpečnosti).

Czech Republic. 2025. Decree No. 408/2025 Coll., on Regulated Services.

Czech Republic. 2025. Decree No. 410/2025 Coll., on Security Measures for Providers of Regulated Services under the Regime of Lower Obligations.

Czech Republic. 2025. Decree No. 409/2025 Coll., on Security Measures for Providers of Regulated Services under the Regime of Enhanced Obligations.

Government of the Czech Republic. 2025. Draft Decree on Security Measures for Providers of Regulated Services under the Regime of Lower Obligations — Public Consultation (ODok). Accessed December 24, 2025. https://odok.gov.cz/portal/veklep/material/pripominky/ALBSDGQCWPDA/.

Government of the Czech Republic. 2025. Draft Decree on Security Measures for Providers of Regulated Services in the Higher Obligations Regime – ODok Material. ODok Portal – VeKLEP. Accessed December 27, 2025. https://odok.gov.cz/portal/veklep/material/ALBSDGQC3VXQ/.

Mentzelou, Konstantina, Panos T. Chountalas, Fotis C. Kitsios, Anastasios I. Magoutas, and Thomas K. Dasaklis. 2025. "Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach" Journal of Cybersecurity and Privacy 5, no. 4: 97. https://doi.org/10.3390/jcp5040097

Seeba, M., Valgre, M., Matulevičius, R. (2025). Evaluating Organization Security: User Stories of European Union NIS2 Directive. In: Krogstie, J., Rinderle-Ma, S., Kappel, G., Proper, H.A. (eds) Advanced Information Systems Engineering. CAiSE 2025. Lecture Notes in Computer Science, vol 15701. Springer, Cham. https://doi.org/10.1007/978-3-031-94569-4_4

Bolgouras, V., Zarras, A., Leka, C. et al. Eu regulatory ecosystem for ethical AI. AI Ethics 5, 5063–5080 (2025). https://doi.org/10.1007/s43681-025-00749-x

Claudio Novelli, Federico Casolari, Philipp Hacker, Giorgio Spedicato, Luciano Floridi, Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity, Computer Law & Security Review, Volume 55, 2024, 106066, ISSN 2212-473X, https://doi.org/10.1016/j.clsr.2024.106066.

Winther, Rune, and Rune Fredriksen. 2025. “Safe AI vs Safe Use of AI.” Paper P7886 in Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference. Singapore: Research Publishing, Singapore.