DOI: 10.36137/2025E

INSTYTUT KOLEJNICTWA

Railway Reports – Issue 203 (March 2025)

ISSN 0552-2145 (print) ISSN 2544-9451 (on-line)

Security Regarding Storage and Processing of Data, which are Relevant for Railway Transport Operation, in Case of Using Cloud Services

Marek PAWLIK[1]

Summary

There is no doubt that safety is one of the key prerogatives of the railway transport. This prerogative has gained presently a new dimension as a result of growing use of cloud services to support railway transport. The article therefore begins with defining and describing railway transport safety and cloud services, and then broadly describes railway security in the context of the use of cloud services.

Keywords: security, cloud services, data processing, railway transport

1. Key data on railway transport operations – introduction

Although it may seem to users (passengers and shippers) that railway transport, as a 19th century invention, does not benefit from digital data processing, in practice very many areas of this mode of transport are digitised. Railway, like other modes of transport, involves three components:

- transport infrastructure – fixed installations necessary for the functioning of transport (in the case of railways, these are: railway stations, railway lines, holding sidings, marshalling yards, loading ramps, etc.);
- means of transport – vehicles capable of moving on the transport infrastructure (in the case of railways, these are: locomotives, passenger coaches and freight wagons, electric and diesel multiple units, as well as selfpropelling vehicles operating individually and vehicles in shunting trainsets and forming trains);
- transport organization – regulations, procedures, personnel, and documentation related to the operation and maintenance of transport infrastructure and means of transport (in the case of railways, these include numerous regulations: traffic, signaling, tidiness, etc., as well as personnel involved in operation, e.g., traffic controllers, gangers, train drivers, train crews, and personnel involved in maintenance, e.g., rolling stock inspectors, acceptance commissioners, trackmasters, railway automation engineers, as well as rules for creating documentation and the operational and maintenance documentation itself).

Numerous digital solutions are used in each of these components. Examples include computer-based traffic control systems, remote power control systems, wireless data collection systems for traction energy billing, trackside detection of rolling stock defects, control of engines, doors, lighting, public address in rolling stock, rolling stock tracking systems, digital communication systems, systems for collecting and analysing data from diagnostic systems, dispatching systems – local control centres and emergency management centres, timetabling systems (mainly long-term timetabling for passenger traffic, but in parallel for goods trains thousands of individual timetables per day), passenger information systems in stations, passenger stops and on-board of rolling stock as well as for Internet access, seat reservation and ticketing systems at ticket offices, vending machines and on the Internet.

Systems to ensure their full security were built in the twentieth century as physically separated and dedicated exclusively to railway transport. The approach, for economic reasons alone, was almost completely abandoned globally. Today, railways benefit from both digital technologies used in various indus-

[1] Ph.D., D.Sc. Eng. prof.; Railway Research Institute, Deputy Director for Railway Interoperability; e-mail: mpawlik@ikolej.pl.

tries (e.g. standardised signal amplifiers and network switches), as well as transmission means that are used for many purposes and are beyond the control of railway companies (e.g. fibre optic cables used for mobile communication and the Internet).

Railway systems have life cycles of several decades (e.g. 40-year rolling stock life cycles or 30-year life cycles of computerised signalling systems), combined with several years' life cycles of successive generations of information systems (e.g. operating systems), as well as the dynamic continuous development of computer techniques (e.g. artificial intelligence, malware, big data technologies), and the rapid increase in the availability of many hardware and software digital solutions (e.g. signal generators, password cracking systems, sites discussing vulnerabilities, sites offering the possibility to order hacking services for cryptocurrencies) mean that the threat of loss of availability, authenticity, integrity and/or confidentiality of data must be taken very seriously. Since the beginning of 2022, the number of attacks has been increasing exponentially, due in part to the use of bots to search for less secure sites and the geopolitical situation (struggles between states/blocs of states in cyberspace referred to as cyberwar).

Regardless of the digital solutions that contribute to the railway system present in each of the three components that make up the railway as a transport system (infrastructure, means of transport, transport organization), railway entities, including in particular infrastructure managers and railway undertakings as major and often large companies, use digital solutions to support their activities(e.g. financial and accounting systems supporting asset management, personnel management, communication between employees and with contractors and customers). These systems, too, are currently vulnerable to cyberattacks and, for such systems too, loss of data availability, authenticity, integrity and/or confidentiality can lead to serious consequences.

There is therefore no doubt that it is necessary to ensure cybersecurity, defined as (…) *the resilience of networks and information (IT) and operational (OT) systems, with a given level of trust, to any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or related services offered or accessed through these networks and systems* (…). The challenge in this regard remains only and exclusively that of defining and ensuring *a level of trust* appropriate to railway transport.

2. Safety in railway transport and railway transport in view of security

As already mentioned, digital solutions based on data processing are used in railway transport in many areas. For ensuring traffic safety, i.e. minimising the occurrence and impact of possible train accidents and incidents; for ensuring transport safety and security in railway areas, i.e. minimising, detecting and assisting in the response to intrusions, fires, theft, etc.; for ensuring data security, in particular complying with the provisions of GDPR with regard to personal data, e.g. provided by passengers when purchasing tickets.

All these aspects are recognised and taken into account in the activities of railway companies. Particular attention is paid to traffic safety, i.e. control and communication systems. The principle is, that inoperative systems or systems whose correct operation is questionable shall not be used, replacing the operation of systems in degraded situations with personnel and appropriate procedures. This results in a decrease in capacity (the ability to carry out transport services), and therefore delays and sometimes the need to cancel or reroute some connections. From the point of view of traffic safety and transport safety, as well as GDPR legal regulations, this approach is considered to be the right one, although it does not build a good image for the railways.

However, it is important to look at railway transport from the point of view of the role it plays in the national economy, the defense of the country and the functioning of society. In this context it should be mentioned that:

- Many economic actors depend on the efficient and timely provision of transport services. Economic growth in recent decades has largely been based on improving logistics and the use of services such as door-to-door delivery and delivery at a specified time, both in supply chains from subcontractors and in customer service. Prolonged disruptions to railway operations, including those caused by unauthorised digital interference, therefore threaten many economic actors.
- Digital interference with railway transport can very seriously affect the operational capabilities of the military and the support provided to allies. Railways have played and continue to play a vital role in the evacuation of refugees, the delivery and movement of military equipment, the supply of ammunition and spare parts. For example, breaches of data confidentiality can be used to track preparations for military action and loss of data authenticity to disinformation.
- Digital intrusions into railway transport can dramatically reduce the operational capabilities of different types of services in the event of disasters. This applies to both natural disasters and artificially induced construction disasters such as the destruction of a dam. In certain situations, the black scenarios show that if railway transport is paralysed at the same time, the impact will be much more severe.

- Since February 2022, railway transport is used for diplomatic purposes. Several hundred government delegations, many prime ministers and presidents including the US president, have visited Kyiv using railway transport. The use of trains in this regard is safer than the use of other modes of transport. From this point of view, too, any unauthorized digital interference with the functioning of railway transport is unacceptable.
- Railway transport, also under peacetime conditions, is used to transport dangerous goods (flammables, explosives, corrosives, radioactive materials, etc.). Many of these loads are also transported by road. Protection means for railway transport are defined by RID regulations and for road transport by ADR regulations. The systems used by railway infrastructure managers to track high-risk goods and the systems used by railway undertakings to detect and prevent derailments are digital ones, and the quantities of dangerous goods transported on a single train can be up to two orders of magnitude greater than in case of road transport (trucks with semi-trailers up to 42/44 tons, freight trains up to 3,600/4,000 tons). In addition, trains sometimes carry different loads in different wagons, and the interaction of different dangerous goods can be very dangerous. Such interactions in other modes of transport are not encountered.
- Railway transport is used by many people to commute to work or school every day. Railway transport between cities is also a very important factor in economic, scientific and social development.

Looking at railway transport as an element indispensable to the smooth functioning of the state under various conditions, including in critical moments, shows that on the one hand, the principle of replacing inoperative systems with personnel and procedures must be preserved (for the safety of passengers, employees and bystanders), but on the other hand, it is necessary to guard well against possible cyberattacks which, with little involvement of the attackers and minimal traffic safety risks, can easily lead to serious disruption of the military forces, the state and its services.

3. Cloud services, a brief overview and cybersecurity challenge

Following "Fundamentals of Azure" (2nd edition, Microsoft Press 2016, ISBN: 978-1-5093-0296-3), the general characteristics and advantages of cloud services can be presented as follows:

(…) *Cloud computing provides a modern alternative to the traditional on-premises datacenter. A public cloud vendor is completely responsible for hardware purchase and maintenance and typically provides a wide variety of platform services that you can use. You lease whatever hardware and software services you require on an as-needed basis, thereby converting what had been a capital expense for hardware purchase into an operational expense. It also allows you to lease access to hardware and software resources that would be too expensive to purchase. Although you are limited to the hardware provided by the cloud vendor, you only have to pay for it when you use it. Cloud environments typically provide an online portal experience, making it easy for users to manage compute, storage, network, and application resources. For example, a user can use the portal to create a virtual machine (VM) configuration specifying the following: the compute node size (with regard to CPU, RAM, and local disks), the operating system, any predeployed software, the network configuration, and the location of the node. The user then can deploy the VM based on that configuration and within a few minutes access the deployed compute node. This quick deployment compares favourably with the previous mechanism for deploying a VM, which could take weeks just for the procurement cycle.* (…)

It is possible to identify a number of cloud providers that would certainly be interested in offering services to such a large customer as railway transport. Potential providers include: Alibaba Cloud, Amazon Web Services, Baidu Cloud, Cisco, Dell, Google, HPE, Huawei Cloud, IBM Cloud, Microsoft Azure, Oracle Cloud, Rackspace, Red Hat, SAP, Tencent, VMware. Cloud providers are listed in alphabetical order as neutral, as their market shares depend on how the share is estimated and change significantly from year to year.

The crucial question, however, is not whether cloud services are cheaper and more convenient than the classic solutions used up to now, but how, in an environment where information security needs to be ensured with the increase in cyberattacks and incidents, related to information security, it can be ensured that not only the security of information used by railway information (IT) and operational (OT) systems is maintained, but also increased. In doing so, it should be noted that, according to the 'Threat Landscape: Transport Sector' issued in March 2023 by the European Union Agency for Cybersecurity ENISA covering the years 2021/2022, the following types of cyberattacks should be taken into account in the case of transport: *ransomware, threats against data*, *malware*, *denial of service* (DoS, DDoS, RDoS attacks), *vulnerability exploitation*, *social engineer-*

ing, *attacks to suppliers and supply-chain attacks*, *breach/intrusion*, *credential harvesting* and *spoofing of geolocation*.

4. Information security with special focus on cloud services

PKP Polskie Linie Kolejowe S.A. and PKP Cargo S.A. currently have the formal status of key service operators granted in respect of the NIS Directive (EU Directive 2016/1148). Such status will be granted by law in the middle of next year to almost all infrastructure managers and railway undertakings in respect of the NIS2 Directive (EU Directive 2022/2555). The Directive on measures for a high common level of security for networks and information systems requires operators of essential services to adequately protect themselves against cyber threats, take appropriate action in cases of cyberattacks and incidents and exchange relevant data with the competent authorities. Defining and improving the relevant procedures is done by implementing an Information Security Management System (ISMS). The largest railway companies already have such systems in place. The others will have to implement them in the near future.

The ISMS system consists primarily of procedures related to information security management verified for compliance with the requirements of the PN-EN ISO/IEC 27001:2017-06 standard [1]. Regardless of the policies and procedures, when implementing an ISMS, it is necessary to determine appropriate security measures for data storage and processing systems. The choice of protection means is at the discretion of the entity and should be based on risk acceptance criteria. Protection means are selected taking into account the risk assessment and evaluation and the principles of information security. The principles of risk assessment and evaluation for railway transport are defined by Regulation (EU) 402/2013. On the other hand, the principles of information assurance are defined by the PN-EN ISO/IEC 27002:2017-06 standard [2]. With regard to cloud services, the provisions of PN-EN ISO/IEC 27002 are complemented by the provisions of PN-ISO/IEC 27017 [3] defining information security principles for cloud services. Both standards 27002 and 27017 refer to the same fourteen types of security controls, which are briefly discussed on the basis of these standards in the following subsections, referring to general provisions and provisions specific to cloud services. Standard 27017:2017-06 also contains additional requirements for cloud services, which are outlined in subsection 4.15.

It should be noted that all three standards on which this article is based have been replaced by new editions between 2021 and 2023. In addition, the 2023 Core Standard 27001 was revised in 2024 (details are indicated in the literature).

Binding decisions and analyses carried out for specific services that would be implemented using cloud services must be carried out on the basis of standards current at the time of the work. This does not change the perception of the risks associated with the use of cloud services for railway transport. Thus, the article deliberately relies on the provisions of outdated standards, especially as standard 27017 is quoted quite extensively. Meanwhile, it is not the intention to make the text of the standard available, but to draw the attention of the readers to the challenges and risks associated with the use of cloud services for railway transport.

Before analysing the provisions of the 27017 standard, attention should also be drawn to the need to take into account in the future use of cloud services also the requirements of the EN ISO/IEC 27018:2020 standard, relating to the interface between cloud services and the protection of personal data based on personally identifiable information (PII).

4.1. Information security policy

Objective according to 27002:2017-06:

Management provides guidance and support for information security activities in accordance with business requirements and applicable legal and regulatory requirements.

The policy should be adopted by management and communicated to employees. It should also take into account requirements derived from the business strategy, from regulations and legal and contractual provisions, and from the current and anticipated environment in which information security risks exist. For railway transport, it seems natural to link information security management with a safety management system (*SMS*), referred to in the Railway Safety Directive (EU Directive 798/2016). Linking ISMS and SMS in the case of smaller entities will allow both systems to naturally use the same resources and cover both IT and OT systems with appropriate provisions. For large entities using many disparate technical solutions operated, supervised and maintained by different internal services, linking ISMS and SMS may not be justified.

For cloud services in relation to security policy,27017:2017-06 notes that:	
Cloud service customer	**Cloud service provider**
An information security policy for cloud computing should be defined as a topic-specific policy of the cloud service customer. The cloud service customer's information security policy for cloud computing should be consistent with the organisation's acceptable levels of information security risks for its information and other assets. *When defining the information security policy for cloud computing, the cloud service customer should take the following into account:* – *information stored in the cloud computing environment can be subject to access and management by the cloud service provider;* – *assets can be maintained in the cloud computing environment, e.g., application programs;* – *processes can run on a multi-tenant, virtualized cloud service;* – *the cloud service users and the context in which they use the cloud service;* – *the cloud service administrators of the cloud service customer who have privileged access;* – *the geographical locations of the cloud service provider's organisation and the countries where the cloud service provider can store the cloud service customer data (even temporarily).*	*The cloud service provider should augment its information security policy to address the provision and use of its cloud services, taking the following into account:* – *the baseline information security requirements applicable to the design and implementation of the cloud service;* – *risks from authorised insiders;* – *multi-tenancy and cloud service customer isolation (including virtualisation);* – *access to cloud service customer assets by staff of the cloud service provider;* – *access control procedures, e.g., strong authentication for administrative access to cloud services;* – *communications to cloud service customers during change management;* – *virtualization security;* – *access to and protection of cloud service customer data;* – *lifecycle management of cloud service customer accounts;* – *communication of breaches and information sharing guidelines to aid investigations and forensics.*

The provisions of 27017:2017-06 relating to safety policy should be read in conjunction with the provisions of Directive 798/2016 on railway safety, which clearly stipulate that both the railway infrastructure manager and the railway undertaking are responsible for all risks, regardless of whether the measures to reduce the occurrence of risks and/or the measures to reduce the consequences of the occurrence of risks are carried out by internal services or outsourced to another entity/other entities. In accordance with the provisions of Directive 798/2016 and the regulations defining the so-called common safety methods that are important for safety may be outsourced, but in such cases the infrastructure manager and/or railway undertaking should supervise their implementation.

It is relatively easy to imagine that railway entities will enforce various protection means on cloud service providers, for which they will of course have to pay accordingly, but it should be considered much less likely that railway infrastructure managers and railway undertakings will be able to supervise the activities of cloud service providers.

4.2. Organisation of information security

Objectives according to 27002:2017-06:

– *Establish a governance structure to initiate and oversee the implementation and operation of information security in the organisation.*
– *Ensure security of teleworking and use of mobile devices.*

Responsibility for information security should be defined and assigned. This includes both fully internal activities and cooperation with authorities, both those responsible for information security and those responsible for railway safety, as well as cooperation with other entities that are key to the functioning of the entity, in the case of railway transport in particular, cooperation and exchange of information between infrastructure managers and railway undertakings.

For cloud services with regard to security organization, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities, and confirm that it can fulfil its allocated roles and responsibilities. The information security roles and responsibilities of both parties should be stated in an agreement. *The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service provider.*	*The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.*
The cloud service customer should identify the authorities relevant to the combined operation of the cloud service customer and the cloud service provider.	*The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organisation and the countries where the cloud service provider can store the cloud service customer data.*

Many years of experience in cooperation with railway and IT entities indicate that IT entities and their employees do not understand the risks, that may arise for railway transport from the possible loss of availability, authenticity, integrity and/or confidentiality of data. On the other hand, the use of cloud services for part of the services is perfectly legitimate, but requires adequate resources and competences. Therefore, it should be considered natural to strive for the definition of a railway entity responsible for cloud services. Such an entity, in accordance with the provisions of Directive 797/2016, could be considered the infrastructure manager, as the entity responsible for the part of the infrastructure necessary for the safe operation of railway transport. The cloud service provider would then not be supervised by multiple railway infrastructure managers and multiple railway undertakings, but, like the managers and undertakings, by the national authority responsible for railway safety - the Railway Transport Office (UTK in case of Poland).

Standard 27002:2017-06, with regard to organizations, also defines requirements for teleworking, which, in accordance with the provisions of 27017:2017-06, also apply when cloud services are used.

4.3. Human resources safety

Objectives according to 27002:2017-06:
- *Ensure that employees and contractors understand their responsibilities and are suitable candidates to fulfil the roles for which they are intended.*
- *Ensure that employees and contractors are aware of their information security responsibilities and fulfil them.*
- *Safeguard the interests of the organisation during the transition or termination process.*

It is necessary to verify job applicants and persons gaining access to sensitive data, taking into account the nature of such data and the risks associated with its possible unauthorized use. This applies to both the parent organisation and contractors. The responsibilities of the parties should be formally regulated. Particular attention should be paid to the rules for dealing with possible disciplinary dismissals or termination of contracts.

In the light of railway regulations and taking into account the broad understanding of security in railway transport, it should be pointed out that railway infrastructure managers and railway undertakings using cloud services offered by external providers should supervise, at least, the hiring, training and dismissal procedures of the provider of such services and the rules of cooperation of such provider with its sub-providers. The alternative is to build their own resources or a railway cloud run by an entity supervised by both the data security authority and the railway safety authority.

For cloud services, with regard to resource security, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should add the following items to awareness, education and training programmes for cloud service business managers, cloud service administrators, cloud service integrators and cloud service users, including relevant employees and contractors: – *standards and procedures for the use of cloud services;* – *information security risks relating to cloud services and how those risks are managed;* – *system and network environment risks with the use of cloud services;* – *applicable legal and regulatory considerations.*	*The cloud service provider should provide awareness, education and training for employees, and request contractors to do the same, concerning the appropriate handling of cloud service customer data and cloud service derived data. This data can contain information confidential to a cloud service customer or be subject to specific limitations, including regulatory restrictions, on access and use by the cloud service provider.*
Information security awareness, education and training programmes about cloud services should be provided to management and the supervising managers, including those of business units. These efforts support effective co-ordination of information security activities.	NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service provider.

4.4. Asset management

Objectives according to 27002:2017-06:

– *Identify the organisation's assets and define the appropriate responsibility for their protection.*
– *Ensure that information is assigned an appropriate level of protection, consistent with its importance to the organisation.*
– *Prevent unauthorised disclosure, modification, deletion or destruction of information stored on media.*

It is necessary to identify information and information-related assets and means of processing information, and to establish and maintain up-to-date records of such assets.

These provisions, as well as the related guidance in the standards, indicate that railway infrastructure managers and railway undertakings should monitor information-related assets. In this regard, it should be recalled that a report by the European Union Agency for Cybersecurity (ENISA), issued in November 2020 and intended for railway transport, highlighted, among other things, cyberattacks on railway transport in the UK that occurred between July 2015 and July 2016. The purpose of these attacks was to collect and transmit in an unknown direction numerous data exchanged between railway systems in preparation for an Advanced Persistent Threat (APT) cyberattack, probably on behalf of the national authorities of a hostile country. The possible loss of control of assets, e.g. historical data carriers, could reduce the time needed to prepare a targeted cyberattack on railway transport to the single days necessary, for example, for artificial intelligence to analyse the collected data.

For cloud services related to asset management, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer's inventory of assets should account for information and associated assets stored in the cloud computing environment. The records of the inventory should indicate where the assets are maintained, e.g., identification of the cloud service.	*The inventory of assets of the cloud service provider should explicitly identify:* – *cloud service customer data;* – *cloud service derived data.*

Cloud service customer	Cloud service provider
The cloud service customer should label information and associated assets maintained in the cloud computing environment in accordance with the cloud service customer's adopted procedures for labelling. Where applicable, functionality provided by the cloud service provider that supports labelling can be adopted.	*The cloud service provider should document and disclose any service functionality it provides allowing cloud service customers to classify and label their information and associated assets.*

4.5. Access Control

Objectives according to 27002:2017-06:

- *Restrict access to information and information processing means.*
- *Provide access to authorised users and prevent unauthorised access to systems and services.*
- *Ensure accountability of users to protect their authentication information.*
- *Prevent unauthorised access to systems and applications.*

Ensuring adequate access control is self-evident, but not as easy as it might seem, given the constant race between security technologies and security breach techniques, and increasingly sophisticated attempts to obtain authentication data, for example through social networks and social engineering.

For cloud services with regard to access control27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer's access control policy for the use of network services should specify requirements for user access to each separate cloud service that is used.	NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service provider.
NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service customer.	*To manage access to cloud services by a cloud service customer's cloud service users, the cloud service provider should provide user registration and deregistration functions, and specifications for the use of these functions to the cloud service customer.*
NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service customer.	*The cloud service provider should provide functions for managing the access rights of the cloud service customer's cloud service users, and specifications for the use of these functions.*
The cloud service customer should use sufficient authentication techniques (e.g., multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks.	*The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risks. For example, the cloud service provider can provide multi-factor authentication capabilities or enable the use of third-party multi-factor authentication mechanisms.*
The cloud service customer should verify that the cloud service provider's management procedure for allocating secret authentication information, such as passwords, meets the cloud service customer's requirements.	*The cloud service provider should provide information on procedures for the management of the secret authentication information of the cloud service customer, including the procedures for allocating such information and for user authentication.*

Cloud service customer	Cloud service provider
The cloud service customer should ensure that access to information in the cloud service can be restricted in accordance with its access control policy and that such restrictions are realised. This includes restricting access to cloud services, cloud service functions, and cloud service customer data maintained in the service.	*The cloud service provider should provide access controls that allow the cloud service customer to restrict access to its cloud services, its cloud service functions and the cloud service customer data maintained in the service.*
Where the use of utility programs is permitted, the cloud service customer should identify the utility programs to be used in its cloud computing environment, and ensure that they do not interfere with the controls of the cloud service.	*The cloud service provider should identify the requirements for any utility programs used within the cloud service.* *The cloud service provider should ensure that any use of utility programs capable of bypassing normal operating or security procedures is strictly limited to authorised personnel, and that the use of such programs is reviewed and audited regularly.*

The choice of the method and strength of authentication mechanisms must be linked to any risk in railway transport which may lead to a breach of railway safety in the broad sense and is related to access to current and/or historical data. The authentication mechanisms adopted, used and supervised therefore require railway expertise in the relationship between information and risks. In addition, infrastructure managers and railway undertakings must supervise the cloud provider's activities in this respect, or the provider should be supervised by both the authority responsible for information security and the authority responsible for railway safety.

4.6. Cryptography

Objective according to 27002:2017-06:

Ensure the appropriate and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

The 27002:2017-06 standard recommends both the development and implementation of a policy for the use of cryptographic security to protect information and a policy for the use, protection and validity periods of cryptographic keys and its implementation at all stages of the key life cycle. In this regard, it should be mentioned that cryptographic keys are currently used by railway control command systems, transmitting electronic movement authorities displayed in the driver's cab on the signalling dashboard and used for the on-going supervision of train driving by drivers. Cryptographic keys can also be used for many other purposes, e.g. to supervise the authorisation at a specific time for specific individuals, e.g. linking drivers to railway vehicles so that it is impossible to start and use the vehicle without being instructed/authorised to do so.

Cryptography can also be used to secure cloud services if justified by appropriate risk analysis.

For cloud services in relation to cryptography, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should implement cryptographic controls for its use of cloud services if justified by the risk analysis. The controls should be of sufficient strength to mitigate the identified risks, whether those controls are supplied by the cloud service customer or by the cloud service provider. *When the cloud service provider offers cryptography, the cloud service customer should review any information supplied by the cloud service provider to confirm whether the cryptographic capabilities:* – *meet the cloud service customer's policy requirements;* – *are compatible with any other cryptographic protection used by the cloud service customer;* – *apply to data at rest and in transit to, from and within the cloud service.*	*The cloud service provider should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the information it processes. The cloud service provider should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.*

Cloud service customer	Cloud service provider
The cloud service customer should identify the cryptographic keys for each cloud service, and implement procedures for key management. *Where the cloud service provides key management functionality for use by the cloud service customer, the cloud service customer should request the following information on the procedures used to manage keys related to the cloud service:* – *type of keys;* – *specifications of the key management system, including procedures for each stage of the key lifecycle, i.e., generating, changing or updating, storing, retiring, retrieving, retaining and destroying;* – *recommended key management procedures for use by the cloud service customer.* *The cloud service customer should not permit the cloud service provider to store and manage the encryption keys for cryptographic operations when the cloud service customer employs its own key management or a separate and distinct key management service.*	NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service provider.

It should be expected that the scale of the use of cryptography by infrastructure managers and railway undertakings will increase markedly in the years to come due to the increasing digitalisation of railway transport and the continued growth of threats due, inter alia, to the rapid development of computer techniques and the continuous increase in the availability of digital hardware and software tools.

4.7. Physical and environmental safety

Objectives according to 27002:2017-06:

– *Prevent unauthorised physical access, damage and disruption to the organisation's information and information processing assets.*
– *Prevent loss, damage, theft or loss of integrity of assets and disruption to the organisation.*

Standard 27002:2017-06 identifies and discusses aspects related to secured areas, including defining their boundaries, securing entrances, securing offices, rooms and facilities and delivery and loading areas, and protecting against external and environmental threats. It also defines recommendations for the placement and protection of equipment taking into account both environmental threats and opportunities for unauthorised access. It considers protection against power failures and support system failures (e.g. fire protection), cabling security, equipment maintenance challenges, removal of assets and their security outside the secured area, and disposal of assets (e.g. hard drives or disk arrays) and transferring them for disposal or reuse. It also addresses the challenges of potentially leaving equipment unattended and the so-called clean desk policy. All these requirements also apply to cloud services.

With regard to the scope of activities of infrastructure managers and railway undertakings, the risk of data collection for APT attacks, but also the risk of data loss and ransomware attacks and damage to reputation should once again be pointed out.

Additionally, for cloud services with regard to physical and environmental security, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should request confirmation that the cloud service provider has the policies and procedures for secure disposal or reuse of resources.	*The cloud service provider should ensure that arrangements are made for the secure disposal or reuse of resources (e.g., equipment, data storage, files, memory) in a timely manner.*

4.8. Safe operation

Objectives according to 27002:2017-06:

- *Ensure correct and secure operation of information processing means.*
- *Ensure information and information processing means are protected from malware.*
- *Protect against data loss.*
- *Record incidents and collect evidence.*
- *Ensure the integrity of production systems.*
- *Prevent the exploitation of technical vulnerabilities.*
- *Minimise the impact of audit activities on production systems.*

Standard 27002:2017-06 broadly defines operational security and related recommendations, taking into account in particular issues such as documenting operations, change management, capacity management, separation/isolation of development, testing, and production environments, protection against malware, backing up data and software and recovering data and software from backups, event logging, protecting information stored in logs, recording administrator and operator activities, clock synchronization, and supervision of production software, including software installation and updates, vulnerability management and minimization of risks related to digital system audits.

From a railway transport point of view, both the protection means for operational safety and their link to solutions designed to ensure business continuity deserve special attention, as outlined in section 4.13.

Both infrastructure managers and railway undertakings must ensure the security of information in both information (IT) and operational (OT) systems without question. Risks, and consequently protection means, depend on the types of threats, which should be identified and analyzed taking into account traffic safety, protection of life, health and property, GDPR legal regulations, maintaining the operational capabilities of the military and emergency services, as well as the safety of citizens and the functioning of the state.

For cloud services in relation to safe operation,27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer's change management process should take into account the impact of any changes made by the cloud service provider.	*The cloud service provider should provide the cloud service customer with information regarding changes to the cloud service that could adversely affect the cloud service. The following will help the cloud service customer determine the effect the changes can have on information security:* – *categories of changes;* – *planned date and time of the changes;* – *technical description of the changes to the cloud service and underlying systems;* – *notification of the start and the completion of the changes.* *When a cloud service provider offers a cloud service that depends on a peer cloud service provider, then the cloud service provider might need to inform the cloud service customer of changes caused by the peer cloud service provider.*
The cloud service customer should ensure that the agreed capacity provided by the cloud service meets the cloud service customer's requirements. *The cloud service customer should monitor the use of cloud services, and forecast their capacity needs, to ensure performance of the cloud services over time.*	*The cloud service provider should monitor the total resource capacity to prevent information security incidents caused by resource shortages.*

Cloud service customer	Cloud service provider
Where the cloud service provider provides backup capability as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider. The cloud service customer should also verify that they meet their backup requirements. *The cloud service customer is responsible for implementing backup capabilities when the cloud service provider does not provide them.*	*The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, as appropriate:* – *scope and schedule of backups;* – *backup methods and data formats, including encryption, if relevant;* – *retention periods for backup data;* – *procedures for verifying integrity of backup data;* – *procedures and timescales involved in restoring data from backup;* – *procedures to test the backup capabilities;* – *storage location of backups.* *The cloud service provider should provide secure and segregated access to backups, such as virtual snapshots, if such service is offered to cloud service customers.*
The cloud service customer should define its requirements for event logging and verify that the cloud service meets those requirements.	*The cloud service provider should provide logging capabilities to the cloud service customer.*
If a privileged operation is delegated to the cloud service customer, the operation and performance of those operations should be logged. The cloud service customer should determine whether logging capabilities provided by the cloud service provider are appropriate or whether the cloud service customer should implement additional logging capabilities.	NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service provider.
The cloud service customer should request information about the clock synchronisation used for the cloud service provider's systems.	*The cloud service provider should provide information to the cloud service customer regarding the clock used by the cloud service provider's systems, and information about how the cloud service customer can synchronize local clocks with the cloud service clock.*
The cloud service customer should request information from the cloud service provider about the management of technical vulnerabilities that can affect the cloud services provided. The cloud service customer should identify the technical vulnerabilities it will be responsible to manage, and clearly define a process for managing them.	*The cloud service provider should make available to the cloud service customer information about the management of technical vulnerabilities that can affect the cloud services provided.*

4.9. Communication security

Objectives according to 27002:2017-06:

– *Ensure the protection of information in networks and supporting means of information processing.*
– *Maintain the security of information transmitted within the organisation and exchanged with external parties.*

An adequate level of security for data exchange must be secured in particular by protecting information in systems and applications, protecting network services from unauthorised access, selecting network security appropriately, or ensuring appropriate levels of service provision. It is also recommended to separate information services, users and information systems in the network structure. From the point of view of risk analysis in railway transport, it will also make sense to separate operational systems potentially with levels of protection depending

on the risks identified, if the operational systems are based on cloud services. For railway transport, it will be necessary to implement a formal policy for the transmission of information, procedures and protection means to protect information transmitted using all means of communication. This should take into account the transfer of information between cooperating entities, appropriate protection of electronically transmitted information, and confidentiality agreements.

In the case of railway transport, the diversity of applications of digital solutions and the scale of the use of information and operational systems in the analyses require the consideration of risks and, following them in security, the possibility of mitigating threats through network segmentation and network microsegmentation.

For cloud services in relation to communication security, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should define its requirements for segregating networks to achieve tenant isolation in the shared environment of a cloud service and verify that the cloud service provider meets those requirements.	*The cloud service provider should enforce segregation of network access for the following cases:* – *segregation between tenants in a multi-tenant environment;* – *segregation between the cloud service provider's internal administration environment and the cloud service customer's cloud computing environment.* *Where appropriate, the cloud service provider should help the cloud service customer verify the segregation implemented by the cloud service provider.*

4.10. Acquisition, development and maintenance of systems

Objectives according to 27002:2017-06:

– *Ensure that information security is an integral part of information systems throughout their life cycle. This includes requirements for information systems providing services on public networks.*
– *Ensure that information security is designed and implemented as part of the life cycle of information systems.*
– *Ensure the protection of data used for testing.*

For railway transport, the requirements in the standard also apply to operational systems (OT).

For cloud services in relation to systems acquisition, development and maintenance, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should determine its information security requirements for the cloud service and then evaluate whether services offered by a cloud service provider can meet these requirements. *For this evaluation, the cloud service customer should request information on the information security capabilities from the cloud service provider.*	*The cloud service provider should provide information to the cloud service customers about the information security capabilities they use. This information should be informative without disclosing information that could be useful to someone with malicious intent.*
The cloud service customer should request information from the cloud service provider about the cloud service provider's use of secure development procedures and practices.	*The cloud service provider should provide information about its use of secure development procedures and practices to the extent compatible with its policy for disclosure.*

Cloud service providers will obviously want to declare that information security is an integral part of their systems throughout the entire lifecycle. However, there is a major concern in the context of a lack of knowledge of risks in railway transport on the side of cloud provider. For example, it can be pointed out that the digital systems installed at one Polish infrastructure manager in terms of hardware are manufactured by an American entity in China. Their software is developed in the European Union, and a trusted employee from Europe each time, as part of the acceptance of the hardware, shows up at the factory, installs the software, checks the hardware and then completely erases the software. This action is to provide 100% certainty that the firmware is malware-free by uploading fully verified software to fully cleaned hardware *during* installation and configuration of the system at its future place of operation. There is some question as to whether this approach is achievable when using cloud services from suppliers in the IT market. Whether and at what scale such an approach will be necessary depends on what services and information will use cloud services.

4.11. Relations with suppliers

Objectives according to 27002:2017-06:

- *Ensure the protection of the organisation's assets shared with suppliers.*
- *Maintain the agreed level of security of information and services provided in accordance with contracts with suppliers.*

Standard 27002:2017-06 draws attention to security policy, the inclusion of security in contracts with suppliers, and supply chains for information and telecommunication technology. For railway transport, similar rules should apply to operational systems (OT). The November 2020 ENISA report points out that railway infrastructure managers have limited capacity to monitor and influence supply chains for operational systems, in particular due to the position of the signalling industry.

For cloud services in relation to supplier relationships, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should include the cloud service provider as a type of supplier in its information security policy for supplier relationships. This will help to mitigate risks associated with the cloud service provider's access to and management of the cloud service customer data.	NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service provider.
The cloud service customer should confirm the information security roles and responsibilities relating to the cloud service, as described in the service agreement. These can include the following processes: – *malware protection;* – *backup;* – *cryptographic controls;* – *vulnerability management;* – *incident management;* – *technical compliance checking;* – *security testing;* – *auditing;* – *collection, maintenance and protection of evidence, including logs and audit trails;* – *protection of information upon termination of the service agreement;* – *authentication and access control;* – *identity and access management.*	*The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider will implement to ensure no misunderstanding between the cloud service provider and cloud service customer.* *The relevant information security measures that the cloud service provider will implement can vary based on the type of cloud service the cloud service customer is using.*

Cloud service customer	Cloud service provider
NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service customer.	*If a cloud service provider uses cloud services of peer cloud service providers, the cloud service provider should ensure information security levels to its own cloud service customers are maintained or exceeded. When the cloud service provider provides cloud services based on a supply chain, the cloud service provider should provide information security objectives to suppliers, and request each of the suppliers to perform risk management activities to achieve the objectives.*

When cloud services are provided based on a supply chain, the supply chain rules also apply to cloud services. This statement is very important in the context of the possible use of cloud services (offered on the market by IT companies) by the operator of a potential railway cloud. Such a railway operator, using its knowledge and experience of railway transport risks, could, taking into account the nature and scale of the risk, decide how to use the public cloud(s) and the information and its security in such cases. Such an opportunity is likely to be particularly valuable during periods of construction, expansion and maintenance work of a possible railway cloud.

4.12. Management of incidents connected with information safety

Objective according to 27002:2017-06:
Ensure a consistent and effective approach to information security incident management, including reporting of incidents and vulnerabilities.

Standard 27002: 2017-06 defines requirements for procedures and processes for reporting incidents, reporting weaknesses/imperfections, and assessment procedures and decision-making processes for responding to cyberattacks and information security incidents, as well as drawing conclusions, taking protective measures for the future, and collecting evidence.

For cloud services in relation to incident management, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should verify the allocation of responsibilities for information security incident management and should ensure that it meets the requirements of the cloud service customer.	*As a part of the service specifications, the cloud service provider should define the allocation of information security incident management responsibilities and procedures between the cloud service customer and the cloud service provider.* *The cloud service provider should provide the cloud service customer with documentation covering:* – *the scope of information security incidents that the cloud service provider will report to the cloud service customer;* – *the level of disclosure of the detection of information security incidents and the associated responses;* – *the target timeframe in which notifications of information security incidents will occur;* – *the procedure for the notification of information security incidents;* – *contact information for the handling of issues relating to information security incidents;* – *any remedies that can apply if certain information security incidents occur.*

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the mechanisms for: – *the cloud service customer to report an information security event it has detected to the cloud service provider;* – *the cloud service provider to receive reports regarding an information security event detected by the cloud service provider;* – *the cloud service customer to track the status of a reported information security event.*	*The cloud service provider should provide mechanisms for:* – *the cloud service customer to report an information security event to the cloud service provider;* – *the cloud service provider to report an information security event to a cloud service customer;* – *the cloud service customer to track the status of a reported information security event.*
The cloud service customer and the cloud service provider should agree upon the procedures to respond to requests for potential digital evidence or other information from within the cloud computing environment.	

In railway transport, detailed regulations apply to actions to be taken in the event of accidents and incidents. The rules applicable in this regard are defined in Directive (EU) 798/2016 on railway safety. They are transposed into the Railway Transport Act. Państwowa Komisja Badania Wypadków Kolejowych PKBWK (The State Commission on Railway Accident Investigation PKBWK) and the accident committees appointed by infrastructure managers and railway undertakings play an important role in this respect. Complementary rules for monitoring the safety situation are contained in Decision 2009/460/EC on a common safety method for assessing whether safety requirements have been achieved.

Cyberattacks and information security incidents may affect the safety of traffic and/or the protection of life, health and property in railway transport, especially if they involve operational systems (OT). Therefore, at the very least, risks to traffic safety and the protection of life, health and property should be taken into account when defining the rules of cooperation between cloud service providers and customers.

4.13. Information security aspects of business continuity management

Objectives according to 27002:2017-06:

– *It is recommended to include information security continuity in the organization's business continuity management systems.*
– *Ensure availability of information processing resources.*

There is no doubt that appropriate actions need to be taken to ensure the continuity of railway transport operations. Such measures should include, but not be limited to, information security continuity issues and ensuring the availability of information processing resources. These become particularly important in situations of digital equipment and system failures, operational disruptions in railway traffic, as well as accidents and incidents. Of course, this also applies to cyberattacks and incidents related to information security. This is particularly true in the case of DoS, DDoS and RDoS attacks.

The relevant requirements defined in 27002:2017-06 are of course also applicable to the use of cloud services, but 27017:2017-06 does not define any additional requirements.

4.14. Compliance

Objective according to 27002:2017-06*:*

Avoid violations of legal, regulatory or contractual obligations related to information security and other security requirements.

In this regard, standard 27002:2017-06 contains provisions indicating the need to organize and document legal and contractual requirements, take into account intellectual property rights, protect records, privacy, and personal data, as well as regulations concerning cryptographic security. It also contains a number of provisions on information security reviews.

For cloud services in relation to compliance, 27017:2017-06 notes that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should consider the issue that relevant laws and regulations can be those of the jurisdictions governing the cloud service provider, in addition to those governing the cloud service customer. The cloud service customer should request evidence of the cloud service provider's compliance with relevant regulations and standards required for the cloud service customer's business. Such evidence can be the certifications produced by third-party auditors.	*The cloud service provider should inform the cloud service customer of the legal jurisdictions governing the cloud service.* *The cloud service provider should identify its own relevant legal requirements (e.g., regarding encryption to protect personally identifiable information (PII)). This information should also be provided to the cloud service customer when requested.* *The cloud service provider should provide the cloud service customer with evidence of its current compliance with applicable legislation and contractual requirements.*
Installing commercially licensed software in a cloud service can cause a breach of the license terms for the software. The cloud service customer should have a procedure for identifying cloud-specific licensing requirements before permitting any licensed software to be installed in a cloud service. Particular attention should be paid to cases where the cloud service is elastic and scalable and the software can be run on more systems or processor cores than is permitted by the licence terms.	*The cloud service provider should establish a process for responding to intellectual property rights complaints.*
The cloud service customer should request information from the cloud service provider about the protection of records gathered and stored by the cloud service provider that are relevant to the use of cloud services by the cloud service customer.	*The cloud service provider should provide information to the cloud service customer about the protection of records that are gathered and stored by the cloud service provider relating to the use of cloud services by the cloud service customer.*
The cloud service customer should verify that the set of cryptographic controls that apply to the use of a cloud service complies with relevant agreements, legislation and regulations.	*The cloud service provider should provide descriptions of the cryptographic controls implemented by the cloud service provider to the cloud service customer for reviewing compliance with applicable agreements, legislation and regulations.*
The cloud service customer should request documented evidence that the implementation of information security controls and guidelines for the cloud service is in line with any claims made by the cloud service provider. Such evidence could include certifications against relevant standards.	*The cloud service provider should provide documented evidence to the cloud service customer to substantiate its claim of implementing information security controls. Where individual cloud service customer audits are impractical or can increase risks to information security, the cloud service provider should provide independent evidence that information security is implemented and operated in accordance with the cloud service provider's policies and procedures. This should be made available to prospective cloud service customers prior to entering a contract. A relevant independent audit, as selected by the cloud service provider, should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the cloud service provider's operations, provided sufficient transparency is provided. When the independent audit is impractical, the cloud service provider should conduct a self-assessment and disclose its process and results to the cloud service customer.*

In this respect, railway transport, unlike many other areas of use of cloud services, may require checks specific to the railway transport safety authority. In Poland, the President of the Railway Transport Office plays such a role.

4.15. Additional requirements for cloud services

Annex A to the 27017:2017-06 standard defines the following additional objectives:

- *It is recommended to clearly define the relationship regarding common roles and responsibilities between the cloud customer and the cloud service provider for information security management.*
- *It is recommended to mitigate information security risks when using a shared cloud virtual environment.*

And refers to the objectives mentioned in subchapters 4.2., 4.4., 4.8., and 4.9.

Annex A to the 27017:2017-06 standard defines additional requirements for cloud services in terms of information security. The annex is normative, which means that its provisions should be treated in the same way as the provisions of the standard. There is also Annex B to the standard, and that annex is informative.

For cloud services in relation to these objectives, 27017:2017-06 points out that:	
Cloud service customer	**Cloud service provider**
The cloud service customer should define or extend its existing policies and procedures in accordance with its use of cloud services, and make cloud service users aware of their roles and responsibilities in the use of the cloud service.	*The cloud service provider should document and communicate its information security capabilities, roles, and responsibilities for the use of its cloud service, along with the information security roles and responsibilities which the cloud service customer would need to implement and manage as part of its use of the cloud service.*
In case of the removal of cloud service customer assets:	
The cloud service customer should request a documented description of the termination of service process that covers return and removal of the cloud service customer's assets, followed by the deletion of all copies of those assets from the cloud service provider's systems. *The description should list all the assets and document the schedule for the termination of service, which should occur in a timely manner.*	*The cloud service provider should provide information about the arrangements for the return and removal of any cloud service customer's assets upon termination of the agreement for the use of a cloud service.* *The asset return and removal arrangements should be documented in the agreement and should be performed in a timely manner. The arrangements should specify the assets to be returned and removed.*
In case of using a shared cloud service virtual environment:	
NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service customer.	*The cloud service provider should enforce appropriate logical segregation of cloud service customer data, virtualised applications, operating systems, storage, and network for:* – *the separation of resources used by cloud service customers in multi-tenant environments;* – *the separation of the cloud service provider's internal administration from resources used by cloud service customers.* *Where the cloud service involves multi-tenancy, the cloud service provider should implement information security controls to ensure appropriate isolation of resources used by different tenants.* *The cloud service provider should consider the risks associated with running cloud service customer-supplied software within the cloud services offered by the cloud service provider.*

Cloud service customer	Cloud service provider
Virtual machine hardening: *When configuring virtual machines, cloud service customers and cloud service providers should ensure that appropriate aspects are hardened (e.g., only those ports, protocols and services that are needed) and that the appropriate technical measures are in place (e.g., anti-malware, logging) for each virtual machine used.*	
Administrator's operational security:	
The cloud service customer should document procedures for critical operations where a failure can cause unrecoverable damage to assets in the cloud computing environment. *Examples of the critical operations are:* – *installation, changes, and deletion of virtualised devices such as servers, networks and storage;* – *termination procedures for cloud service usage;* – *backup and restoration.* *The document should specify that a supervisor should monitor these operations.*	*The cloud service provider should provide documentation about the critical operations and procedures to cloud service customers who require it.*
Monitoring of Cloud Services:	
The cloud service customer should request information from the cloud service provider about the service monitoring capabilities available for each cloud service.	*The cloud service provider should provide capabilities that enable the cloud service customer to monitor specified aspects, relevant to the cloud service customer, of the operation of the cloud services. For example, to monitor and detect if the cloud service is being used as a platform to attack others, or if sensitive data is being leaked from the cloud service.* *Appropriate access controls should secure the use of the monitoring capabilities. The capabilities should provide access only to information about the cloud service customer's own cloud service instances.* *The cloud service provider should provide documentation of the service monitoring capabilities to the cloud service customer.* *Monitoring should provide data consistent with the event logs and assist with SLA terms.*
Alignment of security management for virtual and physical networks:	
NOTE: The range indicated in this row in the column next to it does not require complementary actions on the side of the cloud service customer.	*The cloud service provider should define and document an information security policy for the configuration of the virtual network consistent with the information security policy for the physical network. The cloud service provider should ensure that the virtual network configuration matches the information security policy, regardless of the means used to create the configuration.*

The cited provisions of Annex A to the 27017:2017-06 standard formally apply regardless of whether infrastructure managers and railway undertakings use a public cloud or a cloud intended for railway transport offered by an entity with knowledge and experience allowing for taking into account various types of risks related to railway transport. In the former case, railway operators are dependent on the service providers, and the compensation claim procedures following potential incidents may be both lengthy and limited by contractual provisions. In the latter case, the cloud service provider not only has railway exper-

tise and experience but is also supervised by an entity responsible for information security and a body in charge of railway transport safety. This is particularly important when cloud services are used not only for information systems (IT) but also for operational systems (OT).

5. Conclusions

In the 27002:2017-06 standard, *it is noted that it is very important for an organisation to determine its security requirements, indicating that there are three main sources of these:*

a) *assessing the risks to the organisation, taking into account the overall business strategy and objectives of the organisation. Risk assessment may help identify threats to the assets, assess vulnerability to the threats and the likelihood of their occurrence, and estimate a potential impact;*
b) *legal provisions, regulations, contractual obligations that the organisation, its business partners, contractors and service providers must follow and the sociocultural environment in which they operate;*
c) *a set of principles, objectives and requirements related to information processing that the organisation has developed to support its activities;*

and it is noted that the resources used to implement protection means should be appropriate to the possible damage to the business that could result from their absence.

There is therefore no doubt that a cloud service provider for railway transport must have a security policy implemented, a security system organized and many protection means in place that are tailored to the risks identified by each railway infrastructure manager and each railway undertaking it serves. Risks must be identified taking into account railway transport safety understood as the security of information used for the needs of safety supporting systems, systems supporting the protection of life, health, property and personal data, as well as the security of any information that could be used to reduce the operational capability of the army or emergency services, the security of citizens or attempts to interfere with the functioning of the state.

References

1. EN ISO/IEC 27001:2017: Information technology – Security techniques – Information security management systems – Requirements:
   – replaced by EN ISO/IEC 27001:2023: Information security, cybersecurity and privacy protection – Information security management systems – Requirements;
   – amended in January 2024 in relation to climate changes.
2. EN ISO/IEC 27002:2017: Information technology – Security techniques – Code of practice for information security controls:
   – replaced by EN ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection – Information security controls.
3. ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services:
   – replaced by EN ISO/IEC 27017:2021: Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.