Terrorism – Studies, Analyses, Prevention, 2025, special edition: 273–314

https://doi.org/10.4467/27204383TER.25.023.21526

Expert material

The role of standardisation and conformity assessment in ensuring security and building resilience of critical infrastructure to hybrid threats

Adam Tatarowski

The Technical Property Protection Development Institute TECHOM

https://orcid.org/0009-0007-5503-6819

Introduction

The approach to understanding security has been dynamically evolving in Poland since the 1989 transition period. It was only then that the needs of the market and the state administration for security and safety services began to take shape. Until the enactment of the *Act of 22 August 1997 on the protection of persons and property*, which is still in force today, the security and safety sector in Poland functioned without dedicated statutory regulations. It developed on a market basis and was subject to both positive and negative bottom-up influences – intra-market, as well as top-down influences – from the state administration and from the outside.

An obstacle to the creation of a coherent and transparent legal system that would provide the security and safety sector with a stable foundation

was the lack of a clear vision and decision-making of state regulatory institutions at the level of creating detailed requirements. The development of coherent solutions was further complicated by the conflicting interests of various influential groups whose activities had adverse impact on legislative process. The potential of the standardisation acquis was not realised. Successive legislative initiatives, although necessary and often inspired by European solutions, did not create a coherent structure – they left significant gaps, hampering the growth of competitiveness, transparency and quality of services and organisational as well as technical solutions provided. An example of a much-needed normative act, which, however, did not take into account systemic solutions concerning quality assurance and compliance, was the *Regulation of the Council of Ministers of 24 June 2003 on facilities of particular importance for the security and defence of the state and their special protection,* specifying the issues of protection of these facilities in a situation of a threat to state security.

Alongside the legal 'mainstream' focused on the Act on the protection of persons and property, the need to create a unified approach to protecting and ensuring security for critical infrastructure (CI) began to be recognised in Poland. Although it was understood that certain systems and facilities – such as power grids, telecommunications infrastructure or transport systems – were fundamental to the functioning of the state, for a long time there was a lack of regulations that comprehensively addressed their protection. The Polish legal system lacked the very concept of CI. As Tomasz Szewczyk and Maciej Pyznar point out[1], the Polish state administration encountered this concept mainly in the framework of international cooperation, within the structures of NATO and the European Union. The regulations created at that time focused on selected sectors or referred to the protection of individual objects, but did not create a uniform security system. As a result, activities undertaken in the field of CI protection were dispersed, and issues of administrative responsibility for its security were not clearly defined.

For many countries, the US approach at the turn of the 20th century became a model in trying to sort out this issue. A turning point in this regard was the entry into force of Presidential Decision Directive 63 of 22 May

[1] T. Szewczyk, M. Pyznar, *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne* (Eng. Critical infrastructure protection and asymmetric threats), „Przegląd Bezpieczeństwa Wewnętrznego" 2010, no. 2, p. 54.

1998[2], which introduced the concept of *critical infrastructure* as the systems necessary to ensure the basic functioning of the economy and government. According to it, these are systems, physical and digital, the destruction or disruption of which could lead to serious socio-economic and political consequences. The novelty was the recognition that protecting these systems required a coordinated effort by both government and the private sector, which owned most of the assets deemed critical to the functioning of the state. The directive required individual US federal agencies to develop plans for the protection of CI and to establish mechanisms for information sharing between public and private sectors.

Influenced by the American standards, work on the creation of a unified framework for the protection of CI has started in the EU. In Poland, the initial activities of the state administration in this area focused on selected sectors. There was still a lack of an approach that would integrate the various aspects of infrastructure security in the same management model.

A turning point in the shaping of the Polish CI protection system was the enactment of the *Act of 26 April 2007 on crisis management*, which in Article 3(2) for the first time introduced a definition of CI into the Polish legal order, understood as:

> (...) systems and their functionally related facilities, including buildings, equipment, installations, services that are critical to the security of the state and its citizens and to the smooth functioning of public administration bodies, as well as institutions and businesses.
> CI includes systems:
> a) energy, energy raw materials and fuels supply,
> b) communications,
> c) ICT networks,
> d) finance,
> e) food supply,
> f) water supply,
> g) health care,
> h) transport,
> i) rescue services,
> j) ensuring continuity of public administration,

[2] *Presidential Decision Directive/Nsc-63*, The White House, 22.05.1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm [accessed: 5.03.2025].

k) production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances.

The Act also defined the concept of CI protection, i.e. (...) *actions aimed at ensuring the functionality, continuity and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities, and to limit and neutralise their effects, as well as the rapid restoration of this infrastructure in the events of failures, attacks or other events that disrupt its proper functioning* (Article 3(3)).

In addition, the Act created the Government Centre for Security (RCB), a supra-ministerial structure, reporting directly to the Prime Minister, responsible for planning and programming activities in the field of CI protection (Article 10(1)).

Developing of European regulations and their impact on Polish legislation

At EU level, a breakthrough occurred with the entry into force of *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. Under this directive, CI is defined more generally as (...) *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions* (Article 2). The Directive introduced and further defined the 'object-oriented' approach to the protection of CI, as it focused on the protection of facilities and installations the damage of which could have serious consequences for the functioning of the state. The Polish implementation of the Directive took into account this model more comprehensively. This was due to an awareness of the growing interdependence between public administration and the private sector and the dynamic changes in the global security environment. The solutions adopted in Poland not only strengthened the protection of facilities, but also laid the foundation for overcoming future challenges in maintaining continuity of services.

The Act on crisis management required the RCB to create and systematically update the National Critical Infrastructure Protection Program (NPOIK), which defined in detail the process of identifying CI and protecting it. It added an annex entitled *Standards for ensuring the smooth functioning of critical infrastructure – good practices and recommendations*.

As a whole, it laid the foundation for the standardisation of CI protection, based on the so-called six-pack concerning:

1) physical protection,
2) technical protection,
3) personal protection,
4) information and communication security,
5) legal protection,
6) aspects related to recovery plans.

The Act and the set of documents that complement it, including the NPOIK, have evolved over the years. During this time, a rather complex process for identifying CI has been established, consisting of three stages. The first establishes which system a potential CI site belongs to. Next, it is checked whether the site performs the function referred to in the statutory definition. Finally, it is analysed whether the possible consequences of the destruction or discontinuation of the potential CI will meet the cross-cutting criteria relating to the social impact of the destruction or discontinuation of the facility, equipment, installation or service. These criteria include:

- casualties,
- financial implications,
- the need to evacuate,
- loss of service,
- recovery time,
- international effect,
- uniqueness (in terms of the impossibility of replacing and reconstructing the damaged facility, equipment or installation)[3].

Since the implementation of the NIS Directive[4] in Poland by the *Act of 5 July 2018 on the national cybersecurity system*, parallel to the 'object-based' approach, there is a 'service-oriented' system for selecting operators of essential services, i.e. those that are important to maintaining critical

[3] See in more detail: A. Tatarowski, *Building resilience of critical infrastructure in the light of asymmetric threats and terrorism. Legislative trends in the Polish implementation of the CER Directive with particular reference to aspects of standardisation and certification of organisational and technical solutions,* "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 391–409, https://doi.org/10.4467/27204383TER.24.014.19402.

[4] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security for network and information systems across the Union.*

social or economic activity and are mentioned in the list of important services issued under the Act. In turn, a decision recognising an entity as essential service operator is issued when:

- entity provides essential service,
- provision of this service depends on information systems,
- incident would have a significant effect resulting in disruption to the provision of the essential service by that operator[5].

The coexistence of 'object-oriented' and 'service-oriented' approaches has led to inconsistencies in the overall CI management system. The 'object-oriented' model, based on classic infrastructure protection, did not encompass a system perspective and did not take into account important interdependencies between sectors. In contrast, the 'service' approach, developed within the framework of cyber security regulation, was limited in scope. This dualism was particularly evident in EU policies, in which two separate directives were in place: the Council Directive 2008/114/EC, mandating the protection of physical infrastructure, and the NIS Directive, focusing on ensuring the resilience of information systems and digital services.

Towards a new model for critical infrastructure protection

Over the years, there has been a growing understanding that the CI protection model, focused solely on physical facilities, is insufficient. It has been influenced both by the scientific analysis carried out and by events that have revealed significant gaps in the existing risk management system. Experiences from terrorist attacks (e.g. 11 September 2001), the COVID-19 pandemic, cyber attacks and natural disasters (e.g. Hurricane Sandy)[6] have highlighted that it is not so much the protection of individual facilities, systems or installations that is important, but ensuring the uninterrupted operation of services that are vital for the stability of the state and the security of citizens. A disruption of one service, e.g. fuel supply, can have a knock-on effect and lead to transport problems, food shortages or limited availability of medical care. An interesting concept that has influenced the development of this approach in Poland and the EU is the 'Six Ways

[5] See in more detail: A. Tatarowski, *Building resilience of critical infrastructure...*, p. 394.

[6] M. Wiśniewski, K. Szwarc, W. Skomra, *Continuity of Essential Services as an Emerging Challenge for Societal Resilience*, "IEEE Access" 2023, vol. 11, pp. 44615. https://doi.org/10.1109/ACCESS.2023.3271751.

to Die'[7]. Its most important premise is that the goal of protection should not be the 'physical' CI itself, but ensuring uninterrupted access to services on which the security of citizens depends at 3 levels: individual, social and state. It identifies 6 fundamental threats that can lead to individual death and social and economic destabilisation: lack of food, lack of water, disease, injury, extreme cold and extreme heat.

The US was the first to widely implement a 'service' model of protection. The US Cybersecurity and Infrastructure Security Agency (CISA) produced the *National Critical Functions Set* (NCFS)[8], which defines critical functions as activities and processes necessary to maintain national security, economic stability and the basic functioning of society. The document distinguishes 4 main areas in which 55 critical functions have been identified:

1) connect – ensuring the smooth functioning of telecommunications systems, the internet, data transmission and postal services,
2) distribute – maintaining the continuous movement of people, goods and resources essential to the functioning of the economy and infrastructure,
3) supply – securing key resources including energy, potable water, industrial raw materials and production systems,
4) manage – protection of public administration systems (e.g. important in the US election protection), financial stability, capital markets and crisis management.

Thus, in the NCFS model, it is not individual facilities or systems that are protected, but services, which implies, for example, the need to implement complex solutions to ensure fault tolerance and resource redundancy.

A consequence of the actions described above was the adoption (14 December 2022) in the EU of the groundbreaking CER Directive on the resilience of critical entities[9]. The CER Directive ends the division between 'facility' and 'service' approaches. It formalises a modern approach to infrastructure protection, with a focus on ensuring

[7] M. Bennett, V. Gupta, *Dealing in Security Understanding Vital Services and How They Keep You Safe*, 2010, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [accessed: 22.06.2022].

[8] *National Critical Functions Set*, CISA, https://www.cisa.gov/national-critical-functions-set [accessed: 24.06.2022].

[9] *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*.

the resilience of those providing essential services to society. It introduces a comprehensive risk management model at a system level, taking into account interdependencies between sectors and with a focus on the resilience of entire supply chains. Significantly, the NIS 2 Directive[10] on cyber security was adopted at the same time. The two directives are compatible with each other and, as such, should be implemented in the legal systems of individual Member States.

The groundbreaking role of the CER Directive – the Polish perspective

For Poland, the implementation of the CER Directive is not only another legislative requirement, but also a natural step towards adopting a systemic approach to national security. The experience of CI protection, gained both at the national level and in international cooperation (e.g. within NATO and the EU), is valuable in this regard. Poland has been developing its own methods of risk management and CI protection for years, including the implementation of NPOIK, building cyber security, introducing mechanisms to protect the population[11] and civil defence or enhancing military capabilities[12]. These are solid foundations on which the new architecture of critical entities resilience and the services they provide will be based.

Moreover, Poland has a unique competence to shape the standards of CI protection at the European level. Many years of experience in bringing together the public and private sectors in the area of security, taking into account awareness of new threats and their continuous evolution as well as understanding of the broad socio-technological context, make Poland an important participant in the process of improving resilience mechanisms. The Polish Presidency of the Council of the EU, which runs from 1 January to 30 June 2025, focuses on strengthening 7 dimensions of European security. These are:

- defence and security,
- protection of people and borders,
- resistance to foreign interference and disinformation,

[10] *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)*.

[11] *Act of 5 December 2024 on civil protection and civil defence.*

[12] *Act of 11 March 2022 on the defence of the Homeland.*

– ensuring security and freedom of business,
– energy transition,
– competitive and resilient agriculture,
– health security[13].

In Poland, the RCB is responsible for all substantive work related to the implementation of the CER Directive into the Act on crisis management.

A new phase in critical infrastructure protection for the European Union and its Member States

The implementation of the CER Directive is one of the biggest legislative and operational challenges for EU Member States. It is a milestone in building European resilience to systemic threats – from cyber attacks through infrastructure sabotage to energy, health and other crises involving unknown risks. It is also a clear signal that Member States recognise the need to evolve the CI protection model in a unified, modern direction. The new regulation will allow for more effective countering of current and future threats and enhance resilience at both national and EU-wide levels. The European Commission has set October 2024 as the deadline for its full implementation, but by March 2025, only 9 countries had completed the process of transposing the regulations into national law, while the others – including Poland – are working intensively to finalise them. It is worth mentioning that the concerted efforts of Member States in implementing the CER Directive represent a shift to a new level of integration and solidarity in terms of security. This gives the EU a more resilient, flexible and coordinated security system to respond effectively to the dynamically changing threats of the 21st century.

Ideas behind the Polish implementation of the CER Directive

Conceptual work on the Polish law implementing the CER Directive began within the RCB in the first half of 2023[14], the results of which were discussed

[13] *The Polish presidency of the Council of the EU*, European Council, Council of the European Union, https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/ [accessed: 28.02.2025].

[14] Draft act amending the Act on crisis management and certain other acts, https://legislacja.rcl.gov.pl/docs//2/12386961/13069020/13069024/dokument711601.pdf [accessed: 6.04.2025].

at the 10th National Forum for Critical Infrastructure Protection (2023), and aspects of standardisation and conformity assessment were presented by the article's author[15]. In Q1 2024, formal decisions were taken on the RCB's commitment as executor of the draft amendment. In March 2024, the first draft was circulated for consultation, and its innovative solutions won the appreciation of both the state administration and market stakeholders, especially CI operators. At the current stage of legislative work (March 2025), most of the solutions have already been refined. The law itself is waiting to enter the parliament.

One of the most important areas in the implementation of the CER Directive is to ensure consistent and effective standardisation and conformity assessment mechanisms that will enable a uniform approach to the resilience requirements of critical entities and business continuity of essential services.

The purpose of this article is to contribute to the discussion conducted under the Polish Presidency of the Council of the EU, particularly in the context of the work of the Working Party on Civil Protection – Critical Entities Resilience (PROCIV–CER), the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats and the Working Party on Terrorism (TWP). The paper shows how the European regulations have been translated in the draft Polish law into concrete solutions for risk assessment, standardisation of organisational and technical solutions and services provided to critical entities, as well as conformity assessment (auditing and certification). The author of this paper, as a co-author of the concept of standardisation system in the Polish implementation of the CER, presented the genesis and justification of the adopted solutions and their practical consequences for CI operators and public administration.

National Critical Infrastructure Protection Program as a foundation for ensuring the security of critical infrastructure and a source of inspiration

In the National Critical Infrastructure Protection Program (NPOIK), which has evolved over the years, the CI protection regime is based on

[15] A. Tatarowski, *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER* (Eng. Standardisation and certification of solutions under the CER Directive), *10th National Forum for Critical Infrastructure Protection*, Warszawa 2023, https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami [accessed: 28.02.2025].

the aforementioned so-called six-pack. For the sake of order, the current (2023)[16] description of these assumptions will be quoted, which include:

1) ensuring physical security – a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of actions taken by persons who have attempted to enter or have entered CI in an unauthorised manner;
2) ensuring technical security – a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of disturbances to ongoing technological processes;
3) ensuring personal security – a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of actions taken by persons who have authorised access to CI;
4) ensuring information and communication security – a set of organisational and technical actions aimed at minimising the risk of disrupting CI operations as a result of unauthorised interference with control apparatus and information and communication systems and networks;
5) ensuring legal security – a set of organisational and technical actions aimed at minimising the risk of disrupting CI operations as a result of legal actions of external entities;
6) business continuity and restoration plans, understood as a set of organisational and technical actions leading to the maintenance and restoration of functions performed by CI[17].

This regime corresponds to Article 13 of the CER Directive, concerning resilience measures to be put in place by critical entities. It is worth recalling the first paragraph of this provision:

> 1) Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

[16] *National Critical Infrastructure Protection Program*, Government Centre for Security, 2023. The text of the programme is available at: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej.

[17] *National PCritical Infrastructure Protection Program*, pp. 30–31.

a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;
b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;
c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
d) recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;
e) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;
f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly considering training courses, information materials and exercises.

For the purposes of the first subparagraph, point (e), Member States shall ensure that critical entities take into account the personnel of external service providers when setting out categories of personnel who exercise critical functions.

The above provisions were the starting point for work on a new framework for standardisation in ensuring security and building resilience of CI in Poland. The CER Directive, under Article 3, is based on the principle of minimum harmonisation, meaning that it only sets out a basic regulatory framework and leaves it to the Member States to introduce solutions adapted to national realities, including more stringent ones. Such an approach provides flexibility and the ability to take into account specific national circumstances and allows for a CI protection regime that corresponds to actual threats and operational requirements. The Polish implementation takes advantage of this margin of freedom and designs solutions that not only fully implement the EU guidelines, but also integrate national experiences and lessons learned from existing CI security regulations and practices.

Normalisation as a basis for implementing optimal standardisation

Standardisation, understood as an activity aimed at achieving an optimum degree of order in a particular area by setting out provisions intended to be universally reusable[18], is fundamental to the smooth functioning of societies and economies, and its importance dates back to the beginning of civilisation[19].

Standards organise reality and ensure predictability and coordination of activities on a global scale. From energy production and distribution systems, through transport and telecommunications, to cyber security and risk management, standardisation underpins interoperability and stability. In an era of dynamic technological change and increasing security threats, its role is even more important, as it provides a coherent framework for the functioning of countries, economies and institutions in an increasingly complex world.

Today, standardisation provides important support to EU legislation. A landmark moment in the anchoring of standardisation in the EU socio-economic ecosystem was the adoption and publication on 7 May 1985 of the EC Council Resolution[20] on a new approach to technical harmonisation and standards. According to Teresa Idzikowska and Krzysztof Banaszek, (...) *giving a particularly high priority to the standards and technical specifications that are the product of standardisation activity, in the creation of rules for the free movement of goods and the elimination of barriers to trade, meant a radical change in the status of standards at both*

[18] J. Łunarski, *Normalizacja i standaryzacja* (Eng. Normalisation and standardisation), Rzeszów 2014, Oficyna Wydawnicza Politechniki Rzeszowskiej.

[19] Already in the ancient world, efforts to standardise units of measurement, systems of weights, building and organisational standards were important not only for the development of trade and administration, but also for ensuring the effectiveness of military operations and public safety. Ancient Egypt used precise measurements in the construction of monumental structures such as the pyramids, and in Mesopotamia, uniform systems of weights allowed the economy and exchange of goods to function efficiently. Ancient Rome, on the other hand, developed a system of standardisation in a way that shaped social and military organisation for many centuries. The standardisation of armament and equipment for legionaries provided an operational advantage on the battlefield and increased the efficiency of military logistics. The Romans also applied standards in construction – standardised methods of building roads, aqueducts and military forts enabled the efficient expansion and maintenance of the empire. The Romans also developed the first standardised forms of municipal guards and sewerage systems that minimised health risks in cities.

[20] *Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards.*

national and international level[21]. The model adopted was that legislation should specify only the basic safety and quality requirements, while detailed technical guidelines should be developed within the framework of voluntary European standards. In practice, this allowed the requirements to be flexibly adapted to changing market and technological conditions, while harmonising the most important standards across the European Community.

Since 1 January 2004, the Polish Committee for Standardisation (PKN) has been a member of the European standardisation organisations: European Committee for Standardisation and European Committee for Electrotechnical Standardisation. These are private, non-profit associations, operating under Belgian law. They are not EC bodies. The European standardisation system is distinguished by the fact that European Standards are agreed by all Member States, and each Member State, regardless of its involvement in their development, is obliged to assess and implement them. As a result, there is one European Standard in Europe, available only as an implementation of national standards[22]. For the record, it should be mentioned that a standard has many converging definitions[23]. Quite comprehensible is the one included in the *Act of 12 September 2002 on standardisation*, according to which it is (...) *a document adopted by consensus and approved by an authorised organisational unit, establishing – for general and repeated use – principles, guidelines or characteristics relating to various activities or their results, and aimed at achieving an optimal degree of order in a specified scope* (Article 2(4)).

Awareness of the role played by standardisation as an instrument to support risk and security management was reflected in the CER Directive, which allowed Member States to take into account standards applicable to critical entities. In accordance with recital 34 of the Directive (...) *standardisation should remain primarily a market-driven process. However, there may still be situations in which it is appropriate to require compliance with*

[21] T. Idzikowska, K. Banaszek, *Rola i znaczenie normalizacji w bezpieczeństwie transportu* (Eng. The role and importance of standardisation in transport safety), „Logistyka" 2010, vol. 4.

[22] T. Schweitzer, E. Zielińska, *Działalność normalizacyjna* (Eng. Standardisation activity), in: *Normalizacja*, T. Schweitzer (ed.), Warszawa 2013, Polski Komitet Normalizacyjny, pp. 15–18.

[23] *A World Built on Standards: A Textbook for Higher Education*, S.A. Bøgh (ed.), Nordhavn 2015, Danish Standards Foundation.

specific standards. In turn, Article 16 indicates that (...) *in order to promote the convergent implementation of this Directive, Member States shall, where useful and without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities.*

The proposal for the Polish implementation of the CER Directive fully meets these objectives. It takes into account both the European standardisation acquis and national experience in standardisation of security systems in CI (NPOIK with annexes).

Incorporating standards into legislation – the Polish specificity

The possibility to refer to standards in legislation derives from the aforementioned Act on standardisation. Pursuant to Article 5(4): *Polish Standards may be referred to in legal regulations after they have been published in the Polish language*, and the method of citation taking into account accuracy (dated, undated, general citation) and strength (exclusive or indicative) is defined in PN-EN 45020:2009 *Standardisation and related activities. General vocabulary*. Legislative work to achieve the objectives set by the CER Directive obviously also had to take into account the broadly understood voluntary use of standards, resulting not so much from the Act itself, but from the adopted system of European standardisation. According to the position of PKN, the reference to Polish Standards in a legal provision does not change its voluntary status, unless the legislator wants to change this status, which is only possible by explicitly indicating it in the provisions of another law[24]. This position was used in the first draft of the implementation, in which the standards were referred to. During the first phase of inter-ministerial agreement, opinion and public consultation, the RCB accepted the argumentation of the Government Centre for Legislation (RCL) that standards, as payable standards, should not be referred to in the Act as mandatory for use. Moreover, despite PKN's clear position on the change of the status of a standard from voluntary to mandatory within the meaning of the act in which it is referenced, the principle of voluntary application of standards could be violated. Therefore, an alternative solution was decided upon – standards

[24] *Dobrowolność stosowania norm* (Eng. Voluntary application of standards), Polski Komitet Normalizacyjny, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn [accessed: 28.02.2025].

will be directly referred to not in the Act, but in the implementing acts or in the official lists published in the Bulletin of Public Information (BIP) of the relevant institutions. This approach strikes a balance between ensuring access to standards and respecting the principles of standardisation and regulation. Furthermore, in consultation with the RCL, a construction of the regulations has been developed. It takes into account the existing arrangements while fully complying with the existing regulations on standardisation and the principles of the standardisation system. It was specified that the solutions referred to in the following paragraphs (...) *should meet the requirements set out in the standards, indicated in the implementing act*. This way of writing indicates the need to meet the requirements set out in the standard, but does not impose the standard as a mandatory document to be used.

Mentality and system barriers – the genesis of the problems. The need for a tough approach to the use of standards

The experience of state regulatory institutions, in particular the RCB, CI operators and the market as a whole (including other ordering parties – investors, service providers, suppliers of various organisational and technical solutions, etc.) clearly shows that the protection of CI in Poland has been limited for years by systemic barriers, the sources of which date back to the beginning of the political transformation. They led to a situation where ensuring adequately high security standards was difficult, and in some cases even impossible.

One of the most important problems became the misinterpretation of the legal regulations governing public procurement (EU and Polish) – the lowest price was the dominant and sometimes the only criterion considered. In many cases, the formulation of requirements concerning the quality of equipment or services encountered difficulties both at the level of the contracting authorities and the controlling institutions. The substantive cells at CI operators, responsible for defining security needs, often formulated requirements corresponding to real threats and using proven standards (e.g. NPOIK) and norms. However, at the next stage, at the formal level, these requirements were reduced by procurement departments (or management boards!) which, citing regulations and unwritten rules to eliminate unnecessary costs, removed additional technical or organisational requirements and left only those explicitly included in the law.

The situation was further complicated by inspection bodies, which often equated requirements that went beyond the absolute legal minimum with a breach of the principles of economy. On more than one occasion, control actions were taken against units that had introduced stricter security requirements. As a result, those responsible for procurement did not formulate high standards for fear of accusations of mismanagement or even corruption. In cases where higher requirements were successfully pushed through, external audits may have found them to be unwarranted expenditure, raising suspicions. This systemic arrangement led to a vicious circle:

- CI operators formulate high requirements for CI security based on standards and good practices,
- procurement cells (or boards) reject these requirements citing the need to reduce costs and avoid potential accusations of mismanagement,
- controlling authorities act in a way that de facto favours the lowest price, ignoring real security needs,
- providers of high quality services, equipment and other solutions cannot compete effectively because they have no other arguments than price,
- providers of low quality services and equipment win contracts by offering solutions of questionable effectiveness and origin.

In this situation, it became necessary to introduce regulations that would make the quality and safety requirements for CI impossible to circumvent. The CER Directive, in Article 16 and Recital 34, clearly indicates that Member States should encourage the use of standards, which in the case of Poland required a firmer approach. The adoption of the minimum harmonisation model has allowed the development of mechanisms to eliminate the possibility of circumventing quality requirements and thus close the systemic gaps that have hindered the application of high security standards for years.

Moreover, the draft implementation of the CER Directive takes into account the provisions of the *Act of 5 August 2010 on the protection of classified information* as the most important for ensuring an adequate level of protection of the documentation produced and the solutions used. In addition, the application of these provisions makes it possible to take advantage of the regulations provided for in Article 12 of the *Act of 11 September 2019 – Public procurement law*, which, in certain cases, allows

for the implementation of orders in a mode other than that provided for in the Act. This solution, resulting from the need to adapt the procedures to the specifics of CI, is part of the concept of raising security standards and shaping requirements for services and organisational and technical solutions.

Standardisation of organisational and technical solutions and requirements for services and persons in the Polish proposal for implementation of the CER Directive

CI security standardisation is a process of systemic unification of requirements for CI protection that draws on both international and European standards, as well as national standards, guidelines or recommendations such as NPOIK. It is a process that draws on standardisation, but also precisely defines requirements, unifies them and adapts them to the specifics of CI, taking into account specific threats and growing sectoral interdependencies. It encompasses the entire ecosystem of stakeholders: CI operators, critical actors, service providers, public administrations, supervisory and control bodies, as well as entities or persons conducting validation (audits and certifications) of the solutions used. The main objectives of standardisation are: to ensure consistent and effective protection measures, reduce risks and build systemic resilience to different types of threats.

This process takes the dynamically changing security challenges into account. It requires a flexible approach to updating and improving security measures. The introduction of uniform standards allows for a more effective risk management system, the elimination of its weaknesses and the strengthening of interoperability between those responsible for the security of CI. Consequently, standardisation provides not only a higher level of protection, but also transparency and predictability in terms of requirements and delivery mechanisms.

CI operators and critical entities

The Polish proposal to implement the CER Directive describes the requirements for CI operators and critical entities. According to the draft law, a CI operator is (...) *the owner or holder of a facility, equipment, installation, network, system and service or functionally interconnected*

facilities, equipment, installations, networks, systems and services on the list of critical infrastructure, while a critical entity (i.e. an entity identified under the CER Directive) is (...) *a CI operator included in the list of critical entities, providing at least one essential service, operating in a sector or sub-sector listed in the Annex to the Act and conducting activity on the territory of the Republic of Poland or in maritime areas of the Republic of Poland, referred to in the Act of 21 March 1991 on maritime areas of the Republic of Poland and maritime administration*. Critical infrastructure, in turn, is defined as:

> (...) facility, equipment, installation, network, system and service or functionally interconnected facilities, equipment, installations, networks, systems and services necessary for:
> a) the pursuit of important state interests, including ensuring the functioning of public administration bodies,
> b) ensuring the functioning of enterprises,
> c) satisfying and maintaining the needs of citizens, including those of a local nature,
> d) ensuring the provision of essential services.

A critical entity is a CI operator that provides at least 1 essential service and the occurrence of a so-called 'significant incident' could cause a major disruption to its provision. The inclusion in the list of critical entities is based on an analysis of the thresholds of materiality of the disruptive effect, which will be defined in an implementing act of the Council of Ministers. The assessment of the materiality of the disruptive impact shall take into account, among other things: the number of users dependent on the service in question; the interconnectedness between sectors; the impact of the incident on the economy, society, public safety and the environment; the market share of the entity in question; the geographical area affected by the possible incident; and the availability of alternative means of providing that service.

Standardisation of requirements for CI operators. Statutory requirements and minimum safety standards

The draft implementation of the CER Directive introduces new obligations for CI operators, including a systematic risk analysis and the implementation of appropriate solutions adapted to the results, in line with the so-called NPOIK six-pack.

Legislative work has succeeded in developing an approach that will oblige CI operators to implement the minimum requirements to the extent

indicated. This is a game changer to address the system and operational problems described in the previous chapter, which have so far prevented the implementation of appropriate solutions despite the existence of NPOIK, norms and many other standards. The minimum standards will be set by regulation and will apply to the entire so-called six-pack. They will be developed taking into account recommendations of a specialist nature on the protection of CI, necessary for the implementation of CI security solutions, its location and characteristics and the need to take measures to ensure its security. The author of this article is a co-author of these standards (they are in an approval process). They provide a tool to ensure a consistent and uniform approach to the protection of CI, in line with the requirements set out in the draft Act. This document may have a broad impact on the entire security industry in Poland and Europe and to be a source of knowledge and inspiration not only for CI operators. It is therefore worth describing it in more detail, with a particular focus on physical security, so much emphasised in the CER Directive.

The standards flesh out the concept of CI protection as a process divided into the following stages:

1) identification of the scope of activities, the objectives to be achieved in the protection of CI and the addressees of these activities,
2) identification of critical resources, functions and identification of the network of relationships (dependencies) with other CI sectors, including entities and bodies,
3) identification of roles and responsibilities of participants in the CI protection process,
4) risk estimation,
5) identification of priorities for action and their prioritisation depending on the results of the risk assessment,
6) development and implementation of the CI protection system, including:
   – identification of design criteria and installation of technical security systems in CI facilities,
   – development, application and ongoing updating of CI protection documentation,
7) testing (through exercises) and reviewing (through self-assessment and audit or certification) of the CI protection system and measuring progress towards the goal,

8) improvement understood as introducing modifications and corrections as a result of tests, reviews, measurements and the use of intelligent solutions, which should include the protected assets, the threats to these assets and their levels of protection against identified threats.

The stages that require special attention and care are the risk assessment and the development and implementation of a CI protection system. This system should apply to all types of identified threats, both natural and intentional and technical, and be prepared to restore the functions performed by the CI as quickly as possible. Accordingly, the measures taken to ensure security are aimed at minimising the risk of disruption to the functioning of CI by:

- reducing the likelihood of a risk occurring,
- reducing vulnerability to risks,
- minimising the impact of the risk.

The standards introduce consolidated definitions of terms relevant to the implementation of all scopes from the so-called six-pack. For example, risk-related terms are defined as follows:

- risk – the likelihood of a hazard occurring with its consequences,
- sources of risk – elements or factors that may lead to the occurrence of risk, may arise from hazards, vulnerabilities, characteristics and type of assets, organisational or technical environment, behaviour, actions or mistakes of individuals,
- risk criteria – a set of principles and benchmarks defining the acceptability of risks, established taking into account the objectives of the organisation, the internal and external context and applicable laws, regulations and standards,
- risk identification – the process of finding, identifying and describing risks, including the identification of resources subject to risk, the identification of their sources and potential consequences,
- risk analysis – the process of determining the level of risk by assessing the likelihood of events arising from risks and their potential consequences, taking into account existing vulnerabilities and safeguards,
- risk assessment – the process of comparing the results of a risk analysis with accepted risk criteria to determine the acceptability of the risk and the need for remedial action,

– risk evaluation – the overall process of identifying, analysing and evaluating risks.

The definitions have been developed taking into account a number of standards from the risk field and the context of their application in the standards being developed[25]. It is worth recalling that the risk-based approach has been the philosophy for ensuring CI safety in Poland for many years and has been reinforced by the objectives set by the CER Directive. This approach allows CI operators to use a range of solutions, depending on their own risk assessment. For example, technical security systems (i.e. intrusion detection systems, access control systems and CCTV systems) should, once installed, meet the requirements of the Polish Standard relevant to the technical security system in a degree of security appropriate to the risk assessment, with a degree of security no lower than level three being recommended[26]. The standards describe in great detail the minimum technical parameters that should be used for CI protection equipment.

The draft law also includes a provision that forces operators to request certificates from service providers (when developing and concluding contracts to ensure implementation of the so-called 'six-pack'). In the absence of these, other documents specific to particular solutions, confirming relevant competences of service providers and authorisations necessary for implementation of these solutions, are also taken into account, in accordance with EU mutual recognition rules. In terms of physical security, in the context of the design, installation and maintenance of technical security systems, this can be expected to be a certificate of conformity with the PN-EN 16763 *Services for fire safety systems and security systems*.

[25] PN-ISO 31000:2018-08 *Risk management – Guidelines*; PN-ISO 31000:2012 *Risk management – Principles and Guidelines*; PN-EN ISO/IEC 27005:2025-01 *Information security, cybersecurity and privacy protection – Guidelines on managing information security risk*; PN-ISO/IEC 27005:2014-01 *Information technology – Security techniques – Information security risk management*; PN-EN IEC 31010:2020-01 *Risk management – Risk assessment techniques*; PKN-ISO Guide 73:2012 *Risk management – Vocabulary*.

[26] Pursuant to: PN-EN 50131-1 *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*; PN-EN 60839-11-1 *Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements*; PN-EN 62676-1-1 *Video surveillance systems for use in security applications – Part 1-1: System requirements – General*.

The original idea of standardising requirements for critical entities – security management system, auditing and certification

The original idea behind the implementation of Article 13 of the CER Directive was to establish a security management system for critical entities, which would complimentarily cover aspects relating to risk assessment, quality of service, the organisational-technical solutions used and the assessment of their compliance, as well as those relating, for example, to the implementation of other requirements under sectoral EU legislation. The organisational and technical solutions were based on an information security management system compliant with PN-EN ISO/IEC 27001, taking into account the hard requirements for technical security systems, which were to be installed in accordance with PN-EN 50131 and/or PN-EN 60839 and/or PN-EN 62676. The most important element also became the establishment of a business continuity management system compliant with PN-EN ISO 22301 to the extent necessary to maintain the provision of the essential service.

The culmination of this idea was to formalise audits of the security management system of critical entities and to provide for the possibility of using certification as an alternative to audit. This was based on Article 21 of the CER Directive, which allows Member States to specify requirements for assessing the conformity of the organisational and technical arrangements implemented and to oblige critical entities to apply appropriate security measures. In this way, the security management system proposed in the draft implementation was intended to be a coherent, standardised whole and to address both the problems associated with the lack of uniform requirements and the long-standing difficulties in ensuring high quality security at CI.

The audit commitment covered 3 key pillars: the information security management system, the business continuity management system and the technical security systems. Critical entities were able to perform these audits in a flexible manner, adapted to their specific characteristics and organisational structure. The proposed solution allowed audits to be conducted in an integrated manner, then covering all 3 pillars simultaneously, or in a disconnected manner, e.g. by certifying the information security management system, auditing technical safeguards at the same time and conducting a separate business continuity audit. This model allowed for more freedom in the selection of auditors or certification bodies and also gave the possibility to involve internal auditors to a certain extent. More specifically, some of the organisational and

technical arrangements could be subject to an internal audit, carried out by qualified auditors who were employees of the entity, while some could be certified by external certification bodies. The introduction of mandatory audits and the possibility of certification for compliance with Polish Standards was intended to ensure the unification of requirements and their enforcement, as well as to increase transparency and predictability in terms of the control mechanisms applied. What is more, it became a very important element of the system to oblige the critical entity to demand appropriate competences confirmed by a certificate from service providers who are to implement various organisational and technical solutions for the entity. Thus, already the initial stage of the whole process of implementing the security management system has been secured in terms of quality and compliance with the described requirements. The use of such tools in the Polish implementation of the CER Directive was intended not only to facilitate the implementation of effective security management measures by critical entities, but also to break the vicious circle that had been hindering the raising of CI protection standards for years. The concept described in the course of inter-ministerial arrangements, opinions and a number of public consultations has gained recognition and evolved in the right direction.

Standardisation of requirements for critical entities – an evolved concept, included in the current draft implementation of the CER Directive

The critical entity under the draft law will be required to implement an integrated safety management system for the provision of the essential service. A pillar of this system is to conduct a systematic risk assessment taking into account:

a) threats and associated risks listed in the National Risk Assessment and other risks specific to the essential service provided, including antagonistic threats,
b) the degree of dependence of other sectors or sub-sectors identified in the Annex to the Act on the essential service provided by the critical entity, and the degree of dependence of that critical entity on essential services provided by other entities in other sectors, including, where applicable, neighbouring Member States of the European Union and third countries,
c) the identification of alternative supply chains for the re-establishment of the essential service,
d) risk assessments carried out under separate legislation.

The standardisation of the approach to risk assessment is one of the objectives of the CER Directive, which has been realised in a complementary manner in the Polish proposal. In particular, it is worth citing that the National Risk Assessment, a document for which the RCB will be responsible, will include:

1) identified significant threats, in particular:
   a) constituting a natural disaster or technical failure within the meaning of the provisions of the Act of 18 April 2002 on the state of natural disaster (Journal of Laws of 2017, item 1897),
   b) hybrid,
   c) cyber security,
   d) of a terrorist nature,
   e) that may cause unavailability of essential services,
   f) others that may cause significant adverse effects on the population, economy or cultural assets;
2) threats not clearly identified that may occur in the future;
3) an assessment of the risk of occurrence of identified significant threats.

In carrying out the risk assessment, the critical actor should not only use the 'classic' risk standards mentioned earlier, but also the new technical specification ISO/TS 31050 *Risk management – Guidelines for managing an emerging risk to enhance resilience*, according to which it is important to develop an approach to managing new, hitherto unknown risks, such as those related to the development of artificial intelligence[27].

A further element of the integrated security management system for the provision of the essential service will be the implementation by the critical entity of organisational and technical arrangements that are appropriate and proportionate to the results of the risk assessment, in particular:

a) risk management policies,
b) physical security, including physical protection of the critical entity's buildings and premises and technical safeguards, including access control,
c) protection of critical infrastructure necessary for the provision of the essential service, in accordance with the critical infrastructure

[27] See in more detail: A. Tatarowski, *Building resilience of critical infrastructure...*

protection requirements referred to in the provisions of Chapter 7 of the Act,
d) personal security regarding employees and external suppliers,
e) cyber security, in accordance with the requirements for key entities referred to in the provisions of the Act of 5 July 2018 on the national cybersecurity system,
f) legal security of the provision of the essential service,
g) business continuity and recovery, including maintaining its own back-up systems to ensure security and sustain the operation of the provision of the essential service until it is fully recovered,
h) the ability to protect classified information to the extent necessary for the provision of the essential service,
i) training and exercises of staff to prepare them for various types of threats and incidents,
j) performance of periodic audits and certification.

The above provisions contained in the form of detailed tasks, prepared in accordance with the formal requirements of Article 91(1) of the *Constitution of the Republic of Poland of 2 April 1997*, correspond to the normative assumptions of the information security management system and the business continuity management system, taking into account aspects relating to physical security and technical safeguards, and are therefore elements to meet the requirements set out in the standards to be indicated in the implementing act. The RCB concept envisages the identification of at least the following standards:

1) EN ISO/IEC 27001 *Information security, cybersecurity and privacy protection. Information security management systems. Requirements*,
2) PN-EN ISO 22301 *Security and resilience. Business continuity management systems. Requirements*,
3) PN-EN 50131-1 *Alarm systems. Intrusion and hold-up systems. Part 1: System requirements*,
4) PN-EN 62676-1-1 *Video surveillance systems for use in security applications. Part 1-1: System requirements. General*,
5) PN-EN 60839-11-1 *Alarm and electronic security systems. Part 11-1: Electronic access control systems. System and components requirements*.

This implementing act will be complemented by the possibility for a critical entity authority (i.e. a sector-specific minister or other authority, such as the Chairman of the Financial Supervision Authority) to develop and make available an additional list of standardisation documents (i.e. standards, technical specifications or other documents setting out principles, guidelines or characteristics). This list, published on the entity's

BIP website, will provide a tool for updating and clarifying the necessary requirements. Consequently, the critical entity will be obliged to take into account both the provisions of the implementing act and the complementary list when implementing the relevant organisational and technical solutions, thus allowing for greater flexibility in the context of a dynamically changing regulatory and technological environment. A good example illustrating the rationale for this is the requirements for external security systems. Currently, the technical specification[28] adopted by PKN operates in English, which makes it impossible to refer to it in legal acts. Once it is translated into Polish, which can be expected at the earliest in 2026, it will be easier and much quicker to incorporate it into requirements that will furthermore be targeted at a specific sector or subsector.

As a success may be considered the introduction in the draft act of an obligation for critical entities (translated 1 to 1 of the obligations defined for CI operators) to require from service providers – when developing and concluding contracts ensuring the implementation of organisational and technical solutions – *certificates, taking into account equivalent ones, in accordance with the principles of mutual recognition in the European Union or, in the absence thereof, other documents appropriate for particular solutions, confirming the possession of appropriate competences and authorisations necessary for their implementation*. Conceptually, the list of certificates was to be included in an implementing act, but due to the evolution of organisational and technical solutions and ways of defining competences, it is impossible to publish a list satisfactory to all stakeholders. It was decided that the optimal solution would be for the critical entity authorities to compile and publish such a list on their respective BIPs. In this case, the critical entity authority is obliged – before publishing the list – to consult the relevant sectoral competence council referred to in Article 4c(1)(2) of the *Act of 9 November 2000 on the establishment of the Polish Agency for Enterprise Development*. The same mechanism is applied to CI operators. In the area of physical security, which includes technical security systems, there are various options for confirming competences and qualifications. One example is the certification for compliance with PN-EN 16763, which covers, among other things, the design, installation and maintenance of technical security systems. This standard, published in Polish, has

[28] PKN-CLC/TS 50661-1:2024-10 *Alarm systems – External perimeter security systems – Part 1: System requirements*.

been discussed at many conferences (including those on CI organised by the RCB) and industry training courses, and the market (technical security companies) is adapted to certification for compliance with it. Such certification could be indicated in the originally planned implementing act. On the other hand, the standards on private security services for CI[29], which offer the possibility of certification, could not be used in the regulation as reference documents for assessing the competence of service providers delivering security services due to the lack of their Polish translation.

These standards are gaining increasing interest within the EU itself as well as in Member States. According to a presentation by the Confederation of European Security Services to the PROCIV–CER group, these standards should play a fundamental role in translating the security principles of the CER Directive into concrete operational requirements. It emphasised that private security service providers are an integral part of the security chain and its effectiveness depends on the quality of each link. In this context, the standards were identified as a key tool to enhance the quality of protection of critical entities and increase their resilience to threats. It was also indicated that the use of these standards is a recommended pathway to ensure high standards in the area of CI protection and supports the objectives of the CER Directive[30]. Thus, it should be emphasised that Polish legislative solutions are distinguished by pragmatism and flexibility. They enable the smooth implementation of standards as a tool for enhancing the quality of services. The consultation mechanism, taking into account the opinions of the sectoral competence councils, is an important support for the bodies for critical subjects. As a body representing an entire sector (e.g. the Security and Safety of Property and Persons sector), the sector council gathers information from key stakeholders, allowing for the ongoing identification of needs and the adaptation of competence requirements to changing market and regulatory realities.

Thanks to this mechanism, the various standardisation documents can be incorporated into market practice through the publication of reference

[29] PN-EN 17483-1:2021-11 *Private security services – Protection of critical infrastructure – Part 1: General requirements*; PN-EN 17483-2:2024-03 *Private security services – Protection of critical infrastructure – Part 2: Airport and aviation security services*; PN-EN 17483-3:2024-03 *Private security services – Protection of critical infrastructure – Part 3: Maritime and port security services.*

[30] Confederation of European Security Services, *How standards drive quality and resilience in critical entities security*, 5.02.2025, EU Council PROCIV–CER Working Party.

statements on BIP websites. This solution avoids formal barriers that could inhibit the implementation of organisational and technical solutions by competent service providers and make it difficult to adapt requirements to evolving security challenges. At the same time, the obligation to consult the sector council ensures that the compilations reflect the actual needs of the market, taking into account both operational practice and international standardisation trends. Sectoral competence councils play an important role in shaping qualification and competence standards in specific areas of the economy. They are advisory bodies, brought into existence on the basis of the Act on the establishment of the Polish Agency for Enterprise Development, whose task is to identify competence gaps, recommend educational solutions and support the processes of certification and validation of professional skills. Their particular value is the broad representation of key stakeholders – public administration, educational institutions, industry organisations and enterprises – which allows for effective adaptation of competences to real market needs.

The solutions presented show that the Polish implementation of the CER Directive not only meets its objectives, but also sets out modern legislative solutions, thanks to which the application of standards becomes a real mechanism for improving the quality of services provided to critical entities.

The standardisation of the integrated safety management system for the provision of the essential service is encapsulated by the obligation for critical entities to audit this system, at least once every 3 years, at their own expense. The audit will cover the following:

1) information security management;
2) business continuity management of the essential service;
3) physical security, including physical protection of the critical entity's buildings and premises and technical security, including access control.

The audit would be conducted by:

1) a certification body appropriate to the scope,
2) at least 2 auditors, 1 of whom has completed lead auditor training, are certified as specified in the implementing act and meet the personal and industrial security requirements for access to information classified 'confidential'.

The general premise of an audit is to assess compliance now and in the past; an audit can have a legal and normative purpose and should fulfil a business need. It is based on 7 principles, listed in the relevant standard[31]:

1) integrity as a basis for professionalism,
2) honesty in the presentation of results,
3) professional due diligence,
4) confidentiality,
5) independence,
6) an evidence-based approach,
7) a risk-based approach.

The idea that certification bodies should conduct audits (which, after all, do not have to end in a certificate, just an audit report) had already emerged and was adapted from the Act on the National cybersecurity system. Indeed, certification bodies are institutions whose competences, rules and ethics are defined by regulations stemming from the European conformity assessment system (described in the next chapter). An alternative to a certification body are auditors, who will be competent and give a guarantee of secrecy, confirmed by an appropriate security clearance.

The manner of verification of auditors' qualifications (including their competence) will be specified in the implementing act and will take into account the list of certificates authorising the performance of audits, as well as the scope of expertise and experience of the auditors. In the case of the information security management system and the business continuity management system, it can be expected to refer to the certificates of the lead auditor in a given scope, which are, incidentally, very popular on the market. It can be assumed that for technical security systems, on the other hand, certification of a lead auditor for an information security management system in the specialisation of technical security systems will be required, as there is no standard in the field of security systems that would allow certification of lead auditors. Thus, the certification of a lead auditor for this field draws from the established methodology in the market for auditing information security management systems.

Audits would be allowed to be conducted by internal auditors – employees of the critical entity, who are not subject to a security clearance, but the critical entity may conduct a background check on them. It shall

[31] PN-EN ISO 19011:2018 *Guidelines for auditing management systems*.

in particular take into account information obtained from criminal records (the National Criminal Register and analogous registers in EU countries). The terms of reference are uniform for auditors who are employees of the critical entity and external auditors, so an internal auditor must have the competence of a lead auditor in order to conduct an audit under the Act.

The audit may be replaced by certification of the organisational and technical arrangements by an approved body. In such a case, the holding of a certificate by the critical entity in the relevant scope shall be considered equivalent to the fulfilment of the audit obligation.

The CER Directive also sets objectives for the control and punishment of critical entities, which are also implemented in the Polish proposal. Critical entities will be subject to fines in cases where:

- do not carry out a systematic risk assessment,
- do not implement organisational and technical solutions,
- do not keep records of the solutions implemented,
- do not follow up on audit recommendations,

and others.

Inspiration for auditing and certification in the implementation of the CER Directive. Mandatory and voluntary conformity assessment

The intention of the European Community countries was to develop such a model of conformity assessment system, which would harmonise the requirements for products within the common European market. This goal was guided by the principle of mutual recognition, known in the literature as the Cassis de Dijon[32], according to which goods legally manufactured and marketed in one EU country should be allowed to enter the markets of other Member States[33]. In view of the objectives of removing barriers to trade while ensuring safety for its consumer and user, the manufacturer of a product or the manufacturer's authorised representative or importer of that product is involved in the conformity

[32] The name refers to the European Court ruling on the introduction of a liqueur of that name on the German market.

[33] Judgment of the Court of 20 February 1979 – Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. – Reference for a preliminary ruling: Hessisches Finanzgericht – Germany. – Measures heaving an effect equivalent to quantitative restrictions. - Case 120/78, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:61978CJ0120 [accessed: 28.02.2025].

assessment system in a differentiated manner (mandatory or voluntary area), depending on the type of product in question. In a nutshell, the entire scope of EU legislation on conformity assessment relates primarily to the safety of products and their authorisation to be placed on the market. The EU legislation introduces a framework for the market surveillance of products to ensure that these products meet high requirements in terms of protecting public interests such as general health and safety, health and safety in the workplace, consumer protection, environmental protection and public security[34]. A general framework of rules and principles has been defined in relation to accreditation and market surveillance:

1) 'accreditation' means an attestation by a national accreditation body that a conformity assessment body meets the requirements set out in harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes needed for the performance of specific conformity assessment activities;
2) 'national accreditation body' means the sole authoritative body in a Member State that performs accreditation with authority derived from the State;
3) 'conformity assessment' means the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled;
4) 'conformity assessment body' means a body that performs conformity assessment activities including calibration, testing, certification and inspection [35].

In Polish legislation, the conformity assessment system is regulated by the *Act of 13 April 2016 on conformity assessment and market surveillance systems*, which primarily defines the principles of operation of the conformity assessment system in Poland and the principles of operation of the control system for products placed on the market. Its two main objectives are:

[34] *Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.*

[35] Ibid. See also: *Regulation (EU) 2019/515 of the European Parliament and of the Council of 19 March 2019 on the mutual recognition of goods lawfully marketed in another Member State and repealing Regulation (EC) No 764/2008*; *Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC*; *Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety*.

– elimination of risks to the life or health of users and consumers posed by products, as well as risks to the environment,
– creation of conditions for reliable assessment of products through their testing, inspection and certification by competent and independent bodies.

The infrastructure of the conformity assessment system consists of notified, certifying, testing (research and calibration laboratories), inspection and accreditation bodies. In Poland, the national accreditation body is the Polish Centre for Accreditation.

The aforementioned Act, like the European legislation, focuses on mandatory conformity assessment, which is evident in the very definitions cited in the Act, where, for example, a certificate is understood as (...) *or product manufacturing process complies with the requirements* (Article 4, point 4). A notified body, in turn, is a conformity assessment body (i.e., in accordance with Article 4(11), one as referred to in Article 2(13) of Regulation (EC) No. 765/2008) operating in the regulated area – in accordance with Article 4(12). As Anna Stankowska, Adam Muszyński and Sławomir Wilczyński write[36]:

> (...) where the law lays down requirements with regard to the subject matter, conformity assessment shall be obligatory and the conformity assessment bodies/organisations which by law undertake such assessment shall be identified where the law so requires. The conformity assessment body (third party) designated in the directive to participate in the conformity assessment must be notified. Notification serves to formally demonstrate the competence of that body to carry out specific conformity assessment tasks.

Patterns from the mandatory conformity assessment system, developed at the EU level and clarified in Poland, were an important point of reference when formulating legislative solutions for auditing and certification of organisational and technical solutions implemented by critical entities. It should be emphasised that the standards applicable to these solutions are not subject to mandatory certification, but it is possible to assess compliance with them on a voluntary basis. For the purposes of the draft law, the following definitions have therefore been adopted.

[36] A. Stankowska, A. Muszyński, S. Wilczyński, *System oceny zgodności* (Eng. Conformity assessment system), in: *Normalizacja*, T. Schweitzer (eds.), Warszawa 2013, Polski Komitet Normalizacyjny, p. 169.

The certification body was defined as (...) *a conformity assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on conformity assessment and market surveillance systems* (Journal of Laws of 2022, item 1854) *or authorised to certify pursuant to the provisions of the Act of 12 September 2002 on standardisation* (Journal of Laws of 2015, item 1483), which not only takes into account the provisions of Regulation (EC) No 765/2008 of the European Parliament and of the Council, but also provides opportunities for certification bodies that are not accredited. Indeed, accreditation, it should be emphasised, is required for the scopes set out in the said Regulation and the Act on conformity assessment and market surveillance systems. On the other hand, entities authorised to certification in accordance with the provisions of the Standardisation Act do not operate in the regulated area, but in a voluntary one, and have the possibility to use the only voluntary certification mark in Poland which is legally authorised, i.e. the PN mark[37].

A certificate is described as (...) *a document issued by a certification body confirming that a product, installation, system, process, service or person complies with the relevant requirements*. This is a very important definition, as the use of the term certificate is often colloquial and misused. There are also common cases – whether intentional or not – of directing interested parties to the definition set out in the Act on conformity assessment and market surveillance systems, which – when the context is not taken into account – is misleading and has great potential for manipulation and misinformation. This was particularly noticeable in the technical security systems industry. Certification, on the other hand, means (...) *the actions of a certification body demonstrating that a product, installation, system, process, service or person complies with the relevant requirements.*

The draft implementation of the CER Directive adapted the existing accreditation and authorisation mechanisms in the European and Polish legal framework as tools for validating the competence of conformity assessment bodies against standards relating to information security management system, business continuity management system and technical security systems. Taking these mechanisms into account allowed for a smooth insertion of the auditing and certification system into the well-

[37] *Regulation of the Council of Ministers of 11 October 2010 on the method of granting and using the mark of conformity with the Polish Standard.*

established legal framework, already regulating the principles of verifying the competence of conformity assessment bodies.

The primary objective was to ensure a high level of reliability and credibility of the conformity assessment process, while avoiding the introduction of overly complex, novel legal mechanisms that could generate difficulties of interpretation and implementation. Accreditation, as a recognised form of formal attestation of the competence of certification bodies, is a guarantee of independence, quality, the highest substantive and organisational level and the application of ethical principles. The analogy is with the mandate pointed in Article 7 (3) of the act of standardisation, which opens a path for entities wishing to operate in the area of certification on a voluntary basis. These solutions correspond to the market, ensure the flexibility of the system and allow it to function smoothly. An important element that completes the above explanations is the certificates operating in the market.

Summary

The year 2025 will be a landmark year for EU Member States as they finalise the transposition of the CER Directive into their national legal systems. Poland, as one of the countries most involved in this process, is setting high standards for CI protection. The proposed legislative solutions, based on normalisation, combining standardisation and conformity assessment, can set a benchmark for the other Member States, especially in the context of growing antagonistic and hybrid threats – and these are one of the biggest challenges for CI security today. In a report on the security and safety of property and persons sector in Poland, Anna Araminowicz, Piotr Klatta, Tomasz Radochoński and Magda Sierżyńska write: *At the local level, successful sabotage can reduce economic potential, causing loss of life and property, as well as endangering the life and health of residents and the environment (e.g. arson attacks on landfill sites). At the national level, any such act, due to its publicity in traditional and electronic media, can cause social unrest, panic, and the impression of chaos in the state. All these effects are targets for action in a hybrid conflict*[38].

[38] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania* (Eng. Protection and Security of Property and Persons – analysis of the sector. Survey report), Kraków 2024, MABEA sp. z o.o., p. 106.

The Polish implementation proposal stands out for its comprehensive approach to the protection of CI, as it integrates the security management system for the provision of essential service, normative requirements and auditing and certification mechanisms. Most important is the obligation to verify the competence of suppliers and service providers by recognised conformity assessment systems, thus eliminating the risks associated with poor quality organisational and technical solutions.

The geopolitical location and experience resulting from the immediate vicinity of the region of war strengthen Poland's position as a state that shapes CI security policy at the European level. The solutions adopted may become the foundation for future initiatives strengthening the resilience of strategic sectors of the economy across the EU.

Bibliography

Araminowicz A., Klatta P., Radochoński T., Sierżyńska M., *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania* (Eng. Protection and Security of Property and Persons – analysis of the sector. Survey report), Kraków 2024, MABEA sp. z o.o.

A World Built on Standards: A Textbook for Higher Education, S.A. Bøgh (ed.), Nordhavn 2015, Danish Standards Foundation.

Confederation of European Security Services, *How standards drive quality and resilience in critical entities security*, 5.02.2025, EU Council PROCIV–CER Working Party.

Idzikowska T., Banaszek K., *Rola i znaczenie normalizacji w bezpieczeństwie transportu* (Eng. The role and importance of standardisation in transport safety), „Logistyka" 2010, vol. 4.

Łunarski J., *Normalizacja i standaryzacja* (Eng. Normalisation and standardisation), Rzeszów 2014, Oficyna Wydawnicza Politechniki Rzeszowskiej.

Schweitzer T., Zielińska E., *Działalność normalizacyjna* (Eng. Standardisation activity), in: *Normalizacja*, T. Schweitzer (ed.), Warszawa 2013, Polski Komitet Normalizacyjny.

Stankowska A., Muszyński A., Wilczyński S., *System oceny zgodności* (Eng. Conformity assessment system), in: *Normalizacja*, T. Schweitzer (ed.), Warszawa 2013, Polski Komitet Normalizacyjny.

Szewczyk T., Pyznar M., *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne* (Eng. Critical infrastructure protection and asymmetric threats), „Przegląd Bezpieczeństwa Wewnętrznego" 2010, no. 2, pp. 53–59.

Tatarowski A., *Building resilience of critical infrastructure in the light of asymmetric threats and terrorism. Legislative trends in the Polish implementation of the CER Directive with particular reference to aspects of standardisation and certification of organisational and technical solutions*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 391–409. https://doi.org/10.4467/27204383TER.24.014.19402.

Tatarowski A., *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER* (Eng. Standardisation and certification of solutions under the CER Directive), *10th National Forum for Critical Infrastructure Protection*, Warszawa 2023, https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami.

Wiśniewski M., Szwarc K., Skomra W., *Continuity of Essential Services as an Emerging Challenge for Societal Resilience*, "IEEE Access" 2023, vol. 11, pp. 44615. https://doi.org/10.1109/ACCESS.2023.3271751.

Internet sources

Bennett M., Gupta V., *Dealing in Security Understanding Vital Services and How They Keep You Safe*, http://resiliencemaps.org/files/Dealing_ in_Security.July2010.en.pdf [accessed: 22.06.2022].

Dobrowolność stosowania norm (Eng. Voluntary application of standards), Polski Komitet Normalizacyjny, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn [accessed: 28.02.2025].

Narodowy Program Ochrony Infrastruktury Krytycznej (Eng. National Critical Infrastructure Protection Program), Rządowe Centrum Bezpieczeństwa, 2023.

National Critical Functions Set, CISA, https://www.cisa.gov/national-critical-functions-set [accessed: 24.06.2022].

The Polish presidency of the Council of the EU, European Council, Council of the European Union, https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/ [accessed: 28.02.2025].

Legal acts

Regulation (EU) 2019/515 of the European Parliament and of the Council of 19 March 2019 on the mutual recognition of goods lawfully marketed in another Member State and repealing Regulation (EC) No 764/2008 (Official Journal of the EU L 91/1 of 29.03.2019).

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Official Journal of the EU L 218/30 of 13.08.2008).

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 27.12.2022).

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 Directive 2) – (Official Journal of the EU L 333/80 of 27.12.2022).

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security for network and information systems across the Union (Official Journal of the EU L 194/1 of 19.07.2016).

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Official Journal of the EU L 345/75 of 23.12.2008).

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Official Journal of the EU L 11/4 of 3.12.2002).

Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards (Official Journal of the EU C 136/1 of 4.06.1985).

Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (Official Journal of the EU L 218/82 of 13.08.2008).

Act of 5 December 2024 on civil protection and civil defence (Journal of Laws 2024, item 1907).

Act of 11 March 2022 on defence of the Homeland (Journal of Laws 2024, item 248, as amended).

Act of 11 September 2019 – Public Procurement Law (Journal of Laws 2024, item 1320).

Act of 5 July 2018 on the national cybersecurity system (Journal of Laws 2024, item 1077, as amended).

Act of 13 April 2016 on conformity assessment and market surveillance systems (Journal of Laws 2022, item 1864, as amended).

Act of 5 August 2010 on the protection of classified information (Journal of Laws 2024, item 632, as amended).

Act of 26 April 2007 on crisis management (Journal of Laws 2023, item 122, as amended).

Act of 12 September 2002 on standardisation (Journal of Laws 2015, item 1483).

Act of 9 November 2000 on the establishment of the Polish Agency for Enterprise Development (Journal of Laws 2025, item 98).

Act of 22 August 1997 on the protection of persons and property (Journal of Laws 2021, item 1995, as amended).

Act of 21 March 1991 on maritime areas of the Republic of Poland and maritime administration (Journal of Laws 2024, item 1125).

Regulation of the Council of Ministers of 11 October 2010 on the method of granting and using the mark of conformity with the Polish Standard (Journal of Laws 2010 No. 198, item 1316).

Regulation of the Council of Ministers of 24 June 2003 on facilities of particular importance for state security and defence and their special protection (Journal of Laws 2003 No. 116, item 1090).

Presidential Decision Directive/Nsc-63, The White House, 22.05.1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm [accessed: 5.03.2025].

Case law

Judgment of the Court of 20 February 1979. – Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. – Reference for a preliminary ruling: Hessisches Finanzgericht – Germany. – Measures heaving an effect equivalent to quantitative restrictions. – Case 120/78, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:61978CJ0120 [accessed: 28.02.2025].

Other documents

ISO/TS 31050 *Risk management – Guidelines for managing an emerging risk to enhance resilience*.

PKN-CLC/TS 50661-1:2024-10 *Systemy alarmowe – Zewnętrzne perymetryczne systemy zabezpieczeń – Część 1: Wymagania systemowe*. (Eng. Alarm systems – External perimeter security systems – Part 1: System requirements).

PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*. (Eng. Risk management – Vocabulary).

PN-EN 16763 *Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych* (Eng. Services for fire safety systems and security systems).

PN-EN 17483-1:2021-11 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 1: Wymagania ogólne*. (Eng. Private security services – Protection of critical infrastructure – Part 1: General requirements).

PN-EN 17483-2:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 2: Usługi ochrony portów lotniczych i lotnictwa.* (Eng. Private security services – Protection of critical infrastructure – Part 2: Airport and aviation security services).

PN-EN 17483-3:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 3: Usługi ochrony morskiej i portowej*. (Eng. Private security services – Protection of critical infrastructure – Part 3: Maritime and port security services).

PN-EN 45020:2009 *Normalizacja i dziedziny związane. Terminologia ogólna*. (Eng. Standardisation and related activities. General vocabulary).

PN-EN 50131-1 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe*. (Eng. Alarm systems – Intrusion and hold-up systems – Part 1: System requirements).

PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i komponentów*. (Eng. Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements).

PN-EN 62676-1-1 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne*. (Eng. Video surveillance systems for use in security applications – Part 1-1: System requirements – General).

PN-EN IEC 31010:2020-01 *Zarządzanie ryzykiem – Techniki oceny ryzyka*. (Eng. Risk management – Risk assessment techniques).

PN-EN ISO 19011:2018 *Wytyczne dotyczące audytowania systemów zarządzania*. (Eng. Guidelines for auditing management systems).

PN-EN ISO 22301 *Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania* (Eng. Security and resilience. Business continuity management systems. Requirements).

PN-EN ISO/IEC 27001 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji. Wymagania* (Eng. Information security, cybersecurity and privacy protection. Information security management systems. Requirements).

PN-EN ISO/IEC 27005:2025-01 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji*. (Eng. Information security, cybersecurity and privacy protection – Guidelines on managing information security risks).

PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*. (Eng. Risk management – Principles and guidelines).

PN-ISO 31000:2018-08 *Zarządzanie ryzykiem – Wytyczne*. (Eng. Risk management – Guidelines).

PN-ISO/IEC 27005:2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*. (Eng. Information technology – Security techniques – Information security risk management).

Draft act amending the act on crisis management and some other acts, https://legislacja.rcl.gov.pl/docs//2/12386961/13069020/13069024/dokument711601.pdf [accessed: 6.04.2025].

Adam Tatarowski

Chairman of the Competence Council for the Protection and Security of Property and Persons at the Polish Agency for Enterprise Development. Expert of the Government Centre for Security in the field of standardisation and conformity assessment

of organisational and technical solutions used in ensuring the security of critical infrastructure. President of the Department of Technical Development for the Protection of Property TECHOM – a specialised certification body and a continuing education institution operating within the educational system. President of the All-Poland Association of Engineers and Technicians of Technical Security and Security Management 'POLALARM'. Member of the Standardisation Council at the Polish Committee for Standardisation.

Contact: tatarowski@techom.com